Giáo trình Multimedia

Môn học: **Multimedia**

Thời lượng: **30 tiết LT + 15 tiết TH**

Giảng viên: **Đỗ Thị Bắc**

Email: ***Bacthu2003@yahoo.com***

Design By :Nguyễn Thành Kiên

Website: www.k3c-cntt.com

Multimedia

Error!

Các lĩnh vực tìm hiểu

Thông tin về giảng viên

Error!

[Đỗ Thị Bắc]

Tên giảng viên: **Đỗ Thị Bắc**

Bộ môn: ***Các hệ thống thông tin***

Đơn vị công tác: Khoa Công nghệ thông tin - Đại học Thái Nguyên

E-mail: ***Bacthu2003@yahoo.com***

Mobil: **0983.192.599**

Giới thiệu chung về môn học

Số đơn vị học trình: **3 (2 lý thuyết - 1 thực hành)**

Thời gian học: **Kỳ 8-ĐH, Kỳ 5-KS2**

Mục tiêu môn học

Error!

Mục tiêu môn học

Nội dung của môn học không ch nhằm trang bi cho sinh viên những kiến thức trên lĩnh vực lý thuyết mà còn cả trên lĩnh vực thực hành thực tế. Môn học "*Multimedia*" nhằm trang bị cho sinh viên:

- Kiến thức cơ bản về multimedia;
- Hiểu được các ứng dụng rộng rãi của Multimedia trong đời sống;
- Nắm bắt được các yêu cầu và xu hướng phát triển ứng dụng hiện nay;
- Hiểu các cấu trúc, các bước thiết kế ứng dụng ;
- Nắm bắt được một số công cụ có sẵn để thiết kế ứng dụng;

Yêu cầu

Error!

Yêu cầu

Để tiếp thu tốt kiến thức, sinh viên cần:

- Tìm hiểu trước nội dung: kiến trúc máy tính, xử lý ảnh, mạng máy tính, đồ hoạ.
- Tham khảo thêm một số tài liệu cung cấp trong phần tài nguyên hoặc đọc thêm.
- Chuẩn bị tốt các bài thực hành theo yêu cầu giáo viên.

Nhiệm vụ của sinh viên

Tham gia các phần học lý thuyết và nắm vững kiến thức chuyên môn.

Hoàn thành đầy đủ các bài thực hành.

Đánh giá sinh viên:

1 điểm chuyên cần

1 điểm kiểm tra kiến thức

1 điểm thực hành

Hệ thống nội dung bài giảng

Error!
Những nội dung chính

1. Tổng quan về multimedia
2. Các lĩnh vực ứng dụng của multimedia
3. Các yêu cầu của hệ thống multimedia
4. Các loại dữ liệu multimedia
5. Quá trình xây dựng và phát triển ứngdụng multimedia

Cơ sở dữ liệu

Phân tích thiết kế hệ thống

Khai phá dữ liệu

Multimedia

E-learning

Tổng quan về multimeia

Error!
Mục tiêu cần đạt được

Sau khi nghiên cứu xong phần này, sinh viên có thể:

Có cái nhìn tổng quan về lĩnh vực multimedia.
Hiểu các khái niệm cơ bản về media, multimedia.
Phân loại được các loại media.

Giải thích tính đa lớp,đa chiều,tương tác của các ứng dụng multimedia.

Phân biệt được khái niệm chuẩn và đặc tả.

Biết một số chuẩn thông dụng.
Liệt kê và phân tích được những vấn đề liên quan đế multimedia.
Biết các thành phần chính của hệ quản trị CSDL multimedia.

Error!
Điều kiện tiên quyết

Để tiếp thu tốt kiến thức, sinh viên cần:

- Có những hiểu biết về kiến trúc máy tính, xử lý ảnh, mạng máy tính, đồ hoạ máy tính.
- Tham khảo thêm một số tài liệu cung cấp trong phần tài nguyên hoặc đọc thêm.

Error!
Nội dung chính

Thông tin trong cuộc sống hiện đại

Các khái niệm cơ bản

Các chuẩn multimedia thông dụng

Các lĩnh vực liên quan đến multimedia

Thông tin trong cuộc sống hiện đại

Error!
Đặt vấn đề

Phương thức truyền thông cổ xưa?

- Người truyền tải, báo tin, truyền lệnh

- Chim bồ câu đưa thư

- Tiếng nói, hình ảnh, chữ viết

Phương thức truyền thông trong cuộc sống hiện đại.

- Điện thoại cố định, điện thoại di động

- Internet

So sánh giữa các phương thức

-

-

- .....

Phân tích các yếu tố tác động đến việc nảy sinh vấn đề

- **Các *nhu cầu* về truyền thông đa phương tiện** - Có

Ví dụ minh hoạ.

- **Khả năng về *kinh tế* -** Có thể đáp ứng
- **Khả năng đáp ứng về *khoa học kỹ thuật* -** Đảm bảo

Đánh giá về giá trị của thông tin trong cuộc sống.

Vai trò của thông tin

- Hỗ trợ cho việc ra quyết định
- Sự phát triển của thông tin gắn liền với sự phát triển của lịch sử xư hội loại người.

Xem xét đánh giá của Tạp chí "Thế giới phụ nữ" về 10 **nghề** có "**giá"** nhất thế kỷ 21

- Nghề "Môi giới thông tin"
- Quan điểm của bạn?

Error!
Câu hỏi xin ý kiến
Tại sao các chương trình quảng cáo thu hút được sự chú ý của trẻ thơ?
Nó đa mầu sắc.

Nó kích thích được nhiều hơn 1 giác quan của trẻ.

Vì trẻ hiểu nội dung truyền tải.

Vì nó kích thích được thính giác trẻ.

Chỉ mới 6- 12 háng tuổi trẻ đã biết yêu thích những nhân vật trong đoạn phim quảng cáo?

Error!

Vấn đề nảy sinh

Multimedia là gì?

Các vấn đề liên quan đến truyền thông đa phương tiện?

Các yêu cầu đặt ra cần giải quyết?

Xu hướng phát triển?

Các lĩnh vự ứng dụng?

...

Đây là các vấn đề sẽ được giải quyết trong chương trình môn học.

Error!

Đọc chi tiết

Khi công nghệ phát triển, người tiêu dùng ngày càng đòi hỏi khắt khe hơn. Trong thời đại của thông tin tốc độ cao, chúng ta mong muốn nhận được các thông tin ngay tức thì và đồng thời, thông qua nhiều cách thức khác nhau. Nhu cầu này giải thích tại sao các kênh tin tức trên truyền hình thường xuyên có các dòng chữ chạy phía dưới màn hình trong khi phát thanh viên nói và các hình ảnh đã thâu băng trước đó trôi qua. Nhu cầu đó giải thích tại sao các Website ngày nay ngoài nội dung và các siêu liên kết còn gồm thêm các hình ảnh đồ hoạ, hoạt ảnh và âm thanh.

Những nhu cầu này đã mở rộng cách chúng ta làm việc, học tập và giải trí. Nói một cách đơn giản, các thông tin "một chiều" không còn phù hợp với hầu hết chúng ta nữa. Thông tin, các bài học, trò chơi và mua sắm sẽ lôi cuốn hơn và khiến chúng ta chú ý hơn nếu chúng ta có thể tiếp cận và sắp xếp chúng trong các cách thức khác nhau, thậm chí theo một ý thích nào đó mà chúng ta chợt nảy ra. Những nhu cầu này và các tiến bộ về công nghệ đã tương quan mật thiết với nhau để đưa nghệ thuật và khoa học truyền thông đa phương tiện lên một tầm cao mới, dẫn đến kết quả là các sản phẩm có khả năng đan kết văn bản, hình ảnh đồ hoạ, hoạt ảnh, âm thanh và video.

Khi chúng ta sử dụng các sản phẩm này - cho dù là một bộ bách khoa toàn thư trên Web hay một trò chơi video trên CD- thì có nghĩa là chúng ta không đơn thuần chỉ làm việc với một chương trình máy tính. Chúng ta đã trải nghiệm qua một sự kiện truyền thông đa phương tiện. Các sản phẩm truyền thông đa phương tiện ngày nay đều thu hút nhiều giác quan cùng một lúc và đáp ứng với nhu cầu thay đổi của chúng ta với tốc độ ngày càng gia tăng.

Các khái niệm cơ bản

Error!

Nội dung tìm hiểu

Khái niệm về media

Khái niệm về Multimedia

Tính tương tác của các ứng dụng Multimedia

Tính đa lớp, đa chiều của các ứng dụng Multimedia

Phương tiện mới

Error!

Hoạt động đọc và tìm hiểu

Thế nào là phương tiện?

Trong suốt chiều dài lịch sử, thông tin đã được chuyển tải thông qua một phương tiện duy nhất. Âm thanh, chẳng hạn như giọng nói của con người, chính là một loại phương tiện đó và qua nhiều thế kỉ trước khi chữ viết được sử dụng rộng rãi thì nói chuyện là một cách thức chủ yếu để trao đổi thông tin. Sau này con người bắt đầu kể chuyện và để lại thông tin về cuộc sống của mình thông qua các hình vẽ, các bức tranh. Sự ra đời của chữ viết đã cho con người một phương tiện khác nữa để diễn đạt ý nghĩ của mình. Ngày nay, con người thường sử dụng lời nói, âm thanh, âm nhạc, văn bản, hình ảnh, đồ hoạ, hoạt ảnh và video để truyền tải thông tin. Những thứ này là tất cả các loại phương tiện khác nhau (thuật ngữ media là số nhiều của medium) và mỗi phương tiện thường được dùng để biểu đạt các loại thông tin nhất định.

Như vậy trong ý nghĩa này, phương tiện chỉ đơn giản là một cách thức để truyền đạt thông tin.

Truyền thông đa phương tiện là gì?

Kể từ lâu con người đã khám phá ra rằng các thông điệp sẽ trở nên tác động hơn (có nghĩa là người nghe sẽ hiểu và nhớ chúng dễ hơn) khi chúng được biểu đạt thông qua một kết hợp của các phương tiện khác nhau. Loại kết hợp này chính là ý nghĩa của thuật ngữ truyền thông đa phương tiện.

Truyền thông đa phương tiện là sử dụng nhiều hơn một loại phương tiện vào cùng một thời điểm

Ví dụ:

· Giáo viên sử dụng bảng đen trong lớp học để viết các lời giải thích cho bài giảng của họ.

· Sử dụng phim ảnh, truyền hình kết hợp nhiều loại phương tiện (âm thanh, video, hoạt ảnh, hình ảnh tĩnh và chữ) để tạo ra nhiều loại thông điệp khác nhau có khả năng cung cấp thông tin và sự tiêu khiển cho mọi người theo những cách thức độc nhất và đầy ý nghĩa.

Thế nào là một hệ truyền thông đa phương tiện?

Các hệ thống thông tin đa phương tiện dùng nhiều phương tiện giao tiếp khác nhau (văn bản, dữ liệu ghi, dữ liệu số, đồ hoạ, hình ảnh, âm thanh, video..). Nhiều ứng dụng là đa phương tiện theo ý nghĩa là chúng dùng nhiều dạng trên. Tuy nhiên, thuật ngữ "đa phương tiện" thường được dùng để mô tả các hệ thống phức tạp hơn, nhất là các hệ thống hỗ trợ hình ảnh và âm thanh. Các thông tin mới chủ yếu được tạo ra bên ngoài máy tính. Lời nói, nhạc, hình ảnh và phim được chuyển từ dạng Analog (tương tự) sang Digital (số) trước khi được dùng trong các ứng dụng trong máy tính. Ngược lại, với văn bản, đồ hoạ và thậm chí phim hoạt hình đều được tạo trên máy tính và vì vậy nó chỉ đáp ứng những mục tiêu nhất định, không thể mở rộng ứng dụng được.

Một hệ nền máy tính, mạng thông tin hay dụng cụ phần mềm là một hệ đa phương tiện nếu nó hỗ trợ ứng dụng tương tác cho ít nhất là một trong các dạng thông tin sau, không kể văn bản và đồ hoạ: âm thanh, hình ảnh tĩnh hoặc phim video chuyển động.

Tính tương tác của các chương trình truyền thông đa phương tiện

Ngày nay, công nghệ máy tính đã đưa các sản phẩm truyền thông đa phương tiện trên PC tiến thêm một bước xa hơn. Không giống như sách, phim hay chương trình truyền hình, máy tính có thể nhận dữ liệu nhập từ người sử dụng, do vậy nó có thể chứa các sự kiện truyền thông đa phương tiện tương tác có bao gồm vai trò người sử dụng.

Thuật ngữ tương tác được hiểu là người sử dụng và chương trình phản ứng qua lại với nhau.

Chương trình liên tục cung cấp cho người sử dụng một tập các lựa chọn để cho người sử dụng chọn, nhằm điều khiển các hoạt động của chương trình. Và thậm chí kiểm soát những gì họ thấy và nghe được. Bằng cách nhận vào dữ liệu nhập vào từ người sử dụng, các phương tiện tương tác tạo ra một vòng lặp phản hồi, nói chung hoạt động như sau:

· Bắt đầu vòng lặp người sử dụng kích hoạt chương trình tương tác và chọn thông tin cần xem.

· Chương trình đáp ứng lại bằng cách hiển thị ra cho người sử dụng thông tin với các lựa chọn.

· Người sử dụng đáp ứng bằng cách chọn một lựa chọn, chẳng hạn như di chuyển đến một nơi khác trong chương trình hoặc chọn thông tin khác.

· Chương trình đáp ứng với lựa chọn của người sử dụng và thường đưa ra một tập các tuỳ chọn mới.

· Quá trình tiếp diễn - đôi khi nhịp độ rất nhanh và phức tạp như trong nhiều trò chơi máy tính, cho tới khi người sử dụng ngừng chương trình.

Như vậy, các chương trình truyền thông đa phương tiện được mô tả là có tính tương tác nếu chúng nhận dữ liệu nhập từ người sử dụng và cho phép người sử dụng điều khiển dòng chảy thông tin hoặc hoạt động của chương trình.

Phương tiện mới

Tương tác không chỉ liên quan đến một máy tính và một con chuột. Phương tiện mới (một thuật ngữ bao gồm tất cả các loại công nghệ truyền thông đa phương tiện tương tác) có thể kết hợp nhiều công nghệ truyền thông khác nhau chẳng hạn như truyền hình cáp, các đường dây điện thoại, các mạng riêng, mạng Internet và các công nghệ khác.

Phương tiện mới được tạo ra như một sự hội tụ nhiều loại công nghệ, cho phép các cá nhân riêng lẻ cũng như các tổ chức lớn giao tiếp và truyền đạt thông tin bằng cách sử dụng máy tính và các hệ thống truyền thông.

Phần cốt lõi của phương tiện mới là một khái niệm được gọi là sự hội tụ kỹ thuật số. Người ta dùng các máy tính để tạo ra các loại thông tin kỹ thuật số khác nhau, từ loại chỉ thuần là văn bản đến thông tin video. Tất cả những loại thông tin kỹ thuật số này có thể chuyển đến người sử dụng theo cùng một con đường - có thể là qua một đĩa CD-ROM, một đường dây truyền hình cáp hay qua đường vệ tinh. Tha vì phải chuyển tải phim ảnh trong các trong các băng hình hay băng video, chuyển tải âm nhạc trên các băng nhạc hay đĩa compact và chuyển tải sách bằng các trang in giờ đây ta có thể chuyển tải các loại thông tin khác nhau đến các máy tính hay hộp truyền hình cáp với cùng một cách thức. Do vậy, ta có một tập hợp các thông tin kết hợp với nhau và hội tụ vào một luồng thông tin kỹ thuật số.

Đối với người sử dụng, công nghệ này có nghĩa là thông tin truyền thông đa phương tiện có thể được lưu trữ và chuyển tải theo nhiều cách. Nếu bạn sử dụng PC, thông tin truyền thông đa phương tiện có thể có trong một đĩa compact, một đĩa DVD, đĩa cứng, mạng Internet hay một dịch vụ trực tuyến. Nếu bạn sử dụng các đặc tính thu tín hiệu truyền hình trong Windows 98, Windows 2000 bạn còn có thể nhận được các thông tin như trên ở dạng thức chương trình phát hình được chuyển đến màn hình của bạn. Nếu bạn sử dụng một dịch vụ chẳng hạn như WebTV, bạn có thể sử dụng đồng thời các chương trình phát hình và thông tin Internet.

Tuỳ theo công nghệ được dùng, một số các sự kiện truyền thông đa phương tiện là những ứng dụng một người sử dụng và chạy đơn độc chẳng hạn như một quyển sách tham khảo hay một chương trình dạy học tren CD-ROM. Các sự kiện khác có thể liên quan nhiều hơn đến một người sử dụng. Ví dụ như các trò chơi nhiều người có thể được truy xuất thông qua môt mạng cục bộ hay mạng Internet, các cuộc hội thảo video cho phép những người tham gia nhìn

thấy nhau và chia sẻ dữ liệu trong thời gian thực thông qua đường dây điện thoại hay các kết nối vệ tinh hoặc các chương trình truyền hình tương tác nhận các dữ liệu người sử dụng thông qua một Website hay một phòng tán gẫu trên Web.

Thông tin đa lớp, đa chiều

Các nhà phát triển truyền thông đa phương tiện liên tục cố gắng để tìm ra cách thức làm cho sản phẩm của họ lôi cuốn người sử dụng hơn cho dù

sản phẩm đó là một trò chơi hành động nhịp độ cao hay một bản hướng dẫn trên đĩa hoặc một website thương mại điện tử.

Một chiến lược cơ bản trong việc phát triển thông tin truyền thông đa phương tiện là cung cấp thông tin được sắp thành lớp và thông tin đa chiều.

Yêu cầu này có nghĩa là sản phẩm phải cung cấp cho người sử dụng các mảnh thông tin một cách đồng thời, chẳng hạn như một hình ảnh 3 chiều đang quay tròn của một mô tơ, một đoạn âm thanh mô tả các chức năng của nó và các hộp văn bản hiển thị tạm thời về các thông tin thêm khi người sử dụng trỏ chuột vào các phần nhất định của hình mô tơ.

Trong một cách thức trình bày đa chiều, người sử dụng có cơ hội để trải nghiệm các thông tin từ nhiều góc độ khác nhau, ví dụ một người sử dụng nào đó có thể sẽ chỉ xem phần minh hoạ sống động của một dự án tạo cảnh quan, trong khi người sử dụng khác sẽ chọn đọc đoạn văn bản mô tả.

Một trong những cách để khiến cho những văn bản thuần và hình ảnh lôi cuốn người xem là thêm vào các thông tin có yếu tố thời gian chẳng hạn như âm thanh, hoạt hoạ và video. Tuy nhiên, điều quan trọng là ở chỗ các phương tiện thông tin bổ sung không chỉ đơn thuần là lặp lại vai trò của các nội dung và hình ảnh tĩnh. Thực vậy, việc theo dõi một đoạn video chỉ đơn thuần là đọc các đoạn văn trên màn hình là rất nhàm chán. Nhưng nếu cùng với đoạn văn bản đó là phần video hiển thị kèm theo để diễn tả thì nội dung phần văn bản sẽ thú vị hơn rất nhiều.

Ngày càng nhiều các tư liệu giáo dục, bao gồm các cuốn sách giáo khoa, và sách bách khoa toàn thư đang được phát triển thành các sản phẩm truyền thông đa phương tiện. Những sản phẩm này có sử dụng âm thanh, hoạt ảnh và đoạn trích video để làm cho phần nội dung sống động hơn.

Điều cơ bản là ta phải biết tập trung vào nội dung của chương trình. Đó là cái mà người sử dụng cần. Ví dụ, sức lôi cuốn của một bộ phim hoạt hình chính là cở cốt truyện hấp dẫn, cách xây dựng nhân vật tốt. Tương tự, các bộ phim hành động sử dụng công nghệ hoạt ảnh và đồ hoạ máy tính để cải tiến tạo ra các đối tượng hoặc các môi trường trên màn hình chẳng hạn như chuỗi giấc mơ trong phim The Matrix (Ma Trận) sẽ kém hấp dẫn nếu cốt truyện tẻ nhạt.

<!--[endif]-->

Media

Error!
Khái niệm về media

Phân tích theo chiều dài lịch sử việc truyền tải thông tin được phát triển như thế nào?

- Giọng nói, biểu cảm
- Chữ viết
- Hình vẽ, biểu tượng, tranh vẽ
- Kết hợp: Âm thanh, hình ảnh, văn bản, video,...

Khái niệm:

Media là ***phương tiện*** qua đó thông tin được **nhận biết, diễn đạt, ghi nhớ, chuyển tải**.

Chú ý:

Khái niệm trên chỉ muốn định nghĩa đến media trong lĩnh vực công nghệ thông tin.

Error!
Vấn đề nảy sinh

Con người có thể nhận biết được thông tin thông qua:

- Cảm giác?
- Xúc giác?
- Thính giác?
- Thị giác?
- Kết hợp?

- ...?

Con người có thể diễn đạt thông tin thông qua :

- Biểu lộ cử chỉ? (Đây có là 1 cách mã hoá?

Nhưng trong môi trường máy tính.....?????

Nên xem phần phân loại dưới đây để rõ thêm.

Phân loại media

Error!
Phân loại media

Dưa vào tiêu chí phân loại khác nhau dẫn đến có nhiều cách phân loại khác nhau.

a. Cách phân loại thứ nhất:

Media được chia thành 5 loại đó là:

- ***Sự nhận thức*** (Perception): Là các media cho phép **nhận biết** thông tin trong môi trường tin học.
  - Ví dụ: Thị giác, thính giác, ...

- ***Sự trình bày*** (Representation): Là các media dùng để **biểu diễn** hay **mã hoá** thông tin.
  - Ví dụ:
    - Mã hoá văn bản dùng bảng mã ASCII.
    - Mã mã JPEG dùng để mã hoá ảnh, ...

- ***Vật trình bày*** (Presentation):Là media của hệ thống cho phép **chuyển đổi** giữa sự nhận thức và sự trình bày.
  - Ví dụ: Giấy, màn hình, bàn phím, ..

- ***Vật lưu trữ*** (Storage): Là media cho phép **lưu trữ** thông tin.
  - Ví dụ: Ổ đĩa cứng, CD, DVD, ...

- ***Vật chuyển tải*** (Transmission): là các media cho phép **chuyển tải** thông tin liên tục.
  - Ví dụ: Cáp đồng trục, cáp quang, kênh liên lạc viễn thông, ...

b. Cách phân loại thứ 2: (Dựa vào yếu tố thời gian)

Media được chia thành 5 loại đó là:

- ***Media liên tục:*** Yếu tố thời gian tham gia vào việc truyền đạt ngữ nghĩa của thông tin. Nếu bỏ qua yếu tố này thì thông tin sẽ không còn đầy đủ ý nghĩa của nó.

Ví dụ: Phim ảnh, Tiếng nói, âm thanh,...

- ***Media rời rạc***:Yếu tố thời gian không tham gia vào việc truyền đạt ngữ nghĩa của thông tin. Nếu bỏ qua yếu tố này thì cũng không làm mất đi giá trị của thông tin.

Ví dụ: Văn bản, ảnh tĩnh

Multimedia

Error!
Các hoạt động trước khi tìm hiểu khái niệm
1. Mời các bạn xem những nội dung được cung cấp sau:

a. Một bức ảnh.

b. Một video quảng cảo.

c. Một chương trình truyền hình.

2. Cảm nhận của bạn?

Cảm nhận của bạn có thể về:

Số những nội dung thông tin được cung cấp đồng thời?

Số những thông tin được cung cấp dưới nhiều góc độ khác nhau về cung 1 nội dung?

Chúng cùng lúc tác động lên bao nhiêu gíc quan của bạn?

Chúng dùng hình thức truyền thông (phân phối) nào?

Thông tin có dễ được tiếp nhận hơn khi nó được biểu đạt bằng nhiều media?

...

Ảnh
Error!

Chương trình truyền hình Việt Nam
Error!
Bạn hiểu thế nào về khái niệm multimedia?

Sau đây đề nghị bạn tham gia trả lời các câu hỏi, bằng cách điền từ hoặc cụm từ mà bạn cho là đúng nhất vào ô chữ nhật.

1. Multimedia là việc sử dụng

một loại media vào cùng một thời điểm để chuyển tải thông tin.

2. Multimedia là sự

các phương tiện như văn bản,đồ hoạ, âm thanh, hình ảnh,...

Error!
Đặt vấn đề

Ý kiến đánh giá của bạn về quan điểm sau:

1. Trăm hay không bằng tay quen!

2. Trăm nghe không bằng một thấy!

3. Đánh giá của tạp chí:"Computer Technology Reseach-1993"

Con người chỉ có thể **biết** được **20%** những gì họ **nhìn** thấy;

Con người chỉ có thể **biết** được **30%** những gì họ **nghe** thấy;

Con người chỉ có thể **biết** được **50%** những gì họ **nhìn và nghe** thấy;

Nhưng có thể biết tới trên 80% những gì họ vừa **nhìn** vừa **nghe** và cùng được **tham gia**;

Vậy phải chăng điều đó nói lên giá trị của sự kết hợp nào đó?

Error!
Định nghĩa Multimedia

1. Multimedia là việc sử dụng hơn một loại phương tiện vào cùng một thời điểm để chyển tại thông tin.

2. Multimedia là sự **phối hợp** các **phương tiện** như: Văn bản, đồ hoạ, âm thanh, hình ảnh, ... để thực hiện một phiên **giao tác** giữa con người với các đối tượng khác thông qua **môi trường máy tính**, trong đó các **phương tiện**

được sử dụng có **mối quan hệ** thống nhất về ngữ nghĩa và vật lý, **cho phép** con người **tương tác** với các đối tượng và phương tiện đó.

Tính đa lớp đa chiều

Error!
Tìm hiểu

Để thấy rõ được tính chất này, đề nghị các bạn cho ý kiến của riêng mình về những nội dung sau:

1. Khi xem các chương trình truyền hình ngày nay, tại cùng một thời điểm các bạn tiếp nhận được bao nhiêu luồng thông tin khác nhau. (Giả sử xem chương trình VTV1 lúc18h45 chương trình thị trường)

2. Hãy xem xét một mô hình thí nghiệm ảo thường dùng trong giáo dục thông qua các CD. Ví dụ bài thí nghiệm mô phỏng thí nghiệm vật lý lớp 6 về động cơ 3 chiều. Bạn thấy người ta có thể tiếp cận thông tin về cùng một vấn đề nhưng trên các khía cạnh khác nhau như: Text, âm thanh, video.... Như vậy các mảnh thông tin có được cung cấp đồng thời không?

3. Hãy xem xét một số tài liệu như: Sách điển tử, từ điển, Sách bách khoa toàn thư, ... Các bạn có thể vừa được đọc thông tin cung cấp bởi các dòng văn bản, vừa có thể nghe tiếng phát âm, hoặc vừa có thể xem minh hoạ hấp dẫn thông qua các đoạn video hoặc ảnh. Điều này khiến các bạn cảm nhận được rằng thông tin trong các ứng dụng multimedia được tổ chức theo các lớp?

4. Bạn đã xem một bản đồ số hoá? Bạn cảm nhận được tính đa lớp của các thông tin trên bản đồ số hoá? Người ta hoàn toàn có thể biểu diễn cùng lúc một lớp hoặc một số lớp thông tin khác nhau trên bản đồ như: Lớp thông tin về đường biên, lớp thông tin về địa danh vùng miền, lớp thông tin về tài nguyên rừng, sông, ...?

Đây chỉ là một số gợi ý giúp bạn dễ cảm nhận hơn về tính đa lớp đa chiều của các ứng dụng multimedia. Nếu chưa rõ bạn cùng đừng băn khoăn! Mọi sự sẽ rõ ràng ngay thôi.
Error!
Nhận xét chung

Các ứng dụng multimedia luôn mang tính đa lớp đa chiều về dữ liệu, về nội dung trình bày và phương pháp thể hiện. Ngoài việc sử dụng dữ liệu text và ảnh người ta thường thêm thông tin biểu diễn bằng âm thanh và video (thêm chiều thời gian).

Mục đích: Làm cho các ứng dụng đó lôi cuốn người sử dụng hơn, thân thiện với người sử dụng hơn, Kích thích được nhiều hơn các giác quan của người sử dụng trong cùng một thời điểm để cảm nhận vấn đề. Điều lý thú là người dùng có quyền được trải nghiệm các thông tin từ các góc độ khác nhau. Những vấn đề đó cũng làm cho người dùng thoả mãn hơn, sáng tạo hơn, khám phá hơn, linh hoạt hơn, thích ứng dụng hơn, ...

Tính tương tác

Error!
Tìm hiểu

1. Bạn đã từng lướt qua các cuốn sách điện tử trên mạng hoặc CD? Bạn có cảm nhận gì về sự giống và khác nhau giữa sách truyền thống và sách điện tử ngày nay?

2. Bạn đã từng tham gia vào một trò chơi giải trí? Bạn thấy người chơi có quyền gì?

Bạn có thể đánh giá và nhận xét trên một số khái cạnh như:

Người sử dụng và các sản phẩm (sách điện tử, trò chơi, ...) có khả năng phản ứng qua lại với nhau?

Khả năng giao tiếp đơn hay đa chiều?

Khả năng điều hướng trong chương trình?

Khả năng siêu liên kết?

....

Error!
Khái niệm và đặc trưng tương tác

Sự tương tác ở đây có thể hiểu là phản ứng qua lại giữa người sử dụng và chương trình.

Sự tương tác có thể thấy qua khía cạnh:

- Người sử dụng có thể lựa chọn giải pháp.
- Người sử dụng có thể điều khiển dòng chảy thông tin và hoạt động của chương trình.

- Chương trình cung cấp khả năng điều hướng, siêu liên kết.

Đa số các sản phẩm multimedia đều có tính chất tương tác.

Các chuẩn multimedia thông dụng

Error!
Nội dung nghiên cứu

1. Định nghĩa về chuẩn.

2. Sự khác biệt giữa chuẩn và đặc tả.

3. Tại sao cần có chuẩn và sự quan trọng của nó.

4. Một số khía cạnh về chuẩn.

5. Giới thiệu một số chuẩn thông dụng trong multimedia

Một biểu tượng mô tả chuẩn! >

Các bạn có thể tham khảo thêm về vấn đề này thông qua việc tìm kiếm thông tin trên mạng bằng cách dùng một hệ thống tìm kiếm mà bạn biết băng một trong các từ khoá tìm kiếm chẳng hạn như: standard, Scomr, ims, mpeg,...

Định nghĩa

Error!
Định nghĩa về chuẩn

- Định nghĩa của ISO:

"Chuẩn là các **thoả thuận** trên **văn bản** chứa các **đặc tả kĩ thuật** hoặc các **tiêu chí chính xác** khác được **sử dụng** một cách **thống nhất** như các luật, các chỉ dẫn, hoặc các định nghĩa của các đặc trưng, **để đảm bảo** rằng các **vật liệu, sản phẩm, quá trình**, và **dịch vụ phù hợp với mục đích** của chúng".

- Các ví dụ:
  - Ví dụ 1: Xin nói về chuẩn được dùng rộng rãi trên thế giới là LEGO.
    - Với các đối tượng LEGO bạn có thể xây dựng mọi thư bạn muốn. Thậm chí có các đối tượng với kích cỡ khác nhau và

màu khác nhau, chúng đều khớp với nhau và chúng có thể được kết hợp lại theo mọi cách vì các đối tượng tuân theo các luật nhất định.
        - Trẻ em vẫn thích chơi với nó vì khả năng tạo ra các hình thù mới không bị hạn chế.
        <!--[if !vml]-->
    - Ví dụ 2: Xin nói về Internet.
        - Chúng ta có thể trao đổi thông tin trên mạng chính là nhờ chuẩn. Internet bao gồm các chuẩn được công nhận bởi IEEE. Các chuẩn quan trọng nhất trong Internet là:
            - HTTP (Hypertext Transfer Language)
            - HTML (Hypertext Markup Language)
            - FTP (File Trans Prototol)
            - SMTP ()
            - TCP/IP (Tran Coltrol Protocol/)

<!--[endif]-->

So sánh chuẩn và đăc tả

Error!
Sự khác biệt giữa chuẩn và đặc tả

- Chuẩn (Standard).

- Đăc tả (Specification)

- Tổ chức IEEE giải thích sự khác biệt như sau:

- **Đặc tả được phát triển bởi các uỷ ban không được công nhận bởi thế giới**. Một vài ví dụ về các uỷ ban nổi tiếng như: IEFT (Internet Engineering Task Force), W3C (World Wide Web Consortium), OMG (Object Management Group).

- **Chuẩn là một đặc tả được phát triển và công nhận bởi các uỷ ban chuẩn được công nhận trên thế giới**. Các tổ chức mà thực hiện công việc kiểu như thế này được gọi là Standards Development Organization (SDO). Ví dụ về các uỷ ban này là: IEEE, ISO, IEC, ITU, ANSI, BSI, CSA, JIS, DIN, và CEN.

- Có thể tóm tắt sự khác biệt như bảng dưới đây:

Đặc tả	Chuẩn
Tiến triển nhanh	Tiến triển chậm
Mang tính thử nghiệm	Là kết luận cuối cùng
Quy mô rộng	Quy mô hẹp
Tham khảo ý kiến của ít người	Tham khảo ý kiến của nhiều người

- Cần hiểu sự khác biệt này để có thể nhận thức được sự khó khăn của toàn bộ quá trình chuẩn hoá. Để thiết lập một chuẩn từ ban đầu có thể sẽ mất 10 năm.

Vai trò

Error!

Tại sao chuẩn là quan trọng

Bạn có thể thấy vai trò quan trọng của chuẩn bằng cách đặt vấn đề ngược lại, nếu không có chuẩn?

Các lí do sau đây tuy có đánh giá trên khía cạnh nhỏ e-Learning nhưng hoàn toàn nó không làm mất đi ý nghĩa thực tiễn của nó.

Các ý kiến này được đưa ra dựa vào phát biểu của Wayne Hodgins tại TechLearn.

1. Tính truy cập được (Accessibility): nếu chúng ta sử dụng các hệ thống các chương trình, các thiết bị, ... tuân theo chuẩn thì rất dễ sử dụng nội dung ở mọi nơi bằng cách sử dụng trình duyệt (browser). Ngay cả các chuẩn không liên quan đến e-Learning như HTTP cũng giúp cho việc truy cập thông tin dễ dàng hơn nhiều

2. Tính khả chuyển (Interoperability): không những chúng ta có khả năng truy cập nội dung từ mọi nơi mà thậm chí không phụ thuộc vào các công cụ chúng ta dùng

tại nơi đó. Do đó, chúng ta có thể sử dụng các LMS khác nhau để truy cập vào cùng nội dung. Và ngược lại, với một LMS có thể sử dụng nhiều nội dung tạo bởi các công cụ khác nhau

3. Tính thích ứng (Adaptability): các chuẩn cũng giúp việc đưa ra các nội dung học tập phù hợp với từng cá nhân. Một ví dụ là meta-data. Nếu chúng ta sử dụng meta-data giống nhau để mô tả nội dung thì có thể xác định chính xác những gì một học viên cần. Một LMS/LCMS hiểu meta-data sẽ có khả năng

hiểu và sử dụng các thông tin có trong meta-data, từ đó phân phối nội dung phù hợp với yêu cầu của từng học viên

4. Khả năng sử dụng lại (Re-usability): chỉ với việc sử dụng chuẩn chúng ta mới có thể sử dụng lại nội dung chúng ta phát triển hoặc mua

5. Tính bền vững (Durability): bạn vẫn sử dụng được nội dung ngay cả khi công nghệ thay đổi. Hơn nữa, với nội dung tuân theo chuẩn bạn không phải thiết kế lại hoặc làm lại

6. Tính giảm chi phí (Affordability): với các lí do ở trên rõ ràng là nếu người bán nội dung và hệ thống quản lý tuân theo chuẩn, hiệu quả học tập sẽ tăng rõ rệt, thời gian và chi phí sẽ giảm. Do đó ROI (Return On Investment) sẽ tốt hơn nhiều

Error!

Tình huống thực tế

Chúng ta đã biết chuẩn quan trọng nhưng thực tế thì như thế nào?

Chúng ta đã thấy không có chuẩn chúng ta không thể đưa cho khách hàng các nội dung và hệ thống quản lý hiệu quả, có chất lượng tốt. Hãy hợp tác với nhau, các đối tác tham gia là người bán, khách hàng, các nhà giáo dục, và học viên, ...

Tuy nhiên sẽ khó khăn trong quá trình thiết lập ra một chuẩn nếu có quá nhiều người, tổ chức và thậm chí các chính phủ tham gia (như Mỹ và uỷ ban châu Âu). Không ai ngăn cản quá trình chuẩn hoá và mọi người nhìn thấy tính cần thiết của chuẩn nhưng quá trình thiết lập chuẩn mất nhiều thời gian và phức tạp. Ngay cả khi mọi người phối hợp với nhau tốt thì cũng mất khá nhiều thời gian để đưa ra chuẩn.

Nhiều người bán sản phẩm nói rằng sản phẩm của họ tuân theo chuẩn nào đó trong khi họ chưa hề được cấp chứng nhận.

Như thực tế đã thấy, tuân theo tuẩn nào đó (ví dụ AICC) cũng có nhiều mức khác nhau. Nếu người bán nào nói rằng sản phẩm của họ tuân theo AICC, hãy hỏi họ sản phẩm đó tuân theo bao nhiêu AGR, là những AGR nào.

Error!

Chi tiết thêm về AICC

Giải thích về tính phức tạp của AICC và các mức độ của chúng.

Download

Error!

Kinh nghiệm để hiểu thêm về chuẩn

Giới thiệu một số kinh nghiệm thực tế cho mọi người quan tâm về chuẩn!

Download

Các lĩnh vực liên quan đến Multiedia

Error!
Hoạt động gợi mở-Câu hỏi xin ý kiến

Sau đây là một câu hỏi rất mờ, có nhiều cách trả lời khác nhau. Bạn hãy tham gia bằng cách điền từ thích hợp nhất vào ô trống.

Theo hiểu biết của bạn, multimedia liên quan tới những lĩnh vực:

1. Liên quan đến

lĩnh vực khác nhau.

2. Liên quan đến các lĩnh vực

,

3.

liên quan đến lĩnh vực tâm lý

4.

liên quan đến vấn đề xử lý ngôn ngữ tự nhiên

Error!
Tham khảo

Có thể nói multimedia liên quan đến hầu hết các lĩnh vực như:

- Audio

- Images

- Video

- Natura Language Processing (Xử lý ngôn ngữ tự nhiên)

- CPU Power

- Psychology (Tâm sinh lý)

- Networking (mạng)

- Storage System (Hệ thống lưu trữ)

- Data Compression (Nén dữ liệu)

- Information Retrieval (Truy tìm thông tin)

Ngoài ra có thể còn có những khía cạnh khác, các bạn thể tìm hiểu thêm thông tin trên các kênh truyền thông khác và đánh giá những nhận định đó.

Đây là những gợi ý mang tính quyết định. Các bạn có thể tự đưa ra những giải thích thoả đáng cho mình bằng những vốn hiểu biết sắn có. Nếu còn thấy có những vấn đề mang tính ***"cam go"*** thì đừng nản, khi càng nghiên cứu sâu thêm về những kiến thức của môn học này ở phần sau bạn sẽ tự giải toả ngay được thôi.

Câu hỏi tự kiểm tra

Error!

Nhóm câu hỏi phân tích, tổng hợp, sáng tạo để nâng cao tầm hiểu biết.

1. Đánh giá và nhận định của bạn về vấn đề bản quyền nói Riêng và bản quyền của các sản phẩm multimedia nói chung.

2. Hãy đưa ra một ý tưởng tạo bạo trong việc xây dựng một ứng dụng multimedia nào đó phục vụ cho cuộc sống hiện đại của thế kỷ mang đậm phong cách CNTT và tri thức.

3. Bạn được hưởng lợi gì từ những sản phẩm multimedia đã từng dùng?

4. Theo bạn xu hướng mới cho các sản phẩm multimedia nói chung ?

5. Hãy chọn một sản phẩm multimedia nào đó (có thể một trang web) và đưa ra những đánh giá của bạn về những yếu tố thành công và chưa được trong thiết kế đó. Từ đó rút kinh nghiệm cho chính bản thân.

6. ...

Các câu hỏi này các bạn có thể thảo luận và làm việc theo nhóm và trao đổi ý kiến với nhau. Các nhóm tự dàn xếp thời gian, phương thức hoặc đăng ký tại các chartroom nếu cần. Chúc các bạn tìm được nhiều chân trời mới!

Error!

Nóm câu hỏi Đúng /Sai

Trong mỗi câu sau đây, Các bạn hãy chọn một trong hai phương án bằng cách kích chuột vào True (đúng) hoặc False (Sai)

Thông tin là tất cả những hiểu biết.

True

False

... kinh nghiệm, tri thức, đã hiểu

2. Chuẩn là tất cả các quy định mà mọi người bắt buộc phải tuân theo.

True

False

—

"Bắt buộc"? Nếu tôi không tuân thủ thì tôi .... hội nhập.

Multimedia

Thông tin về giảng viên

Giới thiệu chung về môn học

Tài liệu tham khảo

Hệ thống nội dung bài giảng

Tổng quan về multimeia

Thông tin trong cuộc sống hiện đại

Các khái niệm cơ bản

Các chuẩn multimedia thông dụng

Các lĩnh vực liên quan đến Multiedia

Câu hỏi tự kiểm tra

Tài nguyên tham khảo

Ứng dụng của multimedia trong cuộc sống

Các yêu cầu của hệ thống multimedia

Các loại dữ liệu multimedia

Quá trình xây dựng và phát triển ứng dụng multimedia

Đọc thêm

Danh sách các học liệu mở

Hệ thống các từ viết tắt

Tài nguyên tham khảo

- http://www.itu.org
- http://mpeg.telecomitalialab.com

- http://www.imc.org
- http://www.ietf.org

« Previous | Next »

Tài liệu tham khảo

1. Multimedia và ứng dụng trong thực tiễn, NXB Thống Kê, Nguyễn Thế Hùng.
2. Multimedia và ứng dụng, NXB Thống Kê, song ngữ Anh-Việt.<!--[endif]-->
3. E-learning - Hệ thống đào tạo từ xa, NXB Thống kê.
4. Nhập môn xử lý ảnh , Lương Mạnh Bá.
5. Truyền hình số có nén và Multimedia, NXB Khoa học và kỹ thuật, Trần Trọng Kim.
6. Fred T.Hofstetter University of Delaware, Multimedia Literacy, McGraw-Hill.
7. V.S.Subrahmanian, Principles of Multimedia Database System, Morgan Kaufmann Publishers Inc.
8. Tay Vaughan, Multimedia: Making it work, Fifth Edition. McGraw-Hill.
9. Interractive Multimedia Design, YOSHIKO OGURA

Đọc thêm

1. Tập bài giảng về Hệ quản trị cơ sở dữ liệu đa phương tiện-Thầy: Đặng Đình Đức, Viện công nghệ thông tin.
2. Tập bài giảng Multimedia-Nhóm giáoviên, CNT-ĐHTN
3. Interactive Multimedia Design, Yoshiko Ogura, Kmitnb, Facalty of IT

Đọc thêm

I. Tập bài giảng về Hệ quản trị cơ sở dữ liệu đa phương tiện-Thầy: Đặng Đình Đức, Viện công nghệ thông tin.

MỤC LỤC

Chương 1

MỞ ĐẦU

Ngay từ ban đầu, máy tính đã được coi là các thiết bị xử lý biểu tượng (*symbolic*) - các thiết bị có đầu vào là các biểu tượng theo luật alphabet và đầu ra là tập các biểu tượng của cùng dạng trên. Điều này đã trở thành mô hình cho các môi trường tính toán chuẩn dựa trên cơ sở máy *Turing* đã quen thuộc.

Tuy nhiên, trong những năm gần đây xuất hiện nhu cầu vô cùng lớn về khả năng khai thác và xử lý dữ liệu với số lượng khổng lồ mà nó là điều không dễ dàng diễn tả chỉ với việc sử dụng các ký tự. Dưới đây là một số thí dụ về các kiểu dữ liệu như vậy:

· Dữ liệu hình ảnh (*Image data*): Ví dụ chẳng hạn một học viên phẫu thuật ở Miami mong muốn thực hành một ca phẫu thuật trên một bệnh nhân ảo có những

triệu chứng sinh lý nào đó. Trên thực tế để tìm ra bệnh nhân với những triệu chứng mong muốn, học viên phẫu thuật phải truy vấn cơ sở dữ liệu (CSDL) ảnh phân tán và kích thước lớn chứa ảnh X quang hay MRI (*Magnetic Resonance Imaging*) của các bệnh nhân với các triệu chứng tương tự. Đôi khi các triệu chứng có thể dễ dàng mô tả bằng văn bản. Tuy nhiên trong nhiều trường hợp khác, nó có thể dễ dàng hơn cho học viên phẫu thuật nếu có thể trình diễn hình ảnh của loại mẫu (*pattern*) mà anh ta đang tìm kiếm trong các ảnh X quang của bệnh nhân. Trong cả hai trường hợp này, một CSDL hình ảnh phải được duy trì. Nó có thể được truy vấn trên cơ sở các tiêu chí rất khác nhau - đầu vào là văn bản hay ảnh phù hợp (*matching*).

· Dữ liệu Video (*Video data*): Trong một ngữ cảnh tương tự, một ai đó mong muốn có những bài giảng bằng băng hình về một chủ đề kỹ thuật nào đó (thí dụ, *PR-Quadtrees*). Điều này đòi hỏi phải truy vấn thư viện băng hình mà nó bao gồm tập hợp vô số các băng hình với nội dung kỹ thuật. Ví dụ Trường đại học Maryland đề nghị các khóa học mới sẽ sử dụng kết nối vệ tinh nhân tạo đến các vị trí khác nhau trên các quốc gia. Trong tương lai, các băng hình được tạo ra theo cách này có thể được xâm nhập bằng máy tính, tạo sẵn cho sinh viên các tài liệu khoá học phục vụ trong nhiều năm với nhiều chủ đề và nhiều thày giáo khác nhau. Việc truy vấn của sinh viên đòi hỏi xâm nhập số lượng lớn băng hình liên quan đến PR-Quadtrees.

· Dữ liệu âm thanh (*Audio data*): Một sinh viên học về lịch sử đang nghiên cứu về Ai Cập cổ đại mong muốn tiếp cận với một vài cuộc phỏng vấn trước đây trên đài phát thanh của những người Ai Cập nổi tiếng (thí dụ *William Flinders Petrie*) để có thể biết chi tiết về những khám phá của họ về những nơi ở khác nhau của người Ai Cập. Có lẽ một khía cạnh nghiên cứu của anh ta liên quan đến một vấn đề đã tồn tại từ lâu gây tranh cãi trong nhiều năm giữa *Petrie* và *Gardiner*. Trong trường hợp này anh ta mong muốn tiếp cận với những băng audio cũ có nội dung liên quan đến lĩnh vực Ai Cập học. Thí dụ tương tự, nỗ lực điều tra của cảnh sát về dấu vết của kẻ đe doạ đánh bom mong muốn có khả năng nhận dạng giọng nói tương ứng với tín hiệu từ điện thoại của kẻ đó thông qua CSDL lưu giữ các mẫu giọng nói của các tổ chức khủng bố khác nhau.

· Dữ liệu tài liệu (*Document data*): Một CSDL văn bản truyền thống bao gồm các đoạn văn bản, các từ, câu, đoạn văn, chương… Một CSDL tài liệu khác văn bản ở chỗ nó không chỉ chứa các thông tin dạng văn bản thô mà còn chứa đựng cả cấu trúc và hình ảnh nhúng. Thí dụ, dữ liệu tài liệu được tạo ra, chèn vào và phục hồi nhờ sử dụng các ngôn ngữ đánh dấu chuẩn như HTML hay SGML. Trong các trường hợp như vậy cấu trúc của tài liệu có thể được khai thác dựa trên mục lục dữ liệu. Cách khác, giả sử chúng ta xem xét một quyển sách. Quyển sách không chỉ

chứa dữ liệu văn bản mà còn chứa cả hình ảnh. Một số hình ảnh có thể là những hình vẽ trong khi một số khác là những bức ảnh. Giả sử người sử dụng tìm một bức ảnh của hoàng đế *Mughal* tên là *Akbar* nhưng không thể tìm ảnh trong CSDL hình ảnh. Tuy nhiên, nếu anh ta có một thư viện điện tử số để truy cập thì anh ta có thể tìm thấy bức ảnh mong muốn nhờ xem xét kỹ những cuốn sách liên quan về lịch sử Ấn Độ. Như vậy, dữ liệu tài liệu bao gồm phương tiện quan trọng mà trong đó các thông tin có thể được lưu trữ dưới dạng điện tử.

· Dữ liệu viết bằng tay (*Handwritten data*): Nhiều người trong chúng ta thường ghi những ghi chú trên những mẩu giấy nhỏ, điều này thường gây mất thông tin khi chúng ta giặt quần áo hay vì một lý do nào đó mà những gì chúng ta ghi bị mờ đi. Một số ghi chú có thể là không quan trọng, nhưng có rất nhiều cái cần được giữ gìn. Xu thế gần đây cả trên thương trường hay trong giới nghiên cứu người ta cho rằng ghi chép điện tử ngày càng phổ biến hơn trong tương lai. Người sử dụng sẽ sử dụng các thiết bị điện tử để ghi chép và lưu trữ. Mặc dù có rất nhiều ghi chú có thể chuyển sang được dạng mã văn bản ASCII bằng kỹ thuật phân tích viết tay, nhưng có rất nhiều ghi chú không thể thực được bởi vì các ghi chú thường chứa cả các nét loằng ngoằng hay các biểu đồ khối… Người sử dụng sử dụng ghi chép điện tử mong muốn trong tương lai có thể đưa ra các truy vấn như "*Tìm mọi đoạn tài liệu được thực hiện vào tháng 1-1998 liên quan đến John Smith*". Truy vấn như vậy có thể được thực hiện dễ dàng nhờ chỉ số hoá tập hợp các ghi chú theo nội dung của chúng.

Các kiểu dữ liệu liệt kê trên đây chỉ là một phần trong rất nhiều hình thức biểu hiện của dữ liệu phát sinh tự nhiên trong các ứng dụng khác nhau. Một minh chứng là chỉ với việc xem xét dữ liệu hình ảnh chúng ta đã phải đương đầu với lượng các định dạng của nó (ví dụ như: GIF, TIFF, PCX…). Tình hình tương tự cũng xảy ra đối với việc mô tả các kiểu dữ liệu khác.

Một cách phi hình thức, hệ thống quản trị cơ sở dữ liệu đa phương tiện (*Multimedia Database Management System - MMDBMS*) là một khung làm việc để quản lý các kiểu dữ liệu khác nhau mà chúng được thể hiện trong rất nhiều khuôn dạng khác nhau. Để làm việc thành công thì một MMDBMS phải có các khả năng sau:

· Nó phải có khả năng truy vấn đồng bộ dữ liệu (dữ liệu media và dữ liệu văn bản) được thể hiện trong các định dạng khác nhau. Thí dụ, một MMDBMS sẽ có khả năng truy vấn và tích hợp dữ liệu mà nó được lưu trong các CSDL quan hệ khác nhau (ví dụ: PARADOX, DBASE...) mà có thể sử dụng các lược đồ khác nhau, cũng như việc truy vấn tệp phẳng và dữ liệu lưu trữ trong DBMS hướng đối

tượng hay DBMS không gian. Việc xử lý các truy vấn như vậy là khá phức tạp bởi vì trên thực tế việc nhận biết được nội dung (*content*) của các kiểu dữ liệu media là vấn đề thách thức và nó phụ thuộc rất nhiều vào kiểu dữ liệu và cách thức lưu trữ chúng. Cuối cùng, truy vấn có thể mở rộng đối với nhiều kiểu vật mang (*media*) dữ liệu và MMDBMS phải có khả năng kết hợp các kết quả từ các nguồn dữ liệu khác nhau và các kiểu *media* khác nhau.

· Tương tự, phải có khả năng truy vấn dữ liệu biểu diễn trong media khác nhau. Ví dụ một MMDBMS phải có khả năng truy vấn không chỉ trong CSDL hình ảnh mà còn cả trong CSDL âm thanh và CSDL quan hệ, sau đó kết hợp các kết quả với nhau.

· MMDBMS phải có khả năng khai thác các đối tượng mang tin (media) từ một thiết bị lưu trữ cục bộ một cách trơn tru, không có jitter (phải liên tục). Bởi vì các đối tượng mang tin (Video, âm thanh...) thường chiếm một không gian vô cùng lớn. Thí dụ nó có thể chiếm đến 10 Gigatebytes bộ nhớ do vậy những dữ liệu dạng này cần được lưu trữ trong các bộ nhớ ngoài (Disk, CD-ROM, Floppy...) hay tổ hợp các thiết bị đó.

· MMDBMS phải có khả năng tạo ra các câu trả lời từ truy vấn (khái niệm *"answer to a query"* được coi như cấu trúc toán học) và có khả năng trình diễn các câu trả lời này bằng các phương tiện nghe nhìn. Mặc dù vậy, hình thức và nội dung của trình diễn có thể khác nhau từ ứng dụng này đến ứng dụng khác, do đó người sử dụng phải xác định được cấu trúc của hình thức và nội dung của các trình diễn kết quả thu được từ hệ thống.

· Điều cuối cùng là mỗi một hệ thống có đầy đủ các đặc tính yêu cầu trên là chưa đủ mà còn cần phải có khả năng phân phối các trình diễn theo một cách nào đó nhằm thoả mãn các yêu cầu khác nhau về chất lượng thể hiện của các thiết bị. Ví dụ, nếu MMDBMS quyết định rằng một luồng dữ liệu âm thanh và một luồng dữ liệu Video phải được thể hiện cùng một lúc, để làm được việc đó MMDBMS phải đảm bảo được rằng sự thể hiện này không bị ảnh hưởng do hiện tượng như *jitter* hay trục trặc nào đó. Một điều quan trọng hơn là MMDBMS phải quan tâm tới việc dữ liệu đang được phân phối cho các thiết bị ra liên quan (loa, bàn phím, màn hình…) mà chúng có thể để tập trung tại các nút mạng phân tán. Do đó, các nhân tố như khả năng sẵn sàng của vùng đệm và độ rộng băng thông cần được lưu tâm khi phân phát trình diễn tới người sử dụng. Hơn nữa, đòi hỏi về chất lượng dịch vụ cho biết rằng các tính chất hiệu năng khác nhau cần được tối ưu theo các ràng buộc nói trên.

Do những nỗ lực trong mọi lĩnh vực của loài người mà việc tạo ra và quản lý các kho lưu trữ *multimedia* đã được thúc đẩy từ trước, trong đó có các cố gắng của cả giới nghiên cứu và lĩnh vực thương mại. Đó là nội dung chính của tài liệu này mà công nghệ CSDL được phát triển trong suốt 40 năm qua làm nền móng cho việc xây dựng MMDBMS. Ngày nay, các ngôn ngữ truy vấn, kỹ thuật chỉ mục, các thuật toán khai thác dữ liệu, các phương pháp cập nhật đã được phát triển cho nhiều loại CSDL như quan hệ, CSDL hướng đối tượng, CSDL không gian, thời gian và các CSDL khác. Mỗi một ngôn ngữ này là sự mở rộng, cải tiến của các ngôn ngữ trước đó và các thuật toán được áp dụng cho các các kiểu dữ liệu mới và quan trọng, hay các mô hình lý luận. Với dữ liệu đa phương tiện, nó cũng tương tự theo góc độ này. Những cái mới và dữ liệu nổi trội/mô hình lý luận phải phù hợp với các nghiên cứu mang tính

lý thuyết và các thử nghiệm trong lĩnh vực thương mại, với sự hỗ trợ tối đa từ các công nghệ đang có (không có sự phát minh lại) trong khi đang quên đi các hướng mới. Ví dụ một ngôn ngữ truy vấn CSDL hình ảnh nên quan tâm và tận dụng thành tựu của các ngôn ngữ truy vấn CSDL đã được nghiên cứu trong hơn 30 năm, hơn là bắt đầu từ một cái tạp nham. Hoàn toàn tương tự cho các hình thức khác của dữ liệu cũng như các chủ đề nghiên cứu khác (chỉ mục, khai thác, cập nhật, phiên giao dịch,...).

1.1 Các kịch bản đa phương tiện

Hãy xem xét một cuộc điều tra với quy mô lớn của cảnh sát về tình hình buôn bán ma túy. Thông thường, để thực hiện thành công một cuộc điều tra như vậy lực lượng cảnh sát sử dụng một số lượng lớn các thiết bị điện tử để thực hiện theo dõi các đối tượng nghi ngờ dính líu đến các tổ chức ma tuý. Với một cuộc điều tra như vậy có thể sử dụng các thiết bị dưới đây để thu thập thông tin:

1. Cảnh sát có thể sử dụng camera theo dõi (*surveillance camera*) để ghi lại các hình ảnh về hoạt động đang diễn ra tại các địa điểm khác nhau. Ví dụ mỗi camera theo dõi có thể giám sát các hoạt động đang diễn ra tại một địa điểm trong một khoảng thời gian tương đối dài (có thể là trong 6 tháng). Tại mỗi địa điểm họ thu được khoảng vài triệu hình ảnh. Vì chỉ mỗi một cuộc điều tra như vậy đã đòi hỏi từ 50 đến 100 camera theo dõi đặt tại các địa điểm khác nhau, do đó số hình ảnh video cần được quản lý là nhiều đáng kể. Quan trọng hơn nữa là với thúc ép của pháp luật, cần thực hiện hàng trăm cuộc điều tra như vậy tại những địa điểm xác định trong một khoảng thời điểm tại nhiều vùng khác nhau với rất nhiều hình thức tội phạm tương tự như cuộc điều tra về ma tuy như điều tra về các đường dây lừa đảo, các tội phạm liên quan đến tài chính, các cuộc điều tra về khủng bố, các cuộc điều tra về gián điệp… Số lượng dữ liệu video thu được theo cách đó phục vụ cho các cuộc điều tra là lớn khủng khiếp.

2. Một tình huống khác, lực lượng cảnh sát được lệnh thực hiện các cuộc nghe trộm điện thoại (*telephone wiretaps*) tại một địa điểm sau đó tập hợp lại các dữ liệu âm thanh là các cuộc đàm thoại cho là đáng ngờ. Mặc dù số lượng các cú điện thoại có thể khác nhau giữa các tội phạm, nhưng các tổ chức tội phạm (như đường dây ma tuy) rất hay sử dụng liên lạc điện thoại. Theo chiều hướng đó số lượng các chuỗi âm thanh thu được trong một khoảng thời gian từ các cuộc điều tra là rất lớn. Do vậy việc tổ chức và tìm kiếm dữ liệu *audio* này có ý nghĩa vô cùng lớn.

3. Ngoài tất cả những gì trình bày ở trên, lực lượng cảnh sát có thể có một số lượng lớn các bức ảnh chụp (*still photographs*) từ các điều tra viên (có thể trong

quá trình theo dõi một kẻ tình nghi). Hơn nữa, trong các cuộc điều tra tội phạm quy mô lớn có thể phát hiện ra số lượng đáng kể các tội phạm với tội danh nhẹ (ví dụ hình ảnh những kẻ buôn bán ma tuý lẻ bị chụp khi đang tiến hành bán ma tuý hay một hành vi liên quan đến ma tuý có thể được phát hiện mà bản thân nó có liên quan đến người trong bức ảnh). Tất cả những hình ảnh này phải được lưu lại dưới dạng kỹ thuật số, sẵn sàng cho các công việc tìm kiếm và khai thác khi cần.

4. Cảnh sát cũng có thể phải xem xét một số lượng lớn các tư liệu (*document*) đã tìm được tại những nơi có liên quan đến những vụ án đang điều tra hay những vụ án khác. Một lượng lớn tư liệu có thể liên quan trực tiếp đến vụ án nhưng vào thời điểm ban đầu thì chúng có thể không được rõ ràng. Khi một cuộc điều tra về ma tuý đang diễn ra, mọi cái trở nên minh bạch khi mà ngày càng có nhiều mối liên hệ với các chứng cứ đã thu được trong cuộc điều tra này hay các cuộc điều tra trước đây cũng có thể là những cuộc điều tra đang diễn ra cùng thời điểm.

5. Một tình huống khác, cảnh sát có thể xâm nhập đến các dữ liệu có quan hệ cấu trúc (*structured relational data*). Dữ liệu dạng này có thể bao gồm, thí dụ như dữ liệu trong các giao dịch ngân hàng của một vài tội phạm. Điều này là đặc biệt quan trọng bởi vì một số trùm ma tuý sử dụng rất nhiều hình thức rửa tiền, việc "*Lần theo dấu vết đồng tiền*" thường khám phá được rất nhiều điều thú vị. Các dữ liệu khác thuộc thể loại này có thể bao gồm những thông tin chán ngắt như những cuốn danh bạ điện thoại để xác định, nhận dạng người bị tình nghi.

6. Cảnh sát cũng có thể sử dụng hệ thống thông tin địa lý (*GIS*) chứa đựng những dữ liệu địa lý liên quan đến cuộc điều tra ma tuý đang được triển khai. Ví dụ cảnh sát nghi ngờ rằng một tuyến đường nào đấy đang được sử dụng để vận chuyển ma tuý. Để kiểm tra giả thuyết trên, họ phong toả một trong những tuyến đường đó (có lẽ ban đầu là kiểm tra một cách khắt khe trên tuyến đường này), theo cách đó làm tập trung hướng vận chuyển ma tuý. Mẫu (*pattern*) của luồng ma tuý sẽ cung cấp cho cảnh sát các thông tin rất quan trọng về các vị trí đầu mối của ma tuý. Để thực thi chiến dịch trên, cảnh sát có thể sử dụng các hệ thống GIS để quản lý dữ liệu địa lý. Các hệ thống GIS này quản lý các thông thông tin bao gồm thông tin về bản đồ đường đi, cũng có thể là các thông tin thu được về địa hình của những vùng lân cận của những thủ phủ trên núi (như *Medellin, Colombia*). Nhận thức về địa hình cũng như các hình thức sử dụng các phương tiện để vận chuyển ma tuý có thể mang lại cho cảnh sát những đầu mối có giá trị để xác định được các tuyến đường đi qua các địa hình có khả năng là vùng hoạt động của tội phạm.

Hình 1.1 là sơ đồ về các kiểu khác nhau của dữ liệu và các bộ phần mềm trọn gói được sử dụng trong các mẫu về Kịch bản đa phương tiện. Cần chú ý rằng các

nguồn về hình thức dữ liệu đề cập trên chỉ là mẫu nhỏ của nguồn dữ liệu đa dạng và phong phú, có sẵn trong một ứng dụng. Với sự bùng nổ về khả năng ứng dụng dữ liệu đa phương tiện, mỗi một lĩnh vực ứng dụng (dù trong ngành công nghiệp du lịch hay trong các hoạt động luật pháp) có thể có nguồn dữ liệu và kiểu media rất lớn và đa dạng từ ứng dụng này sang ứng dụng khác.

Error!

Trở lại các kịch bản đa phương tiện mẫu đã đề cập phần trên, bây giờ chúng ta đưa ra một số câu truy vấn hay gặp mà người sử dụng hệ thống đa phương tiện cảnh sát (ở đây là lực lượng cảnh sát) có thể hay sử dụng để giải quyết công việc của mình.

· **Query 1.1 (Image Query).** Giả sử rằng một cảnh sát có bức ảnh ngay trước mắt anh ta. Thí dụ, đó là bức ảnh chụp chính diện từ các cuộc điều tra mới đây. Cơ quan điều tra có thể nghi ngờ một người trong bức ảnh đang sử dụng một bí danh nào đó. Do vậy họ mong muốn giải quyết được vấn đề đặt ra là *"Tìm tất cả các bức ảnh từ thư viện ảnh trong đó có sự xuất hiện của người đang bị nghi ngờ"*.

Đây là một vấn đề rất thú vị bởi vì nó có thể được giải quyết bởi một trong hai khả năng. Thứ nhất là cảnh sát có thể biết trước tên của người trong bức ảnh. Trong trường hợp này truy vấn được thực hiện bằng việc sử dụng thông tin văn bản đã biết trước về các bức ảnh khác nhau trong thư viện ảnh để tìm ra một bức ảnh có kết hợp ghi chú bằng văn bản. Hoặc với cách khác, cảnh sát có thể cần đến việc áp dụng các kỹ thuật xử lý ảnh để tìm sự tương đồng giữa khuôn mặt trong bức ảnh vừa chụp với các khuôn mặt trong các bức ảnh có sẵn trong thư viện ảnh căn cước. Phương án thứ 2 thường được thực hiện ngay sau khi phương án thứ nhất thất bại.

· **Query 1.2 (Audio Query).** Trong một trường hợp khác, khi cơ quan cảnh sát đang nghe lại một băng ghi âm theo dõi những đối tượng tình nghi. Thí dụ, nội dung băng là một cuộc đàm thoại giữa một nhân vật A (người đang bị theo dõi) với một nhân vật B (người đang tiếp xúc với A). Dựa vào nội dung của cuộc đàm thoại, cơ quan cảnh sát mong muốn tìm kiếm thông qua CSDL các mẫu giọng nói để có thể xác định được người B. Nếu yêu cầu như trên thành công thì nó có thể cung cấp cho cảnh sát những chứng cứ hay có thể là những định hướng cho quá trình điều tra tội phạm.

Truy vấn trên đây chỉ bao hàm xử lý tiếng nói. Đặc điểm của lời nói được lưu trữ một cách đặc biệt trong một véctơ đặc trưng (*feature vector*) phản ánh các giá trị của các tham số khác nhau là "quan trọng" và liên quan đến quá trình ghi âm vừa qua. Để xác định xem một mẫu lời nói (giọng nói của nhân vật B) có tương đồng với một vector trong cơ sở dữ liệu tiếng nói hay không, chúng ta cần một số kỹ thuật dựa vào các CSDL tiếng nói có thể được đánh chỉ mục để thuận tiện hơn trong việc khai thác một cách nhanh chóng các dãy âm thanh tương tự (*similar*).

· **Query 1.3 (Text Query).** Mặt khác, cơ quan cảnh sát có thể xem qua các tập tài liệu như các file văn bản lưu trữ các bài báo cũ. Đó là hồ sơ cảnh sát về những vụ án giết người chưa được giải quyết, về các chứng cứ… Cảnh sát mong muốn giải quyết vấn đề đặt ra bằng cách đưa ra câu truy vấn như "*Tìm tất cả các tư liệu (từ tập các tài liệu văn bản) liên quan đến mối quan hệ trong các giao dịch tài chính của tổ chức thuốc phiện Cali với ABC Corp*".

Lần nữa, chúng ta thấy đây là một truy vấn khá thú vị, nó hướng vào lĩnh vực CSDL văn bản. Một từ khoá tìm kiếm đơn giản thông qua tập hợp các tài liệu không đảm bảo sẽ đảm bảo cho chúng ta kết quả chính xác, ngay cả khi chỉ mục cho việc tìm kiếm trong tài liệu văn bản này đã tồn tại. Cuối cùng nó càng không có sự đảm bảo là các tài liệu sẽ đề cập đến các từ "*Cali*", "*finance*" và "*ABC Corp*". Ví dụ một tư liệu nói về việc chuyển tiền từ tài khoản ngân hàng của *Jose Orojuelo* sang tài khoản của *John Smith* có thể là một tư liệu có giá trị. Nó có ý nghĩa vì *Jose Orojuelo* là một người đứng đầu nhóm buôn bán thuốc phiện tại *Cali* và *John Smith* là một quan chức cao cấp trong *ABC Corp*. Văn bản phải được đánh chỉ mục không chỉ theo từ khóa mà còn dựa trên nội dung ngữ nghĩa của từ khóa. Chỉ khi nào thực hiện được điều đó thì mới có hy vọng thu được các kết quả một cách chính xác và cô đọng.

· **Query 1.4 (Video Query)** Hãy xem xét một ví dụ sau, cơ quan cảnh sát đang kiểm tra một đoạn băng video theo dõi, ghi lại một nạn nhân bị tấn công nhưng đáng tiếc là kẻ tấn công đã giấu mặt trong khi gây án. Trong trường hợp này cơ quan cảnh sát mong muốn giải quyết vấn đề bằng đưa ra câu hỏi truy vấn "*Tìm tất cả các đoạn băng video mà có sự xuất hiện của nạn nhân trong vụ tấn công*". Với việc kiểm tra các đoạn băng video, cảnh sát hy vọng có thể thu được một số thông tin bổ ích cho việc nhận dạng kẻ gây án. Đặc biệt là trong trường hợp kẻ gây án có quen biết với nạn nhân. Một kịch bản tương tự cũng có thể nảy sinh trong khi cuộc buôn bán ma tuý đang diễn ra giữa hai tổ chức buôn bán ma tuý.

Cũng cần chú ý rằng trong trường hợp trên cảnh sát không đòi hỏi cung cấp các khung (*frame*) video về các hành động đã xảy ra. Thay vào đó họ yêu cầu các đoạn (*segment*) video (có lẽ là liên tiếp nhau) trong đó có hành động xảy ra. Điều này đòi hỏi MMDBMS không chỉ có khả năng tìm ra các frame video về các hành động đã xảy ra mà nó còn phải có khả năng tổng hợp các frame này thành những đoạn video liền mạch.

Bây giờ chúng ta sẽ thảo luận một vấn đề phức tạp hơn mà cơ quan cảnh sát phải đối phó. Mỗi một vấn đề đặt ra ở trên chỉ tiếp cận với một hình thức dữ liệu riêng lẻ. Mặc dù khái niệm về dữ liệu đa phương tiện đã trở nên phổ biến thông qua các dữ liệu nghe nhìn nhưng chúng ta phải biết rằng dữ liệu đa phương tiện không phải chỉ có dữ liệu tiếng nói và dữ liệu audio mà còn rất nhiều kiểu dữ liệu khác như các dữ liệu dạng các ghi chú, dữ liệu văn bản, dữ liệu quan hệ, dữ liệu về địa lý, các bản đồ địa hình, các mô hình không gian 3 chiều… Do vậy một truy vấn phức tạp hơn là việc trộn và tìm ra dữ liệu tương tự từ các nguồn khác nhau. Làm được điều đó sẽ cho phép cơ quan cảnh sát đặt ra các yêu cầu tiếp cận các nguồn dữ liệu tập trung trong các gói dữ liệu phức tạp và trên các phương tiện (*media*) khác nhau sử dụng các kỹ thuật lưu trữ khác nhau.

· **Query 1.5 (Simple Heterogeneous Query)** Giả sử rằng cơ quan cảnh sát đưa ra một vấn đề ”*Tìm tất cả những tù nhân đã bị kết án về tội mưu sát tại Mỹ và những người này trong thời gian gần đây đã thực hiện việc chuyển tiền điện tử từ ABC Corp vào tài khoản riêng của họ*”.

Xét bề ngoài của yêu cầu trên có vẻ như đây không có gì khác biệt với các truy vấn thông thường. Trước hết, nó chỉ bao hàm việc xử lý các câu truy vấn dựa vào các CSDL văn bản chuẩn ban đầu. Nhưng đáng tiếc là thực tế không phải như vậy, bất kỳ ai trong cơ quan pháp luật đều hiểu rằng giải quyết vấn đề trên là một công việc hết sức khó khăn. Lý do thứ nhất là để tìm được những người đã chuyển tiền điện tử từ *ABC Corp* vào tài khoản ngân hàng của họ thì phải đủ khả năng giám sát các hoạt động chuyển tiền điện tử của *ABC Corp*. Thực tế là *ABC Corp* có tài khoản trong hàng trăm ngân hàng trên khắp thế giới. Nếu nhìn nhận một cách lạc quan, chúng ta giả sử rằng cảnh sát đã có trong tay danh sách tài khoản của *ABC Corp* trong các ngân hàng trên khắp thế giới, hơn nữa, họ có quyền giám sát các giao dịch về tài chính liên quan đến các tài khoản này. Tuy nhiên các ngân hàng này có thể nằm rải rác trên khắp thế giới và một điều chắc chắn là các ngân hàng khác nhau sẽ xây dựng các báo cáo về các giao dịch đáng ngờ dưới các hình thức khác

nhau. Việc thu thập danh sách tài khoản nhận tiền của *ABC Corp* từ các báo cáo của những ngân hàng này đòi hỏi khả năng tự động xử lý báo cáo với định dạng khác nhau. Thứ hai, nhiệm vụ còn lại là xác định những ai đã nhận tiền từ

ABC Corp đã từng bị kết án với tội mưu sát lưu trữ trong kho dữ liệu tội phạm Bắc Mỹ. Các dữ liệu này cũng được quản lý theo các cách khác nhau. Trên thực tế chỉ xét riêng nước Mỹ tại các bang khác nhau cũng có sự khác nhau trong việc lưu trữ các hồ sơ tội phạm. Một số bang thì sử dụng các file phẳng một số thì sử dụng *Dbase, Oracle,* một số khác thì dùng *Sybase...*

Với truy vấn có mức độ phức tạp hơn đòi hỏi tiếp cận tất cả các khuôn dạng dữ liệu văn bản nói trên, nhưng còn phải thêm vào đó là kiểu dữ liệu hình ảnh.

· **Query 1.6 (Heterogeneous Multimedia Query).** Giả thiết rằng cơ quan cảnh sát đưa ra truy vấn ”*Tìm tất cả những người đã chụp ảnh với Jose Orojuelo và họ đã bị bắt trong vụ mưu sát tại Mỹ và gần đây họ đã nhận tiền chuyển vào tài khoản từ ABC Corp* ”.

Trong truy vấn này chúng ta không chỉ phải xác định những người thoả mãn yêu cầu trong Query 1.5 mà còn phải xác định trong những người tìm được từ Query 1.5ai đã chụp ảnh với *Jose Orojuelo*. Với nhiệm vụ này có thể đòi hỏi phải tiếp cận với:

§ Cơ sở dữ liệu thẻ căn cước chứa tên cũng như hình ảnh của mọi người.

§ Cơ sở dữ liệu các hình ảnh chứa các ảnh chụp liên quan đến các vụ điều tra (đã được trình bày trong phần trước)

§ Các dữ liệu video theo dõi để thấy được cuộc gặp gỡ giữa một kẻ khả nghi và *Jose Orojuelo* đã được ghi lại trước đó.

§ Các thuật toán xử lý ảnh để xác định ai xuất hiện trong bức ảnh chụp hay trong băng video.

Nhìn chung, các truy vấn này đòi hỏi phải tiếp cận đến các hình thức thường khác nhau của dữ liệu quan hệ, dữ liệu hình ảnh và các thuật toán xử lý ảnh.

· **Query 1.7 (Complex Heterogeneous Multimedia Query).** Một giả thuyết phức tạp hơn, cơ quan cảnh sát cần hỏi câu truy vấn “*Tìm tất cả những ai đã liên lạc với Jose Orojuelo và họ đã bị kết án bởi tội mưu sát tại Bắc Mỹ và những ai gần đây nhận tiền chuyển vào tài khoản riêng từ ABC Corp*”.

Trong truy vấn này khái niệm giao tiếp (*contact*) giữa người thoả mãn Query 1.5 và *Jose Orojuelo* bao hàm ý nghĩa rộng lớn của cách giao giao tiếp. Thí dụ, một

hình thức giao tiếp có thể thông qua ảnh chụp, ảnh theo dõi hay ảnh video: hai người được xem như là giao tiếp nếu họ chụp chung ảnh. Mặt khác, hai người giao tiếp nếu họ hội thoại với nhau. Thí dụ, nếu băng ghi âm cho thấy ai đó nói với *Jose Orojuelo* trên điện thoại thì nó thoả mãn "giao tiếp" trong câu truy vấn trên đây. Tương tự, thư điện tử là một hình thức khác của giao tiếp giữa những người liên quan. Cuối cùng thư đánh máy và thư viết tay trao đổi giữa *Jose Orojuelo* và ai đó cũng thoả mãn tiêu chí "giao tiếp" nói trên. Như vậy, để trả lời được câu truy vấn trên đây, ta cần xâm nhập đến dải rộng dữ liệu văn bản khác nhau (để trả lời truy vấn Query 1.5), bao gồm các DBMS quan hệ khác nhau, cũng như các loại dữ liệu khác nhau như ảnh, video, audio, văn bản và chữ viết tay.

1.3 Các ứng dụng khác

Các kịch bản mẫu về ứng dụng đa phương tiện trên đây đã mô tả phần lớn các hình thức dữ liệu multimedia và các lập luận có thể bắt gặp. Tuy nhiên ta còn thấy nhiều thí dụ khác về đa phương tiện từ các lĩnh vực khác nhau.

1.3.1 Các dịch vụ đa phương tiện trong giáo dục

Ngày nay, nhiều trường đại học đã cung cấp chương trình giáo dục từ xa giành cho những ai không có điều kiện tham gia lớp học với những lý do khác nhau như do điều kiện địa lý hay thời gian để có thể theo các khoá học. Khoá học như vậy ngày nay thông thường được tiến hành với việc gửi các băng ghi hình (nếu không bị hạn chế về thời gian thì các buổi học kết hợp tham khảo các tư liệu đa phương tiện là rất tốt). Trong một tương lai không xa, người sử dụng máy tính có thể truy cập trực tuyến các kho tài liệu dưới dạng băng hình, băng tiếng liên quan đến việc học tập. Thí dụ một sinh viên có thể truy cập đến một trong các dịch vụ trên máy chủ của nhà cung cấp dịch vụ và đưa ra câu truy vấn có thể như "*Tìm tất cả các bài giảng với chủ đề PR-quadtrees có trong thư viện tài liệu*". Thư viện có thể chứa đựng thông tin về chủ đề này trong các phương tiện lưu trữ khác nhau (các băng video bài giảng, các tập tài liệu in) liên quan đến chủ đề trên. Giải pháp truy vấn đòi hỏi khả năng duyệt qua các tư liệu để tìm được các phần phù hợp, nó có thể là một *video clip*. Ngoài các bài giảng, người sử dụng có khả năng lựa chọn được tài liệu mà họ cho là phù hợp nhất.

1.3.2 Ngành công nghiệp điện ảnh

Trong một tương lai rất gần, nhu cầu về phim ảnh theo yêu cầu (*on demand*) sẽ rất lớn. Người sử dụng có thể dễ dàng chọn các bộ phim tại nhà và xem chúng qua TV tại nhà. Trong thời gian hiện nay cách thức chọn phim mà người sử dụng mong

muốn là rất phong phú. Cũng như việc ứng dụng đa phương tiện trong lĩnh vực giáo dục miêu tả ở trên, trong lĩnh vực điện ảnh người sử dụng có thể lựa chọn phim mong muốn bằng cách trộn cả truy vấn tìm kiếm và duyệt. Thí dụ, người sử dụng muốn xem một bộ phim *Alfred Hitchcock* nhưng trong đó không có sự tham gia diễn xuất của *Jimmy Stewart* (có lẽ anh ta đã xem một số bộ phim kiểu này trước đây và đã trở nên nhàm chán với sự diễn xuất của *Jimmy Stewart*). Một hệ thống đa phương tiện hỗ trợ tương tác như vậy của người sử dụng thì phải có khả năng tìm kiếm hiệu quả những bộ phim thoả mãn nhu cầu của người sử dụng. Hơn thế nữa, người sử dụng nên có được khả năng xem trước những mẩu phim giới thiệu mà họ mong muốn. Ngoài ra, họ nên được quyền xem xét các bài phê bình về bộ phim, với sự cân nhắc như vậy có thể giúp người sử dụng lựa chọn được những bộ phim mà anh ta thực sự muốn xem.

1.3.3 Lời khuyên của các chuyên gia

Rất nhiều chúng ta không muốn phải trả giá cắt cổ cho việc sửa chữa ô tô. Trong nhiều trường hợp, việc sửa chữa có thể thực hiện dễ dàng, rẻ tiền nếu ta có chút ít tri thức cơ bản về những việc cần làm. Sách hướng dẫn sử dụng nhiều khi vô ích vì nó quá dày để thực hành. Một ý tưởng thú vị là tạo ra trợ giáo tự động (*assistant*) hay các tác tử (*agent*) cho các công việc khác nhau từ sửa chữa ống nước cho đến sửa chữa ô tô.

Thí dụ với việc sửa chữa ô tô, chúng ta muốn tương tác với chương trình để chỉ ra trên màn hình cái chúng ta cần nhìn thấy dưới mui xe. Hướng dẫn sử dụng quá súc tích: các câu như "*miếng đệm cao su 16-inch đặt ở bên phíc cắm của cuộn dây đánh lửa*" cho ta quá nhiều ý nghĩa. Người trợ giáo tự động sửa chữa ô tô sẽ chỉ ra ảnh (có thể lấy ra từ tài liệu hướng dẫn điện tử) của các chi tiết liên quan đến xe ô tô. Người sử dụng dễ dàng quan sát ảnh này và xác định phần vật lý nào trong xe tương ứng với phần đánh dấu trong ảnh. Giả sử phải thay thế toàn bộ miếng đệm, hệ thống sẽ in ra toàn độ đặc tả kỹ thuật của nó cùng với danh sách các nhà cung cấp trong vùng nơi họ sống.

1.3.4 Công nghiệp du lịch

Rất nhiều người lập kế hoạch nghỉ hè cho gia đình hàng năm phải đến các đại lý du lịch hay trong sách quảng cáo du lịch để tìm ra địa điểm du lịch phù hợp tài chính và thoả mãn nhu cầu nghỉ ngơi của họ. Nhưng ta có thể lập kế hoạch toàn bộ chuyến du lịch tại nhà. Hệ thống đa phương tiện cài đặt đại lý du lịch thông minh cho người sử dụng khả năng khớp nối các nhu cầu du lịch của họ, sau đó hỏi hệ thống để tìm ra vị trí thoả mãn. Hệ thống có thể cho lại nhiều điểm đến đều thoả

mãn yêu cầu người sử dụng. Hệ thống sẽ in ra toàn bộ hành trình, chi tiết về khách sạn, lịch bay...

1.3.5 Shopping tại nhà

Tương tự như công nghiệp du lịch, ta có thể sử dụng cùng khái niệm để thương mại sản phẩm đến khách hàng. Như trong trường hợp của công nghiệp du lịch, khách hàng có thể gọi hay xâm nhập các nhà cung cấp dịch vụ mà họ cung cấp thông tin trực tuyến về các sản phẩm đang có và các thông tin thương mại khác.

1.4 Kết luận

Các thí dụ liệt kê trên đây cùng chia sẻ các khía cạnh chung mà có thể là cách trừu tượng để hình thành lõi dữ liệu sẽ trình diễn và lõi của thuật toán sẽ cài đặt. Các khía cạnh chung này là độc lập với bất kỳ ứng dụng cụ thể nào.

>

Chương 2

CẤU TRÚC DỮ LIỆU ĐA CHIỀU

Phần lớn dữ liệu đa phương tiện liên quan đến không gian và thời gian. Dữ liệu loại này còn được gọi là dữ liệu *n* chiều, xuất phát từ thực tế là dữ liệu có các thuộc tính trong không gian n chiều. Thí dụ, không gian có hai hay ba chiều, không gian-thời gian có 4 chiều (các trục x, y, z, t). Ta sẽ nghiên cứu kỹ thuật biểu diễn thông tin *n* chiều.

Phần lớn các kỹ thuật lưu trữ dữ liệu n-chiều đều sử dụng việc tách "phân cấp" không gian và được biểu diễn bởi các cây. Gốc cây biểu diễn toàn bộ vùng. Nút biểu diễn vùng, cành biểu diễn việc phân hoạch vùng ra tiểu vùng.

Có nhiều cấu trúc dữ liệu khác nhau được sử dụng để biểu diễn việc tách phân cấp vùng. Ta sẽ nghiên cứu cây k-d, cây tứ phân điểm, cây tứ phân MX và cây R. Mỗi chúng thực hiện tách không gian theo cách khác nhau và có ưu điểm và nhược điểm riêng.

2.1 Mở đầu

Error!

Một trong kịch bản về ứng dụng đa phương tiện là dữ liệu có nguồn gốc thông tin địa lý (GIS). Một hình thức đơn giản nhất là GIS lưu trữ thông tin về vùng nào đó của trái đất như bản đồ (ảnh) chứa các đặc trưng nổi trội. Trong trường hợp này, bản đồ là ảnh hai chiều, một số điểm trên bản đồ được xem như các đối tượng cần quan tâm. Các điểm này có thể được lưu trữ trong nhiều cấu trúc dữ liệu đặc biệt. Hình 2.1a) là bản đồ đơn giản có một số điểm quan tâm trên nó. Các điểm được đánh dấu bởi địa danh (thí dụ như *Banja Luka, Brcko*). Thay vì điểm quan tâm, ứng dụng có thể quan tâm đến vùng bản đồ. Trong trường hợp này cấu trúc dữ liệu phải có khả năng lưu trữ thông tin về các vùng. Hình 2.1b) biểu diễn cùng bản đồ nhưng chứa một số vùng quan tâm.

Chương này chỉ ra cách biểu diễn dữ liệu bản đồ trên hình 2.1 bằng các loại cây k-d, cây tứ phân và cây R.

2.2 Cây k-d (k-d Trees)

Cây k-d được sử dụng để lưu trữ dữ liệu điểm k-chiều như chỉ ra trên hình 2.1a. Không sử dụng nó để lưu trữ dữ liệu vùng. Như vậy, cây 2-d (khi k=2) lưu trữ dữ liệu điểm 2-chiều, cây 3-d lưu trữ dữ liệu điểm 3-chiều... Thí dụ này đề cập đến dữ liệu điểm 2-d, sau đó khái quát lên dữ liệu điểm 3-d.

2.2.1 Cấu trúc nút

Error!

Trong cây 2-d, mỗi nút có cấu trúc bản ghi nhất định với kiểu như sau:

```
nodetype = record
        INFO: infotype;
        XVAL: real;
        YVAL: real;
```

LLINK: nodetype;

RLINK: nodetype;

end

Trường INFO có thể có kiểu bất kỳ do người sử dụng định nghĩa và phụ thuộc vào ứng dụng cụ thể. Thí dụ, nó có thể là trường xâu ký tự mô tả địa danh,

hay nó có thể là bản ghi bao gồm các trường *name:string* và *population:integer*...

Trường XVAL, YVAL biểu thị tọa độ điểm kết hợp với nút.

Các trường LLINK và RLINK trỏ đến hai cành.

Error!

Giả sử T trỏ đến gốc của cây 2-d. Nếu N là nút trong cây, thì mức của N được xác định qui nạp như sau:

Cây 2-d là cây nhị phân bất kỳ nếu thoả mãn điều kiện sau:

1. Nếu N là nút trong cây và *level(N)* là chẵn thì mỗi nút *M* trong cành rẽ nhánh từ N.LLINK có tính chất M.XVAL < N.XVAL, mỗi nút *P* trong cành rẽ nhánh từ N.RLINK có tính chất P.XVAL ³ N.XVAL.

2. Nếu N là nút trong cây và *level(N)* là lẻ thì mỗi nút *M* trong cành rẽ nhánh từ N.LLINK có tính chất M.YVAL < N.YVAL, mỗi nút P trong cành rẽ nhánh từ N.RLINK có tính chất P.YVAL ³ N.YVAL.

2.2.2 Chèn và tìm kiếm trong cây 2-d

Việc chèn nút N vào cây do T trỏ tới được phát biểu phi hình thức như sau:

> Kiểm tra xem N và T có thống nhất các trường XVAL và YVAL hay không. Nếu thống nhất thì chỉ việc viết đè nút T và kết thúc. Nếu không hãy rẽ trái nếu N.XVAL<T.XVAL hoặc rẽ phải trong trường hợp ngược lại. Giả sử P là nút con ta đang khảo sát. Nếu N và P thống nhất các trường XVAL và YVAL thì chỉ cần viết đè P và kết thúc, nếu không thì rẽ trái khi N.YVAL<P.YVAL hoặc rẽ phải trong trường hợp ngược lại. Lặp thủ tục này, hãy rẽ nhánh theo XVAL khi ta đang ở mức chẵn trong cây, và theo YVAL khi ta đang ở mức lẻ.

Error!

Thí dụ trên hình 2.3 là lưới bản đồ. Gốc (0, 0) ở góc dưới trái của lưới. Mỗi tế bào

có kích thước 8, do vậy kích thước bản đồ là 64x64. Giả sử ta phải xây dựng cây 2-d , trường INFO chỉ chứa tên địa điểm.

Danh sách các địa điểm như sau đây:

Thành phố	(XVAL, YVAL)
Banja Luka	(19, 45)
Derventa	(40, 50)
Teslic	(38, 38)
Tuzla	(54, 40)
Sinj	(4,4)

Error!

Khởi động cây là rỗng. Hình 2.4 là trình tự chèn vào cây. Các cây này được xây dựng như sau đây:

1. Khi chèn *Benja Luka* vào cây có một nút với *INFO=Benja Luka, XVAL=19, YVAL=45*. Nút này biểu diễn toàn bộ vùng bản đồ. Tổng quát, mỗi nút *N* biểu diễn vùng *Reg(N)*. Các trường *XVAL* và *YVAL* của nút *N* xác định điểm trong *Reg(N).* Điểm (*N.XVAL, N.YVAL*) chia *Reg(N)* thành 2 phần bằng cách vẽ đường thẳng đứng qua điểm trong vùng (nếu nút ở mức chẵn) hay vẽ đường nằm ngang qua điểm trong vùng (nếu nút ở mức lẻ).

2. Khi chèn *Derventa*, phải so sánh các trường *XVAL* của nó với trường này của *Benja Luka*. Chúng ta rẽ phải vì tọa độ x (40) của *Derventa* lớn hơn của *Banja Luka (19).* Kết quả trên hình 2.4b. *Benja Luka* chia đôi vùng bằng đường thẳng đứng (đường *a* của hình 2.5) - mọi điểm nằm bên phải có tọa độ *x* lớn hơn hay bằng 19, bên trái có tọa độ nhỏ hơn 19. *Derventa* biểu diễn vùng bên phải của đường thẳng đứng a) của hình 2.5.

3.

Error!

Khi chèn *Teslic*, trước hết ta so sánh trường *XVAL* của *Teslic* và *Benja Luka*. Trường này của *Teslic* là 38, của *Benja Luka* là 19, vậy ta phải rẽ phải. Sau đó so sánh trường *YVAL* của *Testic* với *YVAL* của *Derventa*.*YVAL* của *Testic* là 38, của *Derventa* là 50, do vậy phải rẽ trái. Kết quả trên hình 2.4c. *Derventa* chia đôi vùng bằng đường nằm ngang b) của hình 2.5.Vùng phía trên đường thẳng có tọa độ *x* lớn hơn hay bằng 19, tọa độ *y* lớn hơn hay bằng 50. Vùng phía dưới đường thẳng có toạ độ *x* nhỏ hơn 19 và tọa độ *y* nhỏ hơn 50.

4. Khi chèn *Tuzla*, trước hết phải so sánh *XVAL* của *Tuzla* và *Banja Luka*. Giá trị *XVAL* của *Tuzla* là 54, còn của *Benja Luka* là 19, vậy phải rẽ phải. Sau đó so sánh *YVAL* của *Tuzla (40)* và *Derventa (50)*, vậy phải rẽ trái. Tiếp tục so sánh *XVAL* của *Tuzla (54)* và *Teslic (38)*, vậy phải rẽ phải (hình 2.4d).

5. Cuối cùng, khi chèn thành phố *Sinj*, ta phải so sánh *XVAL* của *Sinj* và *Benja Luka*. Ta rẽ trái vì tọa độ *x* của *Sinjnhor* hơn của *Benja Luka*. Kết quả được mô tả trên hình 2.4d và 2.4e.

Trong trường hợp tồi nhất thì độ cao của cây 2-d với k nút là (k-1), việc tìm kiếm nút cho trước sẽ mất O(k) lần.

2.2.3 Huỷ bỏ trong cây 2-d

Công việc phức tạp nhất với cây 2-d là huỷ bỏ điểm khỏi cây. Giả sử T là cây 2 chiều, điểm sẽ huỷ bỏ có tọa độ (x, y). Bước thứ nhất của việc huỷ bỏ là tìm ra nút N trong T sao cho N.XVAL=x và N.YVAL=y. Nếu N là nút lá thì huỷ N là dễ dàng, chỉ việc đặt NIL cho LLINK, RLINK trong nút cha N, giải phóng vùng nhớ N. Nếu N là nút trong cây thì tình hình phức tạp hơn. Trong trường hợp này, cây con có gốc tại N.LLINK (đặt tên là T_l) hay tại N.RLINK (đặt tên là T_r) là không rỗng. Cái ta muốn bây giờ là tìm nút R từ T_l hay T_r có thể thay thế nút N và có thể lần lượt được huỷ bỏ khỏi cây con. Như vậy các bước của thuật toán huỷ bỏ nút N bên trong cây sẽ là:

Bước 1: Tìm nút ứng viên thay thế R trong T_i với iÎ{l, r}.

Bước 2: Thay thế mọi trường không có liên kết của N bởi các trường của R.

Bước 3: Huỷ bỏ đệ qui R khỏi T_i.

Đệ qui trên đây có điểm dừng vì T_i với iÎ{l, r} có độ cao nhỏ hơn cây T.

Bước phức tạp nhất trong thuật toán trên là tìm ra nút ứng viên thay thế. Nút R muốn thay thế phải có quan hệ không gian với mọi nút P trong T_l và T_r sao cho N dẫn tới P. Có nghĩa rằng, nếu P ở phía tây nam N thì P phải ở tây nam R, nếu P ở tây bắc N thì P phải ở tây bắc R, ... Như vậy, nút mong muốn thay thế R phải thoả các tính chất sau:

1. Mọi nút M trong T_l thoả M.XVAL<R.XVAL nếu level(N) là chẵn và M.YVAL<R.YVAL nếu level(N) là lẻ.

2. Mọi nút M trong T_r thoả M.XVAL³R.XVAL nếu level(N) là chẵn và M.YVAL³R.YVAL nếu level(N) là lẻ.

Nếu T_r không rỗng và level(N) là chẵn, thì bất kỳ nút nào trong T_r mà có trường XVAL nhỏ nhất thì là nút ứng viên thay thế. Thí dụ, trong hình 2.4e, nếu ta lấy N là nút chứa *Banja Luka*, thì nút ứng viên thay thế từ cây con bên phải là nút liên kết với Testic vì nó có tọa độ x nhỏ nhất trong các nút của cây con phía phải *Banja Luka*.

Mặt khác, nếu T_r không rỗng và level(N) là lẻ thì bất kỳ nút nào trong T_r mà có trường YVAL nhỏ nhất thì là nút ứng viên thay thế.

Tổng quát thì việc tìm kiếm nút thay thế từ cây con bên trái chỉ có thể thắng lợi dưới một số điều kiện nhất định. Nếu *level(N)* là chẵn thì nút thay thế phù hợp trong T_l là nút bất kỳ nếu thoả mãn trường XVAL của nó có giá trị lớn nhất. Tương tự nếu *level(N)* là lẻ thì ta có thể sử dụng nút bất kỳ trong T_l mà có trường YVAL lớn nhất để làm nút thay thế.

Vấn đề xảy ra là có thể có nhiều nút trong T_l cùng có XVAL (hay YVAL) lớn nhất, trong trường hợp này điều kiện thứ hai trong định nghĩa cây 2-d có thể bị vi phạm bởi bước 3 vừa mô tả trên. Tổng quát thì, nếu N là nút trong và ta muốn huỷ bỏ N khỏi T thì tìm thay thế từ cây con phải vì việc tìm ứng viên thay thế trong cây trái là không thể.

Cái gì xảy ra nếu N có cây phải rỗng (N.RLINK=NIL)? Trong trường hợp này ta có thể chọn nút thay thế R từ T_l có giá trị x nhỏ nhất trong T_l (nếu level(N) là chẵn) hay có giá trị y nhỏ nhất trong T_l (nếu level(N) là lẻ). Sau đó ta sửa đổi bước 2 trong thuật toán trên đây như sau:

Bước 2 (sửa đổi): Thay thế toàn bộ các trường không có liên kết của nút N bằng nút R. Đặt N.RLINK=N.LLINK và N.LLINK=NIL.

2.2.4 Truy vấn khoảng trong cây 2-d

Truy vấn khoảng trên cây 2-d có tên T là truy vấn theo chỉ định điểm (x_c, y_c) và khoảng r. Kết quả cho lại là tập điểm (x, y) trong cây T sao cho (x, y) nằm trong khoảng r của (x_c, y_c). Nói cách khác khoảng truy vấn xác định vòng tròn bán kính r có tâm (x_c, y_c) và tìm mọi điểm trong cây 2-d nằm trong vòng tròn.

Khi xử lý truy vấn khoảng, ta nhớ lại rằng mỗi nút N trong cây 2-d biểu diễn vùng R_N, nếu vòng tròn và vùng R_N không giao nhau thì không tìm thấy điểm nào trong cây con có gốc là nút N. Hãy quan sát các vùng trong hình 2.5d.

1. Nút có nhãn *Banja Luka* biểu diễn vùng chứa các điểm (x, y) của các số thực.

2. Nút có nhãn *Derventa* biểu diễn vùng chứa mọi điểm (x, y) với x³19; nó có thể được thu nhận bởi biểu thức {(x, y) | x³19}.

3. Nút có nhãn *Teslic* biểu diễn vùng chứa mọi điểm (x, y) với x³19 và y<50; nó có thể được thu nhận bởi biểu thức {(x, y) | x³19&y<50}.

4. Nút có nhãn *Tuzla* biểu diễn vùng chứa mọi điểm (x, y) với x³38 và y<50; nó có thể được thu nhận bởi biểu thức {(x, y) | x³38&y<50}.

5. Cuối cùng, nút nhãn *Sinj* biểu diễn vùng chứa mọi điểm (x, y) với x<19.

Tổng quát thì mỗi nút N có nhiều nhất 4 ràng buộc kết hợp biểu diễn kết nối các vùng:

1. XLB: Ràng buộc này biểu diễn cận dưới (*Lower Bound*) của x và có khuôn dạng x^3c_1.

2. XUB: Ràng buộc này biểu diễn cận trên (*Upper Bound*) của x và có khuôn dạng $x<c_2$.

3. YLB: Ràng buộc này biểu diễn cận dưới của y và có khuôn dạng y^3c_3.

4. YUB: Ràng buộc này biểu diễn cận trên của y và có khuôn dạng $y<c_4$.

Có thể mở rộng định nghĩa kiểu dữ liệu *nodetype* thành *newnodetype* bằng cách gộp các trường vừa mô tả trên như sau:

```
newnodetype = record
```

INFO: infotype;

XVAL,YVAL: real;

XLB, XUB, YLB, YUB: real È {+¥, -¥};

LLINK, RLINK: newnodetype;

end

Khi xen nút ta chỉ phải làm như sau đây:

1. Với gốc cây: đặt -¥ vào XLB và YLB, đặt +¥ vào XUB và YUB.

2. Nếu nút N có nút P là cha và mức *level(P)* là chẵn thì

   N.XLB=P.XLB nếu N=P.LLINK

   N.XLB=P.XVAL nếu N=P.RLINK

   N.XUB=P.XVAL nếu N=P.LLINK

   N.XUB=P.XUB nếu N=P.RLINK

   N.YLB=P.YLB

   N.YUB=P.YUB

3. Nếu nút N có nút P là cha và mức *level(P)* là lẻ thì

   N.YLB=P.YLB nếu N=P.LLINK

   N.YLB=P.YVAL nếu N=P.RLINK

   N.YUB=P.YVAL nếu N=P.LLINK

   N.YUB=P.YUB nếu N=P.RLINK

   N.XLB=P.XLB

   N.XUB=P.XUB

Thí dụ sau đây xem xét truy vấn khoảng trên bản đồ *Bosnia* (hình 2.6). Cho trước vòng tròn tâm (35, 46) và bán kính 9.5. Câu trả lời là hai điểm *Testic* và *Derventa* sẽ thoả mãn.

Tiến trình truy vấn như sau. Vùng biểu diễn gốc cây 2-d không cắt vòng tròn, vậy ta kiểm tra xem *Banja Luka* có trong vòng tròn? Câu trả lời là nó không nằm trong. Tiếp tục xem xét hai cành của *Banja Luka*, bên trái biểu diễn mọi điểm (x, y) thoả x<19. Vì vùng này không cắt vòng tròn nên ta sẽ không xem xét cành này. Mặt khác cành phía phải của *Banja Luka* biểu diễn mọi điểm (x, y) thoả $x^3$19, chắc chắn nó cắt vòng tròn. Kiểm tra xem cành bên phải (*Derventa*) có trong vòng tròn? Câu trả lời là có, vậy ta cho lại mã của nó. Sau đó hãy khảo sát cành của *Derventa*. Vùng biểu diễn bởi tập điểm (x, y) thoả $x^3$19 và y<50. Vùng này cắt vòng tròn, vậy phải kiểm tra cành có trong vòng tròn? Câu trả lời là có, vậy ta trả lại cành của nó (*Testic*). Hãy xem xét con của *Testic* (*Tuzla*). Vùng này được biểu diễn bởi tập

điểm (x, y) thoả x³38 và y<50, và vùng này cắt đường tròn. Vậy cần kiểm tra xem *Tuzla* trong vòng tròn? Câu trả lời là không, do vậy có thể dừng tại đây.

2.2.5 Cây k-d với k³2

Cây 2-d để biểu diễn điểm trong không gian 2-d. Cây k-d với k³2 biểu diễn điểm trong không gian k-d. Thí dụ, cây 3-d biểu diễn các điểm (x, y, z) và cây 4-d biểu diễn điểm dưới dạng (x, y, x, t)... Tổng quát, điểm trong không gian k-d có dạng $(x_1, ..., x_k)$, trong đó x_i là số thực.

Để biểu diễn nút cây k-d, ta giả sử rằng các trường XVAL, YVAL sử dụng trong cây 2-d bị loại bỏ, thay vì *nodetype* hay *newnodetype* sẽ có trường VAL mới. Nó là mảng độ dài k của các số thực.

Cây T có cấu trúc nút như vậy được gọi là cây k-d nếu với mỗi nút N trong cây T ta có:

1. Giả sử level(N) mod k=i.

2. Với mỗi nút M trong cành trái của N ta có M.VAL[i]<N.VAL[i].

3. Với mỗi nút P trong cành phải N ta có P.VAL[i]³N.VAL[i].

Mọi thuật toán của cây 2-d tổng quát hóa cho cây k-d với k³2. Nếu k=1 ta có cây tìm kiếm nhị phân chuẩn.

2.3 Cây tứ phân điểm (Point Quadtrees)

Một cây tứ phân điểm giống như cây 2-d nó được sử dụng để biểu diễn các điểm dữ liệu trong không gian hai chiều. Có điều không giống như cây 2-d là cây tứ phân điểm luôn phân một vùng thành 4 phần. Trong cây 2-d, nút N phân một vùng thành hai phần do vẽ một đường thẳng đi qua điểm (N.XVAL, N.YVAL). Đường kẻ này có thể là đường nằm ngang nếu cấp của N là lẻ hoặc là đường thẳng đứng trong trường hợp cấp của N là chẵn. Đối với cây tứ phân điểm thì nút N phân một vùng mà nó biểu diễn do vẽ cả đường thẳng đứng và đường nằm ngang qua điểm (N.XVAL, N.YVAL). Bốn phần được tạo ra được gọi là các góc NW (Tây Bắc), SW (Tây Nam), NE (Đông Bắc) và SE (Đông Nam) xác định bởi nút N và mỗi góc tương ứng với một con của nút N. Do đó các nút trong cây bốn nhánh có thể xác định 4 cành. Trước khi thực hiện các thao tác đối với cây bốn cành chúng ta đưa ra định nghĩa đơn giản của cấu trúc nút cho một nút của cây tứ phân như sau:

qtnodetype = record

INFO : infotype;

XVAL: real;

YVAL: real;

NW, SW, NE, SE : qtnodetype;

end

2.3.1 Chèn và tìm kiếm trong cây tứ phân điểm

Bây giờ chúng ta hãy khảo sát tập 5 điểm (*Banja Luka, Derventa, Teslic, Tuzla* và *Sinj*) đã được thể hiện với cây 2-d, nó sẽ được thể hiện như thế nào thông qua một cây tứ phân. Hình 2.7 thể hiện việc chèn từng điểm vào cây, còn hình 2.8 cho thấy cây tứ phân được xây dựng như thế nào.

Tiến trình này được mô tả như sau:

1. Khởi đầu cây tứ phân là rỗng, việc chèn *Banja Luka* tạo ra nút gốc của cây được gán nhãn với cặp (19, 45).

2. Việc chèn *Derventa* tạo ra vùng miêu tả bởi *Banja Luka* được phân thành 4 phần thông qua việc vẽ một đường nằm ngang và một đường thẳng đứng qua (19, 45). *Derventa,* ở vị trí (40, 50), nằm trong góc phần tư NE, do vậy *Banja*

Error!

Luka có con NE là *Derventa*.

3. Việc chèn *Teslic* được tiến hành như sau: *Teslic* nằm theo hướng Đông Nam của *Banja Luka*. Do vùng này hiện tại chưa có điểm nào nên chúng ta đặt *Teslic* làm con SE của *Banja Luka*.

4. Việc chèn *Tuzla* phức tạp hơn. Chúng ta thấy rằng *Tuzla* nằm ở SE của *Banja Luka*. Do vậy chúng ta chuyển đến nhánh SE của *Banja Luka*. Kết quả là góc phần tư SE được chia bởi vẽ đường nằm ngang và đường thẳng đứng qua điểm *Teslic*.

Với kết quả bốn phần được tạo ra, *Tuzla* ở góc SE và như vậy *Tuzla* trở thành nút con SE của *Teslic*.

5. Cuối cùng, việc chèn *Sinj* là không quá phức tạp bởi vì nó nằm ở SW của *Banja Luka*. Do hiện tại con trỏ này là rỗng nên ta đặt nút này chứa thông tin liên quan đến *Sinj*.

Nhìn chung chiều cao của một cây tứ phân chứa *n* nút có thể có giá trị lớn nhất là *n-1*, điều đó có nghĩa là thời gian để tìm kiếm hay chèn là nhỏ hơn số lượng nút.

2.3.2 Thao tác xoá trên cây tứ phân điểm

Error!

Khi xoá nút N từ cây tứ phân có gốc T cũng có những nét giống như chúng ta đã thực hiện với cây 2-d để tìm một nút thay thế thích hợp cho các nút không phải là lá. Đối với trường hợp các nút lá thì việc xoá không có vấn đề gì: Chúng ta đặt trường liên kết tương ứng của nút cha của N trỏ tới NIL và giải phóng không gian lưu trữ.

Việc xoá trong cây tứ phân là rất phức tạp. Hình 2.9 chỉ ra tại sao lại phức tạp. Đầu tiên mỗi nút trong cây tứ phân thể hiện một vùng và vùng này được định nghĩa hơi khác hơn so với cây 2-d. Đối với cây 2-d nó đủ để kết hợp 4 ràng buộc dưới dạng x^3c_1, $x<c_2$, y^3c_3, $y<c_4$ với các hằng số c_1,..., c_4. Do đó như trong trường hợp cây 2-d khi mà chúng ta mở rộng *nodetype* thành cấu trúc nút mới *newnodetype*, chúng ta cũng có thể mở rộng cấu trúc nút *qtnodetype* thành một cấu trúc nút mới *newqtnodetype* với cùng kiểu trường như trên đây (XLB, YLB, XUB, YUB).

newqtnodetype = record

INFO: infotype;

XVAL, YVAL : real;

XLB, YLB, XUB, YUB : real È {-¥, +¥};

NW, SW, NE, SE : newqtnodetype

end

Khi chèn nút N vào cây T chúng ta cần đảm bảo những điểm dưới đây:

1. Nếu N là gốc của cây T, thì N.XLB=-¥, N.YLB=-¥, N.XUB=+¥, và N.YUB=+¥.

2. Nếu P là cha của N thì khi đó bảng dưới đây mô tả những giá trị của các trường XLB, YLB, XUB, YUB của N tuỳ thuộc vào việc N là con NW, SW, NE hay SE của P. Chúng ta sử dụng ký hiệu w=(P.XUB–P.XLB) và h=(P.YUB – P.YLB).

Trường hợp	**N.XLB**	**N.XUB**	**N.YLB**	**N.YUB**
N= P.NW	P.XLB	P.XLB+w´0.5	P.YLB+h´0.5	P.YUB
N= P.SW	P.XLB	P.XLB+w´0.5	P.YLB	P.YLB+h´0.5
N= P.NE	P.XLB+w´0.5	P.XUB	P.YLB+h´0.5	P.YUB
N= P.SE	P.XLB+w´0.5	P.XUB	P.YLB	P.YLB+h´0.5

Để vận dụng thành công kỹ thuật xoá trong với cây tứ phân điểm thì khi xoá một nút trong N ta phải tìm một nút thay thế R từ một trong các cây con của N (từ một trong N.NW, N.SW, N.NE, N.SE) sao cho mỗi nút R_1 trong N.NW là ở phía tây bắc của R, mỗi nút R_2 trong N.SW ở phía tây nam R, mỗi nút R_3 trong N.NE ở phía đông bắc của R và mỗi nút R_4 trong N.SE ở phía đông nam của R.

Hãy xem xét cây tứ phân trên hình 2.8 và hình 2.9. Giả sử chúng ta muốn xoá *Banja Luka* từ cây tứ phân này. Trong trường hợp này, nút thay thế thực tế được tìm là *Teslic*. Không nút nào khác thoả mãn những điều kiện đã đặt ra ở trên.

Tuy nhiên, không phải luôn có khả năng tìm được một nút thay thế. Do vậy trong trường hợp xấu nhất việc xoá một nút N có thể yêu cầu việc chèn lại một số nút trong cây con trỏ bởi N.NE, N.SE, N.NW và N.SW. Trong phần sau ta sẽ khảo sát cây tứ phân MX cho phép xóa nút một cách dễ dàng hơn.

4.3.3 Truy vấn khoảng trong cây tứ phân điểm

Các truy vấn khoảng trong cây tứ phân được thực hiện gần như cách thức thực hiện trong cây 2-d. Mỗi nút trong một cây tứ phân thể hiện một vùng và phương pháp tính tóan và truy vấn khoảng tránh việc tìm kiếm các cành bắt nguồn từ những nút mà các vùng liên quan đến chúng không giao với đường tròn định nghĩa bởi truy vấn khoảng. Đại thể như nếu chúng ta đang tìm kiếm cây tứ phân điểm bắt nguồn từ T với tất cả các điểm trong một đường tròn C, tâm (xc, yc) và có bán kính là r, giải thuật được nêu ra như sau:

Giải thuật 2.1

proc RangeQueryPointQuadtree(T: newptnodetype, C: circle)

1. If region(T) Ç C = Æ then Halt

2. else

   (a) If (T.XVAL, T.YVAL)Î C then print (T.XVAL, T.YVAL);

   (b) RangeQueryPointQuadtree(T.NW, C);

   (c) RangeQueryPointQuadtree(T.SW, C);

   (d) RangeQueryPointQuadtree(T.NE, C);

   (e) RangeQueryPointQuadtree(T.SE, C);

End proc

2.4 Cây tứ phân matrix MX (MX-Quadtrees)

Trong cả hai trường hợp cây 2-d và cây tứ phân điểm, hình thù của cây phụ thuộc vào thứ tự các đối tượng được chèn vào cây. Đặc biệt, thứ tự ảnh hưởng đến chiều cao của cây, do đó ảnh hưởng đến độ phức tạp của các thao tác tìm kiếm và chèn. Mỗi nút N của cây 2-d và cây tứ phân điểm biểu diễn vùng và phân chia vùng thành 2 (trường hợp cây 2-d) hoặc 4 (trường hợp cây tứ phân) vùng con. Việc phân chia có thể không đều vì nó phụ thuộc vào vị trí điểm (N.XVAL, N.YVAL) trong vùng biểu diễn bởi N.

Ngược lại, mục tiêu của cây *MX-quadtree* là để đảm bảo hình dạng (và chiều cao) của cây độc lập với số lượng các nút của cây, cũng như thứ tự chèn các nút này. Thêm nữa, *MX-quadtree* tập trung vào việc đem lại các giải thuật xoá và tìm kiếm có hiệu quả.

Một cách ngắn gọn, cây *MX-quadtree* làm việc như sau: Đầu tiên chúng ta giả định rằng bản đồ đang được phân thành một lưới kích thước (2^k x 2^k). Người phát triển ứng dụng tự do lựa chọn k và một khi nó được chọn thì nó phải cố định.

MX-quadtree có cấu trúc nút tương tự như cây tứ phân điểm, đó là chúng có kiểu *newqtnodetype*. Có một sự khác biệt là gốc của *MX-quadtree* miêu tả vùng xác định bởi XLB = 0, XUB = 2^k, YLB = 0, YUB = 2^k. Hơn nữa, khi một vùng được phân chia, nó được chia ở giữa. Do vậy, nếu N là một nút, khi đó các vùng thể hiện bởi bốn cành của N được mô tả theo bảng dưới đây. Trong bảng này, w ký hiệu chiều rộng của vùng được biểu diễn bởi N và được cho bởi w= N.XUB – N.XLB.

Do tất cả các vùng được biểu diễn bởi các nút trong *MX-quadtree* là các vùng vuông, nên w = N.YUB – N.YLB.

Con	XLB	XUB	YLB	YUB
NW	N.XLB	N.XLB +w/2	N.YLB +w/2	N.YLB +w
SW	N.XLB	N.XLB +w/2	N.YLB	N.YLB +w/2
NE	N.XLB +w/2	N.XLB +w	N.YLB +w/2	N.YLB +w
SE	N.XLB +w/2	N.XLB +w	N.YLB	N.YLB +w/2

2.4.1 Chèn và tìm kiếm trong MX-Quadtree

Error!

Chúng ta hãy xem xét cách chèn điểm vào cây *MX-Quadtree*. Mỗi điểm (x, y) trong cây *MX-Quadtree* biểu diễn vùng 1x1 mà góc dưới bên trái là (x, y). Điểm chèn vào nút biểu diễn vùng 1x1 tương ứng với điểm này. Giả sử bây giờ chúng ta muốn chèn các điểm A, B, C và D như trên hình 2.12, hãy tiến hành các bước như dưới đây:

Error!

1. Việc chèn điểm A với toạ độ (1, 3) như sau: Là nút gốc biểu diễn toàn bộ vùng và A nằm trong NW. Do vậy, cành NW của gốc tương ứng vùng 2x2 mà góc dưới bên trái của nó là điểm (0, 2). Điểm A nằm trong góc NE của vùng này. Hình 2.12a chỉ ra kết quả cây tứ phân MX sau khi chèn điểm A. Hình 2.13a chỉ ra việc phân chia vùng. Chú ý rằng điểm A được chèn vào mức 2 của cây và mức này bằng giá trị k. Tổng quát là điểm luôn được chèn vào mức k trong cây tứ phân MX.

2. Việc chèn điểm B với toạ độ (3, 3) sẽ xác định được B thuộc nhánh NE của gốc. Do vậy cành NE của nút gốc tương ứng vùng 2x2 với góc dưới bên trái là (2, 2). Điểm B lại nằm trong góc NE của vùng này. Kết quả được thể hiện trên hình 2.12b và 2.13b.

3.

Việc chèn điểm C với tọa độ (3, 1) được tiến hành như sau: C nằm trong góc SE của toàn vùng. Điều này đòi hỏi tạo nút mới là nút con SE của gốc. C nằm trong vùng con NE của nút này. Hình 2.12c và 2.13c chỉ ra kết quả.

4. Cuối cùng, hình 2.12d và 2.13d biểu diễn kết quả sau khi chèn D.

2.4.2 Thao tác xoá trong MX-Quadtrees

Thao tác xoá trong một *MX-Quadtrees* là một thao tác tương đối đơn giản bởi vì toàn bộ các điểm đều nằm ở cấp cuối (đều là các nút lá). Lưu ý rằng nếu N là một nút không phải lá trong cây *MX-Quadtrees* với gốc là T thì khi đó vùng biểu diễn bởi nút N có ít nhất một điểm thuộc cây. Nếu chúng ta muốn xoá một điểm (x, y) từ cây T, việc đầu tiên là thiết lập liên kết tương ứng của cha nút N tới NIL. Nói cách khác nếu M là cha của N và M.DIR trỏ tới N thì thiết lập M.DIR=NIL và cho lại N để giải phóng vùng nhớ. Bây giờ tiến hành kiểm tra xem bốn trường liên kết của M đều là NIL? nếu đúng ta khảo sát cha của M (ta gọi nó là P). Vì M là con của P, ta tìm trường liên kết DIR1 sao cho P.DIR1=M. Sau đó thiết lập P.DIR1=NIL và tiếp tục kiểm tra xem toàn bộ các trường liên kết của P có là NIL? Nếu đúng, tiếp tục tiến trình. Toàn bộ tiến trình đòi hỏi phải duyệt qua cây một lần từ đỉnh xuống đáy (để tìm nút sẽ xóa) và một lần đi ngược cây. Như vậy toàn bộ tiến trình sẽ là O(k) lần.

Hãy xem xét tiến trình làm việc ra sao với cây MX trên hình 2.12d. Giả sử ta muốn xoá D. Việc xóa nút D không khó khăn vì ta tìm ra nó và đặt NIL vào trường liên kết SE của cha nó (cái trỏ đến D). Để xác định xem cha của D có hỏng? ta kiểm tra xem bốn trường liên kết nó là NIL? Không đúng vậy vì C và D có cùng cha.

Mặt khác, xem xét việc huỷ bỏ A từ cây tứ phân MX trong hình 2.12d. Khi đặt NIL vào trường NE của cha nút A, ta thấy rằng cha của A kết thúc bởi 4 trường rỗng. Như vậy cha của A bị hỏng. Khi điều đó xảy ra, ta khảo sát cha của cha A (là gốc) và đặt NIL vào liên kết NW của gốc. Khi kiểm tra xem gốc có toàn bộ bốn trường liên kết là NIL? Điều đó không xảy ra và không thể *collapsing*. Kết thúc.

2.4.3 Truy vấn khoảng trong MX-Quadtrees

Các truy vấn khoảng trong *MX-Quadtrees* được thực hiện một cách hoàn toàn tương tự như cây tứ phân điểm. Chỉ có hai điểm khác biệt đó là : Nội dung của các trường XLB, XUB, YLB và YUB là khác nhau. Điểm khác biệt thứ hai là trong cây *MX-Quadtrees* tất cả các điểm nằm ở các nút lá, do vậy đường tròn định nghĩa bởi truy vấn khoảng cần được thực hiện chỉ ở cấp độ lá.

2.4.4 PR-Quadtrees

PR-Quadtrees là một sự biến thể của *MX-Quadtrees*. Trong *MX-Quadtrees* tất cả các điểm được lưu tại các nút lá. Vì thế khi xem xét một *MX-Quadtrees* biểu diễn vùng 2^k x 2^k, việc tìm kiếm và chèn là quy trình O(k).

Nhớ lại rằng mỗi nút N trong cây MX biểu diễn một vùng, Reg(N). Bằng cách mở rộng cấu trúc dữ liệu để bao gồm điểm trong nó, ta có thể điều chỉnh luật chia vùng cho cây tứ phân MX bằng cách đòi hỏi nút N bị chia nếu Reg(N) chứa hai hay nhiều điểm. Nếu N chứa 1 điểm thì nó được lưu trong nút N thay cho nút lá. Điều này tránh được việc mở rộng nút N và làm giảm thời gian chèn và tìm kiếm.

2.5 Cây R (R-Trees)

Trong phần này chúng ta sẽ giới thiệu một kiểu cấu trúc dữ liệu mới gọi là *R-Trees*, cấu trúc này có thể được sử dụng để lưu trữ các vùng chữ nhật của một hình ảnh hay bản đồ. *R-Trees* đặc biệt hữu ích trong việc lưu trữ dữ liệu số lượng lớn trên đĩa. Do việc truy cập đĩa thường rất chậm, *R-Trees* cung cấp một cách thuận tiện trong việc cực tiểu hoá số lần truy cập đĩa.

Mỗi *R-Trees* kết hợp với một thứ tự là một số nguyên K. Mỗi nút *R-Trees* không phải là lá bao gồm một tập từ K/2 đến K hình chữ nhật. Bằng trực quan thấy rằng mỗi nút không lá trong *R-Trees* trừ nút gốc ít nhất phải là một nửa. Đặc điểm này làm cho *R-Trees* thích hợp với việc truy vấn đĩa bởi vì mỗi truy cập đĩa mang lại một trang chứa đựng một vài hình chữ nhật (ít nhất K/2). Hơn nữa, do việc lưu trữ một số hình chữ nhật trong một trang, chiều cao của *R-Trees* sử dụng để lưu trữ tập hợp các hình chữ nhật, thường rất nhỏ. Do vậy số lần truy cập đĩa giảm bớt so với các cây mô tả trên.

Một hình chữ nhật hoặc là "thực" hoặc là một hình bao hàm một nhóm hình chữ nhật. Các nút lá bao gồm một hình chữ nhật "thực" trong khi các nút không lá bao

gồm các hình chữ nhật nhóm từ một tập các hình chữ nhật. Hình 2.14 chỉ ra cách nhóm các hình chữ nhật như sau.

Nhóm	Các chữ nhật
G1	R1, R2, R3
G2	R4, R5, R6, R7
G3	R8, R9

Error!

Hình 2.14 chỉ ra cây R bậc 4 liên kết với các chữ nhật trên hình 2.14. Cấu trúc của một *R-Trees* được định nghĩa như sau:

rtnodetype = record

$Rect_1$, ..., $Rect_k$: Rectangle;

P_1, ..., P_k : rtnodetype;

end

Ta không đi chi tiết kiểu dữ liệu *Rectangle* trên đây. Có nhiều cách biểu diễn chữ nhật.

2.5.1 Chèn và tìm kiếm trong R-Trees

Khi chèn một hình chữ nhật mới vào một *R-Trees* ta làm theo những bước dưới đây:

1. Chúng ta xem xét trong số các hình chữ nhật liên quan với nút gốc hình nào cần được mở rộng ít nhất (về mặt diện tích) để chứa hình chữ nhật được chèn. Ví dụ nếu chúng ta chèn hình chữ nhật R_{10} (hình 2.16) vào cây R trên hình 2.15 thì cách dễ nhất là mở rộng nhóm G1 bởi vì việc mở rộng các nhóm khác

thì diện tích bị bao phủ bởi nhóm này sẽ tăng đáng kể.

2. Do đó từ những liên kết của G1 (từ gốc, hình 2.15) chúng ta sẽ chèn R10 vào khe có sẵn.

3.

Bây giờ chúng ta xem xét việc chèn R11. Nhóm mà diện tích của nó phải được mở rộng tối thiểu trong trường hợp này là G2. Tuy nhiên, con G2 của gốc đã đầy. Do vậy có một vài lựa chọn khác như trên hình 2.17.

4. Từ 2 lựa chọn trên hình 2.17, ta muốn có giải pháp trong hình 2.17b vì diện tích tổng thể của các chữ nhật nhóm là nhỏ nhất.

5. Hình 2.18 chỉ ra cách làm không đúng khi chèn chữ nhật R11. Tiếp cận này không khả thi vì nút biểu diễn nhóm chứa chữ nhật R11 có thể là chỉ chứa duy **Error!**

nhất một chữ nhật.

2.5.2 Xoá trong cây R-Trees

Việc xóa các đối tượng từ cây *R-Trees* có thể gây ra một nút trong cây *R-Tree* trở nên thiếu hụt (*underflow*). Nhắc lại rằng một *R-Tree* bậc k phải bao gồm ít nhất K/2 hình chữ nhật trong nó. Khi chúng ta xoá một hình chữ nhật từ một *R-Tree*, chúng ta phải đảm bảo rằng nút đó không bị thiếu hụt. Ví dụ, xem xét *R-Trees* như hình 2.15 trình bày trên. Giả thiết chúng ta muốn xoá chữ nhật R9. Nút chứa R9 chỉ còn lại một nút trong nó nếu thực hiện xoá R9, kết quả là nút này sẽ phản ánh một điều kiện hụt. Trong trường hợp này chúng ta phải tạo ra nhóm logic mới. Một khả năng là sắp xếp lại các nhóm như sau:

Group	Rectangles
G_1	R_1, R_2, R_3
G_2	R_4, R_6, R_7
G_3	R_5, R_8

Cây R mới là kết quả của việc xóa nút R9, nó được thể hiện trên hình 2.19.

Error!

2.6 So sánh các cấu trúc dữ liệu

Trong chương này ta đã khảo sát 4 loại cấu trúc dữ liệu: cây k-d, cây tứ phân điểm, cây tứ phân MX và cây R. Mỗi chúng đều có ưu điểm và nhược điểm nhất định.

· Cây tứ phân điểm rất dễ cài đặt. Tuy nhiên, cây tứ phân điểm có k nút thì có thể có độ cao là k, như vậy làm tăng độ phức tạp cho chèn và tìm kiếm (nó có thể là O(k)). Hơn nữa mỗi so sánh đòi hỏi so sánh hai tọa độ.Việc xóa nút trong cây loại này là khá khó khăn. vì việc tìm kiếm nút ứng viên thay thế cho nút đang xóa thông thường là không đơn giản. Cuối cùng truy vấn khoảng trong cây này cần O(2Ön), n là tổng số bản ghi trong cây.

· Cây k-d rất dễ cài đặt. Tuy nhiên, cây k-d chứa k nút có thể có độ cao k, do vậy chèn và tìm kiếm có thể phức tạp. Trong thực tế đường dẫn từ gốc tới lá của cây loại này dài hơn trong cây tứ phân điểm bởi vì cây này là cây nhị phân. Độ phức tạp tồi nhất của tìm kiếm dải trong cây k-d là: **Error!**

. Khi k=2, thì độ phức tạp còn **Error!**

như cây tứ phân điểm.

· Cây tứ phân MX đảm bảo có độ cao nhất là O(n), trong đó vùng được biểu diễn có ($2^n x 2^n$) tế bào. Nói cách khác việc chèn, xóa và tìm kiếm trong cây loại này cần thời gian là O(n). Tìm kiếm dải của cây này rất hiệu quả - $O(N+2^h)$, trong đó N là tổng số điểm kết quả truy vấn và h là độ cao của cây.

· Tương tự với cây R. Tuy nhiên, cây R có thể có nhiều chữ nhật lưu trong cùng nút, nó phù hợp với xâm nhập đĩa từ bằng giảm độ cao của cây.

· Một bất lợi của cây R là các chữ nhật bao kết hợp với các nút khác nhau có thể phủ lên nhau. Như vậy, việc tìm kiếm trong cây R thay vì đi theo một vết như các cây khác, là phải đi theo nhiều vết trong cây. Trường hợp này lại làm tăng số lần thâm nhập đĩa.

· Tổng thể, cây R hiệu quả hơn cây k-d và cây tứ phân điểm trong các ứng dụng đa phương tiện bởi vì ứng dụng loại này đòi hỏi dung lượng đĩa rất lớn phải xâm nhập. Tuy nhiên nếu chỉ số nhỏ thì sử dụng cây tứ phân MX sẽ hiệu quả hơn.

Chương 3

CƠ SỞ DỮ LIỆU ẢNH

Chương này sẽ trình bày CSDL ảnh là gì? Sự khác nhau về truy vấn giữa CSDL ảnh với CSDL văn bản.

Các định nghĩa trừu tượng về nội dung ảnh được đề xuất. Mô tả nội dung ảnh có thể thực hiện bằng tay hay tự động. Cả hai trường hợp đều cần cấu trúc dữ liệu để lưu trữ. Một vài kỹ thuật xử lý ảnh được khảo sát.

Ba kỹ thuật tổng quát để hiện thực CSDL ảnh sẽ được trình bày. Chúng bao gồm, thứ nhất, CSDL ảnh được cài đặt bằng cách mở rộng mô hình quan hệ theo phương pháp đối tượng-quan hệ. Thứ hai, cài đặt bằng các cấu trúc dữ liệu n chiều như mô tả trong chương trước. Cuối cùng là cài đặt bằng phương pháp biến đổi ảnh.

Vài chục năm gần đây nhiều cơ quan tham gia thu thập dữ liệu ảnh. NASA thu thập lượng lớn ảnh trái đất. US và nhiều nước khác lưu trữ ảnh hộ chiếu. Các bệnh viện có vô số ảnh chụp X quang và ảnh cắt lớp.

Trong mô hình dữ liệu quan hệ truy vấn thường thực hiện với văn bản. Trong CSDL ảnh, với yêu cầu tìm ảnh của ai đó thì câu truy vấn là "*Cho trước ảnh mẫu, hãy tìm kiếm mọi ảnh trong CSDL gần giống ảnh mẫu và cho biết các thuộc tính của ảnh cho lại*". Hai đặc tính quan trọng của truy vấn này là: câu truy vấn có ảnh kèm theo. Thứ hai, truy vấn hỏi ảnh "tương tự". ,Trong trường hợp này phải xác định thế nào là tương tự.

3.1 Ảnh thô

Phát biểu phi hình thức thì nội dung ảnh bao gồm các đối tượng trong ảnh mà ta cho nó là quan trọng từ góc nhìn của ứng dụng. Các đối tượng trong ảnh phải có các đặc tính kết hợp như sau:

1. Mô tả hình dạng: Mô tả hình dạng/vị trí của vùng trong đó có đối tượng.

2. Mô tả đặc tính: Mô tả đặc tính của từng điểm ảnh (hay nhóm điểm ảnh) trong ảnh. Thí dụ giá trị RGB của điểm ảnh, mức xám trong ảnh đen trắng... Tổng quát thì không thể kết hợp các đặc tính với từng pixel mà phải xử lý từng tế bào (*cell*) – là nhóm các pixel vào cùng thời điểm.

Thí dụ, hãy xem xét tập ảnh pic1.gif trên hình 3.1. Hình trên có hai đối tượng quan tâm tương ứng với hai mặt người, gọi chúng là đối tượng o_1 và o_2. Hình chữ nhật bao quanh mặt người xác định mô tả hình dạng của mặt người. Tuy nhiên mô tả hình dạng không nhất thiết phải là chữ nhật, chúng có thể là đa giác hay tập các chữ nhật.

Mô tả đặc tính kết hợp với mặt người thông thường bao gồm tập các cặp theo khuôn dạng (*PropName, PropValue*). Đặc tính bao gồm hai thành phần: tên đặc tính (thí dụ: R, G, B) và miền đặc tính xác định miền giá trị gán cho đặc tính (thí dụ: {0,...,8}).

Thí dụ với tệp ảnh *pic1.gif* trên đây, đối tượng o_1 tương ứng với mặt người bên trái, có các đặc tính sau:

1. Mô tả hình dạng: chữ nhật: XLB=10, XUB=60, YLB=5, YUB=50.

2. Mô tả đặc tính: Thí dụ, điểm ảnh tại (14, 17) có R=5, G=1 và B=3.

Tương tự với đối tượng 0_2, chúng có thể có các thuộc tính sau:

1. Mô tả hình dạng: chữ nhật: XLB=80, XUB=120, YLB=20, YUB=55.

2. Mô tả đặc tính: Thí dụ, điểm ảnh tại (90, 30) có R=2, G=7 và B=4.

Chú ý rằng, tổng quát thì thay vì xác định đặc tính cho từng pixel của ảnh, ta có thể chia vùng ảnh kích thước (a x b) pixels thành (m x n) tế bào, trong đó, a mod m=0, b mode n=0, m<a và n<b. Có nghĩa rằng, mỗi tế bào này sẽ biểu diễn vùng chữ nhật có độ lớn (a div m)x(b div n) pixel. Tế bào có hình chữ nhật.

Các định nghĩa hình thức được phát biểu như sau:

Định nghĩa 3.1: Mỗi ảnh I có cặp số nguyên dương (m, n) kết hợp và được gọi là độ phân giải lưới của ảnh. Nó chia ảnh ra (m x n) tế bào có kích thước bằng nhau, được gọi là lưới ảnh.

Mỗi tế bào của ảnh I bao gồm tập các điểm ảnh.

Định nghĩa 3.2: Thuộc tính tế bào là bộ ba (*Name, Values, Method*), trong đó *Name* là xâu ký tự chỉ tên đặc tính, *Values* là tập giá trị có thể gán cho đặc tính, *Method* là giải thuật cho ta biết cách tính toán các đặc tính.

Thí dụ với ảnh đen trắng. Đặc tính của tế bào có thể là:

(bwcolor, {b, w}, bwalgo)

trong đó, tên đặc tính là *bwcolor* và các giá trị có thể là *b* và *w*. *bwalgo* có thể là giải thuật có đầu vào là tế bào và cho lại *b* hay *w*. Đôi khi tổ hợp *b/w* của các pixel trong tế bào.

Mặt khác, với ảnh đa mức xám (0=w và 1=b), ta có đặc tính sau:

(graylevel, [0, 1], grayalgo)

trong đó, tên đặc tính là *graylevel*, giá trị của nó là số thực trong khoảng [0, 1] và phương thức *grayalgo* có đầu vào là tế bào để tính mức xám. Như đã nghiên cứu về cây R, tế bào được đặc trưng bởi các cạnh bao (xác định bởi 4 số nguyên) là XLB, XUB, YLB và YUB.Thí dụ, nếu tế bào mô tả tập các pixel

Error!

{(i, j) | XLB £ i £ XUB & YLB £ j £ YUB}

sau đó một phương thức tính giá trị trung bình có thể là:

trong đó, *findgray(i, j)* cho lại mức xám của điểm ảnh (i, j).

Thí dụ với ảnh màu, ta có ba đặc tính sau:

(red, {0, ..., 7}), (green, {0, ..., 7}), (blue, {0, ..., 7})

Như vậy, nếu tế bào có các đặc tính:

red=3; green=7; blue=1

thì nó chỉ ra một tổ hợp cụ thể của các thuộc tính RGB kết hợp với nút đó.

Tổng quát thì, người xây dựng CSDL ảnh phải quyết định các đặc tính tế bào nào được quan tâm sau đó khớp các đặc tính lại để thoả mãn yêu cầu và tạo ra các phương thức kết hợp để xác định các đặc tính này.

Định nghĩa 3.3 Một hình dạng (*shape*) đối tượng là tập P bất kỳ của các điểm, mà nếu p, q Î P, sau đó tồn tại trật tự các điểm p_1, ..., p_n trong P thoả mãn

1. $p=p_1$ và $q=p_n$ và

2. Với mọi 1 £ i < n, p_{i+1} là láng giềng của p_i; nếu $p_i = (x_i , y_i)$ và $p_{i+1} = (x_{i+1},y_{i+1})$ thì (x_{i+1},y_{i+1}) thoả mãn 1 trong các điều kiện sau đây:

$(x_{i+1},y_{i+1}) = (x_i+1,y_i)$ $(x_{i+1},y_{i+1}) = (x_i-1,y_i)$

$(x_{i+1},y_{i+1}) = (x_i,y_i+1)$ $(x_{i+1},y_{i+1}) = (x_i,y_i-1)$

$(x_{i+1},y_{i+1}) = (x_i+1,y_i+1)$ $(x_{i+1},y_{i+1}) = (x_i+1,y_i-1)$

$(x_{i+1},y_{i+1}) = (x_i-1,y_i+1)$ $(x_{i+1},y_{i+1}) = (x_i-1,y_i-1)$

Cái mà định nghĩa trên đây đề cập đến là với hai điểm bất kỳ của tập các điểm ảnh đang xem xét trong hình dạng, tồn tại một đường đi giữa chúng và nó nằm hoàn toàn trong hình dạng.

Định nghĩa 3.4 Chữ nhật là hình dạng đối tượng, P, mà tồn tại các số nguyên XLB, XUB, YLB, YUB thoả mãn

$$P=\{(x, y) \mid XLB \pounds x < XUB \ \& \ YLB \pounds y < YUB\}$$

Định nghĩa 3.5 CSDL ảnh (*IDB-Image Database*) bao gồm bộ ba (GI, Prop, Rec) trong đó:

1. *GI* là tập các ảnh lưới có dạng (Image, m, n),

2. *Prop* là tập các đặc tính tế bào, và

3. *Rec* là ánh xạ để kết hợp tập các chữ nhật mô tả đối tượng trong mỗi ảnh.

Chú ý rằng nếu biểu diễn dữ liệu ảnh theo hình thức trên đây thì phải quan tâm đến hai nhân tố quan trọng:

· Ảnh thường là đối tượng rất lớn bao gồm trường $(p_1 \times p_2)$ pixel. Việc lưu trữ các đặc tính trên cơ sở pixel là không hiện thực. Do vậy phải sử dụng các giải thuật nén ảnh.

· Cho trước ảnh I (nén hay để thô), điều quan trọng là phải xác định đặc trưng nào xuất hiện trong ảnh. Việc này thường được thực hiện bằng cách chia ảnh thành tập các vùng chữ nhật đồng nhất, mỗi chúng được gọi là đoạn (*segment*). Tiến trình tìm kiếm các đoạn này gọi là phân đoạn ảnh (*segmentation*).

Một khi dữ liệu ảnh được phân đoạn, ta cần có thao tác khớp ảnh (*match*) để ánh xạ toàn bộ hay một phần ảnh này với toàn bộ hay một phần ảnh khác.

3.2 Biểu diễn ảnh nén

Error!

Hãy xem xét ảnh hai chiều I có (p_1 x p_2) pixel. I(x, y) mô tả một hay nhiều thuộc tính của pixel. Thí dụ, I(x, y) có thể có giá trị trong khoảng [0, 255] để biểu diễn mã hóa giá trị RGB của ảnh.

Tổng quát thì lập luận về ảnh bằng xem xét mọi pixel là không thực tế bởi vì mỗi p_1 và p_2 có thể có tới 1024 hay nhiều hơn. Dẫn tới có đến hàng triệu phần tử trong ma trận ảnh I. Quan điểm chung là biến đổi ma trận I thành biểu diễn nén của ma trận như hình 3.2.

Việc tạo lập biểu diễn nén (*Compressed Representation*) cr(I) của ảnh I bao gồm hai phần:

1. *Chọn kích thước*. Người thiết kế CSDL ảnh chọn kích thước h cho ảnh nén. Kích thước ảnh càng lớn thì càng có ảnh gần gũi với ảnh gốc. Tuy nhiên khi kích thước tăng thì việc làm chỉ số cho biểu diễn ảnh càng phức tạp. Do vậy phải cân bằng các yếu tố. Giả sử rằng kích thước lựa chọn cho cr(I) là cặp số nguyên dương (h_1, h_2).

2. *Lựa chọn phép biến đổi*. Người sử dụng phải lựa chọn phép biến đổi để có khả năng chuyển đổi ảnh thành dạng nén. Nói cách khác, họ phải chọn phép biến đổi sao chovới ảnh I cho trước và bất kỳ cặp số 1£i£h_1 và 1£j£h_1, thì sẽ xác định được giá trị cr(i, j) nào đó.

3.2.1 Biến đổi Fourier rời rạc (DFT - Discrete Fourier Transform)

Error!

Đây là biến đổi rất nổi tiếng, được nghiên cứu khá nhiều. Theo biến đổi Fourier rời rạc ta có:

trong đó, j là số phức **Error!**

.

DFT có rất nhiều đặc tính hay. Thí dụ, có thể khôi phục ảnh gốc I từ biểu diễn DFT. Cho trước ảnh I với (p_1 x p_2) và biểu diễn DFT(I), ta có thể áp dụng đảo DFT (ký hiệu là DFT^{-1}) lấy bất kỳ điểm ảnh (x, y) nào trong I làm đầu vào và sử dụng giá trị của DFT(x, y) để tính các giá trị của ảnh gốc. Đặc tính này của DFT có thể ứng dụng vào nén và giải nén ảnh. Nhưng chú ý rằng, không phải tất cả các lược đồ nén đều được 100% biến đổi ngược, như vậy một số dữ liệu bị mất mát.

3.2.2 Biến đổi cosin rời rạc (DCT – Discrete Cosine Transform)

Error!

Đây là giải thuật nổi tiếng, là nền tảng của nén ảnh JPEG. Tương tự DFT, DCT có thể lấy đảo và cho bởi

Error!

trong đó,

Việc tính toán DCT được thực hiện khá nhanh.

Cả DFT và DCT thường được cải tiến nhằm tính toán nhanh hay nâng cao chất lượng nén. Nhóm kỹ thuật nén ảnh khác hay được sử dụng là dựa trên biến đổi *wavelet.*

Error!

Giả sử IDB là tập hợp các ảnh và các vùng quan tâm được đánh dấu bởi các chữ nhật như trên hình 3.3. Giả sử r_1,..., r_n là các vùng quan tâm. Sau đó tập {cr(r_1),...,cr(r_n)} được biểu diễn dễ dàng bởi các kỹ thuật chỉ số hóa đa chiều (thí dụ cây R).

3.3 Xử lý ảnh: Phân đoạn

Cho đến bây giờ ta đã giả sử rằng các vùng trong ảnh nơi chứa các đặc trưng quan tâm, có thể nhận ra bằng cách nào đó, và nội dung của các vùng quan tâm được xác định bằng cách nào đó. Phần này khảo sát nhanh cách phân chia ảnh cho trước thành các vùng đồng nhất, gọi chúng là đoạn (segment).

Giả sử ảnh I chứa (m x n) tế bào. Trường hợp tồi nhất là tế bào tương ứng pixel, nhưng tổng quát thì tế bào là tập chữ nhật các pixel.

Vùng liên thông Â trong ảnh I là tập các tế bào mà nếu các tế bào (x_1, y_1), ... (x_n, y_n)ÎÂ, tồn tại trật tự các tế bào $C_1,...,C_n$ trong Â thoả mãn

1. $C_1=(x_1,y_1)$ và

2. $C_n=(x_n,y_n)$ và

3. khoảng cách Euclidean giữa C_i và C_{i+1} với mọi 1£ i<n là 1.

Hình 3.4 chỉ ra ba vùng R1, R2, R3, mỗi chúng là vùng liên thông. Hơn nữa, ta có:

1. $(R_1ÈR_2)$ là vùng liên thông.

2. $(R_2ÈR_3)$ là vùng liên thông.

3. $(R_1ÈR_2ÈR_3)$ là vùng liên thông.

4. Nhưng $(R_1ÈR_3)$ không phải là vùng liên thông. Khoảng cách Đề các giữa tế bào (2,3) của R_1 và (3,4) của R_3 là **Error!**

Thuộc tính đồng nhất kết hợp với ảnh I là hàm H lấy vùng liên thông bất kỳ Â trong ảnh I làm đầu vào và cho lại "true" hay "false". Dưới đây là các thí dụ về tính chất đồng nhất:

1. Giả sử d là số thực trong khoảng từ 0 đến 1 và ảnh khảo sát là ảnh đen-trắng. Có thể định nghĩa tính chất đồng nhất**Error!**

như sau: **Error!**

cho lại "true" nếu trên (100*d)% của tế bào trong vùng R có cùng màu. Giả sử ta mô tả ba vùng như biểu diễn trong bảng dưới đây:

Vùng	Tổng số pixel đen	Tổng số pixel trắng
Error!		
R_1	800	200
R_2	900	100
R_3	100	900
Error!		

Giả sử ta xem xét một vài tính chất khác như **Error!**

, Error!

và **Error!**

. Bảng sau đây chỉ ra cho chúng ta thấy kết quả các thuộc tính đồng nhất cho lại:

Vùng	**Error!**	**Error!**	**Error!**
Error!			
R_1	true	false	false
R_2	true	true	false
Error!			
R_3	true	true	false

2.

Error!

Giả sử ảnh xem xét với các pixel có giá trị thực giữa từ 0 đến 1. Giá trị này ta gọi là mức đen trắng (b-w level). Giá trị 0 mô tả trắng, 1 mô tả đen và độ xám được biểu diễn bởi giá trị nào đó xác định trong khoảng 0 và 1. Hãy khảo sát tính đồng nhất khác chút ít so với trên đây. Ta có hàm f thực hiện gắn các số từ 0 đến 1 vào từng pixel. Hơn nữa, ta còn có hệ số nhiễu (*noise factor*) 0£h£1, và mức ngưỡng d như trường hợp trên đây. **Error!**

là *true* nếu

Nói cách khác, tính chất đồng nhất sử dụng hàm cơ sở f và mức nhiễu cực đại cho phép h. Việc xem xét mức bw của tế bào (x, y) là tương đương với kết quả của hàm f nếu

|bw-level(x, y) –f(x, y)|<h

Nghĩa là nếu cả hai khác nhau không quá giá trị h.

Sau đó kiểm tra xem có đủ nhiều tế bào (xác định bởi hệ số d) trong vùng phù hợp với kết quả của hàm f. Nếu có, hãy coi vùng R là đồng nhất và nó cho lại giá trị "true". Mặt khác nó cho lại giá trị "false".

3. Trước hết phân lớp mọi mức bw-level. Thí dụ, có thể phân lớp mọi bw-level giữa 0 và 0.1 là 1, mọi bw-level giữa 0.1 và 0.2 là 2, ... cho đến mức bw-level giữa 0.9 và 1 là mức 10. Tương tự như trên đây, nếu d nằm giữa 0 và 1 thì $H^{class}(R)$ cho lại "true" nếu trên (100*d)% của tế bào trong vừng R rơi vào cùng lớp.

4. Tính chất đồng nhất khác nữa được ký hiệu là H^{dyn}, đó là phiên bản động của hàm H^{class}. H^{class} đặt mức ưu tiên cho các lớp chứ không phải đặt động. Ngược lại, ta có thể nói rằng R là đồng nhất, tuỳ theo giá trị **Error!**

, nếu trên (100*d)% của tế bào trong vùng R nằm trong dải h của số thực r nào đó.

Cuối cùng, chú ý rằng dự báo đồng nhất không phải chỉ trên cơ sở các mức b/w hay các mức xám. Nó dự báo tuỳ ý, khi cho trước vùng R, giá trị "true" hay "false" cho lại dựa trên một vài tính toán. Nó có thể quan tâm đến các hệ số như độ sâu, cường độ, kết cấu, lược đồ màu...

Cho trước ảnh I với tập pixel (m x n), hãy xác định đoạn của I với dự báo đồng nhất P là các tập $R_1,...,R_k$ thoả mãn:

1. $R_i \cap R_j=0$ với mọi $1 \le i \ne j \le k$,

2. $I= R_i \cup ... \cup R_k$,

3. $H(R_i)$=true với mọi $1 \le i \le k$, và

4. Với mọi i, j khác nhau, $1 \le i, j \le n$, và $R_i \cup R_j$ là vùng liên thông thì $H(R_i \cup R_j)$=false.

Thí dụ, hãy xem xét vùng (4x4) chứa *b-w levels* chỉ ra trên bảng sau:

Error! Cột Hàng	**1**	**2**	**3**	**4**
1	0.1	0.25	0.5	0.5
2	0.05	0.30	0.6	0.6
3	0.35	0.30	0.55	0.8
4	0.6	0.63	0.85	0.90

Hãy xem xét hàm dự báo đồng nhất **Error!**

. Hàm dự báo đồng nhất này cho biết vùng R được xem như đồng nhất nếu tồn tại r sao cho mỗi tế bào trong vùng có mức bw là v thoả mãn

|v-r| £ 0.03

Theo cách phân lớp này, dễ dàng thấy rằng ta có 5 vùng hình thành từ phân đoạn ảnh trên theo **Error!**

như trên hình 3.5.

R_1={(1,1), (1,2)}

R_2={(1,3), (2,1), (2,2),(2,3)}

R_3={(3,1),(3,2),(3,3),(4,2),(4,2)}

R_4={(3,4),(4,3),(4,4)}

R_5={(1,4),(2,4)}

Dưới đây là phương pháp đơn giản tìm kiếm phân đoạn ảnh theo dự báo đồng nhất H:

1. *Bẻ gẫy*: Bắt đầu bằng toàn bộ ảnh. Nếu là đồng nhất, thực hiện xong và ảnh chính là đoạn hợp lệ. Nếu không, chia ảnh thành 2 phần và thực hiện lặp cho đến

khi ta tìm ra $R_1,...,R_n$ các vùng đồng nhất và thoả mãn mọi điều kiện (trừ điều kiện 4) trong định nghĩa thuộc tính đồng nhất.

2. *Trộn*: Kiểm tra xem những R_i nào có thể trộn vào nhau. Kết thúc bước này ta có các đoạn hợp lệ $R'_1,...,R'_k$ của ảnh, trong đó k£n và mỗi R'_i là hợp nhất của một vài R_j.

Giải thuật cài đặt các bước trên có thể mô tả dễ dàng bằng ba hàm và hàm chính có tên *segment* như sau:

Giải thuật 3.1

```
function segment(I:image)
SOL=0;
check_split(I);
merg(SOL);
end function
function check_split(R)
if H(R)=”true” then addsol(R)
else
    {X=split(R);
    check_split(X.part1);
    check_split(X.part2);
    }
end function
procedure addsol(R)
SOL=SOLÈ{R}
```

end procedure

function merge(S)

while S¹Æ do {

Pick some Cand in S;

merged=false;

S=S-{Cand};

Enumerate S as C_1,...,C_k;

while i £ k do

{if adjacent(Cand, C_i) then

{Cand=Cand È C_i;

S=S-{C_i};

merged=true;

}

else {i=i+1;

if merged then S=SÈ{Cand};

merged=false;

}

}};

end function

3.4 Truy vấn trên cơ sở tương tự

Tại đây ta đã nghiên cứu kỹ thuật lấy ảnh làm đầu vào, cho lại phiên ảnh nén của ảnh đầu vào nhờ biến đổi ảnh DCT, DFT hay *wavelet*. Câu hỏi cần trả lời là: Cách

nào có thể xác định nội dung của phân đoạn (hay ảnh phân đoạn) tương tự với ảnh khác (hay tập ảnh khác) hay không?

Có nhiều trường hợp ứng dụng, khi có CSDL ảnh lớn, người sử dụng mong muốn truy vấn như "*Đây là ảnh của một người. Hãy cho biết đó là ai?*".

Có hai tiệm cận chính đến truy vấn ảnh trên cơ sở tương tự.

1. *Tiệm cận thước đo*: Trong tiệm cận này ta giả sử rằng có thước đo khoảng cách d để so sánh hai đối tượng ảnh. Hai đối tượng ảnh càng gần nhau thì chúng càng tương tự nhau. Vấn đề truy vấn trên cơ sở tương tự có thể được phát biểu như sau: Cho trước ảnh vào i, hãy tìm láng giềng gần nhất của i trong tập ảnh. Cho đến nay, tiệm cận thước đo được sử dụng nhiều nhất trong các CSDL ảnh.

2.

Error!

Tiệm cận biến đổi: Tiệm cận thước đo giả sử rằng quan niệm tương tự là "cố định"; có nghĩa rằng, trong bất kỳ ứng dụng nào, chỉ một quan niệm tương tự được sử dụng để làm chỉ mục dữ liệu (mặc dù nhiều ứng dụng sử dụng nhiều quan niệm tương tự khác nhau). Tương tự câu châm ngôn "Cái đẹp nằm trong mắt của người xem" thì cũng đúng với "Cái tương tự nằm trong mắt của người xem". Thí dụ với hai ảnh, người này cho rằng hai con vật giống nhau (hai con khỉ), nhưng chuyên gia động vật cho rằng hai ảnh khác nhau: con đười ươi (hình 3.6a) và con tinh tinh (hình 3.6b). Tương tự với xâu ký tự "*AI*" và "*intelligence*". Dưới con mắt người làm tin học thì chúng tương đương, nhưng với các chuyên gia sinh học thì AI lại là *Artificial Insemination* (thụ tinh nhân tạo)...

Do vậy, người sử dụng phải chỉ ra cái gì được coi là tương tự, thay cho việc để toàn bộ công việc cho hệ thống.

3.4.1 Tiệm cận thước đo

Giả sử ta xem xét tập đối tượng Obj với các đặc tính pixel $p_1,...,p_n$. Mỗi đối tượng o được xem như tập S(o) của bộ (n+2) (*n+2 tuple*)có khuôn dạng sau:

(xcoord, ycoord, $v_1,...,v_n$)

trong đó, v_i là giá trị của thuộc tính p_i kết hợp với tọa độ pixel (x, y). Rõ ràng, S(o) chứa (w x h) của bộ (n+2), trong đó w là độ rộng và h là độ cao của chữ nhật kết hợp với o.

Thông thường, một đối tượng là toàn bộ ảnh hay đoạn ảnh. Thí dụ, cho trước CSDL ảnh mặt người. Nó bao gồm ảnh của nhiều người chụp dưới các điều kiện khác nhau thì một đối tượng có thể bao gồm nhiều mặt người.

Trong tiệm cận thước đo, mức độ khác nhau được xác định bởi hàm khoảng cách d. Hàm d từ tập X đến khoảng cách đơn vị [0, 1] được gọi là hàm khoảng cách nếu thoả mãn các tiên đề sau đây. Với mọi x, y, z Î X ta có:

d(x, y)=d(y,x)

d(x,y)£d(x, z)+d(z,y)

d(x,x)=0

Gọi d_{Obj} là hàm khoảng cách trong không gian mọi đối tượng. Tuy nhiên, chương trước cho ta thấy đối tượng được xem như tập các điểm trong không gian k-chiều với k=n+2. Do vậy việc tính toán cho d_{Obj} là khá phức tạp.

Error!

Thí dụ, hãy xem xét tập Obj gồm các ảnh với kích thước (256x256), có ba thuộc tính (red, green, blue) được gán giá trị từ tập {0, ..., 7}. Ta định nghĩa hàm khoảng cách d_1 giữa hai ảnh như sau:

Rõ ràng tính toán trên là tiến trình khá nặng nề bởi vì tổng kép này dẫn tới 65536 phép tính. Ngay việc sử dụng cấu trúc dữ liệu cây R hay cây tứ phân nào đó cũng không cho kết quả khả quan.

Để giải quyết vấn đề này, nhiều nhà nghiên cứu đã gợi ý kỹ thuật quan trọng khác thay thế. Các kỹ thuật này hình thành dựa trên việc sử dụng hàm tách đặc trưng "tốt" có tên *fe* (*Feature Extraction Function*). Thí dụ các hàm này có thể là DFT và DCT. Dựa trên quan điểm này, hàm fe ánh xạ các đối tượng vào các điểm đơn trong không gian s-chiều, trong đó s thông thường hơi nhỏ so với (n+2). Do vậy có thể có hai rút gọn có thể đạt được:

1. Hãy nhớ lại rằng đối tượng o là tập các điểm trong không gian (n+2) chiều. Ngược lại, fe(o) là điểm đơn.

2. fe(o) là điểm trong không gian s chiều và s<<(n+2).

Hình 3.7 biểu diễn tiệm cận thước đo. Ý tưởng cơ bản là trước hết ánh xạ các đối tượng vào các điểm trong không gian s chiều, sau đó tổ chức mọi đối tượng nhờ cấu trúc dữ liệu không gian như cây R. Tuy nhiên, bằng trực giác thì ánh xạ có thể bảo toàn khoảng cách: Nếu o_1, o_2, o_3 là các đối tượng mà $d(o_1, o_2)£d(o_1, o_3)$ thì $d'(fe(o_1), fe(o_2))£d'(fe(o_1), fe(o_3))$, trong đó d là thước đo trong không gian gốc n+2 chiều và d' là thước đo trong không gian mới s chiều. Nói cách khác, ánh xạ tách đặc trưng có thể bảo toàn quan hệ khoảng cách trong không gian gốc.

Error!

Kết quả là, cho trước đối tượng truy vấn o, ta chuyển đổi o sang fe(o) và thử tìm ra điểm p trong không gian s-d sao cho d'(p,fe(o)) nhỏ nhất có thể. Thuật toán hình thức dưới đây sử dụng ký pháp d làm thước đo trong không gian (n+2)-d và d' là thước đo trong không gian s ít chiều hơn.

Thuật toán 3.2 IndexCreation

Input: Obj - tập các đối tượng.

1. T=NIL. (* T là cây tứ phân hay cây R rỗng cho dữ liệu s-chiều*)
2. if Obj=Æ then return T and Halt
3. else
    a. Compute fe(o).
    b. Insert fe(0) into T.
    c. Obj=Obj-{0}.
    d. Go to 2.

Tiến trình hình thức để tìm câu trả lời tốt nhất khi truy vấn đối tượng thể hiện bằng giải thuật sau:

Thuật toán 3.3 FindMostSimilarObject

Input: Cây T có kiểu đã mô tả trên đây, đối tượng o.

1. bestnode=NIL;
2. if T=NIL then return bestnode. Halt
3. else

    tìm láng giềng trong T gần fe(o) nhất nhờ kỹ thuật tìm kiếm láng giềng gần nhất. Nếu tồn tại nhiều láng giềng như vậy thì trả lại tất cả chúng.

Để tìm mọi đối tượng tương tự khi truy vấn đối tượng trong khoảng cho trước e, ta có thể sử dụng tiệm cận trên cơ sở truy vấn khoảng. Giả sử rằng o_1, o_2 trong Obj ta có

$d(o_1, o_2) £ d'(fe(o_1),fe(o_2))$

Giải thuật 3.4 FindSimilarObjects

Input: Cây T có kiểu như trên. Đối tượng o. Dung sai 0< e£ 1.

1. Thực hiện truy vấn khoảng trên cây T với tâm fe(o) và bán kính e.
2. Gọi $p_1,...,p_r$ là các điểm cho lại.
3. for i=1 to r do
    a. if $d(o, fe^{-1}(p_i)) £ e$ then print $fe^{-1}(p_i)$.

Giải thuật trên đây của *Faloutsos* chỉ làm việc khi thước đo khoảng cách trong không gian có kích thước nhỏ (thí dụ, không gian s) lớn hơn hoặc bằng thước đo khoảng cách d.

3.4.2 Tiệm cận biến đổi

Tiệm cận trên cơ sở biến đổi là tổng quát hơn tiệm cận thước đo. Cho trước hai đối tượng o_1, o_2, mức không tương tự giữa chúng tương ứng với giá (tối thiểu) của biến đổi đối tượng o_1 vào o_2, hoặc ngược lại.

Trong mô hình này tồn tại tập các toán tử biến đổi $to_1,...,to_r$. Trong trường hợp ảnh, các toán tử này có thể là dịch chuyển, quay và co dãn. Toán tử mở rộng cũng có thể được bao gồm việc sửa đổi một hình dạng bằng cách thêm hình dạng mới vào nó. Toán tử cắt có thể lựa chọn hình dạng từ đối tượng đang tồn tại. Người sử dụng có thể lựa chọn ra tập con của các toán tử để sử dụng. Hơn nữa họ có thể bổ sung toán tử mới nếu họ muốn. Mỗi toán tử có một hàm đánh giá (*cost*) kết hợp. Chi phí (cost) càng cao thì thao tác càng ít có cơ hội được sử dụng.Thí dụ ta có hàm tên là *paint* với bốn đối số: paint(color1, val1, color2, val2), giá của hàm này được xác định như sau:

$cost(paint(color1, val1, color2, val2))=diff(color1, color2)^3+(val1-val2)^2$

trong đó, diff(red, green)=3=diff(green, red), ...

Biến đổi đối tượng o thành đối tượng o’ là trật tự các thao tác biến đổi $to_1,...,to_r$ và trật tự các đối tượng $o_1,...,o_r$ sao cho

1. $to_1(o)=o$,

2. $to_i(o_{i-1})=o_i$, và

3. $to(o_r)=o'$.

Error!

Chi phí của trình tự biến đổi trên đây (*Transformation Sequence – TS)* được tính như sau:

Error!

Chú ý rằng có thể có 1, 2, nhiều hay không có trình tự biến đổi nào cho phép ta chuyển đổi đối tượng o thành đối tượng o’. Giả sử TSeq(o,o’) là tập các trình tự biến đổi để chuyển đổi từ o sang o’. Tính không đồng dạng (*dissimilarity*) giữa o và o’, ký hiệu là dis(o,o’), đối với tập toán tử biến đổi TR và tập hàm chi phí CF được xác định như sau:

Thí dụ ta xem xét hai đối tượng o, o’ trên hình 3.8. Hãy khảo sát một vài cách biến đổi từ đối tượng này sang đối tượng khác.

1. TS_1: Trình tự biến đổi này bao gồm thao tác co dãn (co phần tô vạch ngang 50%), tiếp theo thực hiện thao tác co dãn khác (dãn phần tô dọc 100%). Thao tác thứ ba là tô (*paint*) để tô hai pixel tô dọc sử dụng mẫu tô ô vuông. Hình 3.9 mô tả từng bước của cách làm này.

2. TS_2: Trình tự biến đổi theo cách này bao gồm thao tác co dãn (co phần tô ngang 50%). Sau đó áp dụng thao tác paint để tô vùng sọc đứng sử dụng mẫu tô ô

vuông. Cuối cùng áp dụng thao tác co dãn (dãn phần gạch ô vuông 100%). Hình 3.10 mô tả các bước này.

Nếu hàm giá (*cost function*) kết hợp với co dãn không đồng nhất là độc lập với màu và thao tác *paint* chỉ đơn thuần đếm tổng số pixel đang được tô, thì dễ dàng thấy rằng biến đổi TS_2 bao gồm các biến đổi với giá rẻ hơn (vì tô ít hơn TS_1 một pixel).

Mô hình biến đổi có độ mềm dẻo cao hơn mô hình thước đo theo hai lý do sau đây:

1. Người sử dụng có thể đưa ra quan điểm về tính *tương tự* bằng cách chỉ ra các toán tử biến đổi nào được sử dụng hay không được sử dụng.

2. Người sử dụng có thể kết hợp với mỗi thao tác biến đổi một hàm giá để đánh giá mỗi thao tác được áp dụng, phụ thuộc vào các đối số của tóan tử biến đổi. Điều này cho phép người sử dụng có thể có quan điểm cá nhân về *tương tự* theo nhu cầu của họ.

Mô hình trên cơ sở thước đo có hai lợi thế: Trước hết, bắt buộc người sử dụng chỉ sử dụng một thước đo tính *tương tự* (hay tính khác biệt), hệ thống có thể dễ dàng chỉ số hóa dữ liệu để tối ưu thao tác tìm kiếm đối tượng láng giềng gần nhất. Lợi thế thứ hai, việc tính toán để hiệu quả là tương đối dễ.

3.5 Các hình mẫu khác của CSDL ảnh

Phần này phải trả lời câu hỏi: Tập ảnh được lưu trữ như thế nào để hỗ trợ các thao tác truy vấn ảnh? Tổng quát thì có nhiều cách biểu diễn CSDL ảnh:

· *Biểu diễn IDB* (*Image Database*) *như các quan hệ*: Cách dễ làm nhất là biểu diễn IDB như tập các quan hệ.

· *Biểu diễn IDB bằng các cấu trúc dữ liệu không gian*: Ý tưởng cơ bản của kỹ thuật này khá đơn giản. Nếu mọi đối tượng được biểu diễn bằng chữ nhật (hay khái quát hóa chữ nhật thành không gian có số chiều cao hơn), thì ta có thể biểu diễn tập chữ nhật nhờ các cấu trúc dữ liệu không gian như cây R...

· *Biểu diễn IDB bằng biến đổi ảnh*: Ý tưởng cơ bản của phương pháp này xuất phát từ số lượng pixel trọng yếu trong ảnh (thí dụ,1024x1024) là rất lớn. Tuy nhiên, có thể tồn tại tính *tương tự* giữa các phần khác nhau của ảnh. Ta có thể biểu

diễn ảnh bằng nén nội dung cơ bản thành véctơ đơn có giá trị thực với độ dài k (người thiết kế lựa chọn k)? Thông thường, k nhỏ hơn 100 hay 200, thủ tục tính các giá trị véctơ được thực hiện thông qua biến đổi như DFT hat DCT.

Khi truy vấn ảnh, tính chất ảnh phụ thuộc vào các hệ số như điều kiện ánh sáng, vị trí máy chụp, vị trí vật thể... Thí dụ trong CSDL ảnh mặt người đang khảo sát, hai ảnh của cùng một người có thể khác nhau, nó phụ thuộc vào các hệ số thực tế như thời gian chụp, ánh sáng, máy ảnh...

Do vậy, CSDL ảnh phải có khả năng truy vấn dữ liệu trên cơ sở tính *tương tự* giữa ảnh truy vấn và ảnh chứa trong CSDL ảnh.

3.6 Biểu diễn IDB bằng các quan hệ

Bất kỳ một CSDL ảnh IDB=(GI, Prop, Rec) nào đều có thể biểu diễn bằng mô hình quan hệ như sau:

1. Hãy tạo lập quan hệ gọi là *images* với lược đồ

(Image, ObjId, XLB, XUB, YLB, YUB)

trong đó, *Image* là tên tệp ảnh; *ObjId* tên giả, tạo ra cho đối tượng chứa trong ảnh; và *XLB, XUB, YLB, YUB* mô tả chữ nhật. Nếu R là chữ nhật xác định bởi XLB, XUB, YLB, YUB và R nằm trong Rec(I), thì tồn tại bộ:

(I, newid, XLB, XUB, YLB, YUB)

trong quan hệ *images*. Hình 3.11 chỉ ra quan hệ *images* kết hợp với CSDL ảnh mặt người trong hình 3.1. (Chú ý rằng việc tạo ra quan hệ images được thực hiện bằng ứng dụng các phương pháp phân đoạn và các kỹ thuật khớp ảnh (*matching*) trong xử lý ảnh).

Image	ObjId	XLB	XUB	YLB	YUB
pic1.gif	o_1	10	60	5	50
pic1.gif	o_2	80	120	20	55
pic2.gif	o_3	20	65	20	75
pic3.gif	o_4	25	75	10	60
pic4.gif	o_5	20	60	30	80
pic5.gif	o_6	0	40	15	50
pic6.gif	o_7	20	75	15	80
pic6.gif	o_8	20	70	130	185
pic7.gif	o_9	15	70	15	75

Hình 3.11

2. Với mỗi đặc tính pÎProp, hãy tạo quan hệ R_p có lược đồ sau

(Image, XLB, XUB, YLB, YUB, Value)

trong đó, *Image* là tên tệp ảnh. Không như trường hợp trên, ở đây XLB, XUB, YLB và YUB chỉ ra tế bào chữ nhật trong ảnh, và Value chỉ ra giá trị của đặc tính p.

Tổng thể thì ảnh có ba loại đặc tính sau:

1. *Đặc tính mức pixel*: Đề cập đến các đặc tính như màu RGB của từng điểm ảnh.

2. *Đặc tính mức vùng/đối tượng*: Một số đối tượng trong ảnh có đặc tính riêng. Thí dụ, đối tượng o_1 của pic1.gif có đặc tính NAME và AGE, tương ứng với các giá trị "*Hatch, Jim*" và 31.

3. *Các đặc tính mức ảnh*: Các đặc tính này là của toàn bộ ảnh như ảnh được chụp khi nào và ở đâu, ai chụp, loại thiết bị chụp, ai được phép xâm nhập...

Tóm lại, cho trước đặc tính p bất kỳ, ta có thể biểu diễn nó như quan hệ Rp. Tuy nhiên, trong thực tế, việc biểu diễn mỗi giá trị pixel như bộ trong quan hệ là không thể. Thay vì đó, ta chỉ biểu diễn đơn thuần các đặc tính mức ảnh, đối tượng/vùng như các quan hệ và không biểu diễn các đặc tính mức pixel.

3.6.1 Truy vấn biểu diễn quan hệ trong IDB

Nếu dữ liệu ảnh được lưu trữ trong khuôn mẫu quan hệ, thì phải có khả năng sử dụng SQL để truy vấn trực tiếp các quan hệ này. Hãy xem xét thí dụ truy vấn đơn giản sau "*tìm các ảnh có Jim Hatch*" và khảo sát tại sao áp dụng thẳng SQL là không thích hợp. Truy vấn này có thể viết như sau đây:

```
SELECT      image

FROM        images I, name N

WHERE       I.objid=N.objid AND

            N.name="Jim Hatch"
```

Không may là truy vấn trên đây không thực hiện đầy đủ như mong muốn. Trong hầu hết các ứng dụng cỡ lớn, việc suy luận ra nội dung ảnh thường được thực hiện bởi các giải thuật xử lý ảnh như đã mô tả tóm tắt trong các phần trước. Cho đến bây giờ, ta chú ý rằng, các giải thuật xử lý ảnh thông thường chỉ đúng đắn một phần. Như vậy, nếu đặc tính NAME kết hợp với ảnh mà được xác định bởi chương

trình xử lý ảnh, thì ta còn phải giả sử rằng các quan hệ này chứa các thuộc tính xác suất.

Để khái quát, ta cho rằng mỗi đối tượng có giá trị kết hợp với mỗi đặc tính pÎProp. Như vậy, mỗi quan hệ R_p kết hợp với đặc tính mức đối tượng/vùng cũng như các đặc tính mức ảnh chỉ có hai thuộc tính: id của đối tượng (vùng) và giá trị cho đặc tính. Do vậy, khi trở lại thí dụ trong hình 3.1 thì quan hệ NAME sẽ có khuôn dạng sau:

ObjId	Name
o_1	Jim Hatch
o_2	John Lee
o_3	John Lee
o_4	Jim Hatch
o_5	Bill Bosco
o_6	Dave Dashell
o_7	Ken Yip
o_8	Bill Bosco
o_9	Ken Yip

Sự cần thiết của xác suất

Một chương trình xử lý ảnh mà đang cố gắng nhận dạng con người trong các ảnh theo dõi, có thể cho lại nhiều câu trả lời với xác suất khớp ảnh (*match*) khác nhau. Thí dụ, hai đối tượng ảnh được nhận dạng là "*Jim Hatch*" có thể có một vài thuộc tính xác suất kết hợp với khớp ảnh. Do vậy, quan hệ *name* cần phải được mở rộng để chứa thuộc tính xác suất này.

ObjId	Name	Prob
o_1	Jim Hatch	0.8
o_1	Dave Fox	0.2
o_2	John Lee	0.75
o_2	Ken Yip	0.15

o_3	John Lee	1
o_4	Jim Hatch	1
o_5	Bill Bosco	1
o_6	Dave Dashell	1
o_7	Ken Yip	0.7
o_7	John Lee	0.3
o_8	Bill Bosco	0.6
o_8	Dave Dashell	0.2
o_8	Jim Hatch	0.10
o_9	Ken Yip	1

Chú ý rằng quan hệ xác suất trên đây cho thấy rằng chúng ta đã gắn xác suất với các bộ (*tuples*). Có thể đọc các bộ trong quan hệ trên đây như sau. Với bộ thứ nhất:

Xác suất mà Jim Hatch là thuộc tính tên của o_1 là 0.8.

Với đối tượng o_2:

1. Xác suất mà John Lee là thuộc tính tên của o_2 là 0.75.

2. Xác suất mà Ken Yip là thuộc tính tên của o_2 là 0.15.

3. Trong trường hợp này thiếu 10% xác suất.

Hãy xem xét truy vấn phức tạp hơn, thí dụ dưới dạng "*Tìm ảnh chứa cả Jim Hatch và Ken Yip*". Trong trường hợp này, có hai ảnh là ứng viên kết quả: pic1.gif và pic6.gif. Tại sao lại cả hai là ứng viên?

1. Ảnh pic1.gif có hai đối tượng o_1 và o_2, có khoảng 80% xác suất o_1 là Jim Hatch và 15% xác suất o_2 là Ken Yip. Do vậy ảnh này có thể là ứng viên.

2. Ảnh pic6.gif có hai đối tượng o_7 và o_8, có khoảng 70% xác suất o_7 là *Ken Yip* và 10% xác suất o_8 là Jim Hatch. Do vậy ảnh này có thể là ứng viên.

Các câu hỏi đặt ra bây giờ là:

1. Tìm xác suất của pic1.gif chứa cả Jim Hatch và Ken Yip? Câu trả lời có phải là tích của hai xác suất, 0.8x0.15=0.12?

2. Tìm xác suất của pic6.gif chứa cả Jim Hatch và Ken Yip? Câu trả lời có phải là tích của hai xác suất, 0.7x0.1=0.07?

Giả sử rằng câu trả lời cho các câu hỏi trên đây là đúng. Nhưng vấn đề không phải đơn giản như vậy. Hãy khảo sát ảnh pic8.gif với hai đối tượng o_{10} và o_{11}, bảng trên đây được mở rộng bằng chèn thêm hai bộ được nhận biết từ giải thuật xử lý ảnh như sau:

ObjId	Name	Prob
o_{10}	Ken Yip	0.5
o_{10}	Jim Hatch	0.4
o_{11}	Jim Hatch	0.8
o_{11}	John Lee	0.1

Nếu chúng ta không biết về sự phụ thuộc của các kết quả khác nhau (như trường hợp trên đây) thì ta phải đối mặt với 4 khả năng sau:

· Khả năng 1: o_{10} là *Ken Yip* và o_{11} là *Jim Hatch.*

· Khả năng 2: o_{10} là *Ken Yip* và o_{11} không phải là *Jim Hatch.*

· Khả năng 3: o_{10} không phải là *Ken Yip* nhưng o_{11} là *Jim Hatch.*

· Khả năng 4: o_{10} không phải là *Ken Yip,* và o_{11} không phải là *Jim Hatch.*

Sử dụng dữ liệu xác suất trong bảng trên ta có thể ước lượng bốn khả năng liệt kê trên đây và tìm ra xác suất cho mỗi khả năng này. Vì các khả năng từ 1 đến 4 là không tương thích nhau, xác suất mà pic8.gif là câu trả lời truy vấn giống với tổng các xác suất của khả năng 1.

Gọi p_i là xác suất của khả năng i, $1 \le i \le 4$. Sau đó ta có thể phát biểu:

$p_1+p_2 = 0.5$

$p_3+p_4 = 0.5$

$p_1+p_3 = 0.8$

$p_2+p_4 = 0.2$

$p_1+p_2+p_3+p_4= 1$

Phương trình thứ nhất từ sự thật rằng o_{10} là *Ken Yip* theo khả năng 1 và 2, và từ bảng ta có xác suất của o_{10} (là *Ken Yip*) là 0.5.

Phương trình thứ 2 từ sự thật rằng o_{10} là ai đó không phải là *Ken Yip* theo các khả năng 3 và 4, và từ bảng ta biết rằng xác suất của o_{10} (không phải là *Ken Yip*) là 0.5.

Phương trình thứ 3 từ sự thật rằng o_{11} là *Jim Hatch* theo các khả năng 1 và 3, và từ bảng trên ta biết rằng xác suất của o_{11} (là *Jim Hatch*) là 0.8.

Cuối cùng, phương trình thứ 4 từ sự thật rằng o_{11} là ai đó không phải là *Jim Hatch* theo các khả năng 2 và 4, và từ bảng trên ta biết rằng xác suất của o_{11} (không phải là *Jim Hatch*) là 0.2.

Để xác định được xác suất mà pic8.gif chứa cả *Ken Yip* và *Jim Hatch*, chúng ta phải giải hệ phương trình tuyến tính trên để có p_1, chú ý rằng mọi kịch bản xảy ra đều bị ảnh hưởng bởi 4 khả năng. Kết quả thu được cho thấy xác suất của p_1 là không duy nhất. Nó có thể nhỏ hơn 0.3 hay lớn hơn 0.5 hay giá trị nào đó giữa chúng. Cụ thể, khi nhân đơn thuần xác suất 0.5 kết hợp với *Ken Yip* (đối tượng o_{10}) và xác suất 0.8 của *Jim hatch* (đối tượng o_{11}) ta có xác xuất 0.4.

Kết quả này mặc dù là đúng nhưng nó đặt ra vấn đề mới cơ bản. Trong mô hình dữ liệu quan hệ, câu trả lời của bất kỳ truy vấn nào đều có thể lưu trữ như quan hệ. Trong trường hợp các quan hệ với các thuộc tính xác suất, ta muốn các kết quả truy vấn là các quan hệ xác suất. Tuy nhiên, quan hệ xác suất có một thuộc tính xác xuất để vào truy vấn, nhưng kết quả lại cho khoảng xác suất, thí dụ [0.3, 0.5] như suy diễn trên đây.

Sự cần thiết của khoảng xác suất

Thí dụ trên đây cho thấy nếu ta muốn lưu trữ thông tin dưới dạng "*Đối tượng o hiện diện trong ảnh i là X với xác suất p*" thì sẽ gặp khó khăn. Ngược lại, thay thế xác suất điểm bởi khoảng [l, u] cho phép ta thoát khỏi vấn đề này. Quan điểm này cũng có lợi thế khác. Khi chương trình xử lý ảnh nhận ra đối tượng o trong ảnh i là X với xác suất p, thì nếu ta để ý đến sự thật là tồn tại biên lỗi e trong nhận dạng này, cuối cùng ta có xác suất khoảng [p-e, p+e].

Tổng quát, ta hãy quay lại bảng kết hợp xác suất của quan hệ *name* trên đây, mở rộng nó bằng bổ sung pic8.gif và giả sử rằng biên lỗi là ±3%. Vậy, nếu ta có xác suất p trong bảng, thì ta thay thế xác suất này bởi khoảng [max(0, p-0.03), min(1, p+0.03)] để có được bảng như sau:

ObjId	Name	Prob (Lower)	Prob (Upper)
o_1	Jim Hatch	0.77	0.83
o_1	Dave Fox	0.17	0.23
o_2	John Lee	0.72	0.78
o_2	Ken Yip	0.12	0.18

o_3	John Lee	0.97	1.00
o_4	Jim Hatch	0.97	1.00
o_5	Bill Bosco	0.97	1.00
o_6	Dave Dashell	0.97	1.00
o_7	Ken Yip	0.67	0.73
o_7	John Lee	0.27	0.33
o_8	Bill Bosco	0.57	0.63
o_8	Dave Dashell	0.17	0.23
o_8	Jim Hatch	0.07	0.13
o_9	Ken Yip	0.97	1.00
o_{10}	Ken Yip	0.47	0.53
o_{10}	Jim Hatch	0.37	0.43
o_{11}	Jim Hatch	0.77	0.83
o_{11}	John Lee	0.07	0.13

Hãy quay trở lại câu truy vấn "*Tìm ảnh chứa cả Ken Yip và Jim Hatch*". Hãy xem xét lại ảnh pic8.gif và thấy được xác suất của ảnh chứa cả *Ken Yip* và *Jim Hatch*. Trong trường hợp này, sử dụng cả suy diễn và chú giải như đã làm cho xác suất khoảng, ta có thể viết ra các ràng buộc:

1/ $0.47 \pounds p_1+p_2 \pounds 0.53$

2/ $0.47 \pounds p_3+p_4 \pounds 0.53$

3/ $0.77 \pounds p_1+p_3 \pounds 0.83$

4/ $0.17 \pounds p_2+p_4 \pounds 0.23$

5/ $p_1 + p_2 + p_3+p_4 = 1$

Hãy quan sát bất đẳng thức 3 và 4 trên đây. Bất đẳng thức 3 suy diễn từ tri thức *Jim Hatch* là đối tượng o_{11} với xác suất giữa 77 và 83%. Trong trường hợp xác suất điểm, có hai khả năng (khả năng 1 và 3) trong đó đối tượng o_{11} đúng là *Jim Hatch*. Do đó, p_1+p_2 phải ở trong khoảng 77-83%.

Bất đẳng thức thứ 4 được suy diễn từ tri thức rằng đối tượng o_{11} là ai đó không phải là *Jim Hatch* với xác suất 17-23%, vì 100-83=17 và đối tượng o_{11} không phải là *Jim Hatch*. Do đó, p_2+p_4 phải nằm trong khoảng 17-23%.

Giải phương trình tuyến tính trên đây cho giá trị cực tiểu và cực đại của biến p_1, ta có 0.24 và 0.53.

Tiệm cận tổng quát

Hãy định nghĩa quan hệ xác suất trên lược đồ $(A_1,...,A_n)$ là quan hệ thông thường trên lược đồ $(A_1,...,A_n, LB, UB)$ trong đó miền của thuộc tính UB và LB là các số thực trong khoảng đơn vị [0, 1]. Thí dụ, quan hệ *name* là quan hệ xác suất có ba thuộc tính:

(ImageId, ObjectId, Name)

Error!

Quan hệ *name* thoả mãn một vài ràng buộc toàn vẹn:

Error!

Ràng buộc này cho biết rằng một ObjectId chỉ kết hợp với một một ảnh, có nghĩa rằng ảnh khác nhau có ObjectId khác nhau. Ràng buộc sau đây nói rằng trường LB của bộ bất kỳ luôn nhỏ hơn hay bằng trường UB.

Một CSDL ảnh bao gồm quan hệ xác suất gọi là *name* của khuôn dạng nói trên, cùng với tập quan hệ thông thường (không xác suất) $R_1,...,R_k$ tương ứng với đặc tính ảnh. Lý do của sự phân biệt này là vì chỉ thao tác dẫn tới tính không chắc chắn trong CSDL ảnh là nhận dạng các đối tượng trong các ảnh, và nó được thu nhận tự động bởi các quan hệ name. Các đặc tính của ảnh như giá trị màu R, G, B và các đặc tính khác như loại máy chụp, thời gian chụp... thông thường được xác định bởi tính chắc chắn.

Truy vấn thành viên trong CSDL ảnh là truy vấn có hình thức "*Tìm mọi ảnh trong CSDL ảnh mà chứa các đối tượng có tên* $s_1,...,s_n$". Truy vấn này được biểu diễn trong SQL thông thường như sau:

SELECT ImageId

FROM name $T_1,...,T_n$

WHERE T_1. Name=s_1 AND ... AND T_n.Name=s_n AND

T_1.ImageId=T_2.ImageId AND ...AND T_1. ImageId=T_n.ImageId

Kết quả của truy vấn thành viên là bảng chứa 3 trường: ImageId, LB và UB. (im, l, u) trong kết quả nếu với mỗi 1 £ j £ n, tồn tại bộ t_j Î name như sau:

1. t.ImageId = im,
2. t.LB = li và t.UB = u_i và
3. [l, u] = [l_1, u_1] Ä [l_2, u_2] Ä... Ä [l_n, u_n]

trong đó:

[x, y] Ä [x', y'] = [max(0, x+x'-1), min(y, y')]

Sau một loạt suy diễn, toán tử Ä cho lại cùng kết quả như giải chương trình tuyến tính mô tả trước đây. Do vậy, CSDL ảnh phải có cài đặt toán tử Ä.

Việc tăng cường SQL để giải quyết vấn đề trên là đưa thêm toán tử đặc biệt gọi là HAS. Để tìm mọi ảnh chứa các đối tượng tên $s_1,...,s_n$, ta chỉ đơn thuần viết truy vấn

name HAS s1,...,sn

Ngữ nghĩa của cấu trúc đặc biệt này được hiện thực thông qua truy vấn SQL phức tạp hơn như đã mô tả trên.

Cú pháp của SQL thông thường có thể mở rộng để cho phép các điều kiện theo khuôn dạng

name HAS s1,...,sn

như một phần của câu lệnh WHERE. Thí dụ, truy vấn dưới đây sử dụng quan hệ bank (*bank* là bảng thí dụ có các thuộc tính FNAME, LNAME, ACCTYPE, TRANS, AMOUT, DAY, MTH, YR) và HAS để "*Tìm mọi người đã gửi 9000USD và đã chụp ảnh với Denis Jones*".

SELECT I.ImageID

FROM name I, bank B

WHERE I HAS B.name, “Denis Jones” AND

B.trans = deposit AND B.amount > 9000 AND B.name = I.name

3.7 Biểu diễn CSDL ảnh với R-Trees

CSDL ảnh có thể được biểu diễn như cây R. Nếu quan sát mọi thí dụ cho đến thời điểm này, ta thấy rằng các đối tượng thường được biểu diễn bởi chữ nhật. Do vậy CSDL ảnh có thể biểu diễn như sau:

1. Tạo ra quan hệ gọi là *occursin* với hai thuộc tính (ImageId, ObjId) để xác định đối tượng nào trong ảnh nào.

2. Tạo ra cây R để lưu trữ các chữ nhật. Nếu cùng chữ nhật (thí dụ XLB=5, XUB=15, YLB=20 và YUB=30) nằm trong hai ảnh, thì ta có danh sách tràn kết hợp với nút trong cây R.

3. Mỗi chữ nhật có tập trường kết hợp để chỉ ra đặc tính mức đối tượng/vùng của chữ nhật. Các trường này chứa thông tin về “nội dung” chữ nhật.

Để thấy rõ cách biểu diễn này hoạt động ra sao, ta mô tả CSDL mặt người trong hình 3.1 được lưu trữ như thế nào nhờ kỹ thuật cây R.

Trước hết quan hệ *occursin* được mô tả trong bảng sau:

pic1.gif	o_1
pic1.gif	o_2
pic2.gif	o_3
pic3.gif	o_4
pic4.gif	o_5
pic5.gif	o_6
pic6.gif	o_7
pic6.gif	o_8
pic7.gif	o_9

Các nút trong biểu diễn cây R kết hợp với CSDL có cấu trúc sau:

facenode = record

Rec_1, Rec_2, Rec_3: rectangle;

P_1, P_2, P_3: rtnodetype

```
end
rectangle = record
    XLB, XUB, YLB, YUB:          interger;
    objlist:objnode;
    day, mth, yr:integer;
    camera_type:         string;
    other_info: data_record; (* Lưu trữ thông tin về chữ nhật*)
    place: string
end
objnode = record
    objid: string;
    imageid: string;
    data: infotype  (* Lưu trữ thông tin tuỳ ý về đối tượng*)
    nxt:   objnode
end
infotype = record
    objname:      string;
    objdata:      objdata_record;
    Lp, Up:       real;  (* Biên trên, dưới của xác suất *)
    Next:  infotype
end
```

Trong định nghĩa của objnode trên đây, Lp và Up ký hiệu biên trên và biên dưới của xác suất mà sự nhận diện này là đúng.

Hãy xem xét CSDL ảnh đơn giản đã mô tả ở đầu chương, chỉ bao gồm các ảnh pic1.gif, pic2.gif và pic3.gif trong hình 3.1. Giả sử các ảnh này chứa đối tượng o_1, o_2, o_3 và o_4 với khoảng xác suất chỉ ra trên đây trong phiên bản xác suất khoảng của quan hệ name. Hình 3.12 cho thấy cây R được sử dụng để biểu diễn ba ảnh này và bốn đối tượng trên đó. Cây R trên hình 3.12 được xây dựng theo các bước sau:

1.

Error!

Lấy chữ nhật: Trước hết ta xây dựng bảng con mô tả các chữ nhật và ảnh. Hình 3.13 chỉ ra bốn chữ nhật o_1, o_2, o_3 và o_4. Chú ý rằng mặc dù các chữ nhật này có được từ các ảnh khác nhau, chúng ta có thể chồng chúng lên trong cùng một ảnh.

2. *Tạo cây R*: Tạo cây R biểu diễn các chữ nhật trên (hình 3.12). Tại bước này các nút đối tượng trong cây R vẫn chưa được làm đầy.

ObjId	ImageId	XLB	XUB	YLB	YUB
o_1	pic1.gif	10	60	5	50
o_2	pic1.gif	80	120	20	55
o_3	pic2.gif	20	65	20	75
o_4	pic3.gif	25	75	10	60

3.

Error!

Bổ sung đối tượng: Chúng ta bổ sung đối tượng và làm đầy các trường tương ứng của các đối tượng khác nhau lưu trong cây R. Hình 3.14 chỉ ra nội dung của các

nút khác nhau khi đối tượng mới o được bổ sung vào hệ thống, và đối tượng mới này có cùng các trường XLB, XUB, YLB và YUB như đối tượng o_1. Chỉ có một sự khác biệt giữa đối tượng o_1 và đối tượng mới o là ở chỗ đối tượng mới o xuất hiện trong ảnh khác.

3.7.1 Biểu diễn CSDL ảnh bằng cây R tổng quát

Biểu diễn dữ liệu ảnh bằng cây R mô tả trên đây không cho khả năng tìm kiếm láng giềng gần nhất. Lý do là mỗi đối tượng o có chữ nhật liên kết, R_o. Tuy nhiên, chữ nhật này là chữ nhật 2-d như chỉ ra trên hình 3.14. Cách biểu diễn này lưu trữ các thuộc tính của mỗi đối tượng trong trường "Data" của nó. Vì trường "Data" không được sử dụng để tạo ra chỉ số R-tree, có nghĩa rằng truy vấn trên cơ sở các trường này là không hiệu quả, việc tìm kiếm láng giềng gần nhất trở nên nặng nề.

Có hai mở rộng không phức tạp về cây R có thể sử dụng để giải quyết vấn đề này. Thứ nhất dựa trên cơ sở khái niệm của cây R khái quát hóa (gR-tree) mô tả dưới đây. Thứ hai dựa trên cơ sở cây véctơ lồng nhau (telescoping vector tree) sẽ được mô tả sau.

Nhớ lại rằng đối tượng o có thể được biểu diễn bởi vùng trong không gian n+2 chiều, nơi mà mỗi đối tượng có n đặc trưng và không gian hai chiều khác biểu diễn chữ nhật bao đối tượng. Chữ nhật tổng quát hóa cho không gian có số chiều g (có thể coi g=n+2) được xác định bởi tập các ràng buộc sau:

$l_1 \pounds x_1 \pounds u_1$

$l_2 \pounds x_2 \pounds u_2$

…

$l_g \pounds x_g \pounds u_g$

Chú ý rằng khi g=2, chúng ta có n=0, khi đó chữ nhật 2-d là trường hợp đặc biệt của định nghĩa này.

Nếu bây giờ ta có tập đối tượng Obj, chúng ta có thể biểu diễn tập đối tượng này bởi tập ràng buộc (n+2)-d. Cây R khái quát hoá (gR-tree) bậc K hoàn toàn giống cây R trừ các hệ số sau đây.

· Khi nút N biểu diễn chữ nhật bao khái quát hóa GBR(N) của số chiều (n+2), nó được biểu diễn bởi 2x(n+2) trường số thực, cho cận dưới và cận trên của mỗi chiều.

· Khi nút N bị bẻ gẫy, hợp nhất của các chữ nhật bao khái quát hóa với con của chúng chữ nhật bao khái quát hóa kết hợp với N.

· Mỗi nút (không phải là gốc và lá) chứa nhiều nhất k chữ nhật bao khái quát hóa và ít nhất [K/2] chữ nhật khái quát hóa.

· Thông thường, mọi chữ nhật (n+2)-d được lưu trữ tại lá.

Do đó, cây gR được định nghĩa đúng như cây R, trừ khi các nút chứa tập các chữ nhật bao khái quát hóa thay cho tập các chữ nhật bao 2-d. Rõ ràng, cấu trúc của nút được mở rộng để mô tả cận trên và cận dưới của (n+2)-d. Tìm kiếm láng giềng gần nhất có thể được thực hiện hiệu quả như sau đây.

Giả sử R_q là chữ nhật truy vấn (nó có thể biểu diễn đối tượng ảnh). Ta muốn tìm mọi chữ nhật trong cây gR có tên T mà nó gần R_q nhất (mức gần được xác định bởi thước đo d trên các điểm). Ta mở rộng thước đo d để áp dụng vào chữ nhật như sau:

$$d(R, R') = \min\{d(p, p') \mid p \hat{I} R, p' \hat{I} R'\}$$

Tiến trình tìm kiếm được thể hiện trong giải thuật sau:

Giải thuật 3.5

NN_Search_GR(T, R_Q) SOL=NIL; (* cho đến bây giờ chưa có giải pháp *);

Todo = List containing T only;

Bestdist = ¥; (* khoảng cách của giải pháp tốt nhất từ R_Q *);

while Todo ¹ NIL do

{

F=first element of Todo;

Todo = delete F from Todo;

if d(GBR (F), R_Q)) < Bestdist then

{

Compute children N_1,...,N_r of F;

if N_i's are leaves of T then

{

N_{min}= any N_i at minimal distance from R_Q;

Ndist = d (GBR(N_i), R_Q));

if Ndist < Bestdist then

{

Bestdist = Ndist; SOL = N_{min};

}

}

else Todo=insert all N_i's into Todo in order of distance from R_Q;

}

}

Return SOL;

end

3.8 Truy vấn ảnh bằng bố trí không gian

Phần này trình bày loại thao tác truy vấn ảnh khác. Cho trước ảnh I và hai đối tượng o_1 và o_2 trong I, Người sử dụng có các câu truy vấn như sau:

1. o_1 ở phía nam của o_2?
2. o_1 ở phía đông nam của o_2?

3. o_1 ở phía trái của o_2?

4. o_1 phủ lên o_2?

Có bốn câu truy vấn đơn giản mà người sử dụng muốn hỏi về bố trí không gian của các đối tượng trong ảnh. Để trả lời hiệu quả các câu hỏi loại này, trước hết cần có các quan hệ ưu tiên.

Hình 3.15 chỉ ra một vài quan hệ ưu tiên cơ bản mà có thể định nghĩa giữa các đối tượng khi so sánh chúng theo một chiều.

Mở rộng quan hệ ưu tiên từ 1 chiều thành 2 chiều là không phức tạp. Nếu gọi o[x] và o[y] là phép chiếu đối tượng o theo chiều x và y, thì dễ thu được các quan hệ không gian như sau:

1. Ta gọi o_1 ở phía nam của o_2 nếu $B[o_1[y], o_2[y])$ và một trong

$D(o_1[x], o_2[x])$ hay $D(o_2[x], o_1[x])$

hoặc $S(o_1[x], o_2[x])$ hay $S(o_2[x], o_1[x])$

hoặc $F(o_1[x], o_2[x])$ hay $F(o_2[x], o_1[x])$

hoặc $EQ(o_1[x], o_2[x])$ là đúng.

2. Mặt khác, ta nói rằng o_1 ở bên trái o_2 nếu $B[o_1[x], o_2[x])$ hay $M[o_{1ã}], o_2[x])$ là đúng.

o_1 o_2	**Mô tả**	**Ký hiệu**
Error!	o_1 before o_2	$B(o_1,o_2)$
	o_1 meets o_2	$M(o_1,o_2)$
	o_1 overlaps o_2	$OV(o_1,o_2)$
	o_1 during o_2	$D(o_1,o_2)$
	o_1 starts o_2	$S(o_1,o_2)$
	o_1 finishes o_2	$F(o_1,o_2)$
	o_1 equals o_2	$EQ(o_1,o_2)$

Các định nghĩa tương tự có thể dành cho các đặc tính như North, West, East, Northwest, Southwest, Northest, Southest, Right, Below, Above, Equal, Inside, Cover, Overlap, Disjoint.

Ta nhận thấy rằng các cấu trúc dữ liệu nhiều chiều đã khảo sát trong chương trước có thể dễ dàng hỗ trợ các thao tác không gian như mô tả trong chương này.

3.9 Cài đặt

Hệ thống quản trị CSDL (DBMS) hiện nay hỗ trợ CSDL ảnh là hệ thống được cài đặt trên quan điểm hướng đối tượng. Nó giả sử rằng ảnh là các đối tượng, các lớp của đối tượng ảnh có sẵn một số phương pháp sau đây:

1. rotate(ImageId, dir, angle) thực hiện quay ảnh đi một góc nào đó theo chiều kim đồng hồ hay ngược chiều kim đồng hồ, cho lại ảnh kết quả.

2. segment(ImageId, H_Pred) lấy ảnh và tính chất đồng nhất làm đầu vào, cho lại các vùng khi phân đoạn ảnh tuân thủ tính chất đồng nhất H_Pred ở đầu ra. Kết quả ở đây là tập vùng, không chỉ một vùng.

3. edit(image, editop) thực hiện thao tác sửa đổi trên ảnh và cho lại ảnh sau khi sửa đổi. Các thí dụ của thao tác edit bao gồm thay đổi màu nền, thay đổi kết cấu ảnh, thay thế 1 vài mầu bằng vài màu khác, đảo ảnh...

Phần lớn CSDL ảnh hiện nay làm việc như sau:

1. Giả sử rằng toàn bộ ảnh đang được so sánh (tránh việc phân đoạn hoá).

2. Nó giả sửa rằng cho ảnh bất kỳ, nó có thể kết hợp một vài đặc tính nổi trội (như màu ảnh, kết cấu và hình dạng...) với ảnh. Các đặc tính này được lưu như vécto n trường.

3. Với CSDL ảnh, chỉ số được tạo lập, bao gồm các vécto n chiều này. Như vậy, mỗi ảnh I được biểu diễn như một điểm v_1 trong không gian n. Chỉ số như vậy thường là mở rộng đa chiều của cây tứ phân điểm hay cây R.

4. Khi người sử dụng hỏi câu truy vấn theo dạng "*Hãy tìm mọi ảnh tương tự với ảnh truy vấn Q*" nó xử lý bằng cách tìm mọi vécto v_1 sao cho khoảng cách Euclidean giữa vécto v_1 và v_Q nhỏ hơn một ngưỡng xác định. Mọi I như vậy sẽ cho lại tại đầu ra kết quả.

Chương 4

CƠ SỞ DỮ LIỆU VĂN BẢN/TÀI LIỆU

Chương này sẽ trình bày về CSDL văn bản (*text*). Các câu hỏi sẽ được trả lời ở đây bao gồm CSDL văn bản là gì? Vấn đề của truy vấn trong CSDL văn bản là gì? Hai

khái niệm – chính xác (*precision*) và triệu hồi (*recall*) - cho biết đo hiệu năng các giải thuật truy vấn văn bản như thế nào?

Tài liệu được đặc trưng bởi các từ trong nó. Tuy nhiên, một từ có thể có nhiều nghĩa khác nhau khi được sử dụng trong các ngữ cảnh khác nhau (gọi là *polysemy* - đa nghĩa). Mặt khác, nhiều từ khác nhau có thể có cùng nghĩa (gọi là *synonymy*- đồng nghĩa). Chúng ta sẽ khảo sát kỹ thuật phân cụm các tài liệu "tương tự". Truy vấn có đầu vào là tập tài liệu nhỏ, kết quả của truy vấn là tập các tài liệu tương tự với nó.

Kỹ thuật sẽ được sử dụng để thực hiện truy vấn văn bản là Chỉ số hoá ngữ nghĩa tiềm tàng (*LSI - Latent Sematic Indexing*). Nền tảng toán học của LSI là tách các giá trị nổi bật (*SVD-Singular-valued Decomposition*).

Từ khi ra đời, một ứng dụng cơ bản của máy tính là lưu trữ văn bản, thường dưới dạng tệp (có cấu trúc hay phi cấu trúc). Ý tưởng đơn giản ban đầu là: tài liệu D được biểu diễn bởi xâu ký tự. Thí dụ, xâu có thể là toàn bộ tài liệu, hay chỉ là tiêu đề hay tóm tắt tài liệu. CSDL tài liệu chỉ đơn thuần là tập hợp các xâu như vậy được chỉ số hóa theo cách phù hợp nào đó. Thí dụ, nếu biểu diễn tài liệu sử dụng tên tài liệu để chỉ số hóa tài liệu (hình 4.1) thì một phương pháp phù hợp được sử dụng để chỉ số hóa tập hợp các xâu này. Khi người sử dụng muốn tìm tài liệu liên quan đến chủ điểm T, trình tìm kiếm sẽ tìm tài liệu trong CSDL tài liệu chứa T. Điều này dẫn tới ý tưởng nghiên cứu về các thuật toán hiệu quả về khớp (*matching)* xâu hay tìm các xâu ký tự con. Hai vấn đề chính liên quan, đó là:

1. *Đồng nghĩa (synonymy)*: Đó là trường hợp cho trước chủ điểm T, từ T không xuất hiện bất kỳ đâu trong tài liệu D, mặc dù sự thật là D quan hệ chặt chẽ với chủ điểm T trong câu hỏi. Thí dụ, giả sử ta chỉ xem xét tên tài liệu liệt kê trên hình 4.1. Giả sử chỉ số được xây dựng từ các tiêu đề này, thay cho từ toàn bộ tài liệu, và người sử dụng hỏi câu truy vấn sau:

    a. "*Tìm mọi tài liệu liên quan đến chủ điểm money laundering*". Các từ này không thấy xuất hiện trong tiêu đề của tài liệu d_2, thuật toán *match* xâu ký tự bỏ qua tài liệu này.

    b. "*Hãy tìm mọi tài liệu liên quan đến chủ điểm drugs*". Tình này còn tồi tệ hơn bởi vì tài liệu d_6 có thể bị bỏ qua (từ *dope* ít nhiều có cùng nghĩa với *drugs*, có thể bị bỏ qua bởi vì không khớp xâu cùng cú pháp). Tương tự các tài liệu d_2 và d_3 cũng có thể bị bỏ qua – đáng lẽ nó phải được cho lại vì cả hai đều là sự phối hợp hành động chung chống ma tuý (*drug cartel*).

Trong trường hợp này, vấn đề là ở chỗ chỉ số có thể chứa 1 hay nhiều từ được sử dụng để mô tả từng tài liệu, nhưng nó không thể đoán trước, và chỉ số mức ưu tiên, người sử dụng đều muốn tìm mọi từ truy vấn có thể.

Document ID	String
d_1	Jose Orojuelo's Operations in Bosnia
d_2	The Medellin cartel's Financial Organization
d_3	The cali Cartel's Distribution Network
d_4	Banking Operation ang Money Laundering
d_5	Profile of Hector Gomez
d_6	Connection between Terrorism and Asian Dope Operations
d_7	Hector Gomez: Hoe He Gave Agents the Slip in Cali
d_8	Sex, Drugs, and Videotape
d_9	The Iranian Connection
d_{10}	Boating and Drugs: Slips Owned by thw Cali Cartel

Hình 4.1

2. *Đa nghĩa* (*Polysemy*): Vấn đề cơ bản khác là cùng một từ có nhiều ý nghĩa khác nhau trong ngữ cảnh khác nhau. Thí dụ, từ *bank* có các ý nghĩa như sau: cơ quan tài chính, bờ sông, dựa vào... Khi hỏi câu truy vấn tài liệu liên quan đến tài chính thì ta sẽ không quan tâm đến các bài báo có tiêu đề "*Otters on the Banks of the Colorado River*" hay tiêu đề "*Divorce: Don't Bank on Your Spouse*" như là kết quả cho lại mặc dù từ *bank* là yếu tố của các tiêu đề này.

Tiếp theo hai thước đo cơ bản để đánh giá hiệu năng hệ thống khai thác văn bản được trình bày, đó là chính xác (*precision*) và triệu hồi (*recall*). Một tiệm cận mới gọi là Chỉ số hóa ngữ nghĩa tiềm tàng (LSI) được mô tả để xâm nhập CSDL văn bản kích thước lớn trên cơ sở "nội dung ngữ nghĩa". LSI đã chứng tỏ là một trong các phương pháp thành công nhất trong việc chỉ số hoá kho văn bản lớn. Kỹ thuật này cho phép hạn chế các từ và câu mà nó không cho ta khả năng phân biệt giữa các tài liệu khác nhau, nó còn cho phép nhận biết các từ có ý nghĩa khác nhau trong các tài liệu khác nhau. Nó cũng nhận ra các từ tương đương. Kỹ thuật LSI kết

hợp hiệu quả véctơ *vec(d)* tần số với bất kỳ tài liệu d nào. Véctơ này được sử dụng cho mọi truy vấn. Vì tài liệu d bây giờ được biểu diễn bởi véctơ *vec(d)*, vấn đề lưu trữ CSDL tài liệu (trong mô hình LSI) tương đương với việc lưu trữ tập véctơ có số chiều khá lớn (thông thường véctơ có khoảng 200 trường).

Tiếp theo, một cấu trúc dữ liệu đặc biệt được mô tả, gọi chúng là cây véctơ thu gọn (*telescoping vector tree – TV-tree*), được sử dụng cho LSI. Khi người sử dụng khai thác mọi tài liệu về chủ đề nhất định (họ chỉ ra tập từ khóa), thì truy vấn Q được xem như tài liệu d_Q, tài liệu này có véctơ kết hợp *vec*(d_Q). Sau đó ta tìm cấu trúc dữ liệu TV-tree để tìm n láng giềng gần nhất của véctơ tài liệu truy vấn *vec*(d_Q) có lưu tâm đến thước đo khoảng cách cụ thể.

4.1 Chính xác (precision) và triệu hồi (recall)

Giả sử D là tập hữu hạn các tài liệu, A là thuật toán bất kỳ lấy xâu chủ điểm t làm đầu vào và cho lại tập A(t) của tài liệu làm đầu ra, ta có A(t) Í D. Trực quan thì, ta có thể suy nghĩ về A như mã hóa một thuật toán hay kỹ thuật khai thác tài liệu.

Giả sử rằng, chúng ta có tính chất thích hợp (*relevant*) với hai đối số: chủ điểm *t* và tài liệu d. Trực quan thì, nếu *relevant(t,d)* là *true*, thì có nghĩa rằng tài liệu *d* được xem như thích hợp với chủ điểm *t*. Chúng ta không quan tâm cụ thể đến việc tính chất thích hợp này được cài đặt như thế nào. Thí dụ, tính chất thích hợp có thể được thực hiện bằng tay trên tập thử cụ thể D_{test} Í D của các tài liệu và tập thử tương tự T_{test} của các chủ điểm.

Error!

Hình 4.2 mô tả tình huống này. Vòng tròn trắng trên hình chỉ ra mọi tài liệu thích hợp với chủ điểm truy vấn *t*, trong khi vòng tròn tô chỉ ra các tài liệu do thuật toán truy vấn tài liệu cho lại khi đòi hỏi truy vấn tài liệu liên quan đến chủ điểm *t*.

Error!

Ta nói rằng độ chính xác của thuật toán *A* liên quan đến tính chất *relevant* và tập kiểm thử D_{test} là P_t% cho chủ điểm tÎ T_{test} nếu

Error!

Để tránh chia cho 0 cho nên đã cộng thêm 1 vào tử số và mẫu số. Ta nói rằng độ chính xác của thuật toán *A* với sự thừa nhận tính chất *relevant*, tập thử tài liệu D_{test}, và tập thử chủ điểm T_{test} là P% nếu

Nói cách khác, độ chính xác của thuật toán *A* của truy vấn thông tin với thừa nhận các tập thử phù hợp và định nghĩa liên quan, được đo bởi việc quyết định bao nhiêu câu trả lời thuật toán cho lại là thực sự đúng. Do đó, ta có thể đếm tổng số đối tượng trong phần giao đường tròn (hình 4.2), sau đó chia số này cho tổng đối tượng trong vòng tròn tô (các số này đều được cộng thêm 1).

Error!

Ngược lại, *recall* của thuật toán *A* là thước đo bao nhiêu tài liệu là kết quả đúng đã được truy vấn cho lại. Độ chính xác hỏi câu hỏi "*Bao nhiêu tài liệu do thuật toán A tìm ra là đúng?*". *Recall* hỏi câu hỏi "*Bao nhiêu tài liệu được tìm ra bởi thuật toán A?*".

Error!

Sử dụng cùng ký pháp như độ chính xác, *recall* R_t kết hợp với chủ điểm t cho bởi công thức sau:

Error!

Tỷ lệ *recall* tổng thể R kết hợp với bộ thử D_{test} của tài liệu và T_{test} của chủ điểm cho bởi:

Nói cách khác (hình 4.2) ta cần đếm mọi tài liệu trong phần giao của hai vùng (và cộng thêm 1) rồi chia nó cho tổng số thành phần trong vùng không tô (cộng thêm 1).

Error!

Thí dụ, giả sử tổng các đối tượng trong mỗi vùng của hình 4.2 được chỉ ra trong hình 4.3. Sau đó, độ chính xác của truy vấn chủ điểm cụ thể cho bởi:

Error!

Cùng cách suy diễn, *recall* của cùng chủ điểm này được tính như sau:

Độ chính xác và *recall* hình thành hai cách nổi tiếng nhất để đo thuật toán truy vấn văn bản "tốt như thế nào". Trong nhiều trường hợp, một thuật toán với độ chính xác rất cao có thể có *recall* rất tồi. Thí dụ, thuật toán không cho lại cái gì có thể có độ chính xác 100%, nhưng thuật toán này không hữu ích. Mặt khác, thuật toán với tỷ lệ *recall* rất cao có thể có độ chính xác rất tồi. Thuật toán luôn cho lại mỗi tài liệu với 100% *recall* nhưng lại không được sử dụng nhiều.

6.1 Danh sách dừng, gốc từ và bảng tần số

Trong phần này, một số kỹ thuật cơ bản sử dụng trong phần lớn các hệ thống truy vấn tài liệu/văn bản được trình bày.

Danh sách dừng (*Stop List*) kết hợp với tập tài liệu *D* là tập *StopL* của các từ không thích hợp lắm (*deemed irrelevant*), mặc dù nó có thể xuất hiện thường xuyên. Thí dụ, hệ thống SMART của *Cornell University* sử dụng *stop list* với 439 từ. Thí dụ các từ xuất hiện trong danh sách dừng có thể là *the, and, for, with*... Rõ ràng, danh sách dừng có thể khác nhau vì *D* khác nhau. Thí dụ, nếu *D* là tập tài liệu kết hợp với các bài báo khoa học của Bộ môn máy tính, *University of Meryland*, thì hiệu quả nếu đưa từ *(word) computer* vào danh sách dừng liên kết với cơ sở tài liệu này. Ngược lại, không nên cho từ *computer* vào danh sách dừng của tập tài liệu về địa chất. Như chúng ta đã dự đoán, mục tiêu của danh sách dừng là hạn chế các từ "vô dụng" từ góc nhìn tìm kiếm và chỉ số hoá.

Thông thường, một số từ có thể là biến thể cú pháp của từ khác. Thí dụ, từ *drug*, *drugged* và *drugs* là cùng chia sẻ từ gốc (*word stem*)-*drug*. Tài liệu d_1 chứa từ *drugged*, có thể là về *drug* khi tài liệu tương tự d_2 có được từ d_1 bằng cách thay thế mọi từ *drugged* trong d_1 bởi *drug*. Bằng giảm các từ khác nhau về từ gốc, ta có thể nhóm các từ suy diễn từ cùng gốc. Do vậy, thay vì chỉ số hóa tài liệu trên cơ sở ba từ khác nhau – *drug*, *drugged* và *drugs* – chúng ta chỉ cần sử dụng một từ cho chúng, đó là *drug*.

Giả sử *D* là tập *N* tài liệu, *T* là tập *M* từ/từ gốc trong tài liệu *D*. Giả sử rằng không có từ trong danh sách dừng *D* trong *T* và mọi từ trong *T* đều là từ gốc. Bảng tần số với tên FreqT kết hợp với *D* và *T* là ma trận (MxN) như sau Freq(i,j) bằng tổng lần xuất hiện của từ t_i trong tài liệu d_j.

Thí dụ, hãy xem xét tập tài liệu D={d_8, d_9, d_{10}} chỉ ra trong hình 4.1. Hơn nữa, giả sử ta có tài liệu khác tên d_{11} với tiêu đề "*Drugs, drugs, drugs*". Các từ có trong bốn tiêu đề tài liệu này là *sex, drug, videotape, iran, connection, boat, slip, own, cali*và*cartel*. Chú ý rằng các từ như *and* và *the* không được liệt kê trong danh sách

này bởi vì chúng có mặt trong danh sách dừng *D*. Tương tự, các từ như *owned* được thay thế bởi các từ gốc *own*. Bảng tần số cho bốn tài liệu này là:

Term/document	**d_8**	**d_9**	**d_{10}**	**d_{11}**
sex	1	0	0	0
drug	1	0	1	3
videotape	1	0	0	0
iran	0	1	0	0
connection	0	1	0	0
boat	0	0	1	0
slip	0	0	1	0
own	0	0	1	0
cali	0	0	1	0
cartel	0	0	1	0

Trong bảng tần số FreqT, mỗi tài liệu d_j được biểu diễn bởi cột j của FreqT. Tương tự, sự xuất hiện của term/word t_i được biểu diễn bởi cột i. Nhưng tại sao tần số lại quan trọng? Nó có ích lợi gì? Để trả lời phi hình thức câu hỏi này, ta sẽ xem xét thí dụ đơn giản chứa một vài tài liệu với 5 thuật ngữ như trong bảng sau đây:

Term/document	**d_1**	**d_2**	**d_3**	**d_4**	**d_5**	**d_6**
t_1	615	390	10	10	18	65
t_2	15	4	76	217	91	816
t_3	2	8	815	142	765	1
t_4	312	511	677	11	711	2
t_5	45	33	516	64	491	59

Khi khảo sát tài liệu này ta thấy d_1 và d_2 là tương đương bởi vì phân bổ các từ trong d_1 phản ánh phân bổ từ trong d_2. Cả hai chứa rất nhiều t_1 và t_4, tương đối ít t_2 và t_3, và chứa vừa phải t_5. Cùng mạch như vậy, ta có d_3 và d_5 cũng tương tự. Tuy nhiên, d_4 và d_6 là hoàn toàn khác.

Có cần quan tâm đến độ dài tương đối của tài liệu hay không? Việc đếm đơn thuần các từ không cho thấy tầm quan trọng các từ trong tài liệu. Thí dụ, nếu một từ xuất hiện ba lần trong tài liệu dài 10 từ thì nó được xem là quan trọng. Mặt khác nếu nó xuất hiện ba lần trong tài liệu dài 1 triệu từ thì ý nghĩa của nó bị giảm. Do vậy, trong bảng tần số, chúng ta quan tâm đến tỷ lệ tổng số lần xuất hiện của từ trong tài liệu với tổng số toàn bộ từ có trong tài liệu. Bổ sung vào thước đo này, có nhiều thước đo tầm quan trọng của khái niệm/từ (*Term/Words*) được đề xuất trong nhiều tài liệu. Trong phần tiếp theo ta chỉ giả sử đơn thuần rằng FreqT(i,j) là số thực lớn hơn hay bằng 0, và giá trị chính xác của nó được xác định theo một trong hai cách nói trên. Cần chú ý rằng, một vài định nghĩa khác của FreqT(i,j) cũng được đề xuất trong tài liệu này.

Bây giờ giả sử rằng người sử dụng muốn khai thác (*retrieve*) *n* tài liệu đầu tiên trong CSDL tài liệu D mà nó thích hợp (*relevant*) với truy vấn Q. Thí dụ, người sử dụng có thể phát biểu "*Find the 25 documents that are maximally relevant with respect to banking operations and drugs*". Trong trường hợp này, truy vấn Q thử tìm lấy ra các tài liệu thích hợp với hai từ khóa, sau khi lấy từ gốc, là *bank* và *drug*. Nếu ta suy nghĩ truy vấn Q là tài liệu thì ta tìm kiếm các cột trong FreqT mà nó "gần" nhất tới véctơ kết hợp với Q. Tính "gần" được xác định trong khái niệm thước đo như sau đây:

1.

Error!

Khoảng cách khái niệm (term distance): Giả sử $vec_Q(i)$ biểu thị tổng số lần xuất hiện khái niệm t_i trong Q. Sau đó khoảng cách khái niệm giữa Q và tài liệu d_r được xác định bởi:

Dĩ nhiên thước đo này là khá tuỳ ý.

2.

Error!

Khoảng cách cosin (cosine distance): Thước đo này được sử dụng rộng rãi trong thế giới CSDL và được mô tả như sau đây:

Tại đây, ta tính tích các véctơ kết hợp với truy vấn Q và tài liệu d_i, và chia nó cho tích căn bậc hai của các véctơ liên quan.

Trong trường hợp xấu nhất, cần đến O(N) so sánh, mỗi so sánh cho một tài liệu, mỗi so sánh cần O(M) thời gian cho từng khái niệm. Vậy, sẽ cần O(MxN) thời gian để tìm giải pháp tốt nhất. Tuy nhiên ngay cả với CSDL rất nhỏ như CSDL chứa các bài báo khoa học của Bộ môn máy tính, *University of Meryland* từu 1990 thì (MxN) có thể là hàng trăm triệu hay hàng tỷ phép so sánh. Kỹ thuật chỉ số hoá ngữ nghĩa tiềm tàng (*LSI-Latent Sematic Indexing*) sẽ làm giảm đáng kể thời gian nói trên.

4.3 Chỉ số hoá ngữ nghĩa tiềm tàng (LSI)

Ý tưởng cơ bản của chỉ số hoá ngữ nghĩa tiềm tàng (*LSI-Latent Sematic Indexing*" là các tài liệu tương tự có tần số xuất hiện từ tương tự. Tuy nhiên, với bất kỳ CSDL tài liệu không tầm thường nào đều có tổng số tài liệu M và tổng số khái niệm N là rất lớn. Nếu ta muốn chỉ số hoá các bài báo khoa học của trường đại học bằng *full text,* chúng ta sẽ nhanh chóng nhận ra rằng tổng số khái niệm sẽ là hàng trăm ngàn chứ không phải hàng triệu. Cho trước hàng trăm ngàn tài liệu kỹ thuật đang tồn tại, bảng tần số sẽ lớn ghê gớm (MxN), có đến hàng trăm triệu đầu vào. Xử lý bảng lớn như vậy là khó khăn đáng kể.

Cái LSI sẽ làm là sử dụng kỹ thuật gọi là tách giá trị khác thường (*SVD-Singular Value Decomposition*), nó được quen biết trong lý thuyết ma trận, để giảm kích thước bảng tần số xuống còn ít hơn (MxN). Tổng quát, bất kỳ giảm thiểu nào đều dẫn tới mất mát thông tin, do vậy, ta phải đảm bảo rằng SVD phải có "năng lực thông tin – *information efficient*" cao nhất có thể. Có nghĩa rằng, chúng chỉ mất phần bảng tần số ít ý nghĩa nhất. Nói cách khác, kỹ thuật LSI sử dụng ma trận (MxN) để biểu diễn ma trận nhỏ hơn (KxK). Nó được thực hiện bằng loại bỏ vài hàng và vài cột của ma trận tần số gốc. Thông thường K có giá trị khoảng 200 cho tập hợp tài liệu lớn.

Nhớ lại rằng, mỗi cột trong ma trận tần số biểu diễn một tài liệu. LSI coi mỗi tài liệu là một véctơ độ dài K bởi đơn thuần giữ lại K hàng có ý nghĩa nhất trong bảng tần số. Các bước cơ bản của LSI như sau:

1. *Tạo bảng*: Tạo ma trận tần số FreqT.

2. *Xây dựng SVD*: Tính toán phân chia giá trị véc tơ khác thường (A, S, B) của FreqT bằng cách chia FreqT thành ba ma trận A, S, B (xem phần sau).

3. *Nhận dạng véctơ*: Với mỗi tài liệu d, gọi vec(d) là tập các khái niệm trong FreqT mà các hàng tương ứng của nó không bị loại bỏ trong ma trận đơn S.

4. *Tạo chỉ số*: Lưu trữ tập các véctơ vec(d) được chỉ số bởi một trong các kỹ thuật như nghiên cứu sau.

Khi khai thác tài liệu tương tự với tài liệu truy vấn d_Q, ta chỉ đơn giản tìm cấu trúc chỉ số tạo ra trên đây và tìm tài liệu d trong lưu trữ sao cho vec(d_0) gần nhất với vec(d) thừa nhận thước đo đã chọn trên véctơ .

4.3.1 Nền tảng của phân chia giá trị khác thường (SVD)

Error!

Nhớ lại rằng ma trận M được gọi là ma trận bậc (m x n) nếu có m hàng và n cột. Nếu ma trận M_1 có bậc (m_1 x n_1) và M_2 có bậc (m_2 x n_2), sau đó ta gọi tích (M_1 x M_2) là xác định rõ ràng nếu $n_1 = m_1$. Bậc của ma trận tích (M_1 x M_2) là (m_1 x n_2). Thí dụ, hãy xem xét hai ma trận A và B như sau:

A có bậc (2x2) và B có bậc (2x3). Ta gọi (A x B) là xác định rõ ràng và có bậc (2x3).

Error!

Tổng thể, giả sử tích (M_1 x M_2) của hai ma trận là định nghĩa tốt. Nếu

thì tích (M_1 x M_2) là ma trận sau:

Error!

trong đó,

Error!

Thí dụ,

Cho trước ma trận M bậc (m x n), đổi chỗ (*transpose*) M ký hiệu là M^T có được nhờ chuyển hàng M thành cột M^T. Hàng thứ nhất của M thành cột thứ nhất của M^T, hàng thứ m của M thành cột thứ m của M^T.

Do vậy, M^T là ma trận (n x m). Thí dụ,

Error!

Ta sẽ sử dụng cách biểu diễn véctơ để đề cập đến ma trận bậc (1x m). Hai véctơ x và y của cùng bậc được gọi là trực giao (*orthogonal*) nếu $x^T y=0$. Thí dụ,

x=(10, 5, 20)

y=(1, 2, -1)

Error!

Hai véctơ trên là trực giao vì:

Error!

Ma trận M được gọi là trực giao nếu ($M^T M$) là ma trận đơn vị. Thí dụ hãy xem xét ma trận:

Dễ dàng thấy rằng ma trận M^T x M là ma trận đồng nhất, do vậy nó là trực giao.

Ma trận M là ma trận chéo (*diagonal*) nếu bậc của M là (m x m) và với mọi 1£ i, j £ m, thì

i ¹ j ® M(i, j) = 0

Error!

Nói cách khác, M là ma trận chéo nếu nó là ma trận vuông và mọi phần tử không nằm trên đường chéo của nó có giá trị 0. Chú ý rằng không đòi hỏi các phần tử trên đường chéo phải khác 0. Thí dụ ma trận A, B dưới đây là ma trận chéo còn ma trận C là không:

Ma trận chéo M bậc (m x m) được gọi là không tăng (*nonincreasing*) nếu với mọi 1£ i, j £ m, thì

i £ j ® M(i, j) ³ M(j, j)

Nói cách khác, nếu đi theo đường chéo từ đỉnh xuống đáy thì các giá trị giảm dần. Theo thí dụ trên, B là ma trận chéo không tăng, nhưng ma trận A không phải như vậy.

Giả sử FreqT là bảng tần số bất kỳ (nó là ma trận bậc M x N). Phân chia giá trị khác thường (SVD) của FreqT là bộ ba (A, S, B) trong đó:

1. FreqT=(A x S x B^T),
2. A là ma trận trực giao bậc (M x M), có nghĩa là $A^TA=I$,
3. B là ma trận trực giao (N x N), có nghĩa là $B^TB=I$,
4. S là ma trận chéo được gọi là ma trận khác thường (*singular matrix*).

Error!

Rõ ràng là cho trước ma trận bất kỳ M bậc (m x n), thì có thể tìm ra SVD (A, S, B) của M, trong đó S là ma trận chéo không tăng. Thí dụ, SVD của ma trận

Error!

được cho bởi

Tại đây, giá trị bất thường là 5 và 2, và dễ thấy rằng ma trận bất thường là không tăng.

Error!

Ý tưởng cơ bản của LSI là cho trước ma trận tần số FreqT, ta có thể phân chia nó

thành SVD TSD^T, trong đó S là không tăng (hình 4.4a). Tuy nhiên nếu FreqT có bậc (M x N) thì T có kích thước (M x M), S có bậc (M x R), trong đó R là bậc của FreqT, và D^T có bậc (R x N).

Cái hay của LSI là ta có thể làm giảm khó khăn cơ bản bằng giới hạn các giá trị đơn có ý nghĩa nhất từ ma trận khác thường S như trên hình 4.4b. Việc này được thực hiện như sau:

1. Chọn số nguyên k nhỏ hơn R.

2. Thay thế S bởi S^*, nó là ma trận (k x k), trong đó $S^*(i, j) = S(i, j)$ với 1£i, j£k.

3. Thay thế ma trận D^T kích thước (R x N) bằng ma trận D^{*T} kích thước (k x N), trong đó $D^{*T}(i, j) = D^T(i, j)$ nếu 1£ i £k và 1£ j £N.

4. Tương tự, thay thế ma trận T có kích thước (M x M) bằng ma trận T^* có kích thước (M x K).

Nói cách khác, LSI bỏ đi các giá trị ít ý nghĩa nhất và giữ lại phần còn lại của ma trận. Gọi tích $T*S*D^{*T}$ là Freq*. Nền tảng của kỹ thuật LSI là ở chỗ nếu chọn k một cách hợp lý thì k hàng xuất hiện trong ma trận đơn S^* biểu diễn k khái niệm quan trọng nhất (từ quan điểm khai thác) xuất hiện trong toàn bộ tập tài liệu.

Error!

Để thấy rõ LSI làm giảm kích thước theo cách này như thế nào, hãy khảo sát thí dụ đơn giản. Giả sử FreqT có SVD sau:

Error!

Người thiết kế hệ thống khai thác tài liệu có thể đặt giá trị 3 làm mức ngưỡng (chú ý rằng trong ma trận đơn trong phân chia trên đây có các giá trị đơn thứ tư và thứ năm rất nhỏ so với cái khác). Do vậy, người thiết kế CSDL tài liệu phải chọn cẩn thận để giảm kích thước ma trận bằng làm giảm hai hàng cột cuối của ma trận đơn. Kết quả là:

Thông thường, kích thước ma trận đơn trong miền lớn vừa phải là 200. Hãy khảo sát ý nghĩa của nó như sau.

1. Kích thước của bảng tần số gốc là (M x N), trong đó M là tổng số khái niệm và N là tổng số tài liệu. Dễ dàng có đến M = 1 triệu và N=10,000 ngay CSDL tài liệu nhỏ.

2. Bây giờ kích thước của ba ma trận sau khi đã giảm thiểu kích thước của ma trận đơn, giả sử còn 200:

· Kích thước của ma trận thứ nhất là M x R. Với các số trên đây ta có 1 triệu x 200 = 200 triệu đầu vào.

· Kích thước ma trận đơn là 200 x 200 = 40,000 đầu vào. (Sự thật trong 40,000 đầu vào thì chỉ 200 cần phải lưu trữ; toàn bộ các đầu vào còn lại có giá trị 0).

· Kích thước ma trận cuối cùng là R x N. Với các số trên đay ta có 200 x 10,000 = 2 triệu đầu vào.

Cuối cùng ta có khoảng 202 triệu đầu vào trong bảng sau khi áp dụng SVD.

3. Ngược lại, (M x N) gần tới 10 tỷ, nói cách khác SVD làm giảm đáng kể không gian sử dụng khoảng 1/50 so với bảng tần số gốc.

Chú ý rằng: Trong nhiều trường hợp ma trận gốc M x N là ma trận rải rác, nó có thể lưu trữ được bởi vì số phần tử nhỏ hơn M x N rất nhiều. Trong trường hợp này phân chia SVD lại làm tăng tổng số lưu trữ.

Tính toán thực sự của SVD kết hợp với ma trận là câu hỏi phức tạp trong lý thuyết ma trận, do vậy ta không đi chi tiết ở đây. May thay, ta không phải làm việc đó tiếp theo, vì thuật toán SVD nổi tiếng có sẵn trong các thư viện MATLAB và LAPPACK (*http://usi.utah.edu/software/math/pub/LAPACK/lug/node55.html*).

4.3.2 Khai thác tài liệu sử dụng SVD

Giả sử ta đã tạo ra một biểu diễn SVD, TS^{*} x D^{*T}, của bảng tần số. Hãy quan sát biểu diễn này để trả lời hai câu hỏi sau: Cho trước hai tài liệu d_1 và d_2 trong kho lưu trữ, tính "tương tự" của chúng như thế nào? Cho trước xâu ký tự/tài liệu truy vấn Q, n tài liệu nào trong kho lưu trữ mà chúng "thích hợp nhất" với truy vấn đó?

Error!

Trước hết, nhắc lại khái niệm tích vô hướng của hai véctơ (có cùng độ dài). Giả sử $x=(x_1,...,x_w)$ và $y=(y_1,...,y_w)$ là hai véctơ giá trị thực. Tích vô hướng của **x** và **y** được tính như sau:

Tính tương tự của hai tài liệu

Error!

Giả sử d_i và d_j là hai tài liệu. Tính tương tự của hai tài liệu theo biểu diễn SVD TS^* x D^{*T} của bảng tần số được cho bởi giá trị tích vô hướng hai cột trong ma trận D^{*T} kết hợp với hai tài liệu đó:

Ở đây ma trận đơn sau khi rút gọn sẽ có kích thước (R x R). Chú ý rằng thay vì so sánh toàn bộ M khái niệm cho hai tài liệu này, ta chỉ so sánh R khái niệm, nó là số nhỏ hơn M rất nhiều (thông thường là 200).

Tìm kiếm phù hợp p đầu tiên cho truy vấn Q

Giả sử Q là truy vấn. Ta coi Q như tài liệu và tạo lập véctơ vec_Q cho nó như trên đây. Tuy nhiên, có một điểm khác là: Chỉ R khái niệm quan trọng là được xem xét chứ không phải xem xét tất cả N. Khi được hỏi để tìm ra p khái niệm phù hợp nhất với Q, ta sẽ phải tìm p tài liệu $d_{a(1)}$, ...,$d_{a(p)}$ như sau:

1. Với mọi 1 £ i £ j £ p, tính tương tự giữa vec_Q và $d_{a(i)}$ lớn hơn hay bằng *tính tương tự* giữa vec_Q và $d_{a(j)}$, và

2. không có tài liệu d_z nào mà tính tương tự giữa d_z và vec_Q vượt quá *tính tương tự* của $d_{a(p)}$

Điều này có thể thực hiện bằng sử dụng bất kỳ cấu trúc chỉ số hoá nào cho không gian R-d. Cấu trúc chỉ số hoá như vậy bao gồm cây R, cây k-d như đã nghiên cứu trước đây. Tuy nhiên, tổng quát thì cấu trúc chỉ số hóa như cây R và k-d không làm việc tốt với dữ liệu có số chiều ³ 20. Do vậy cần phải có kỹ thuật nào đó tốt hơn. Cây TV (*TV-tree*) được mô tả sau đây là cấu trúc chỉ số hoá phù hợp hơn cho loại dữ liệu nhiều chiều này.

4.4 Cây TV (TV-tree)

Mục tiêu cơ bản của cây véctơ thu gọn (*TV-Telescopic Vector Tree*) là xâm nhập điểm dữ liệu trong không gian có số chiều rất lớn sao cho hiệu quả cao. Trên đây ta thấy, tài liệu d được xem như véctơ **d** có độ dài k, trong khi ma trận giá trị đơn, sau khi phân chia, có kích thước (k x k). Do vậy, mỗi tài liệu được xem như điểm trong không gian k chiều. Một *CSDL tài liệu* như mô tả trên đây được xem như tập hợp của các điểm như vậy và được chỉ số hoá phù hợp.

Khi người sử dụng biểu diễn truy vấn Q, thực tế là họ xác định véctơ vec(Q) có độ dài k. Ta phải tìm p tài liệu trong CSDL mà nó phù hợp nhất với Q. Có nghĩa rằng

ta phải tìm ra k láng giềng gần nhất với truy vấn Q có mặt trong CSDL tài liệu. Cây TV là cấu trúc dữ liệu mượn từ cây R.

Cây TV cố gắng quyết định một cách mềm dẻo và động việc rẽ nhánh như thế nào, trên cơ sở dữ liệu đang xem xét. Ý tưởng là nếu nhiều véctơ phù hợp với một số thuộc tính (nếu nhiều tài liệu đều có các khái niệm chung), thì ta phải tổ chức chỉ số bằng rẽ nhánh đến các khái niệm đó (trường các véctơ) mà nó phân biệt giữa các véctơ/tài liệu này. Thí dụ, trong CSDL tài liệu chứa tập các báo cáo của Trường đại học *Maryland*, từ như *database* có thể xuất hiện trong hàng nghìn tài liệu. Để phân biệt tiếp theo giữa các bài báo có từ *database*, ta phải tổ chức chỉ số theo cách mà có thể rẽ nhánh theo sự hiện diện hay vắng mặt của vài từ khác mà nó có khả năng phân biệt hơn.

4.4.1 Tổ chức cây TV

Trước khi định nghĩa cây TV để lưu trữ các điểm k chiều (k-d) thì ta phải chỉ ra hai tham số sau:

1. *NumChild*: số nút con cực đại mà 1 nút bất kỳ trong cây TV có thể có.

2. μ: là số lớn hơn 0 và nhỏ hơn hay bằng k, gọi nó là số chiều tích cực (*number of active dimensions*).

Sử dụng ký pháp TV(k, NumChild, μ) để gọi cây TV, nó được sử dụng vào việc lưu trữ dữ liệu k-d, với NumChild là số nút con cực đại, μ số chiều tích cực. Như cây R, mỗi nút trong cây TV biểu diễn một vùng. Với mục đích sử dụng này, mỗi nút N trong cây TV chứa ba trường sau:

1. *N.Center*: Biểu diễn điểm trong không gian k-d.

2. *N.Radius*: Là số thực lớn hơn 0.

3. *N.ActiveDims*: Là danh sách của nhiều nhất μ chiều. Mỗi chiều là một số giữa 1 và k. Do vậy, *N.ActiveDims* là tập con của {1,...,k} của số μ hay nhỏ hơn.

Giả sử x và y là những điểm trong không gian k-d, và *ActiveDims* là tập các chiều tích cực. *Khoảng cách tích cực* giữa x và y, được gọi là act_dist(x, y), cho bởi:

Error!

trong đó, x_i, y_i là giá trị của chiều thứ i của lần lượt x và y. Thí dụ, giả sử k=200, μ=5 và AvtiveDims={1,2,3,4,5} và giả sử rằng:

x=(10,5,11,13,7, x_6, x_7,...,x_{200})

y=(2,4,14,8,6,y_6,y_7,...,y_{200})

Error!

Sau đó khoảng cách tích cực giữa x và y được cho bởi:

Chú ý rằng khoảng cách tích cực giữa hai véctơ bỏ qua mọi trường mà nó không tích cực.

Cho trước nút N trong cây TV là nút biểu diễn vùng chứa mọi điểm x, trong đó khoảng cách tích cực giữa x và *N.Center* nhỏ hơn hay bằng *N.Radius*.

Thí dụ, nếu chúng ta có nút N với tâm ở tại

N.Center=(10, 5, 11, 13, 7, 0, 0, 0, 0,..., 0)

và *N.ActiveDims*={1,2,3,4,5}, thì nút này biểu diễn vùng chứa mọi điểm x mà nó thỏa mãn:

Error!

Ta sử dụng ký pháp *Region(N)* để gọi vùng biểu diễn bởi nút N trong cây TV.

Ngoài các trường *Center, Radius, ActiveDims*, nút N trong cây TV còn chứa trường *Child* của các con trỏ *NumChild* đến nút khác của cùng loại.

Như trong trường hợp cây R, cây TV có các đặc tính sau:

1. Mọi dữ liệu được lưu trên các nút lá.

2. Mỗi nút trong cây TV (trừ gốc và các lá), trong đó ít nhất một nửa chúng phải có giá trị, do vậy, ít nhất nửa số con trỏ *Child* phải khác NIL.

3.

Error!

Nếu N là nút và $N_1,...,N_r$ là con của nó, thì

4.4.2 Chèn vào cây TV

Hãy xem xét trường hợp có không gian 5-d (khi ta chỉ có 5 khái niệm rút ra từ tập hợp tài liệu), và ta muốn chèn vài véctơ vào cây TV với tên TV(5, 3, 2). Giả sử rằng toàn bộ không gian là siêu hình cầu (*hyper-spher*) có tâm tại (0,0,0,0,0) và bán kính 50. Khởi đầu cây TV là rỗng.

1. Giả sử véctơ thứ nhất sẽ chèn là (5,3,20,1,5). Nó được sử dụng để tạo ra nút gốc với các tính chất sau:

   Root.Center=(0,0,0,0,0).

   Root.Radius=50.

   Trong trường hợp này, gốc cũng là lá, có con trỏ đến thông tin phù hợp với điểm v_1=(5,3,20,1,5).

   Giả sử Root.ActiveDims={2,3}.

Error!

Hình 4.5a chỉ ra tình huống này.

2. **Error!**

Giả sử véctơ tiếp theo được chèn vào là $\mathbf{v}_2$=(0, 0, 18, 42, 4). Trong trường hợp này ta cũng tạo thêm lá mới như trên đây. Hình 4.5b mô tả tình huống này.

3. Giả sử sau đó ta chèn véctơ $\mathbf{v}_3$=(0, 0, 19, 39, 6). Hình 4.5c mô tả tình huống này. Tại đây, nút gốc đã đầy, nó không thể có nút con khác nữa.

4. Giả sử véctơ tiếp theo được chèn vào là $\mathbf{v}_4$=(9, 10, 2, 0, 16). Vùng biểu diễn bởi gốc cây chứa nhiều hơn 3 đầu vào, vượt quá khả năng của gốc. Do vậy ta phải phân chia (*split*) gốc. Có nhiều chiến lược phân chia gốc cây. Lý tưởng là, cái ta muốn làm là lấy 4 véctơ tham gia sau đó nhóm chúng thành hai nhóm. Cách khác là chia vùng biểu diễn bởi gốc thành hai phần sao cho mỗi phần chứa 2 trong 4 véctơ. Dưới đây ta sẽ trao đổi một vài chiến lược phân chia khác. Nhưng cái lo lắng bây giờ là việc phân chia nhóm sẽ sinh ra các nút như nhau cùng tồn tại. Giả sử chiến lược phân chia tạo ra $\mathbf{v}_1$ và $\mathbf{v}_4$ ở cùng phần và $\mathbf{v}_2$ và $\mathbf{v}_3$ cùng ở phần bên kia. Trước hết $\mathbf{v}_2$ và $\mathbf{v}_3$ là tương tự vì chúng ở gần nhau theo quan niệm "khoảng cách tích cực" nói trên. Ba kết quả được chỉ ra trong hình 4.5d. Các giá trị của trường bán kính và tâm của nút con được làm đầy bởi giá trị bất kỳ, ta sẽ chỉ ra chúng được xác định như thế nào. Chú ý rằng gốc cây bây giờ có hai nút con: S_1 và S_2, mỗi nút con biểu diễn một vùng như trên hình 4.5d. *Mọi nút lá bây giờ đều ở mức 2 trong cây*.

5. Giả sử nút tiếp theo được chèn vào là $\mathbf{v}_5$=(18, 5, 27, 9, 9). Để xác định nút con nào của gốc được chèn $\mathbf{v}_5$, ta phải thực hiện thao tác chọn cành (*branch selection*). Hình 4.6a chỉ ra rằng ta chọn cành đến nút con thứ nhất thay cho nút con thứ hai. Thí dụ sau sẽ mô tả chi tiết việc chọn cành.

6. Giả sử véctơ tiếp theo được chèn vào là $\mathbf{v}_6$=(0, 0, 29, 0, 3). Lần nữa ta phải thực hiện chọn cành, lần này ta có thể chọn cành bên phải như hình 4.6b.

7.

Error!

Tiến trình cứ tiếp tục như vậy để chèn các nút vào cây TV.

Tổng quát thì có ba bước chính trong việc chèn véctơ mới **v** vào cây TV như sau:

1. *Chọn cành (Branch Selection)*: Khi ta chèn véctơ mới vào cây TV và ta đang ở nút N (với các nút con N_i, 1£ i £ NumChild) thì ta phải xác định nút con nào được chèn khóa.

2. *Phân chia (Splitting)*: Ta sử dụng tiệm cận này khi ta đang ở tại nút lá mà nó đã đầy và không thể chèn thêm véctơ **v**. Bước này đòi hỏi phải bẻ gẫy trong nút hiện hành.

3. *Thu gọn (Telescoping)*: Giả sử nút N được bẻ gẫy thành hai nút con N_1 và N_2. Trong trường hợp này hóa ra rằng mọi véctơ trong *Region(N_1)* phù hợp không chỉ với số chiều tích cực của nút cha N mà phải hơn chút nữa. Việc bổ sung các chiều phụ này được gọi là thu gọn (*telescoping*). Thu gọn còn đòi hỏi huỷ bỏ một số chiều tích cực, ta sẽ xem xét sau.

Chọn cành (Branch Selection)

Error!

Hãy xem xét tình huống nút N với 1£ j £ *NumChild* nút con, gọi chúng là $N_1,...,N_{NumChild}$. Hãy sử dụng ký pháp $exp_j(\mathbf{v})$ để chỉ ra tổng số mà ta phải mở rộng $N_j.Radius$ sao cho khoảng cách tích cực của véctơ **v** từ $N_j.Center$ nhỏ hơn hay bằng (N_j.Center+$exp_j(\mathbf{v})$), có nghĩa rằng:

Trước hết, chúng ta chọn mọi j để $exp_j(\mathbf{v})$ là tối thiểu. Nói cách khác, nếu ta có nút $N_1,...,N_5$ với giá trị *exp* là 10, 40, 19 và 32; hai ứng viên lựa chọn để chèn là N_1, N_4 bởi vì việc mở rộng chúng là tối thiểu. Nếu có ràng buộc thì lấy nút có khoảng cách từ tâm của nút đến **v** là tối thiểu.

Phân chia (Splitting)

Khi ta chèn véctơ **v** vào nút lá N mà nó đã đầy thì ta phải phân chia nút N. Ta phải tạo ra các nút con N_1, N_2 và mỗi véctơ trong nút N phải rơi vào một trong các vùng biểu diễn bởi hai nút con này. Có thể phân chia các véctơ trong nút lá N thành hai nhóm (G_1, H_1). Trong trường hợp này ta gộp mọi véctơ trong G_1 trong vùng với tâm c_1 và bán kính r_1, và mọi véctơ H_1 trong vùng với tâm c_2 và bán kính r_2. Có nhiều cách phân chia như vậy. Ta có thể nói phân chia (G_1, H_1) tốt hơn (G_2, H_2) nếu tổng của các bán kính (r_1+r_1') nhỏ hơn tổng bán kính (r_2+r_2'). Tuy nhiên, điều này chưa đủ để nhận ra phân chia tốt nhất. Nếu có ràng buộc, chúng ta sử dụng tham số khác để phân biệt. Nếu (G_1, H_1) và (G_2, H_2) được phân chia để nhóm này tốt hơn nhóm kia và không có phân chia nào tốt hơn từ mỗi chúng, thì ta nói (G_1, H_1) bảo toàn hơn (G_2,H_2) nếu:

r_1+r_1'-act_dist(c_1,c_1') £ r_2+r_2'-act_dist(c_2,c_2')

Tổng quát thì, phân chia (G, H) là phân chia được lựa chọn nếu

1. không có phân chia (G, H) nào tốt hơn hẳn (G, H) và

2. (G^*, H^*) tốt như (G, H) thì (G^*, H^*) không bảo toàn bằng (G, H).

Thu gọn (Telescoping)

Thu gọn xảy ra trước hết là vì có chèn. Giả sử N là nút nơi ta sẽ chèn véctơ **v**. Chèn véctơ **v** gây ra hai cách thay đổi N: Nó đòi hỏi phân chia N thành hai nút con N_1, N_2; đòi hỏi điều chỉnh tập các chiều tích cực của nút N (nếu véctơ **v** không phù hợp về kích thước tích cực với các véctơ khác lưu trong nút N).

Khi nút N bị phân chia thành hai nút con N_1, N_2, thì tập các véctơ tại nút N_1 hay nút N_2 (nhưng không cả hai) phải là tập con của tập véctơ tại N trước khi chèn. Giả sử N_1 có đặc tính này, thì các véctơ trong N_1 không chỉ phù hợp với các chiều tích cực của N mà phù hợp với một số chiều khác. Trong trường hợp này, ta có thể mở rộng tập các chiều tích cực của nút N bằng cách bổ sung các chiều mới. Hình 4.7 chỉ ra nút N đang được phân chia thành hai nút con N_1, N_2. Mọi véctơ $\mathbf{v}_1,...,\mathbf{v}_r$ trong nútN phù hợp với các chiều tích cực $d_1,...,d_s$, trong đó s<a. Giả sử rằng nút N_1 chỉ chứa véctơ $\mathbf{v}_1,...,\mathbf{v}_w$ và nút N_2 chỉ chứa véctơ $\mathbf{v}_{w+1},...,\mathbf{v}_r$, **v** (**v** là véctơ đang xen vào). Nếu $\mathbf{v}_1,...,\mathbf{v}_w$ không phù hợp với chiều $d_1,...,d_s$, mà cả với chiều khác d_{s+1}, thì ta có thể mở rộng tập các chiều tích cực cho nút N_1 như trên hình 4.7. Sự thật rằng nếu phân chia tốt thì mở rộng thu gọn có thể thực hiện trên cả hai nút N_1 và N_2.

Thu gọn có thể thực hiện khi bổ sung véctơ vào nút N, nhưng không cần phân chia. Nếu N ban đầu chứa véctơ $\mathbf{v}_1,...,\mathbf{v}_r$ và **v** là véctơ đang bổ sung, mặc dù rằng véctơ $\mathbf{v}_i,...,\mathbf{v}_r$ ban đầu phù hợp với các chiều tích cực $d_1,...,d_s$ của nút N, bây giờ chúng chỉ phù hợp với tập con (thí dụ $d_2,...,d_s$). Do vậy, tập các chiều tích cực của nút N phải được rút gọn để phản ánh thực tế.

4.4.3 Tìm kiếm trong cây TV

Việc tìm kiếm véctơ **v** trong cây TV được thực hiện đơn thuần là đảo tiến trình chèn. Khi tìm kiếm tài liệu biểu diễn bởi véctơ **v** trong cây TV gốc T ta thực hiện như sau:

Thuật toán 4.1 Search(T,**V**)

if Leaf(T) then {Return (T.Center=v); Halt}

(* Kiểm tra nếu điểm biểu diễn bởi lá bằng v và cho lại giá trị Boolean*)

else

{if vÎ Region(T) then

Return **Error!**

}

end

Trong thuật toán trên, V là phép OR logíc.

4.4.4 Khai thác láng giềng gần nhất trong cây TV

Cuối cùng, vấn đề quan trọng nhất từ góc nhìn khai thác tài liệu là tìm ra p láng giềng gần nhất. Cho trước truy vấn Q biểu diễn bởi véctơ vec(Q), cây TV gốc T biểu diễn véctơ kết hợp với tập tài liệu và cho trước số nguyên p>0, chúng ta muốn tìm ra p phù hợp nhất trong CSDL tài liệu cho truy vấn Q. Trước khi định nghĩa thuật toán, chúng ta đưa ra quan niệm cơ bản như sau:

Error!

Giả sử N là nút. Hãy gọi *min(N,**v**)* và *max (N,**v**)* là khoảng cách cực tiểu và cực đại của **v** từ điểm trong *Region(N)*. Để có hai con số này thì chỉ việc quan sát *N.Center* và *N.Radius* để xác định điểm trong vùng biểu diễn bởi N gần hay xa từ biểu diễn truy vấn vec(Q). Chúng được tính một cách dễ dàng như sau:

Có thể dễ dàng tính được p láng giềng gần nhất như sau. Duy trì mảng SOL có độ dài p (chỉ số chạy từ 1 đến p). Mục đích là cái phù hợp nhất sẽ đặt trong vị trí SOL[1], tiếp tục đặt trong SOL[2]... Khởi đầu, mảng SOL chứa giá trị giả (thí dụ ¥) không đại diện cho tài liệu nào. Thuật toán *NNSearch* sử dụng đoạn trình gọi là *Insert*, nó lấy véctơ **vec** và mảng SOL theo trình tự không giảm dần của khoảng cách tích cực từ đầu vào **vec**; nói cách khác, nếu 1£ i £ j £ p thì khoảng cách tích cực của SOL[i] từ **vec** nhỏ hơn hay bằng khoảng cách tích cực từ SOL[j] đến **vec**. *Insert* cho lại mảng SOL đã chèn **vec** vào đúng vị trí với phần tử thứ p của SOL làm đầu ra.

Thuật toán 4.2 NNSearch(T,**V**, p)

for i=1 to p do SOL[i]=¥;

NNSearch(T, **v**, p);

end (* end of program NNSearch*)

```
procedure NNSearch(T, v, p);
    if Leaf(T) & act_dist(T.val, v) < SOL[p] then
        Inssert T.val  into SOL;
    else
        {
        if Leaf(T)  then r=0;
        else  { Let N1,...,Nr be the children of T;
            Order the Ni in ascending order with respect to
            min(Ni, v); Let Nn(1),...,Nn(r) be the resulting order;
        };
        done=false; i=1;
        while (( i£r) Ù Ø done) do
            {
            NNSearch(Nn(i), v, p);
            if  SOL[p] < min(Nn(i+1), v)  then
                done =true;
            i = i+1;
        }; (* end of while*)
    Return SOL;
    end proc
```

4.5 Các kỹ thuật truy tìm khác

LSI đã chứng minh là một trong cách hiệu quả nhất của việc chỉ số hoá kho văn bản. Tuy nhiên, còn nhiều kỹ thuật khác, có thể ít hiệu quả hơn, đã được nghiên cứu để cạnh tranh với kỹ thuật LSI.

4.5.1 Chỉ số đảo

Chỉ số đảo là phương pháp được sử dụng rộng rãi trong công nghiệp để chỉ số hoá CSDL tài liệu văn bản. Ý tưởng của chúng đơn giản như sau:

1. Bản ghi tài liệu chứa hai trường: *doc_id* và *postings_list*. Trực quan thì danh sách cột trụ (*posting list*) là danh sách các khái niệm (con trỏ đến khái niệm) xuất hiện trong tài liệu. Rõ ràng, chỉ các khái niệm phù hợp xuất hiện trong danh sách này. Danh sách cột trụ được sắp xếp nhờ thước đo phù hợp.

2. Bản ghi khái niệm (*term record*) bao gồm hai trường tương đương: *term* (xâu) và *postings_list*. Danh sách cột trụ chỉ ra tài liệu nào có các khái niệm trong đó.

3. Hai bảng băm được quản lý là *DocTable* và *TermTable*. *DocTable* được xây dựng bởi băm khoá *doc_id*; *TermTable* có được nhờ băm khóa *term*.

Để tìm mọi tài liệu kết hợp với *term*, ta chỉ việc trả lại danh sách cột trụ. Để tìm mọi tài liệu kết hợp với tập khái niệm, ta chỉ việc thực hiện thao tác *giao* trên các danh sách cột trụ.

Vì danh sách đảo rất dễ cài đặt cho nên chúng được thích nghi trong nhiều hệ thống thương mại như MEDLARS và DIALOG. Tuy nhiên, nó có một số yếu điểm sau: Nó không xem xét thoả đáng đến đồng nghĩa và đa nghĩa. Danh sách cột trụ có thể rất dài, đòi hỏi vùng nhớ lưu trữ khá lớn.

4.5.2 Các tệp dấu hiệu (Signature Files)

Ý tưởng cơ bản của các tệp dấu hiệu là kết hợp dấu hiệu s_d với mỗi tài liệu d. Phát biểu phi hình thức là dấu hiệu là biểu diễn danh sách có trật tự các khái niệm có trong tài liệu.

Danh sách các khái niệm, từ đó s_d được suy diễn, có được sau khi thực hiện phân tích tần số, lấp lỗ và sử dụng danh sách dừng. Giả sử danh sách này bao gồm các từ w_1, ..., w_r. Có nghĩa rằng w_1 là quan trọng nhất khi mô tả tài liệu, từ w_2 quan trọng

thứ hai...Dấu hiệu của tài liệu d là biểu diễn phần nào danh sách này, thông thường đạt được nhờ mã hóa danh sách sau khi băm.

MỤC LỤC

LỜI NÓI ĐẦU

Trong vòng vài năm trở lại đây chúng ta nghe nói rất nhiều đến từ multimedia. Vậy, một cách chính xác, multimedia là gì?

Từ lâu thuật ngữ media dùng để chỉ các thực thể như là chiếc máy truyền thanh, máy truyền hình, nghĩa là không phải nói đến một vật mang thông tin đơn thuần, mà là một hệ thống tương đối phức tạp, có cơ cấu, có đối tượng nhắm tới. Loại truyền thông trực tiếp, từ miệng người này đến tai người kia, không sử dụng thành phần (media) trung gian. Không khí truyền các chấn động âm thanh không phải là một media, mà chỉ là một vật mang vật lý làm công việc tải thông tin.

Nếu dùng một máy cassette audio để ghi lời của người nói, nội dung trong cassette không thể đến người nghe bằng cách truy xuất trực tiếp, phải nhờ đến một hệ thống vật lý khác: máy đọc cassette. Nếu để rời, cassette này chỉ được xem là một vật mang. Nếu gộp cùng máy đọc cassette, thì đấy là một hệ thống truyền thông, một media.

Media có mục đích là phát, truyền thông tin, không đòi hỏi chỉ bằng cách nghe và nhìn. Một tờ giấy in chữ nổi cho người mù, đòi hỏi sự sờ mó. Một tấm carte postale có nhạc và mùi hương, đòi hỏi cùng lúc sự nhìn, nghe và ngửi. Bằng chừng ấy, chúng ta có thể nói đến một sự truyền thông đa phương tiện.

Và như vậy, từ multimedia xuất hiện kèm với nhiều danh từ chung khác: centre de ressource multimedia (trung tâm tài nguyên đa phương tiện), post de formation multimedia (trạm đào tạo đa phương tiện), multimedia training (huấn luyện bằng đa phương tiện), multimedia personal computer MDC (máy tính cá nhân với đa phương tiện), digital multimedia system (hệ thống đa phương tiện dạng số...).

Trong nội dung môn học này chúng ta sẽ nghiên cứu các khái niệm cơ bản về Multimedia, hiểu được các ứng dụng rỗng rãi của Multimedia trong đời sống, các yêu cầu và xu hướng phát triển ứng dụng hiện nay của Multimedia, các cấu trúc thiết kế ứng dụng và các bước cần thiết để xây dựng ứng dụng đa phương tiện, nắm bắt được một số công cụ có sẵn trong thực tế để thiết kế các ứng dụng Multimedia.

CHƯƠNG I: GIỚI THIỆU CHUNG VỀ TRUYỀN THÔNG ĐA PHƯƠNG TIỆN

1.1. Thông tin trong đời sống hiện đại

Khi công nghệ phát triển, người tiêu dùng ngày càng đòi hỏi khắt khe hơn. Trong thời đại của thông tin tốc độ cao, chúng ta mong muốn nhân được các thông tin ngay tức thì và đồng thời, thông qua nhiều cách thức khác nhau. Nhu cầu này giải thích tại sao các kênh tin tức trên truyền hình thường xuyên có các dòng chữ chạy phía dưới màn hình trong khi phát thanh viên nói và các hình ảnh đã thâu băng trước đó trôi qua. Nhu cầu đó giải thích tại sao các Website ngày nay ngoài nội dung và các siêu liên kết còn gồm thêm các hình ảnh đồ hoạ, hoạt ảnh và âm thanh.

Những nhu cầu này đã mở rông cách chúng ta làm việc, hoc tập và giải trí. Nói một cách đơn giản, các thông tin "một chiều" không còn phù hợp với hầu hết chúng ta nữa. Thông tin, các bài học, trò chơi và mua sắm sẽ lôi cuốn hơn và khiến chúng ta chú ý hơn nếu chúng ta có thể tiếp cận và sắp xếp chúng trong các cách thức khác nhau, thâm chí theo một ý thích nào đó mà chúng ta chơt nảy ra. Những nhu cầu này và các tiến bộ về công nghệ đã tương quan mật thiết với nhau để đưa nghệ thuật và khoa học truyền thông đa phương tiện lên một tầm cao mới, dẫn đến kết quả là các sản phẩm có khả năng đan kết văn bản, hình ảnh đồ hoạ, hoạt ảnh, âm thanh và video.

Khi chúng ta sử dụng các sản phẩm này - cho dù là một bộ bách khoa toàn thư trên Web hay một trò chơi video trên CD- thì có nghĩa là chúng ta không đơn thuần chỉ làm việc với một chương trình máy tính. Chúng ta đã trải nghiệm qua một sự kiện truyền thông đa phương tiện. Các sản phẩm truyền thông đa phương tiện ngày nay đều thu hút nhiều giác quan cùng một lúc và đáp ứng với nhu cầu thay đổi của chúng ta với tốc độ ngày càng gia tăng.

Phần dưới đây sẽ giới thiệu cho các bạn các khái niệm cơ bản về truyền thông đa phương tiện và giải thích cách hoạt động của các yếu tố truyền thông đa phương tiện.

1.2. Các khái niệm cơ bản

1.2.1. Thế nào là phương tiện?

Trong suốt chiều dài lịch sử, thông tin đã được chuyển tải thông qua một phương tiện duy nhất. Âm thanh, chẳng hạn như giọng nói của con người, chính là một loại phương tiện đó và qua nhiều thế kỉ trước khi chữ viết được sử dụng rộng rãi thì nói chuyện là một cách thức chủ yếu để trao đổi thông tin. Sau này con người bắt đầu kể chuyện và để lại thông tin về cuộc sống của mình thông qua các hình vẽ, các bức tranh. Sự ra đời của chữ viết đã cho con người một phương tiện khác nữa để diễn đạt ý nghĩ của mình. Ngày nay, con người thường sử dụng lời nói, âm thanh, âm nhạc, văn bản, hình ảnh, đồ hoạ, hoạt ảnh và video để truyền tải thông tin. Những thứ này là tất cả các loại phương tiện khác nhau (thuật ngữ media là số nhiều của medium) và mỗi phương tiện thường được dùng để biểu đạt các loại thông tin nhất định.

Như vậy trong ý nghĩa này, phương tiện chỉ đơn giản là một cách thức để truyền đạt thông tin.

1.2.2. Truyền thông đa phương tiện là gì?

Kể từ lâu con người đã khám phá ra rằng các thông điệp sẽ trở nên tác động hơn (có nghĩa là người nghe sẽ hiểu và nhớ chúng dễ hơn) khi chúng được biểu đạt thông qua một kết hợp của các phương tiện khác nhau. Loại kết hợp này chính là ý nghĩa của thuật ngữ truyền thông đa phương tiện.

Truyền thông đa phương tiện là sử dụng nhiều hơn một loại phương tiện vào cùng một thời điểm

Ví dụ:

- Giáo viên sử dụng bảng đen trong lớp học để viết các lời giải thích cho bài giảng của họ.

Sử dụng phim ảnh, truyền hình kết hợp nhiều loại phương tiện (âm thanh, video, hoạt ảnh, hình ảnh tĩnh và chữ) để tạo ra nhiều loại thông

Formatted: Bullets and Numbering

- điệp khác nhau có khả năng cung cấp thông tin và sự tiêu khiển cho mọi người theo những cách thức độc nhất và đầy ý nghĩa.

Formatted: Bullets and Numbering

1.2.3. Thế nào là một hệ truyền thông đa phương tiện?

Các hệ thống thông tin đa phương tiên dùng nhiều phương tiên giao tiếp khác nhau (văn bản, dữ liệu ghi, dữ liệu số, đồ hoạ, hình ảnh, âm thanh, video..). Nhiều ứng dụng là đa phương tiên theo ý nghĩa là chúng dùng nhiều dang trên. Tuy nhiên, thuật ngữ "đa phương tiện" thường được dùng để mô tả các hệ thống phức tạp hơn, nhất là các hệ thống hỗ trơ hình ảnh và âm thanh. Các thông tin mới chủ yếu được tạo ra bên ngoài máy tính. Lời nói, nhạc, hình ảnh và phim được chuyển từ dang Analog (tương tự) sang Digital (số) trước khi được dùng trong các ứng dụng trong máy tính. Ngược lại, với văn bản, đồ hoạ và thậm chí phim hoạt hình đều được tạo trên máy tính và vì vậy nó chỉ đáp ứng những mục tiêu nhất định, không thể mở rộng ứng dụng được.

Một hệ nền máy tính, mạng thông tin hay dụng cụ phần mềm là một hệ đa phương tiện nếu nó hỗ trợ ứng dụng tương tác cho ít nhất là một trong các dạng thông tin sau, không kể văn bản và đồ hoạ: âm thanh, hình ảnh tĩnh hoặc phim video chuyển động.

1.2.4. Tính tương tác của các chương trình truyền thông đa phương tiện

Ngày nay, công nghệ máy tính đã đưa các sản phẩm truyền thông đa phương tiện trên PC tiến thêm một bước xa hơn. Không giống như sách, phim hay chương trình truyền hình, máy tính có thể nhận dữ liệu nhập từ người sử dụng, do vậy nó có thể chứa các sự kiện truyền thông đa phương tiện tương tác có bao gồm vai trò người sử dụng.

Thuật ngữ tương tác được hiểu là người sử dụng và chương trình phản ứng qua lại với nhau.

Chương trình liên tục cung cấp cho người sử dụng một tập các lựa chọn để cho người sử dụng chọn, nhằm điều khiển các hoạt động của chương trình. Và

thậm chí kiểm soát những gì họ thấy và nghe được. Bằng cách nhận vào dữ liệu nhập vào từ người sử dụng, các phương tiên tương tác tao ra một vòng lặp phản hồi, nói chung hoạt động như sau:

- Bắt đầu vòng lặp người sử dụng kích hoạt chương trình tương tác và chọn thông tin cần xem.
- Chương trình đáp ứng lại bằng cách hiển thị ra cho người sử dụng thông tin với các lựa chọn.
- Người sử dụng đáp ứng bằng cách chọn một lựa chọn, chẳng hạn như di chuyển đến một nơi khác trong chương trình hoặc chọn thông tin khác.
- Chương trình đáp ứng với lựa chọn của người sử dụng và thường đưa ra một tập các tuỳ chọn mới.
- Quá trình tiếp diễn - đôi khi nhịp độ rất nhanh và phức tạp như trong nhiều trò chơi máy tính, cho tới khi người sử dụng ngừng chương trình.

Formatted: Bullets and Numbering

Như vậy, các chương trình truyền thông đa phương tiện được mô tả là có tính tương tác nếu chúng nhận dữ liệu nhập từ người sử dụng và cho phép người sử dụng điều khiển dòng chảy thông tin hoặc hoạt động của chương trình.

1.2.5. Phương tiện mới

Tương tác không chỉ liên quan đến một máy tính và một con chuột. Phương tiên mới (một thuật ngữ bao gồm tất cả các loại công nghệ truyền thông đa phương tiện tương tác) có thể kết hợp nhiều công nghệ truyền thông khác nhau chẳng hạn như truyền hình cáp, các đường dây điện thoại, các mạng riêng, mạng Internet và các công nghệ khác.

Phương tiên mới được tạo ra như một sự hội tụ nhiều loại công nghệ, cho phép các cá nhân riêng lẻ cũng như các tổ chức lớn giao tiếp và truyền đạt thông tin bằng cách sử dụng máy tính và các hệ thống truyền thông.

Phần cốt lõi của phương tiên mới là một khái niệm được gọi là sự hội tụ kỹ thuật số. Người ta dùng các máy tính để tạo ra các loại thông tin kỹ thuật số khác nhau, từ loại chỉ thuần là văn bản đến thông tin video. Tất cả những loại thông tin kỹ thuật số này có thể chuyển đến người sử dụng theo cùng một con đường - có thể

là qua một đĩa CD-ROM, một đường dây truyền hình cáp hay qua đường vệ tinh. Tha vì phải chuyển tải phim ảnh trong các trong các băng hình hay băng video, chuyển tải âm nhạc trên các băng nhạc hay đĩa compact và chuyển tải sách bằng các trang in giờ đây ta có thể chuyển tải các loại thông tin khác nhau đến các máy tính hay hộp truyền hình cáp với cùng một cách thức. Do vậy, ta có một tập hợp các thông tin kết hợp với nhau và hội tụ vào một luồng thông tin kỹ thuật số.

Đối với người sử dụng, công nghệ này có nghĩa là thông tin truyền thông đa phương tiện có thể được lưu trữ và chuyển tải theo nhiều cách. Nếu bạn sử dụng PC, thông tin truyền thông đa phương tiện có thể có trong một đĩa compact, một đĩa DVD, đĩa cứng, mạng Internet hay một dịch vụ trực tuyến. Nếu bạn sử dụng các đặc tính thu tín hiệu truyền hình trong Windows 98, Windows 2000 bạn còn có thể nhận được các thông tin như trên ở dạng thức chương trình phát hình được chuyển đến màn hình của bạn. Nếu bạn sử dụng một dịch vụ chẳng hạn như WebTV, bạn có thể sử dụng đồng thời các chương trình phát hình và thông tin Internet.

Tuỳ theo công nghệ được dùng, một số các sự kiện truyền thông đa phương tiện là những ứng dụng một người sử dụng và chạy đơn độc chẳng hạn như một quyển sách tham khảo hay một chương trình dạy học trên CD-ROM. Các sự kiện khác có thể liên quan nhiều hơn đến một người sử dụng. Ví dụ như các trò chơi nhiều người có thể được truy xuất thông qua một mạng cục bộ hay mạng Internet, các cuộc hội thảo video cho phép những người tham gia nhìn thấy nhau và chia sẻ dữ liệu trong thời gian thực thông qua đường dây điện thoại hay các kết nối vệ tinh hoặc các chương trình truyền hình tương tác nhận các dữ liệu người sử dụng thông qua một Website hay một phòng tán gẫu trên Web.

1.3. Thông tin đa lớp, đa chiều

Các nhà phát triển truyền thông đa phương tiện liên tục cố gắng để tìm ra cách thức làm cho sản phẩm của họ lôi cuốn người sử dụng hơn cho dù sản phẩm đó là một trò chơi hành động nhịp độ cao hay một bản hướng dẫn trên đĩa hoặc một website thương mại điện tử.

Một chiến lược cơ bản trong việc phát triển thông tin truyền thông đa phương tiện là cung cấp thông tin được sắp thành lớp và thông tin đa chiều.

Yêu cầu này có nghĩa là sản phẩm phải cung cấp cho người sử dụng các mảnh thông tin một cách đồng thời, chẳng hạn như một hình ảnh 3 chiều đang quay tròn của một mô tơ, một đoạn âm thanh mô tả các chức năng của nó và các hộp văn bản hiển thị tạm thời về các thông tin thêm khi người sử dụng trỏ chuột vào các phần nhất định của hình mô tơ.

Trong một cách thức trình bày đa chiều, người sử dụng có cơ hội để trải nghiệm các thông tin từ nhiều góc độ khác nhau, ví dụ một người sử dụng nào đó có thể sẽ chỉ xem phần minh hoạ sống động của một dự án tạo cảnh quan, trong khi người sử dụng khác sẽ chọn đọc đoạn văn bản mô tả.

Một trong những cách để khiến cho những văn bản thuần và hình ảnh lôi cuốn người xem là thêm vào các thông tin có yếu tố thời gian chẳng hạn như âm thanh, hoạt hoạ và video. Tuy nhiên, điều quan trọng là ở chỗ các phương tiện thông tin bổ sung không chỉ đơn thuần là lặp lại vai trò của các nội dung và hình ảnh tĩnh. Thực vậy, việc theo dõi một đoạn video chỉ đơn thuần là đọc các đoạn văn trên màn hình là rất nhàm chán. Nhưng nếu cùng với đoạn văn bản đó là phần video hiển thị kèm theo để diễn tả thì nội dung phần văn bản sẽ thú vị hơn rất nhiều.

Ngày càng nhiều các tư liệu giáo dục, bao gồm các cuốn sách giáo khoa, và sách bách khoa toàn thư đang được phát triển thành các sản phẩm truyền thông đa phương tiên. Những sản phẩm này có sử dụng âm thanh, hoạt ảnh và đoạn trích video để làm cho phần nội dung sống động hơn.

Điều cơ bản là ta phải biết tập trung vào nội dung của chương trình. Đó là cái mà người sử dụng cần. Ví dụ, sức lôi cuốn của một bộ phim hoạt hình chính là cở cốt truyện hấp dẫn, cách xây dựng nhân vật tốt. Tương tự, các bộ phim hành động sử dụng công nghệ hoạt ảnh và đồ hoạ máy tính để cải tiến tạo ra các đối tượng hoặc các môi trường trên màn hình chẳng hạn như chuỗi giấc mơ trong phim The Matrix (Ma Trận) sẽ kém hấp dẫn nếu cốt truyện tẻ nhạt.

1.4. Các chuẩn Mutimedia thông dụng

Cần phải đăt ra chuẩn cho tất cả moi cấp đôi của hê đa phương tiên, từ yêu cầu vật lý về mạng cho đến thiết kế giao diện người dùng. Có thể phân loại chuẩn đa phương tiên hiên thời thành chuẩn liên quan đến nôi dung của tài liêu (các chuẩn nén dữ liêu), chuẩn kiểm soát cấu trúc, và chuẩn tương tác.

1.4.1. Chuẩn dành cho kiến trúc tài liệu

1.4.1.1. Ngôn ngữ mô tả cấu trúc và nội dung tài liệu

Ngôn ngữ mô tả cấu trúc và nội dung tài liệu (Standard Generalised Markup Language - SGML) liên quan tới nội dung tài liệu và cấu trúc hợp lý về các khía cạnh như đầu đề và đoạn văn. SGML căn cứ trên quan điểm về định nghĩa dạng tài liệu (DTD). Những định nghĩa này được sử dụng để quản lý việc tạo ra những tài liệu không chỉ sử dụng giới hạn ở những tài liệu có thể in mà còn có thể được sử dụng cho những tài liệu đa phương tiện trên đĩa Compact.

SGML đánh dấu bước chuyển quan trọng trong việc tách thông tin khỏi hình thức trình bày, do đó tạo ra các hình thức trình bày khác nhau của cùng một thông tin.

1.4.1.2. Kiến trúc tài liệu mở (ODA)

Bao gồm hình thức trình bày tài liệu và mở rộng phạm vi nội dung. ODA sử dụng phương pháp tương tự SGML nhưng nhấn mạnh đến trao đổi mờ. Được sử dụng để tạo ra các lớp tài liệu có thể truyền tải giữa các hệ thống máy tính khác nhau mà không làm mất thông tin.

ISO (tổ chức Chuẩn Hoá Quốc Tế) và ITU (Chuẩn Hoá Viễn Thông của Liên Đoàn Viễn Thông Quốc Tế) đã xuất bản ODA dưới dang IS8613 và T.410 Series Recommendation. Những chuẩn này xác định 3 loại tài liệu ODA:

- Tài liệu cấu trúc hợp lý có thể xử lý được (ví dụ: chương, mục, và đoạn bổ xung), cho phép người nhận có thể sửa đổi nội dung.

Formatted: Bullets and Numbering

- Tài liệu đã được định dạng trao đổi cấu trúc trình bày dưới dạng chuỗi trang, với thông tin định vị chẳng hạn khu vực dành cho nội dung ký tự và phông chữ. Không thể sửa đổi được và chỉ in ra được.
- Tài liêu có thể xử lý đã đươc đinh dang cho phép trao đổi cả cấu trúc hợp lý và cấu trúc trình bày, làm cho chúng linh động hơn. Người dùng có thể in ảnh và hiêu chỉnh trước.

Formatted: Bullets and Numbering

ODA hỗ trợ đánh dấu cả cách trình bày và nội dung, kiến trúc tài liệu được tách rời khỏi cấu trúc nội dung. Bảng dưới đây đề cập đến 3 cấu trúc nội dung ký tự, đồ hoa hình, ảnh.

Nội dung	*Chuẩn ISO tương quan*	**Chuẩn ITU tương quan**
Ký tự	Bộ ký tự được mã hoá dành cho truyền thông đa phương tiện thông văn bản (IS6937) Bộ ký tự đồ hoạ mã hoá 8 bit (IS8859)	Ký tự chứa kiến trúc (T.416)
Đồ hoạ hình	Siêu tập tin đồ hoạ máy tính (IS8632)	Kiến trúc chứa ảnh hình học (T.418)
ảnh		Kiến trúc chứa ảnh (T.417)

1.4.1.3. Hytime

Ngôn ngữ cấu trúc tài liêu căn cứ vào thời gian / siêu phương tiên ra đời tháng 11/1992. Dùng để chuẩn hoá một số thiết bi cần thiết trong các ứng dụng siêu phương tiên, đăc biệt là các ứng dung lập đia chỉ các khu vực tài liêu siêu phương tiện và các đối tượng thông tin đa phương tiện thành phần, bao gồm cả việc kết nối, chỉnh hàng và đồng bô hoá. Nó không chuẩn hoá các ký hiêu nội dung dữ liêu,

mã hoá đối tượng thông tin hay xử lý ứng dụng. Hytime cho phép mã hoá theo dòng tuyến tính một ứng dung đa phương tiên hoàn hảo bao gồm cấu trúc, liên kết siêu phương tiện, đồng bộ hoá và định giờ.

Hytime căn cứ trên ngôn ngữ Standard Generralized Markup (SGML) và sử dụng Abstract Syntax Notation 1 (ASN.1), cho phép biểu diễn các chuỗi bit để trao đổi. Nó bổ sung chuẩn cho các đối tượng đa phương tiện đơn lẻ, chẳng hạn JPG cho ảnh tĩnh, MPEG cho tư liêu audiovisual.

1.4.2. Chuẩn dành cho tương tác

- MHEG: đề cập đến các chủ đề như đồng bộ hoá, bộ nhớ đệm, đối tượng nhập.. nó được thiết kế nhằm đáp ứng yêu cầu của ứng dung đa phương tiện chạy trên các trạm từ nhiều hãng khác nhau và trao đổi thông tin theo thời gian thực. Những ứng dụng như thế bao gồm nghiên cứu, hợp tác do máy tính hỗ trợ, hệ xuất bản điện tử và các ứng dụng dùng trong giáo duc đào tao. Chuẩn MHEG được phát triển thành 2 phần:
  - ✓ Phần 1 đề cập đến ghi chú ASN.1
  - ✓ Phần 2 liên quan tới ghi chú trên căn cứ trên SGML.
- SMSL: Ngôn ngữ chuẩn biên soạn siêu phương tiện/đa phương tiện (SMSL) được kết hợp từ ISO và ITU, lien quan đén nhóm nghiên cứu SGML và MHEG. Ngôn ngữ này phát triển script điều khiển tươngtác người dùng với tài liệu siêu phương tiện và đa phương tiện. SMSL được dùng để tạo tính tương thích và tính cơ động giữa các hệ của script đa phương tiện.

Formatted: Bullets and Numbering

1.4.3. Framework và mô hình tham chiếu

Như đã biết, đa phương tiện tác động đến nhiều lĩnh vực phát triển ứng dụng khác nhau. Không tồn tại mô hình tham chiếu đơn nào để kết hợp những mảnh này lai với nhau và xác đinh cách thức chúng giao tiếp nhau.

OII đã khởi xướng nghiên cứu trong lĩnh vực này và đưa ra 3 mô hình tham chiếu hiện có: ODP (Xử lý phân tán mở), mô hình tham chiếu Berkom, Framework và mô hình siêu phương tiện/đa phương tiện (MHMF)

- Xử lý phân tán mở (ODP): ODP là hoạt động kết hợp ISO và ITU có mục tiêu là thúc đẩy các thành phần hệ phân tán hợp tác với nhau trong môi trường đồng nhất. Các chế độ và chuẩn ứng dụng đã được nâng cấp cần phải tương thích với ứng dụng là phương tiên phân tán.
- Mô hình tham chiếu Berkom: Hệ thống truyền thông đa phương tiện thông tin Berkom là dịch vụ cải tiến cho mạng cáp quang. Mô hình này đóng vai trò là nền tảng cho giao diện lập trình ứng dụng. Nó thích hợp cho các ứng dụng đa phương tiện mà có thể di chuyển giữa các hệ khác nhau và cũng hỗ trợ tích hợp các phương tiện khác nhau. Mô hình tham chiếu bao gồm 3 hệ chính:
  - ✓ Hệ hoạt động cung cấp giao diện mạng cho hệ thống trực tiếp đa phương tiện.
  - ✓ Hệ truyền thông đa phương tiện thông cung cấp giao diện lưu thông cho dịch vụ từ xa đa phương tiện.
  - ✓ Hệ ứng dụng chung cung cấp các ứng dụng khác nhau với giao diện trên dịch vụ từ xa đa phương tiện chung.
- Framework và mô hình siêu phương tiện/đa phương tiện (MHMF): MHMF kết hợp từ JTC1 và SC18, làm nền tảng cho việc chuẩn hoá đa phương tiện hiện tại và tương lai. Và hiện vẫn đang được tiếp tục phát triển.

Formatted: Bullets and Numbering

CHƯƠNG II: ỨNG DỤNG CỦA ĐA PHƯƠNG TIỆN TRONG ĐỜI SỐNG

Mặc dù các công nghệ truyền thông đa phương tiện trên PC mới chỉ xuất hiện trong một thời gian tương đối ngắn nhưng chúng ta đã xây dựng được rất nhiều ứng dụng khác nhau: Trong gia đình, trường học, tại nơi làm việc và những nơi khác, các chương trình truyền thông đa phương tiện đều là phần tích hợp trong cách thức mà chúng ta dạy và học, cách chúng ta giao tiếp, quản lý doanh nghiệp và giải trí. Trong chương này chúng ta sẽ tìm hiểu một vài lĩnh vực ứng dụng của công nghệ truyền thông đa phương tiện.

2.1. Truyền thông đa phương tiện trong đào tạo và giáo dục.

2.1.1. Giới thiệu chung

Trong các trường học ngày nay, các máy tính truyền thông đa phương tiện thông đa phương tiện là một phần không thể thiếu của nhiều lớp học và đưa việc học lên một mức độ tương tác mới.

Một hoạt động cải cách chủ yếu trong giáo dục sẽ khuyến khích được cách học tích cực và công tác. Máy tính và truyền thông đa phương tiện sẽ giúp các sinh viên và giảng viên chuyển đổi sang mô hình học tập mới này.

Trong lớp học, các phần trình bày trực quan kết hợp giữa hoạt ảnh, video và âm thanh sẽ thúc đẩy các sinh viên trở thành người tham gia tích cực trong quá trình học. Các chương trình truyền thông đa phương tiện tương tác đưa các khái niệm vào cuộc sống và giúp sinh viên tích hợp phần tư duy cốt lõi và các kỹ năng giải quyết vấn đề.

Bộ bách khoa toàn thư trên CD-ROM là một ví dụ rõ ràng của một ứng dụng truyền thông đa phương tiện tương tác trong ngành giáo dục. Nếu sinh viên phải viết một báo cáo về một vùng nào đó ở Ai Cập thì họ có thể đọc về lịch sử, địa lý

và với một cú nhấp chuột họ có thể thấy các đoạn trích video về sự bận rộn, hối hả trong một thành phố và nghe các đoạn trích của các ngôn ngữ Ai Cập hay bản nhạc địa phương (hình 2.1, 2.2). Kết quả là thông tin đã đi vào cuộc sống và sinh viên thậm chí có thể có các công cụ phần mềm để cho ra các bản báo cáo của họ trong dạng thức của một bản trình chiếu truyền thông đa phương tiện.

Thậm chí trẻ em cũng có thể vừa học vừa vui chơi và chính các sản phẩm truyền thông đa phương tiện trên CD hay trên Internet là những sản phẩm hàng đầu của loại hoạt động này. Bằng cách sử dụng các nhân vật hoạt hình để dẫn đường, các trò chơi truyền thông đa phương tiện chẳng hạn như Reader Rabbit, MathBlaster, JumStart và các chương trình khác có thể giúp học sinh nhỏ làm chủ được các kỹ năng cơ bản trong môi trường tương tác thú vị có cung cấp các phản hồi cá nhân.

Mạng Internet cũng cung cấp một số các công cụ học tập hữu ích ngoài lớp học. Hàng trăm Website hướng về việc học tập cho phép trẻ em tham gia vào các dự án tương tác, câu đố và trò chơi.

- Website www.MaMaMedia.com cho phép trẻ con tạo ra các câu chuyện và câu đố tham gia vào các hoạt động giải quyết vấn đề và chia sẻ các sáng tác của chúng với nhau.
- Một số website cung cấp cơ chế học từ xa (distance learning) như: www.truongthi.com.vn,…Những site này cho phép học viên tham gia vào các lớp, tương tác với người giảng viên, gửi bài tập, dự án, và hoàn tất các kỳ thi trực tuyến.
- Các bộ bách khoa toàn thư trực tuyến:
  www.encarta.com

  www.britannica.com

  www.comptons.com

  www.encyberpedia.com

Formatted: Bullets and Numbering

www.funkandwagnalls.com

www.encyclopedia.com

- Các từ điển trực tuyến:

www.m-v.com

www.onelook.com

www.cup.cam.ac.uk/elt/dictionary/

www.notam.uio.no/~hcholm/altlang/ ..

- Các từ điển đồng nghĩa trực tuyến:

www.thesaurus.com

www.wordsmyth.net

www.links.cs.cmu.edu/lexfn/

- Công cụ tìm kiếm cụm từ:: www.shu.ac.uk/webadmin/phrases/go.html
- Từ điển các từ viết tắt trong tiếng anh: http://www.acronymfinder.com
- Một số site cho phép học trên web như:

www.vovisoft.com

www.quantrimang.com

www.aspvn.net

www.manguon.com

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

2.1.2. Phát triển E-learning trong đào tạo từ xa

Khoảng 2 năm trở lại đây thuật ngữ E-learning bắt đầu được biết đến tại Việt Nam, nhiều hãng, công ty và các trường đại học bắt đầu giới thiệu các sản phẩm E-learning. Điển hình như Cisco với chương trình CCNA/CCNP/CCIE, Intel với mô hình E-learning giới thiệu tại Việt Nam vào tháng 7/2003 và sẽ có khả năng trở thành đối tác chính của Bộ giáo dục- đào tạo trong việc phát triển E-learning trong

thời gian tới, công ty điện toán và truyền số liệu (VDC) kết hợp với Netlearner (Singapo) với dịch vụ đào tạo từ xa bán E-learning khai trương đầu năm 2003, công ty VASC với trang Web: truongthi.com, công ty Hà Thành với trang Web: khoabang.com, FPT với cổng đào tạo trực tuyến,.... Vậy E-learning là gì?, Hệ thống E-learning bao gồm những thành phần gì?; Việc phát triển E-learning trong điều kiện cụ thể của Học viên và các Trung tâm đào tạo như thế nào?.

2.1.2.1. Tổng quát về E-learing

a. Giới thiệu chung

Nhiều nhà chuyên môn cho rằng E-learning - phương pháp giáo dục đào tạo mới được đánh giá là cuộc cách mạng trong giáo dục thế kỷ 21. Theo ông Keith Holtham, Giám đốc phụ trách các giải pháp cho doanh nghiệp khu vực châu Á - Thái Bình Dương (Intel), E-Learning căn bản dựa trên công nghệ mạng ngang hàng (P2P). Đây là giải pháp sử dụng công nghệ cao để hỗ trợ quá trình học tập, cung cấp các dịch vụ đào tạo, khóa học qua mạng Internet hoặc Intranet cho người dùng máy tính. Ưu điểm nổi trội của E-Learning so với các phương pháp giáo dục truyền thống là việc tạo ra một môi trường học tập mở và tính chất tái sử dụng các đơn vị tri thức (learning object). Với công nghệ này, quá trình dạy và học sẽ hiệu quả và nhanh chóng hơn, giúp giảm khoảng 60% chi phí, đồng thời giảm thời gian đào tạo 20-40% so với phương pháp giảng dạy truyền thống. E-learning chuyển tải nội dung phong phú, ấn tượng và dễ hiểu thông qua trang web, bảo đảm chất lượng đào tạo qua những phần mềm quản lý. Mô hình này cho phép học viên cũng như nhân viên tại các công ty chọn học những thứ cần thiết chứ không bó buộc như trước. Bên cạnh đó, học viên có thể học bất cứ lúc nào bằng cách nối mạng mà không cần phải đến trường.

Trên phạm vi toàn cầu hiện nay có nhiều công ty lớn đầu tư vào E-Learning. Năm 2000, thị trường này đã đạt doanh số 2,2 tỷ USD. Người ta dự tính, đến năm 2005, E-Learning trên toàn cầu sẽ đạt tới 18,5 tỷ USD. ở các nước công nghiệp phát triển, điển hình là Mỹ, lĩnh vực này đang phát triển rất nhanh. Thị trường E-Learning ở Mỹ sẽ đạt 11,4 tỷ USD vào năm 2004. Tại châu Á, thị trường này tăng trưởng 25% mỗi năm (đạt 6,2 tỷ USD). Theo số liệu của tập đoàn dữ liệu quốc tế

IDC, năm 2003, thế giới sẽ thiếu khoảng 1,45 triệu chuyên gia mạng, do đó nhu cầu về nguồn nhân lực này ngày càng lớn cùng với mức đô phức tap xung quanh việc thiết kế, triển khai và bảo trì hệ thống mạng máy tính trong nền kinh tế Internet. Chính vì vậy, E-Learning đang được rất nhiều người học quan tâm và theo học.

b. Vậy hiểu một cách chung nhất thì E-learning là gì?

E-learning (electronic learning: Học điện tử): Thuật ngữ bao hàm một tập hợp các ứng dụng và quá trình, như học qua Web, học qua máy tính, lớp học ảo và sự liên kết số. Trong đó bao gồm việc phân phối nội dung các khoá học tới học viên qua Internet, mang intranet/extranet (LAN/WAN), băng audio và video, vê tinh quảng bá, truyền hình tương tác, CD-ROM, và các loại học liệu điện tử khác.

Hình 2.3 mô tả một cách tổng quát khái niệm E-learning. Trong mô hình này, hê thống đào tao bao gồm 4 thành phần, toàn bô hoặc một phần của những thành phần này đươc chuyển tải tới người hoc thông qua các phương tiên truyền thông điện tử.

Hình 2.3: Mô hình E-learning

- Nôi dung: Các nôi dung đào tao, bài giảng đươc thể hiên dưới dang các phương tiên truyền thông điện tử, đa phương tiện. Ví dụ các bài giảng CBT viết bằng toolbookII,…
- Phân phối: Việc phân phối các nội dung đào tạo được thực hiện thông qua các phương tiện điện tử. Ví dụ tài liệu được gửi cho học viên bằng e-mail, học viên học trên website, học qua đĩa CD-Rom multimedia,…
- Quản lý: Quá trình quản lý đào tao đươc thưc hiên hoàn toàn nhờ phương tiện truyền thông điện tử. Ví dụ như việc đăng ký học qua mạng, bằng bản tin nhắn SMS, việc theo dõi tiến độ học tập (điểm danh) được thực hiện qua mạng Internet,..
- Hợp tác: Sự hợp tác, trao đổi của người học trong quá trình học tập cũng được thông qua phương tiện truyền thông điện tử. Ví dụ như việc trao đổi thảo luận thông qua chat, Forum trên mạng,…

Tóm lai E-learning đươc hiểu môt cách chung nhất là quá trình hoc thông qua các phương tiện điện tử.

Formatted: Bullets and Numbering

Ngày nay với sự hội tụ của máy tính và truyền thông E-learning được hiểu một cách trực tiếp hơn là quá trình học thông qua mạng Internet và công nghệ Web.

c. Vài nét về lịch sử E-learning

- Trước năm 1983: Kỷ nguyên giảng viên làm trung tâm. Trước khi máy tính được sử dụng rộng rãi, phương pháp giáo dục "Lấy giảng viên làm trung tâm" là phương pháp phổ biến nhất trong các trường học. Học viên chỉ có thể trao đổi tập trung quanh giảng viên và các bạn học. Đặc điểm của loại hình này là giá thành đào tạo rẻ.
- Giai đoạn 1984-1993: Kỷ nguyên đa phương tiện. Hệ điều hành Windows 3.1, Máy tính Macintosh, phần mềm trình diễn powerpoint đây là các công nghệ cơ bản trong kỷ nguyên đa phương tiện. Nó cho phép tạo ra các bài giảng tích hợp hình ảnh và âm thanh học trên máy tính sử dụng công nghệ CBT phân phối qua đĩa CD-ROM hặc đĩa mềm. vào bất kỳ thời gian nào, ở đâu, người học cũng có thể mua và học. Tuy nhiên sự hướng dẫn của giảng viên là rất hạn chế.
- Giai đoạn : 1994-1999 Làn sóng E-learning thứ nhất

Khi công nghệ Web được phát minh ra, các nhà cung cấp dịch vụ đào tạo bắt đầu nghiên cứu cách thức cải tiếp phương pháp giáo dục bằng công nghệ này. Người thầy thông thái đã dần lộ rõ thông qua các phương tiện: E-mail, CBT qua Intranet với text và hình ảnh đơn giản, đào tạo bằng công nghệ WEB với hình ảnh chuyển động tốc độ thấp đã được triển khai trên diện rộng.

- Giai đoạn : 2000-2005 Làn sóng E-learning thứ hai. Các công nghệ tiên tiến bao gồm JAVA và các ứng dụng mạng IP, công nghệ truy nhập mạng và băng thông Internet được nâng cao, các công nghệ thiết kế Web tiên tiến đã trở thành một cuộc cách mạng trong giáo dục đào tạo. Ngày nay thông qua Web giáo viên có thể kết hợp hướng dẫn trực tuyến (hình ảnh, âm thanh, các công cụ trình diễn) tới mọi người học, nâng cao hơn chất lượng dịch vụ đào tạo. Ngày qua ngày công nghệ Web đã chứng tỏ có khả năng mang lại hiệu quả cao trong giáo dục đào tạo, cho phép đa dạng hoá các môi trường học tập. Tất cả những điều

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

đó tạo ra một cuộc cách mạng trong đào tạo với giá thành rẻ, chất lượng và hiệu quả. Đó chính là làn sóng thứ 2 của E-learning.

d. E-learning có những khác biệt gì so với đào tạo truyền thống?

E-learning khác với đào tạo truyền thống ở ba điểm sau:

- Không bị giới hạn bởi không gian và thời gian: một khoá học E-learning được chuyển tải qua một máy tính tới cho người học, điều này cho phép các học viên có thể linh hoạt lựa chọn khoá học từ một máy tính để bàn hoặc từ một máy tính xách tay với một modem di động chạy pin trên một bãi biển.
- Tính linh hoạt : Một khoá học E-learning được phục vụ theo nhu cầu người học, chứ không nhất thiết phải bám theo một thời gian biểu cố định. Vì thế người học có thể lựa chọn, tham gia khoá học tuỳ theo hoàn cảnh của mình.
- Truy nhập ngẫu nhiên: Bảng danh mục bài giảng sẽ cho phép học viên lựa chọn phần bài giảng, tài liệu một cách tuỳ ý theo trình độ kiến thức và điều kiện truy nhập mạng của mình. Học viên tự tìm ra các kĩ năng học cho riêng mình với sự giúp đỡ của những tài liệu trực tuyến.

Formatted: Bullets and Numbering

Tất nhiên cũng có một số cách học khác. Ví dụ như, các lớp học thông qua trang Web dùng phần mềm hội thảo video trên mạng và các phần mềm khác cho phép các học viên từ xa tham gia một khoá học trên lớp học truyền thống. Một số khoá học trên trang Web theo yêu cầu có giảng viên (hoặc người hướng dẫn) tương tác thường xuyên với từng học viên hoặc với các nhóm học viên.

e. Có nên chuyển đổi sang E-learning hay không?

Trước khi lưu giữ các slide của giảng viên dưới dạng HTML và số hoá lời giảng, chúng ta nên cân nhắc chi phí và lợi ích của việc chuyển đổi này. Để làm điều đó, cần phải xem xét quan điểm của cả hai phía: phía cơ sở đào tạo (hoặc nhà cung cấp dịch vụ đào tạo) và phía người học. Nếu đối với cả phía cơ sở đào tạo và người học, học bằng E-learning có nhiều lợi ích hơn so với bất lợi, thì việc chuyển đổi sang học bằng E-learning có thể là một phương pháp hữu hiệu.

Quan điểm của Cơ sở đào tạo

Cơ sở đào tạo là một tổ chức thiết kế và cung cấp các khóa học trực tuyến E-learning. Đó có thể chỉ là một phòng ban trong công ty khi muốn đào tao nội bộ, hoặc là toàn bộ Trường/Viện/Công ty nếu cơ sở đó bán chương trình đào tạo cho các người học độc lập hoặc cơ sở khác. Hãy thử so sánh ưu và nhược điểm đối với cơ sở đào tạo khi chuyển đổi các khoá học truyền thống sang khoá học E-learning.

Bảng 2.1. Ưu điểm và nhược điểm của E-learning

Ưu điểm	**Nhược điểm**
Giảm chi phí đào tạo. Sau khi đã phát triển xong, một khoá học E-learning có thể dạy 1000 học viên với chi phí chỉ cao hơn một chút so với tổ chức đào tạo cho 20 học viên.	Chi phí phát triển một khoá học lớn. Việc học qua mạng còn mới mẻ và cần có các chuyên viên kỹ thuật để thiết kế khoá học. Triển khai một lớp học E-learning có thể tốn gấp 4 - 10 lần so với một khoá học thông thường với nội dung tương đương.
Rút ngắn thời gian đào tạo. Việc học trên mạng có thể đào tao cấp tốc cho một lượng lớn học viên mà không bị giới hạn bởi số lượng giảng viên hướng dẫn hoặc lớp học.	Yêu cầu kỹ năng mới. Những người có khả năng giảng dạy tốt trên lớp chưa chắc đã có trình độ thiết kế khóa học trên mạng. Phía cơ sở đào tạo có thể phải đào tạo lại một số giảng viên và tìm việc mới cho số còn lại.
Cần ít phương tiện hơn. Các máy chủ và phần mềm cần thiết cho việc học trên mạng có chi phí rẻ hơn rất nhiều so với phòng học, bảng, bàn ghế, và các cơ sở vật chất khác.	Lợi ích của việc học trên mạng vẫn chưa được khẳng định. Các học viên đã hiểu được giá trị của việc học 3 ngày trên lớp có thể vẫn ngần ngại khi bỏ ra một chi phí tương đương cho một khoá học trên mạng thậm chí còn hiệu quả hơn.
Giảng viên và học viên không phải đi lại nhiều.	Đòi hỏi phải thiết kế lại chương trình đào tạo. Việc các học viên không có các kết nối

	tốc độ cao đòi hỏi phía đào tạo phải luôn xây dựng lại các khoá học để khắc phục những hạn chế đó.
Tổng hợp được kiến thức. Việc học trên mạng có thể giúp học viên nắm bắt được kiến thức của giảng viên, dễ dàng sàng lọc, và tái sử dụng chúng.	

Quan điểm của người học

Cá nhân hoặc tổ chức tham gia các khoá học E-learning trên mạng chắc chắn sẽ thấy việc đào tạo này xứng đáng với thời gian và số tiền họ bỏ ra. Bảng dưới đây sẽ so sánh thuận lợi và khó khăn đối với học viên khi họ chuyển đổi việc học tập theo phương pháp truyền thống sang học tập bằng E-learning.

Bảng 2.2: Ưu điểm và nhược điểm của E-learning theo quan điểm của người học

Ưu điểm	Nhược điểm
Có thể học bất cứ lúc nào, tại bất kỳ nơi đâu.	Kỹ thuật phức tạp. Trước khi có thể bắt đầu khoá học, họ phải thông thạo các kỹ năng mới.
Không phải đi lại nhiều và không phải nghỉ việc. Học viên có thể tiết kiệm chi phí đi lại tới nơi học. Đồng thời, họ có thể dễ dàng điều chỉnh thời gian học phù hợp với thời gian làm việc của mình.	Chi phí kỹ thuật cao: Để tham gia học trên mạng, học viên phải cài đặt Turbo trên máy tính của mình, tải và cài đặt các chức năng Plug-ins, và kết nối vào mạng.
Có thể tự quyết định việc học của mình. Học viên chỉ học những gì mà họ cần.	Việc học có thể buồn tẻ. Một số học viên sẽ cảm thấy thiếu quan hệ bạn bè và sự tiếp xúc trên lớp.
Khả năng truy cập được nâng cao. Việc tiếp cận những khoá học trên mạng được thiết kế hợp lý sẽ dễ dàng hơn đối với những người không có khả năng nghe, nhìn; những người học ngoại ngữ hai; và những người không có khả năng học như người bị mắc chứng khó đọc.	Yêu cầu ý thức cá nhân cao hơn: Việc học qua mạng yêu cầu bản thân học viên phải có trách nhiệm hơn đối với việc học của chính họ. Một số người sẽ cảm thấy khó khăn trong việc tạo ra cho mình một lịch học cố định.

Những thuận lợi và khó khăn trên là không tránh khỏi. Với việc chuẩn bị tốt, học viên có thể khắc phục được hầu hết các khó khăn. Nếu chuẩn bị không tốt và việc tổ chức đào tạo bằng E-learning của cơ sở đào tạo chưa được kỹ càng thì học viên sẽ không thấy được những thuận lợi của những khoá học trên mạng. Ví dụ: nếu những bài học không được bố cục rõ ràng và định hướng cụ thể thì việc tự học

sẽ không hứa hẹn điều gì cả. Ngược lại, học viên có thể khắc phục được sự buồn tẻ của việc học trực tuyến bằng cách thảo luận hoặc chat với giảng viên và ban học qua mạng.

2.1.2.2. E-learning và các phương thức đào tạo khác

Nhìn chung các nhà chuyên môn đều cho rằng, trong thế kỷ 21 mô hình đào tạo sẽ bao gồm 3 phương thức: Đào tạo truyền thống, Đào tạo tương tác (Vệ tinh/ISDN/IP), và Đào tạo không tương tác bằng E-learning. Tuỳ theo từng nội dung đào tạo và khả năng tài chính mà các cơ sở đào tạo sẽ sử dụng kết hợp các phương thức đào tạo trong mô hình này ở một mức độ phù hợp.

Bảng2. 3: Các phương thức đào tạo

Phương thức	**Nội dung đào tạo** (Mức độ chuyên môn)	**Số lượng người học**
Đào tạo truyền thống	Cao, phức tạp. Các nội dung đào tạo có tính hàn lâm (dài hạn), chuyên môn cao, đòi hỏi thực tế, thực hành-thực tập, trao đổi thông tin trực tiếp,...	Ít, phải tập trung về cơ sở đào tạo để học tập
Đào tạo từ xa tương tác có giảng viên thông qua truyền hình hội nghị Vệ tinh/ISDN/IP	Trung bình. Các nội dung, chủ đề mang tính phổ cập, giới thiệu, không đòi hỏi trình độ chuyên môn cao, ít thực hành thực tập,... như ở đào tạo không tương tác nhưng đòi hỏi tính chuyên môn cao hơn, cần có sự trao đổi, giải đáp, hướng dẫn của đội ngũ giảng viên và các nhà quản lý.	Nhiều (tới vài trăm học viên/khoá học), học tập trung tại điểm xa cơ sở đào tạo
Đào tạo từ xa không tương tác bằng E-	Trung bình và thấp. Các nội dung, chủ đề mang tính phổ cập, giới thiệu, không đòi hỏi trình độ chuyên môn	Nhiều (tới hàng ngàn học viên), học ở mọi lúc,

learning.	cao, ít thực hành thực tập,... Các nội dung đào tạo phù hợp tốt với khả năng, tự học- tự nghiên cứu thông qua các phương tiện điện tử.	mọi nơi.

2.1.3. Cấu trúc của một hệ thống E-learning điển hình

2.1.3.1. Mô hình chức năng

Mô hình chức năng có thể cung cấp một cái nhìn trực quan về các thành phần tạo nên nôi trường E-learning và những đối tượng thông tin giữa chúng. ADL (Advanced Distributed Learning) - một tổ chức chuyên nghiên cứu và khuyến khích việc phát triển và phân phối học liệu sử dụng các công nghệ mới, đã công bố các tiêu chuẩn cho SCORM (Mô hình chuẩn đơn vị nội dung chia sẻ) mô tả tổng quát chức năng của một hệ thống E-learning bao gồm (hình 2.4).

- Hệ thống quản lý học tập (LMS) như là một hệ thống dịch vụ quản lý việc phân phối và tìm kiếm nội dung học tập cho người học, tức là LMS quản lý các quá trình học tập.
- Hệ thống quản lý nội dung học tập (LCMS): Một LCMS là một môi trường đa người dùng, ở đó các cơ sở đào tạo có thể tạo ra, lưu trữ, sử dụng lại, quản lý và phân phối nội dung học tập trong môi trường số từ một kho dữ liệu trung tâm. LCMS quản lý các quá trình tạo ra và phân phối nội dung học tập.

Hình 2.4: Mô hình chức năng hệ thống E-learning

LMS cần trao đổi thông tin về hồ sơ người sử dụng và thông tin đăng nhập của người sử dụng với các hệ thống khác, vị trí của khoá học từ LCMS và lấy thông tin về các hoạt động của học viên từ LCMS.

Chìa khoá cho sự kết hợp thành công giữa LMS và LCMS là tính mở, sự tương tác. Hình 2.5 mô tả một mô hình kiến trúc của hệ thống E-learning sử dụng công nghệ Web để thực hiện tính năng tương tác giữa LMS và LCMS cung như với các hệ thống khác.

Formatted: Bullets and Numbering

Hình 2.5: Kiến trúc hệ thống E-learning sử dụng công nghệ WEB

Trên cơ sở các đặc tính của dịch vụ Web, người ta thấy rằng các dịch vụ Web có khả năng tối để thực hiện tính năng liên kết của các hệ thống E-learning bởi các lý do sau:

- Thông tin trao đổi giữa các hệ thống E-learning như LOM, gói tin IMS đều tuân thủ tiêu chuẩn XML.
- Mô hình kiến trúc Web là nền tảng và độc lập về ngôn ngữ với E-learning Thông tin trao đổi giữa các hệ thống E-learning như LOM, gói tin IMS đều tuân thủ tiêu chuẩn XML.

Formatted: Bullets and Numbering

2.1.3.2. Mô hình hệ thống

Một cách tổng thể một hệ thống E-learning bao gồm 3 phần chính (hình 2.6):

- Hạ tầng truyền thông và mạng: Bao gồm các thiết bị đầu cuối người dùng (học viên), thiết bị tại các cơ sở cung cấp dịch vụ, mạng truyền thông,...
- Hạ tầng phần mềm: Các phần mềm LMS, LCMS (MarcoMedia, Aurthorware, Toolbook,...)
- Nội dung đào tạo (hạ tầng thông tin): Phần quan trọng của E-learning là nội dung các khoá học, các chương trình đào tạo, các courseware.

Formatted: Bullets and Numbering

Hình 2.6: Mô hình hệ thống E-learning

2.1.3.3. Phát triển nội dung khoá học trong E-learning

Để phát triển E-learning, cần phải song song giải quyết nhiều vấn đề như hạ tầng phần cứng, nhân lực, giảng viên, các phần mềm quản lý học tập (LMS),... và điều quan trọng là phải có được nội dung các khoá học E-learning, một thứ "hàng hoá" trong môi trường đào tạo của nền kinh tế Internet. Phần dưới đây mô tả các phương thức để phát triển nội dung khoá học trong E-learning.

Các cơ sở đào tạo E-learning có thể sử dụng một trong 3 cách dưới đây để phát triển nội dung các khoá học E-learning cho mình.

a. Xây dựng mới toàn bộ

Có thể bao gồm cả việc xây dựng từ đầu các bài giảng truyền thống (bài giảng, giáo trình, sách giáo khoa), sau đó bắt đầu chuyển sang giai đoan chuyển đổi học liệu. Các công việc này có thể bao gồm

- Thiết kế kich bản (giáo án, đề cương)
- Xây dựng các trang hình (hình ảnh tĩnh/động + trang text)
- Xây dựng các đoạn phim (video clip)
- Xây dùng các đoạn âm thanh (audio clip)
- Tích hợp các trang màn hình (tích hợp các loại học liệu thành các đoạn bài giảng hoàn chỉnh)
- Phát triển multimedia (Kết hợp truyền thông đa phương tiện)

Mỗi một quá trình đều cần phải có đội ngũ nhân lực có tính chuyên nghiệp cao và những công cụ phù hợp. Do đó chi phí xây dựng ban đầu là rất lớn cho một chương trình đào tạo có tính hấp dẫn.

b. Mua sản phẩm đã thương mại hoá hoặc đặt hàng

Hiện nay việc mua một sản phẩm đào tạo E-learning bao gồm:

- Mua một khoá học hoặc một chương trình đào tạo với những số lượng User xác định, sau đó sản phẩm đó sẽ được cài đặt tại máy chủ của đơn vị đặt mua.
- Đặt hàng một hãng đã có sản phẩm thương mại hoặc thuê khoán một đơn vị sản xuất một chương trình đào tạo theo đơn đặt hàng.

Để có thể đặt hàng được, hai bên phải tuân theo một tiêu chuẩn nào đó hoặc bên đặt hàng phải đề ra các tiêu chuẩn cho bài giảng E-learning. Mức độ sinh động của bài giảng sẽ quyết định tới giá thành xây dựng bài giảng.

c. Mua lại ý tưởng và chuyển đổi nội dung khoá học cho phù hợp với yêu cầu đào tạo

Đối với một khoá học E-learning, việc thiết kế kich bản (script) là công việc tương đối khó khăn. Nó vừa đòi hỏi tính chuyên môn cao về mặt nội dung (vai trò của giảng viên), vừa đòi hỏi tính kỹ thuật trình bày (vai trò của các chuyên gia máy tính), điều đó trong thực tế chúng ta lại khó có được trong thực tế. Để đơn giản quá

trình này, chúng ta có thể mua chương trình E-learning theo chủ đề đã sẵn có và học làm theo ý tưởng đã có bằng cách :

- Đăng ký theo học trên mạng (học trực tuyến)
- Đăng ký mua sản phẩm đào tao cho 1 User (dang CBT)

Trên cơ sở nội dung các khoá học đã được biết, chúng ta có thể học cách làm và làm lai bằng cách tao mới hoặc chuyển đổi cho phù hợp với yêu cầu của chúng ta (ví dụ như biên tập lại hình ảnh, dịch phần text và audio,...). Cách làm này có thể giảm được thời gian và chi phí so với việc xây dựng mới toàn bộ.

Với cách làm này, sau từ 1-2 năm có thể phát triển được 20-30 khoá học E-learning.

Xem xét trong điều kiện hiên tai của Hoc viên và các trường đại học, viêc sử dụng linh hoạt 3 phương thức trên là tối ưu hơn cả. Ví dụ với các khoá học về công nghệ đã được chuẩn hoá chúng ta sẽ mua mới để sử dụng hoặc biên tập lại, các khoá học về khoa học cơ bản có thể đặt hàng các công ty phần mềm trong nước (như CDIT, VASC, VDC), các khoá học bồi dưỡng nghiệp vu sẽ xây dưng mới.

2.1.4. Kết luận

Đào tạo từ xa được xem là một mô hình giáo dục trong kỷ nguyên thông tin, trong đó E-learning đang được đánh giá là có nhiều ưu thế nhất trong những giải pháp triển khai đào tạo từ xa. Chính vì vậy việc tiếp tục nghiên cứu, tìm hiểu, trao đổi thông tin và thống nhất nhận thức về E-learning để góp phần thúc đẩy sự phát triển E-learning là một việc làm cần thiết và cấp bách.

Một số nhà cung cấp giải pháp E-learing

Sản phẩm hoặc dịch vụ	Nhà cung cấp	Nhận xét
Các khoá học (nội dung): sản phẩm có sẵn, không theo yêu cầu của khách hàng của	www.SkillSoft.com www.Netg.com www.Smarforce.com	Cung cấp nhiều chủ đề

nhà cung cấp duy nhất.		
Các khóa học: sản phẩm có sẵn, không theo yêu cầu của khách hàng của nhiều nhà cung cấp.	www.Elementk.com www.KnowledgePlanet.com www.ThinkQ.com www.Click2learn.com www.Digitallink.com	
Các khoá học hỗn hợp	www.Elementk.com www.Mentergy.com www.Knowledgenet.com	
Khoá học theo nhu cầu khách hàng	www.KnowledgePlanet.com	Rất đắt
Tái sử dụng các nội dung, kiến thức đã có	www.Knowledgemechanics.com www.Learnframe.com	
Các công cu soạn bài giảng: Web site	www.Microsoft.com www.Macromedia.com www.Adobe.com	Tạo và quản lý Website có hỗ trợ đa phương tiên: FrontPage, Dreamweaver, Pagemill
Các công cu soạn bài giảng:Đồ hoạ	www.Macromedia.com www.Adobe.com	Firework Photoshop
Các công cụ soạn bài giảng: Multimedia	www.Macromedia.com www.Click2learn.com www.Apple.com	Authorware DirectorFlash Toolbook

		Quicktime
LMS	www.ThinkQ.com www.Docent.com www.Saba.com www.Learnframe.com www.Geolearning.com www.Digitalthink.com	-
Web hosting	www.Smartforce.com www.Geolearning.com www.Digitalthink.com www.Metergy.com	-
Đánh giá, giám sát, kiểm tra	www.QuestionMark.com www.Zoomerang.com	Đáp ứng nhu cầu khách hàng
Đánh giá (chỉ đánh giá kỹ năng,không có kiểm tra cuối khoá và khảo sát)	www.DDIworld.com www.Digitalthink.com	-
Hội nghị (computer conference)	www.Centra.com www.Mentergy.com www.Interwise.com www.Presenter.com	Hội nghị tương tác, thời gian thực
Sự cộng tác (collaboration)	www.Placeware.com www.Ichat.com www.Mentorware.com	Trao đổi tương tác, thời gian thực
Dịch vụ tư vấn E-	www.Arthurandersen.com	Lưu ý có một số

Learning	www.Accenture.com www.Kpmg.com www.Arthurdlittle.com	công ty có liên kết với nhà cung cấp

2.2. Truyền thông đa phương tiện trong thông tin và bán hàng

Việc các phương tiện như hoạt ảnh, âm thanh và video được đưa vào lĩnh vực thương mại có vẻ như là kỳ cục nhưng xu hướng sử dụng các phương tiện này trong nhiều hoạt động kinh doanh là tất yếu. Các công ty sử dụng các công nghệ phương tiện mới theo nhiều cách để thực hiện các công việc nội bộ cũng như làm việc với khách hàng hiệu quả hơn.

Ví dụ, đào tạo là việc không bao giờ dừng trong các tập đoàn lớn, nhất là khi các công ty mong muốn các nhân viên của mình làm chủ được các công nghệ máy tính mới nhất. Như một sự thay thế hoặc bổ sung cho đào tạo trong các phòng học, nhiều công ty đã triển khai các tư liệu đào tạo tương tác đặc thù. Những tư liệu này rơi vào loại sản phẩm được gọi là sản phẩm đào tạo trên máy tính (Computer Based Training - CBT). Các tập đoàn, công ty đã đầu tư hàng triệu đô la để phát triển các khoá học CBT đặc thù liên quan đến nhiều vấn đề khác nhau chẳng hạn như chính sách của công ty, các hệ thống máy tính tuỳ biến và các quan hệ khách hàng. Nhiều công ty đã sử dụng sản phẩm CBT đặc thù để cho các nhân viên đại diện bán hàng luôn được cập nhật về sự thay đổi liên tục của sản phẩm, dịch vụ và cấu trúc giá – thông tin mang yếu tố quyết định đối với sự thành công của việc bán hàng và quá trình quản lý khách hàng.

Phần mềm dạy học CBT đầu tiên được thiết kế trong đĩa compact vốn rất tiện lợi cho những người làm việc tại công trường và các văn phòng ở xa. Những sản phẩm này có thể gồm các thông tin âm thanh và video cũng như thông tin dạng chữ, thậm chí có thể gồm các cơ chế kiểm tra và đánh giá thời gian thực để đảm bảo rằng người học đã nắm vững các khái niệm hay để đảm bảo rằng các kĩ năng đã được truyền đạt.

Bán hàng và tiếp thị sẽ mang một ý nghĩa mới trong thời đại của công nghệ và truyền thông đa phương tiện. Thông tin trước đây được chuyển tải qua các catalogue dạng bản in thì nay có thể sẽ có trong một catalogue tương tác trên

máy tính và được gửi cho khách hàng ở dạng đĩa CD-ROM hay trưng bày trên Website…

Ở Việt Nam do đặc điểm về phương thức thanh toán bằng tiền mặt nên các hệ thống bán hàng trực tuyến chưa nhiều. Nhưng có thể kể ra một số ví dụ về hệ thống mua bán hàng qua mạng Internet, Vneshop của Việt Nam. Hiện nay hệ thống đang được triển khai tại Trung tâm thông tin - Bộ Thương Mại.

Hình 2.7: Ví dụ về Website thương mại điện tử

Trong một số hệ thống thông tin chẳng hạn trong một viện bảo tàng, hệ thống máy tính truyền thông đa phương tiện ngoài việc nhằm nâng cao hiệu quả, giảm bớt chi phí nhân viên thì còn được sử dụng để phân mục các bộ sưu tập giúp người xem có thể dễ dàng tiếp cận với các hiên vật.

Hay trong du lịch, để giới thiệu, quảng bá các địa danh, danh lam thắng cảnh, những khu di tích, nếu như bằng phương pháp giới thiệu truyền thống là qua các tranh ảnh, ca-ta-lô quảng cáo sẽ không hiệu quả và sát thực, sức lôi cuốn không cao. Thay vào đó là hệ thống giới thiệu đa phương tiện có đầy đủ âm thanh, hình ảnh, cùng các đoạn video thực tế. Trước mắt người xem đồng thời vừa là các đoạn văn bản, hình ảnh, video, vừa là những khúc hát, những lời giới thiệu đặc thù khiến người xem có cảm giác như đang đi du lịch thật.

2.3. Truyền thông đa phương tiện trong y học

Trong y học người ta đã áp dụng xử lý ảnh với việc hình dung và mô phỏng để hoạch định giải phẫu. Điều này giúp các bác sĩ phẫu thuật thực tập được các bước phẫu thuật phức tạp như cắt bỏ khối u não và phẫu thuật định lại cấu trúc não… Bác sỹ phẫu thuật có thể dùng các ảnh này để hoạch định và mô phỏng các bước phẫu thuật. Đối với những bệnh dị dạng về xương thì bác sỹ phẫu thuật có thể thí nghiệm bằng vị trí của mắt, ví dụ như thí nghiệm trên máy tính trước khi phẫu thuật. Các thông tin về cấu trúc mặt và xương bình thường có thể được lưu trữ để làm thông tin tham khảo trong tương lai.

Ngoài việc lên kế hoạch trước khi phẫu thuật, máy tính cũng có thể được kết nối với phòng mổ trong suốt quá trình giải phẫu. Bác sĩ giải phẫu có thể yêu cầu thực hiện mô phỏng một quy trình phẫu thuật do máy tính thực hiện trước khi bắt tay thực hiện giải phẫu cho bệnh nhân. Ví dụ như bác sĩ cũng có thể yêu cầu máy tính cho biết vị trí của một động mạch. Có thể xoay ảnh 3D đến vị trí giống vị trí của đầu bệnh nhân, lúc đó một phần sọ sẽ bị mất và hệ thống máy tính sẽ phóng lớn vùng bệnh tương ứng.

Dưới đây là giới thiệu về bộ tài liệu đa phương tiện của Việt Nam về cấu trúc vùng ben & phẫu thuật Shouldice, trong điều tri thoát vi ben, đã được thực hiện dưới dạng web và được hỗ trợ thêm nhiều phương tiện khác (sách cầm tay, băng video,VCD,SVCD, DVD, CDROM…) chứa thông tin dạng văn bản, hình ảnh tĩnh, phim và âm thanh; thích hợp cho công tác đào tạo huấn luyện kỹ thuật y khoa cho nhiều loại đối tượng khác nhau. Có thể mở rộng việc sản xuất các bộ tư liệu tương tự cho nhiều chuyên đề khác theo mô hình trên.Góp phần hình thành một hệ cơ sở dữ liệu về các kỹ thuật y khoa, ứng dụng khả năng của mạng intranet và internet phục vụ cho việc đào tạo và tự đào tạo trong ngành y tế.

Hình 2.8: Truy cập thông tin văn bản hình ảnh (qua từ 2-3 bước)

Hình 2.9: Truy cập phim minh hoạ

	Phim minh hoạ Phim dược lưu trữ tại máy chủ dưới dang mp4, asf, real… rất nhỏ gon và tải rất nhanh trên internet với dung lương 0,33MB/phút tức khoảng

	20MB/giờ

Hình 2.10: Truy cập khoảng 1000 địa chỉ website liên quan (ở dạng offline)

Hình 2.11: Diễn đàn thảo luận (giúp cán bộ y tế trao đổi thông tin 2 chiều)

Gởi bài viết trả lời thắc mắc, nhận bài viết, thắc mắc

Lớp học trực tuyến: Là lớp học ảo trên mạng với nhiều hình thức kết hợp thông tin như video, giọng nói, chat, bảng minh hoạ công cộng …. Thiết kế để chạy trên môi trường intranet và internet. Mô hình này đã thử nghiệm thành công trên mạng intranet TTĐT&BDCBYT

Bảng công cộng: Mọi thành viên trên mạng đều có thể thao tác , sử dụng để minh hoạ -- Tương tự như sử dụng các công cụ vẽ Paint, PhotoShop, CorelDraw. Hình ảnh tự cập nhật khi có sự thay đổi để mọi người theo dõi

Đàm thoại trực tuyến:

-Bằng văn bản tương tự dịch vụ

chat

-Bằng âm thanh tương tự dịch vụ điện thoại

Chuyển tài liệu bài viết:

Giúp người giảng có thể nhận gởi thông tin
Với các file dạng doc, txt, com, html…

Phim trực tuyến -Dạng ASF

-Có khả năng truyền trực tiếp hình ảnh giảng viên, các cuộc mổ
-truyền các băng video minh hoạ từ đầu máy,VCD.. để giảng dạy

Bộ tài liệu này là kết quả của sự tổng hợp kiến thức từ nhiều nguồn như sách báo, và nhất là internet, đảm bảo cung cấp nguồn thông tin đầy đủ và mới nhất. Hơn nữa, bộ tài liệu được thực hiện dưới sự hướng dẫn của nhiều nhà chuyên môn có kinh nghiệm lâm sàng và nghiên cứu khoa học trong lĩnh vực giải phẫu và phẫu thuật vùng bẹn. Vì thế, bộ tư liệu này có một số ưu điểm như sau:

- Minh họa rõ cấu trúc ống bẹn bằng phim quay xác thật và mô hình 3 chiều.

- Xử lý video hoàn toàn bằng kỹ thuật số trên máy vi tính có trang bị những phần mềm chuyên dụng do đó không cần những máy móc đắt tiền mà vẫn có chất lượng tốt. Kỹ thuật này rất thích hợp giúp cho các nước nghèo sản xuất được những nhiều bộ tài liệu tương tự để phục vụ cho việc đào tạo và tự đào tạo.
- Là bộ tài liệu kỹ thuật đầu tiên trong nước được thực hiện để phổ biến dưới dạng multimedia trên web kết hợp nhiều phương tiện truyền thông khác(tài liệu cầm tay,VCD, SVCD, DVD) tạo hiệu quả cao và phù hợp với nhiều loại đối tượng có sở thích đa dạng và phương tiện khác nhau.
- Bộ tài liệu là bước chuẩn bị kỹ thuật thành công ban đầu cho một hệ cơ sở dữ liệu về các kỹ thuật y khoa trên mạng internet nhằm ứng dụng multimedia cho công tác đào tạo và tự đào tạo của cán bộ y tế, nhất là các cán bô y tế ở vùng sâu vùng xa.

2.4. Truyền thông đa phương tiện trong gia đình

Những người sử dụng trong gia đình có lẽ là những người tiêu dùng nhiều nhất của các sản phẩm truyền thông đa phương tiện. Sự gia đời của mạng Internet, khả năng truy cập đến các chương trình truyền hình tương tác và sự gia tăng các PC truyền thông đa phương tiện giá thành thấp đã cho phép thậm chí là những người mới tập sử dụng máy tính cũng có thể tận dụng sức mạnh của các sản phẩm truyền thông đa phương tiện. Trong gia đình, công nghệ truyền thông đa phương tiện thường được dùng cho các mục đích sau:

- Các tài liệu tham khảo
- Các chỉ dẫn và các tư liệu tự học
- Giải trí

Các sản phẩm truyền thông đa phương tiện tự học và hướng dẫn để người sử dụng tự làm thì có rất nhiều vfa rất đa dạng. Ví dụ, nhiều gia đình có thể sử dụng internet hay một trong các sản phẩm trên đĩa để kết nối đến một công ty đầu tư (chẳng hạn như Prudential) để có các hướng dẫn về việc tạo ra một quỹ đầu tư về hưu. Luc này những công cu tương tác sẽ hỏi các câu hỏi về thu nhập, chi dùng, các mục đích chi tài chính dài hạn và sẵn sàng chấp nhận rủi dro. Sau đó chương

tình sẽ hiển thị một báo cáo vốn đề nghị sự kết hợp đúng đắn của các khoản vốn đầu tư nhằm đáp ứng nhu cầu của khách hàng. Nhiều sản phẩm còn giúp cho các gia đình đầu tư trực truyến, quản lý quỹ đầu tư và đánh giá các khoản vốn đầu tư vào bất kỳ thời điểm nào.

Cho đến hiện giờ, ứng dụng lơn nhất của công nghệ truyền thông đa phương tiện dùng trong thương mại là lĩnh vực giải trí. Các trò chơi video bán trong các hộp đĩa và các CD-ROM dành cho các máy chơi trò chơi chuyên dụng hoặc cho các máy tính để bàn hiện tại rất phổ biến. Dung lượng lưu trữ lớn của các CD-ROM thường cho phép chúng chứa các hoạt ảnh chất lượng cao hơn, các đoạn trích video, các đoạn âm thanh chất lượng kỹ thuật số và nhiều công nghệ trò chơi đa dạng.

Mặc dù các sản phẩm này đã khá tiện lợi, những người tiêu dùng có vẻ như vẫn còn chờ đợi để được trải nghiệm qua loại hình truyền thông đa phương tiện tốt nhất: truyền hình tương tác. Trong những năm gần đây, người ta đã thực hiện một loạt các công việc để làm cho truyền hình trở thành một quá trình hai chiều thay vì là quá trình một chiều vốn đã từng thoả mãn hàng ngàn những người xem truyền hình lười nhác trong nhiều năm trời. Một dạng cơ bản của truyền hình tương tác là cơ chế trả tiền để xem (pay per view). Một hệ thống dùng cáp chỉ cung cấp các dịch vụ trả tiền để xem qua đường dây điện thoại (ví dụ bạn có thể gọi điện thoại và đặt một bộ phim mới ra gần đây) nhưng cơ chế này không có tính tương tác thực sự. Các hệ thống khác chẳng hạn như các hệ thống vệ tinh, các hệ thống khách sạn và các hệ thống trong gia đình đang ngày càng gia tăng cho phép bạn đặt hàng một bộ phim hay một chương trình trả tiền để xem thông qua bộ điều khiển từ xa của bạn hoặc các thiết bị chuyển đổi tín hiệu cáp đặc biệt.

CHƯƠNG III: CÁC YÊU CẦU CỦA HỆ THỐNG ĐA PHƯƠNG TIỆN

3.1. Yêu cầu của ứng dụng đa phương tiện trên máy đơn

Vì khối lượng của các thông tin kỹ thuật số dùng để xây dựng mỗi một giây trong một chương trình là rất nhiều, các nhà chế bản truyền thông đa phương tiện luôn phải xem xét đến thiết bị của người sử dụng - đó là phần cứng mà thông tin sẽ hiển thị trên đó.

Các PC hiện đại thường được gắn đủ tất cả các thành phần truyền thông đa phương tiện cần thiết. Những máy tính này giúp cho người mới học dùng máy tính, hay những người sử dụng máy tính trong gia đình có thể bỏ bớt khoảng thời gian để làm quen ban đầu bởi người sử dụng không phải đối mặt với các vấn đề phần cứng phức tạp chẳng hạn như cấu hình một ổ đĩa CD-ROM, cài đặt một bo mạch âm thanh... Đối với các máy tính cũ hơn có thể ta phải thêm một hay một số thành phần sau để biến một PC thành một PC truyền thông đa phương tiện:

- Sound Card (bo mạch âm thanh)
- Loa
- CD-ROM, DVD drive
- Microphone
- Camera
- Một số thiết bị chuyên dụng khác

Một máy tính truyền thông đa phương tiện cũng cần có đủ sức mạnh xử lý (CPU tốc độ nhanh) và bộ nhớ (RAM) để chứa các chương trình truyền thông đa phương tiện vốn rất thiết bị xử lý và bộ nhớ lớn của máy tính.

Cùng với sự phát triển các ứng dụng truyền thông đa phương tiện, sự gia tăng các tính năng của các máy tính cùng với yêu cầu giảm thiểu chi phí cho người sử dụng, các tổ chức công nghiệp đã đưa ra các yêu cầu về tiêu chuẩn thối thiểu đối với các PC truyền thông đa phương tiện. Và càng ngày các yêu cầu này càng trở nên nghiêm ngặt hơn.

Vào đầu thập niên 90, các công ty phần cứng và phần mềm bắt đầu phát triển tiêu chuẩn máy tính cá nhân truyền thông đa phương tiện (Multimedia Prersonal Computer - MPC) quy định yêu cầu tối thiểu về phần cứng đối với các máy tính cá nhân để được gọi là máy tính có đầy đủ tính năng truyền thông đa phương tiện. Phiên bản cuối cùng của tiêu chuẩn MFC được gọi là MFC mức 3 ra đời năm 1995 quy định cầu hình tối thiểu cho máy tính cá nhân truyền thông đa phương tiện như sau:

- Có ít nhất 8 MB RAM
- Ổ cứng (HDD) 540 MB
- Bộ xử lý (CHIP) 75 MHz
- Một ổ CD-ROM tốc độ 4X và có hỗ trợ các tập tin dạng thức MPEG.

Tuy nhiên ngày nay các PC đều vượt qua cấu hình này khiến cho tiêu chuẩn MPC mức 3 trở nên lỗi thời.

Gần đây các nhà phát triển phần cứng và phần mềm, mà tiêu biểu là Microsoft và Intel tiếp tục phất triển tiêu chuẩn phần cứng cho máy tính cá nhân. Bắt đầu với tiêu chuẩn PC 97, các yêu cầu cấu hình thay đổi tuỳ theo công dụng của PC, ví dụ cấu hình chuẩn cho một PC căn bản thì khác với một PC để giải trí. Các yêu cầu của PC 97 cho một PC căn bản cao hơn các yêu cầu của MPC mức 3:

- Có ít nhất 16 MB RAM
- Vi xử lý (CHIP) 120 MHz
- Có ít nhất một cổng USB

Tiếp theo sau PC 97 là PC 99, nâng mức giới hạn đối với các PC cao hơn nữa:

Đặc tính	**PC cơ bản**	**PC giải trí**

Tốc độ xử lý	300 MHz	300 MHz
RAM	32 MB	64 MB
Số cổng USB tối thiểu	2	2
CD, DVD, Modem hay các thiết bị truyền thông đa phương tiện thông mạng công cộng	Phải có	Phải có
Hỗ trợ bo mạch thông minh (Smart Card)	Phải có	Phải có
Đầu xuất ra TV	Nên có	Nên có
Bộ điều hợp mạng	Nên có	Nên có
Bộ chỉnh tín hiệu truyền hình kỹ thuật tương tự (Analog television)	Nên có	Nên có
Hỗ trợ cho IEEE 1394	Nên có	Nên có

3.2. Chất lượng dịch vụ trong các hệ thống Multimedia

Thuật ngữ "chất lượng của một sản phẩm" sử dụng trong cuộc sống hàng ngày được hiểu một cách đơn giản là mức độ tốt vốn có của sản phẩm. Trong công nghiệp, chất lượng được định nghĩa một cách chính xác hơn là: "sự phù hợp với các yêu cầu khi được đưa vào sử dụng".

Các hệ thống multimedia xử lý dữ liệu liên tục (như là video, âm thanh), và dữ liệu rời rạc được mã hoá (như là đồ hoạ, text), do đó đòi hỏi các hệ thống multimedia phải thoả mãn các yêu cầu về chất lượng dịch vụ nhất định để đáp ứng yêu cầu của người sử dụng. Chất lượng dịch vụ phụ thuộc vào loại phương tiện được sử dụng, khuôn dạng dùng để mã hoá dữ liệu, ứng dụng và loại ứng dụng. Ví dụ, chất lượng dịch vụ của một hội thảo video thì khác so với QoS của một ứng dụng phục hồi dữ liệu video, bởi vì trong một cuộc hội thảo video thì

yêu cầu về thời gian trễ là nhỏ, còn trong ứng dụng phục hồi dữ liệu thì điều này không quá quan trọng.

Mặc khác, các mức hệ thống khác nhau cũng yêu cầu QoS không giống nhau. Ví dụ, trong một hệ thống liên lạc, mô tả QoS ở lớp ứng dụng thường yêu cầu cao hơn so với mô tả QoS ở lớp mạng. Tuy nhiên, các tham số QoS như là băng thông, độ trễ, thì có mặt trong tất cả các lớp.

Để đảm bảo các yêu cầu QoS của các ứng dụng trong các hệ thống multimedia, trước tiên ta cần phải biết được tất cả các tài nguyên mà các ứng dụng sử dụng, bao gồm các tài nguyên xử lý cục bộ và các tài nguyên hệ thống dùng để truyền một luồng media:

- Băng thông
- Các thiết bị vào ra, bao gồm cả các ổ đĩa cứng chứa file hệ thống
- Network adapter và các tài nguyên mạng dùng để truyền các gói dữ liệu giữa các node
- Các CPU dùng để chạy ứng dụng và phần mềm giao thức
- Bộ đệm dùng để lưu trữ phần mềm và dữ liệu

Các tài nguyên đó thường được chia thành 2 loại:

- Tài nguyên động: CPU, bus, network adapter, các hệ thống vào ra, đường truyền..
- Tài nguyên tĩnh: bộ nhớ của các host, các hệ thống trung gian như là router, hoặc switch (xem hình 3.1).

Hình 3.1: Các tài nguyên được sử dụng để truyền một luồng multimedia

Để phân phối một mức QoS cụ thể đến một ứng dụng, hệ thống phải có các tài nguyên phù hợp, và các tài nguyên đó cần có cơ chế quản lý hiệu quả để sẵn sàng phục vụ ứng dụng khi ứng dụng cần sử dụng các tài nguyên đó. Trong nhiều hệ thống máy tính ngày nay, chất lượng và chất lượng của các luồng multimedia bị

hạn chế do thiếu cơ chế quản lý tài nguyên phù hợp dẫn đến sự khan hiếm tài nguyên sử dụng (như trong hình 3.2)

Hình 3.2: Quan hệ tương quan giữa yêu cầu dịch vụ và tài nguyên sẵn có

Qua hình vẽ chúng ta thấy rằng, do sự phát triển về công nghệ, các tài nguyên hệ thống đã dần dần đáp ứng được các yêu cầu của các ứng dụng mới, tuy nhiên vẫn tồn tại sự khan hiếm tài nguyên, do đó việc xây dựng một cơ chế thích hợp để quản lý các tài nguyên là rất cần thiết.

Mặt khác, QoS phần nào phụ thuộc vào nhà cung cấp dịch vụ và người sử dụng dịch vụ. Trong khi người sử dụng dịch vụ muốn sử dụng được nhiều tài nguyên với chi phí thấp nhất có thể, thì nhà cung cấp lại muốn tối thiểu hoá tài nguyên sử dụng và tối đa hoá lợi nhuận thu được. Do đó, để đảm bảo yêu cầu về QoS cũng cần có những thương lượng cần thiết để đảm bảo mục đích chung.

Đặc tả QoS

Mục đích của đặc tả QoS một mặt nhằm cho phép các ứng dụng xây dựng các yêu cầu QoS của chúng, mặt khác các thành phần hệ thống cung cấp QoS chấp nhận đặc tả yêu cầu QoS như là một yêu cầu cho một dịch vụ nhất định. Về mặt bản chất, đặc tả QoS là các khai báo được cho dưới dạng một tập các tham số. Các tham số thường được xem xét bao gồm: (xem hình 3.3)

- Thông lượng
- Độ trễ
- Tỷ lệ lỗi

Trong đặc tả yêu cầu, giá trị của các tham số có thể là:

- Giá trị đơn: xác định mức yêu cầu cụ thể của một tham số
- Một cặp giá trị: đưa ra giá trị tối thiểu có thể chấp nhận được và giá trị kì vọng trung bình của một tham số

- Khoảng giá trị: khoảng nằm giữa giá trị nhỏ nhất và giá trị lớn nhất có thể chấp nhận được của tham số được xét. (minh hoạ trong hình 3.4)

CHƯƠNG ~~H~~IV: MỘT SỐ DỮ LIỆU ĐA PHƯƠNG TIỆN

~~3~~4.1. Ảnh

~~3~~4.1.1. Ảnh và ứng dụng

Hiện tại người ta đòi hỏi các ứng dụng máy tính xử lý nhiều loại ảnh khác nhau trong nhiều ứng dụng khác nhau. Nhu cầu của họ thay đổi tuỳ theo loại ảnh cần hỗ trợ. Ảnh bitonal (trắng và đen) bao gồm văn bản trong các tài liệu kinh doanh như thư từ hay các giấy khổ A4. Thông thường những ảnh này được quét và lưu trữ trong file folder để sử dụng trong các ứng dụng. Công nghệ lưu trữ và quét quang học cũng đang thay thế microform trong hệ quản lý hồ sơ, nơi lưu trữ các tài liệu như bằng sáng chế, báo cáo y khoa, mẫu đơn thuế và báo cáo ngân hàng. Những đề mục nhỏ như biên lai, séc và thẻ tiến dụng được xử lý trong hệ thống sử lý giao dịch khối lượng lớn.

Một loại ảnh bitonal thứ 2, được gọi là line art, bao gồm các đồ hoạ kỹ thuật trong ứng dụng thiết kế được máy tính hỗ trợ (CAD), biểu đồ trong sổ tay kỹ thuật dành cho lĩnh vực quốc phòng và hàng không, lược đồ, lưu đồ, sơ đồ mạch, bản đồ và hoạt hình. Một số tài liệu kinh doanh như đơn từ, là tổng hợp nhiều dòng, văn bản in và menusceript. Để xử lý những ảnh như vậy, cần phải sử dụng hỗn hợp công nghệ nhận dạng và quét.

Ảnh chụp, ảnh nửa tông hoặc khung đơn là các loại ảnh tông liên tục có thang độ xám hoặc mầu. Ảnh thang độ xám chứa đựng nhiều bóng xám. Chúng được sử dụng trong các ứng dụng như dàn trang và các thư viện cho việc biên soạn và phát hành các bài báo hay các ứng dụng về khoa học kỹ thuật như không ảnh, thông tin vệ tinh và dữ liệu về động đất. Thông thường các ứng dụng này yêu cầu ảnh phải có chất lượng cao hơn ảnh hệ thống xử lý tài liệu đã được đề cập trước đó. Chẳng hạn, nhờ vào các ảnh y khoa chụp từ máy quét ảnh cộng hưởng từ MRI và máy

quét chụp cắt lớp bằng tia X dưới sự hỗ trợ của máy tính, các bác sĩ có thể chẩn đoán bệnh từ xa thông qua tia phóng xạ.

Các ứng dụng chuyên biệt được thiết lập riêng cho loại ảnh màu (đa quang phổ) chẳng hạn như sách cũ và bản thảo hiếm ở thư viện hoặc ảnh hội hoạ chất lượng cao cà các đề mục trưng bày trong viện nghệ thuật và viện bảo tàng. Nhu cầu về ảnh chụp có màu trong hệ thống truyền thông đa phương tiện thường ngày như các loại ứng dụng cũng tăng lên. Điển hình là hiện thời, người tiêu dùng và các chuyên gia có thể xử lý và lưu trữ ảnh màu trên đĩa compact ảnh để sau đó hiển thị chúng trên màn hình máy tính hoặc truyền hình. Trong các buổi trình bày trong kinh doanh, các doanh nghiệp có thể sử dụng bộ sưu tập ảnh trên đĩa mềm hoặc CD-ROM.

Ảnh có thể được ứng dụng vào nhiều lĩnh vực hiện đại hơn nữa, tuy nhiên nếu kết hợp giữa ảnh và các công nghệ khác, chẳng hạn như hệ cơ sở tri thức và thuật toán so khớp mẫu –con người sẽ bước vào kỷ nguyên đầy triển vọng hơn và sự kết hợp đó phục vụ cho quá trình điều tra và phát triển, chẳng hạn như dấu tay và ảnh chụp có mục đích nhận diện trong an ninh.

~~3~~4.1.2. Thu ảnh

Thông thường hầu hết các loại ảnh đề cập như trên đều được thu giữ bằng máy chụp hay máy quét quang học có công dụng chuyển đổi ảnh vào mảng điểm hình chữ nhật gọi là các phần tử ảnh (pixels). Hệ quét quang học bao gồm một nguồn sáng, một giá đỡ tài liệu và một bộ dò ánh sáng. Sau mỗi lần chạy, ánh sáng phản xạ được chuyển đổi thành tín hiệu điện, và sau đó sẽ được chuyển đổi dạng số để xử lý và lưu trữ thành mảng phần tử ảnh, kích thước của mảng này phụ thuộc vào loại ảnh được thu:

- Ảnh bitonal chỉ có giá trị cường độ và do đó có thể lưu giữ một bit một phần tử ảnh, với giá trị là 1 hoặc 0.
- Ảnh thang độ xám có nhiều mức xám. Ảnh được lưu giữ trong n bit một phần tử ảnh, nơi mà tổng số độ xám là $2^n - 1$ (ví dụ, 1 ảnh có 15 độ xám + trắng cần được lưu giữ trong 4 bit một phần tử ảnh).

- Cường độ của ba màu chính và màu xám định rõ đặc điểm của ảnh màu. Số lượng màu hiện có trong *n* bit là $2^n - 1$ (ví dụ, cần 8bit một phàn tử ảnh để lưu trữ một ảnh chứa 25màu + trắng).

Kích thước của mảng cũng phụ thuộc vào mật độ, đó là số lượng phần tử ảnh có trong 2,54cm theo một hướng. Thuật ngữ mật độ cũng được dùng để mô tả độ phân giải của máy quét tính theo số lượng điểm trong 2,54cm (dpi). Khi lựa chọn độ phân giải, cần phải xét đến độ phân giải của thiết bị xuất bởi vì chúng có mỗi quan hệ lẫn nhau. Chẳng hạn, độ phân giải của màn hình hiển thị máy tính nằm giữa 70 và 200 dpi, của máy in laze thông thường là 300 dpi, nhưng của máy in offset lên đến 1000 dpi.

Tốc độ thu giữ ảnh cũng thay đổi từ 3 trang A4 trong một phút (đối với loại máy quét để bàn dùng cho máy tính cá nhân) đến 30 trang A4 một phút (đối với loại máy quét tốc độ cao). Loại máy quét như thế thu ảnh của cả những đề mục nhỏ như biên lai, tín dụng hay chi phiếu séc phục vụ cho quá trình xử lý nghiệp vụ. Để thu ảnh, người ta cũng sử dụng loại máy quay số có độ phân giải cao - chẳng hạn như dùng 2 máy camera thu đồng thời nửa phần dưới của tài liệu để đạt tốc độ yêu cầu. Các mảng của thiết bị nạp phát (CCDs) được lắp đặt trong kiểu máy camera như thế.

Đối với loại ảnh có độ phân giải cao (tới 2200x1700) trong lĩnh vực nghệ thuật màu, người ta sử dụng máy quay ảnh hiện có thu giữ, cũng có thu được khung tĩnh từ chuỗi video động bằng bộ số hoá video hay bằng bộ chộp khung. Cần phải lắp đặt các thiết bị đặc biệt để số hoá ảnh quét MRI và CT, giúp cho các bác sĩ có thể chẩn đoán thông qua ảnh quét được hiển thị trên màn hình có độ phân giải cao (2500 x 2000 phần tử có 256 độ xám).

Thiết bị ra ảnh có thể là máy in đen trắng, máy in màu hay máy vẽ (ploter).

Nhìn chung, các hệ thống thu nhận ảnh thực hiện hai quá trình:

- Cảm biến: biến đổi năng lượng quang học (ánh sáng) thành năng lượng điện

- Tổng hợp năng lượng điện thành ảnh

~~3~~4.1.3. Kĩ thuật nén

~~3~~4.1.3.1. Tại sao phải nén

Cần rất nhiều byte để hiển thị một ảnh chưa nén. Lấy một mặt giấy A4 làm ví dụ. Như mô tả ở trên, máy quét có thể thu thông tin trên giấy theo thang độ xám hay bitonal. Sau đó dữ liệu quét thường được lưu giữ tạm thời trên đĩa từ. Bảng 7.1 cho thấy số lượng không gian lưu trữ mà tài liệu này chiếm khi nó được quét với mức độ 200, 300, và 400 dpi.

Bảng 3.1- Yêu cầu lưu trữ của khổ giấy A4 chưa nén

Độ phân giải dpi	Bitonal (Mb)	Thang độ xám (Mb)	Màu sắc (Mb)
200	0.48	1.9 - 7.7	15 – 61
300	1.09	4.4 – 17.4	35 – 140
400	1.93	7.7 – 30.9	62 - 247

Trong đó:

1 tờ giấy A4 có kích thước 210 x 297mm hoặc 8,27 x 11,69mm

Ảnh bitonal cần 1bit / một phần tử

Ảnh thang độ xám cần 4 - 6 bit /1 phần tử ảnh

Ảnh màu cần 32 - 128 bit / 1 phần tử ảnh

Để giảm bớt khoảng không lưu trữ tài liệu, ảnh phải được chuyển đổi sang dạng khác và nhỏ hơn bằng cách loại bỏ những thông tin dư thừa. Nói 1 cách khác,

ảnh cần phải được nén lại để giảm không gian lưu trữ. Một số phương pháp nén ảnh sẽ được trình bày chi tiết trong các phần tiếp theo.

34.1.3.2. Nén ảnh JPEG

Công nghệ nén ảnh JPEG (Joint Photographic Experts Group) là một trong những công nghệ nén ảnh hiệu quả, cho phép làm việc với các ảnh có nhiều màu và kích cỡ lớn. Tỷ lệ nén ảnh đạt mức so sánh tới vài chục lần (chứ không phải phần trăm). Tuy nhiên được cái này bạn phải mất cái khác, đó là quy luật cộng trừ tự nhiên.

Thông thường các ảnh màu hiện nay dùng 8 bit (1 byte) hay 256 màu thay cho từng mức cường độ của các màu đỏ, xanh lá cây và xanh da trời. Như thế mỗi điểm của ảnh cần 3 byte để lưu mã màu, và lượng byte một ảnh màu này chiếm gấp 24 lần ảnh trắng đen cùng cỡ. Với những ảnh này các phương pháp nén ảnh như IFF (Image File Format) theo phương pháp RLE (Run Length Encoding) không mang lại hiệu quả vì hệ số nén chỉ đạt tới 2:1 hay 3:1 (tất nhiên là kết quả nén theo phương pháp RLE phụ thuộc vào cụ thể từng loại ảnh, ví dụ như kết quả rất tốt với các loại ảnh ít đổi màu). Ưu điểm cao của phương pháp này là ảnh đã nén sau khi bung sẽ trùng khớp với ảnh ban đầu. Một số phương pháp nén khác không để mất thông tin như của Lempel - Ziv - Welch (LZW) có thể cho hệ số nén tới 6:1. Nhưng như thế cũng chưa thật đáp ứng yêu cầu đòi hỏi thực tế.

Phương pháp nén ảnh theo thuẩn JPEG có thể cho hệ số nén tới 80:1 hay lớn hơn, nhưng bạn phải chịu mất thông tin (ảnh sau khi bung nén khác với ảnh ban đầu), lượng thông tin mất mát tăng dần theo hệ số nén. Tuy nhiên sự mất mát thông tin này không bị làm một cách cẩu thả. JPEG tiến hành sửa đổi thông tin ảnh khi nén sao cho ảnh mới gần giống như ảnh cũ, khiến phần đông mọi người không nhận thấy sự khác biệt. Và bạn hoàn toàn có thể quản lý sự mất mát này bằng cách hạn chế hệ số nén. Như thế người dùng có thể cân nhắc giữa cái lợi của việc tiết kiệm bộ nhớ và mức độ mất thông tin của ảnh, để chọn phương án thích hợp.

Phương pháp nén ảnh JPEG dựa trên nguyên lý sau: Ảnh màu trong không gian của 3 màu RGB (red Green Blue) được biến đổi về hệ YUV (hay YCBCr) (điều này không phải là nhất thiết, nhưng nếu thực hiện thì cho kết quả nén cao

hơn). Hệ YUV là kết quả nghiên cứu của các nhà sản xuất vô tuyến truyền hình hệ Pal, Secam và NTSC, nhận thấy tín hiệu video có thể phân ra 3 thành phần Y, U, V (cũng như phân theo màu chuẩn đỏ, xanh lá cây và xanh da trời). Và một điều thú vị là hệ nhãn thị của con người rất nhạy cảm với thành phần Y và kém nhạy cảm với hai loại U và V. Phương pháp JPEG đã nắm bắt phát hiện này để tách những thông tin thừa của ảnh. Hệ thống nén thành phần Y của ảnh với mức độ ít hơn so với U, V, bởi người ta ít nhận thấy sự thay đổi của U và V so với Y.

Giai đoạn tiếp theo là biến đổi những vùng thể hiện dùng biến đổi cosin rời rạc (thông thường là những vùng 8 x 8 pixel). Khi đó thông tin về 64 pixel ban đầu sẽ biến đổi thành ma trận có 64 hệ số thể hiện "thực trạng" các pixel. Điều quan trọng là ở đây hệ số đầu tiên có khả năng thể hiện "thực trạng" cao nhất, khả năng đó giảm rất nhanh với các hệ số khác. Nói cách khác thì lượng thông tin của 64 pixel tập trung chủ yếu ở một số hệ số ma trận theo biến đổi trên. Trong giai đoạn này có sự mất mát thông tin, bởi không có biến đổi ngược chính xác. Nhưng lượng thông tin bị mất này chưa đáng kể so với giai đoạn tiếp theo. Ma trận nhận được sau biến đổi cosin rời rạc được lược bớt sự khác nhau giữa các hệ số. Đây chính là lúc mất nhiều thông tin vì người ta sẽ vứt bỏ những thay đổi nhỏ của các hệ số. Như thế khi bung ảnh đã nén bạn sẽ có được những tham số khác của các pixel. Các biến đổi trên áp dụng cho thành phần U và V của ảnh với mực độ cao hơn so với Y (mất nhiều thông tin của U và V hơn). Sau đó thì áp dụng phương pháp mã hóa của Hoffman: Phân tích dãy số, các phần tử lặp lại nhiều được mã hóa bằng ký hiệu ngắn (marker). Khi bung ảnh người ta chỉ việc làm lại các bước trên theo quá trình ngược lại cùng với các biến đổi ngược.

Vì phương pháp này thực hiện với các vùng ảnh (thông thường là 8 x 8 pixel) nên hay xuất hiện sự mất mát thông tin trên vùng biên của các vùng (block) này. Hiện nay người ta đã giải quyết vấn đề này bằng cách làm trơn ảnh sau khi bung nén để che lấp sự khác biệt của biên giới giữa các block. Một hệ nén ảnh theo chuẩn JPEG cùng algorithm làm trơn ảnh đã được công ty ASDG đưa ra trong hệ Art Department Professional.

~~34~~.1.3.3. Nén Fractal

Tất cả các phương pháp nén ảnh đều dựa trên một nguyên lý đơn giản: trong dữ liệu có nhiều phần tử thừa và nén ảnh dựa trên cơ sở tìm ra những phần tử đó và mã hóa chúng. Ví dụ, như số 9999997777 có thể mã hóa thành 6947. Các hình ảnh trên màn hình máy vi tính đặc trưng bởi số điểm (pixel) và số bit dành cho mã mầu của mỗi điểm (bit/pixel).

Phần lớn các hình ảnh (nhất là có độ phân giải cao) không có quy luật giữa các điểm gần nhau, do đó các phương pháp thông dụng hiện nay như biến đổi cosin rời rạc, Wavelet Image Compession (WIC) (theo chuẩn JPEG và MPEG) phải dùng đến biến đổi toán học và xấp xỉ các mối tương quan giữa các pixel. Với các phương pháp nén ảnh Fractal bạn có thể nén ảnh tới tỷ lệ 20:1 - 30:1. Nhưng những ảnh này (vì bị mất thông tin) chỉ là những ảnh gần đúng với ảnh ban đầu, ngoài ra còn có thể xuất hiện biến dạng hình ảnh như đối với phương pháp biến đổi cosin rời rạc.

a. Hình học Fractal và biến đổi Fractal

Một cuộc cách mạng trong vấn đề xử lý ảnh "thế giới thực" đã xảy ra cùng với sự ra đời cuốn sách "Hình học Fractal của tự nhiên" (the Fractal Geometry of Nature) của tác giả Mandelbrot. Theo tác giả, khái niệm Fractal là cấu trúc thể hiện sự gần giống nhau về hình dạng của các hình thể kích cỡ khác nhau. Nếu bạn nghiền một củ khoai tây rán dòn bạn sẽ có vô số những mảnh vỏ lớn nhỏ, các mảnh này có thể gọi là Fractal. Mandelbrot chỉ ra rằng, có thể tìm ra các cấu trúc và qui luật để tạo các hình dạng Fractal, do đó có thể coi Fractal như là các hình cơ bản của hình học phẳng Ơ-cơ-lit cùng với đường thẳng, hình chữ nhật, hình tròn. Fractal không phụ thuộc vào độ phân giải của hình, đó là những hình ảnh nhỏ, có thể vẽ được bằng một bộ hữu hạn thuật toán như quay hình, co dãn, biến đổi từ một hình nào đó. Các phép toán trên thực hiện với các hệ số được gọi là hệ số affin. Một bức tranh có thể được fractal hóa và ta có thể khôi phục nó nhờ các hệ số affin. Trên thực tế đối với các hình rất ngẫu nhiên thì các hệ số affin tìm được rất khó. Trước kia tính bằng tay, người ta phải mất hàng ngày, hàng tuần. Hiện nay công việc đó có thể làm trong 5 phút. Quá trình Fractal hóa đã được hãng

Integrated Systems nghiên cứu và giữ bản quyền. Sau đây là một số bước của quá trình đó.

b. Nén hình ảnh

Chia ảnh thành những vùng không phủ nhau, còn gọi là domen (chẳng hạn bằng các đường thẳng ngang và đứng). Các vùng này phải phủ kín hình ảnh.

Lấy bộ các vùng cơ sở, các vùng này không nhất thiết phủ kín bề mặt bức tranh.

Thực hiện biến đổi Fractal. Với mỗi vùng domen ta tìm vùng cơ sở mà sau biến đổi affin xấp xỉ nhất với domen.

Lưu các hệ số affin vào file. File này gồm 2 phần: đầu file chứa thông tin về vị trí các domen và vùng cơ sở sau đó là bảng các thông số affin cho từng domen.

c. Vẽ lại hình ảnh

Tạo hai hình ảnh cùng cỡ A và B. Cỡ các ảnh này có thể khác với ảnh ban đầu. Các ảnh này có thể là trắng hay đen. Biến đổi các điểm của A vào B. Để làm điều đó trước hết chia B thành các domen như quá trình nén ảnh trên, với mỗi domen của B ta thực hiện biến đổi affin áp dụng với vùng cơ sở A (Các hệ số affin lấy từ file), kết quả có được ta ghi vào B.

Biến đổi giá trị của B vào A giống như lần trước, chỉ có điều đổi vị trí chúng.

Thực hiện biến đổi trên nhiều lần cho đến khi A và B không khác gì nhau.

Quá trình này dẫn đến việc là ta khôi phục được bức tranh ban đầu mà độ chính xác phụ thuộc vào độ chính xác của các biến đổi affin.

Thuật toán quá trình nén và giải nén ảnh được công ty Integrated Systems đưa ra sử dụng số học nguyên cùng các phương pháp làm giảm sự tăng dần của sai số trong các phép toán làm tròn. Các thuật toán đã được tối ưu về mặt thời gian thực hiện. Tuy thế quá trình nén ảnh do phải thực hiện một khối lượng tính toán lớn nên đòi hỏi khá nhiều thời gian so với việc giải nén ảnh. Với máy 386, tốc độ 33 MHz và màn hình VGA các trình thí nghiệm đã thử phim video màu với tốc độ 20 ảnh loại này trong một giây.

d. Những ưu điểm của phương pháp Fractal

Trong quá trình Fractal hóa, bạn sẽ nhận được bộ các chữ số rất nhỏ thể hiện hình ảnh. Do đó hệ số nén của phương pháp là rất lớn, tuy thế chất lượng ảnh sau

khi nén được bảo đảm khá chính xác. Phương pháp rất hiệu quả với những ảnh có độ phân giải cao. Phương pháp này đã được áp dụng không những trong nén dữ liệu mà còn để thể hiện các mối quan hệ giữa các phần tử của các ánh xạ.

~~3~~4.2. Âm thanh

~~3~~4.2.1. Các ứng dụng âm thanh

Âm thanh đóng vai trò quan trọng trong các ứng dụng truyền thông đa phương tiện. Các hiệu ứng đặc biệt của như âm nhạc và tiếng nói có thể được đưa vào các ứng dụng, đặc biệt là các ứng dụng trong hệ thống đào tạo và bán hàng tự động hoặc hệ thống điểm thông tin. Một lời chú thích bằng tiếng nói có thể được dùng để diễn tả những gì đang diễn ra trên màn hình hoặc để làm nổi bật và nhấn mạnh những khái niệm then chốt. Âm thanh có thể được sử dụng kết hợp với hình ảnh tĩnh hoặc động để giải thích cho người sử dụng một ý tưởng hay một quy trình hiệu quả hơn theo cách giải thích chỉ đơn giản bằng văn bản hay đồ hoạ. Âm nhạc có thể được sử dụng để thu hút sự chú ý của khách hàng hoặc để tạo ra được một phong cách riêng biệt.

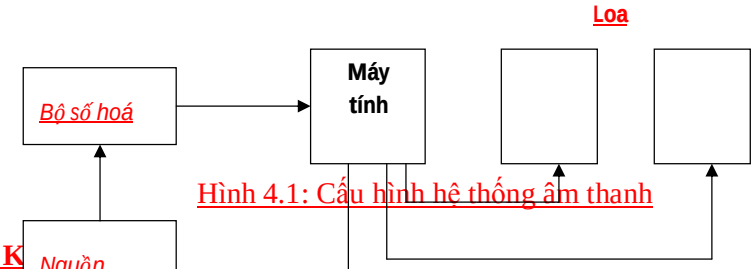
Trong một số lĩnh vực chuyên dụng, tự âm thanh có thể hình thành nên được cốt lõi của một ứng dụng truyền thông đa phương tiện. Chẳng hạn như các hệ thống giúp cho người tàn tật nhìn thấy được. Một dự án mới đây đã đưa đến việc chuyển tải nhật báo đến một thiết bị máy tính đặt tại nhà người sử dụng. Chỉ cần ngồi ở nhà, người sử dụng có thể chọn nghe hệ thống xử lý tiếng nói đọc lớn các bài báo đã được chọn lọc hoặc cho các bài báo đó hiển thị trên màn hình với kiểu chữ lớn. Một khi chi phí giảm và công nghệ được cải tiến thì mối quan tâm của người dùng đến việc sử dụng hệ thống xử lý và nhận dạng tiếng nói trong các ứng dụng kinh doanh nói chung sẽ tăng lên.

~~3~~4.2.2. Ghi âm thanh

Bộ số hoá âm thanh được sử dụng để ghi và số hoá âm thanh tương tự từ băng âm thanh, đĩa ghi, CD-ROM và phiên bản đĩa compact audio gốc hay CD-DA (đĩa

compact âm thanh kĩ thuật số). Có thể dùng micro để thu lại nhạc gốc hoặc sử dụng các nhạc cụ được cài sẵn trong máy tính để soạn nhạc thông qua giao diện MIDI.

Sau khi âm thanh được thu, âm thanh sẽ được lưu trữ ở đĩa cứng hoặc ở môi trường quang học. Nó có thể được hiệu chỉnh và phát lại qua bộ loa nối với máy tính hoặc qua tai nghe. Hiện tại, máy tính có bộ xử lý âm thanh và loa cài sẵn trong máy. Tuy nhiên, hệ thống loa riêng biệt bên ngoài sẽ phát ra âm thanh hay hơn. Nếu nguồn âm thanh là ổ đĩa compact riêng cần phải kết nối với loa (hình ~~3~~4.~~3~~1:)



Hình 4.1: Cấu hình hệ thống âm thanh

4.2.3. K

Do con người dễ nhạy cảm với những thay đổi về chất lượng âm thanh hơn là chất lượng hình ảnh nên đòi hỏi cần phải có các hệ thống truyền thông đa phương tiên để hỗ trơ các chuẩn âm thanh cao. Hiên nay các kĩ thuật dùng để mã hoá thông tin đã được phát triển rất tốt.

Âm thanh được tao ra từ các vi sai áp suất trong không khí. Micro tiếp nhân những vi sai này và phát ra thông qua bộ khuếch đại. Đầu tiên, tín hiệu tương tự này được số hoá bằng bộ chuyển mã tương tự sang tín hiệu số (ADC). Sau đó máy tính lấy mẫu dạng sóng nhập vào theo những khoảng cách đều đặn, rồi sử dụng phương pháp điều biến mã xung (PCM) để chuyển đổi biên độ sang mã nhị phân.

Đối với tiếng nói, tốc độ lấy mẫu là 8kHz và 8 bit – đại diên cho 256 giá tri biên độ khác nhau - được dùng để mã hoá mỗi mẫu. Kĩ thuật giới hạn số lượng như thế này được gọi là phép lượng tử hoá. Phương pháp mã hoá này sẽ tạo ra một dòng dữ liệu âm thanh liên tục 64.000 bit trong một giây (64kbit/s), sau đó được xếp thành từng bó tin để truyền qua mạng. Đối với loại nhạc có chất lượng phát từ đĩa compact, tốc độ lấy mẫu của tín hiệu là 44,1kHz và dùng 16 bit để giải mã mỗi

mẫu. Trong hệ âm thanh nổi, phương pháp mã hoá này sẽ tạo dòng dữ liệu âm thanh liên tục 1,4 triệu bit trong 1 giây.

Việc loại bỏ yên lặng hay dùng các phương pháp mã hoá tốt hơn thì có thể đạt được độ nén cao hơn nữa:

- Phương pháp PCM phi tuyến ấn đinh các điểm giá tri biên độ phi tuyến.
- PCM sai phân mã hoá vi sai của tín hiệu thay chỉ vì mã hoá tín hiệu này. Dãy vi sai thường nhỏ hơn dãy biên độ
- Phương pháp điều biến mã xung không tương ứng (ADPCM) điều chỉnh động dãy giá trị biên độ để tương ứng với dãy biên độ có trong dòng dữ liệu nhập.

Formatted: Bullets and Numbering

43.3. Video

34.3.1. Các ứng dụng video

Các ứng dụng video được chia thành 2 nhóm:

- Nhóm phát lại chất liệu nghe nhìn:
- Nhóm truyền thông nghe nhìn ở thời gian thực

34.3.2. Nén video

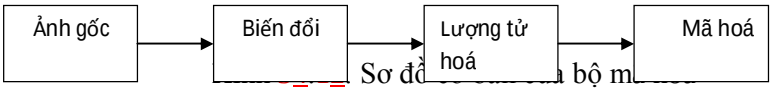
Kỹ thuật nén ảnh số đang đóng một vai trò cực kỳ quan trọng trong các hệ thống viễn thông và multimedia để giải quyết vấn đề băng thông của đường truyền. Các kỹ thuật nén video đều cố gắng làm giảm lượng thông tin cần thiết cho một chuỗi các bức ảnh mà không làm giảm chất lượng của nó đối với người xem. Nói chung, tín hiệu video thường chứa đựng một lượng lớn các thông tin thừa, chúng thường được chia thành hai loại: thừa tĩnh bên trong từng frame (statistical) và thừa động giữa các frame (subjective). Mục đích của nén video là nhằm làm giảm số bit khi lưu trữ và khi truyền bằng cách phát hiện để loại bỏ các lượng thông tin dư thừa này và dùng các kỹ thuật Entropy mã hoá để tối thiểu hoá lượng tin quan trọng cần giữ lại.

Nén dữ liệu được chia thành hai dạng cơ bản: Nén không mất dữ liệu (Lossless) và nén có mất dữ liệu (Lossy). Đối với dạng nén không mất dữ liệu, ảnh

được khôi phục hoàn toàn giống ảnh gốc, tuy nhiên điều này đòi hỏi phải có thiết bị lưu trữ và đường truyền lớn hơn. Các thuật toán của nén không mất dữ liệu thường dựa vào việc thay thế một nhóm các ký tự trùng lặp bởi một nhóm các ký tự đặc biệt khác ngắn hơn mà không quan tâm tới ý nghĩa của dòng bit dữ liệu. Các ví dụ của dạng nén không mất dữ liệu là Run-Length Encoding (RLE), Huffman Coding, Arithmetic coding, Shannon-Fano Coding, LZ78, LZH, LZW....

Đối với dạng nén có mất dữ liệu, ảnh được khôi phục không giống hoàn toàn với ảnh gốc, dạng nén này thích hợp cho việc lưu trữ và truyền ảnh tĩnh, video qua một mạng có băng thông hạn chế. Các dạng nén này thường cho hệ số nén cao hơn, nó liên quan tới việc dùng các phép biến đổi tín hiệu từ miền này sang miền khác. Các ví dụ của biến đổi có mất dữ liệu gồm: Differential Encoding, Discrete Cosine Transform(DCT), Vector Quantization, JPEG (Joint Photographic Experts Group) và MPEG (Motion Picture Experts Group).

Các phương pháp nén ảnh có mất tín hiệu gồm có 4 bước như hình ~~3~~4.~~1~~2.



Sơ đồ [illegible] bộ m[illegible]

Ảnh gốc được biến đổi theo nhiều cách khác nhau. Vào những năm 1980, việc nén và giải nén tín hiệu video dựa trên kỹ thuật DPCM (differential pulse code modulation) đã được CCITT chuẩn hoá theo tiêu chuẩn H.120. Các phương pháp nén dùng DPCM dựa trên nguyên tắc phát hiện sự giống nhau và khác nhau giữa các điểm ảnh (pixels) gần nhau để tìm cách loại bỏ các thông tin thừa. Tuy nhiên, chất lượng ảnh động không đạt được các yêu cầu cần thiết. Để cải thiện chất lượng ảnh động mà không làm tăng số lượng bit so với yêu cầu, kỹ thuật mã hoá chuyển sang dùng các phép biến đổi mà chúng có thể xử lý đồng thời một nhóm các pixels và ta có khái niệm về các bộ mã hoá trên các khối (block-based codecs). Đối với các bộ mã hoá trên các khối ảnh, mỗi điểm ảnh (pixel) sẽ cần ít hơn 1 bit để mã hoá.

Các bộ mã hoá khối có thể dựa trên hai nguyên tắc biến đổi cơ bản: Discrete Cosine Transform (DCT) và Vector Quantization (VQ). DCT được dùng để biến đổi các khối ảnh hai chiều có kích thước 8X8 từ miền không gian sang miền tần số.

Biến đổi DCT là tương tự như biến đổi DFT (Discrete Fourier Trransform). Các hệ số DCT nhận được sẽ được lượng tử hoá (Quantization) và mã hoá (Encode).

Các hệ số DCT nhận được sẽ được lượng tử hoá (Quantisation coding) thành tập các hệ số đơn giản hơn nữa. Mục đích của nó là làm giảm hơn nữa số bit đặc trưng cho một hệ số. Tại bộ mã hoá sẽ có một bảng mã (code book) và bảng các chỉ số nội bộ, từ đó có thể chọn được các từ mã (code word) tương ứng một cách tốt nhất cho tập các hệ số được tạo ra. Quá trình lượng tử hoá cũng đồng thời làm tròn giá trị của các hệ số ở mức nhỏ hơn, đây chính là nguyên nhân gây ra mất tín hiệu, tuy vậy ảnh được khôi phục đạt chất lượng ở mức độ có thể chấp nhận được đối với người xem.

Trong phương pháp VQ, bức ảnh được chia thành các khối có kích thước cố định, một bảng mã (code book) được xây dựng với các chỉ số tương ứng với các khối ảnh này. Như vậy, thay cho việc phải truyền lần lượt các khối của bức ảnh, ta chỉ cần truyền các chỉ số tương ứng của các khối ảnh hoặc chỉ số tương ứng gần đúng nhất so với các khối ảnh cần truyền. Hai phương pháp này cho kết quả không khác nhau nhiều về chất lượng nén ảnh động, tuy nhiên ngày nay biến đổi DCT tỏ ra được ứng dụng rộng rãi hơn trong các sơ đồ nén và giải nén các bức ảnh tĩnh (theo tiêu chuẩn JPEG) và xử lý ảnh động (theo tiêu chuẩn của MPEG).

~~3~~4.3.2.1. Nén tín hiệu ảnh dùng MPEG

MPEG (Moving Picture Expert Group) được ra đời vào năm 1988 nhằm mục đích chuẩn hoá cho nén tín hiệu âm thanh và video. MPEG - 1 có thể nén tín hiệu video tới 1.5Mbit/s với chất lượng VHS và âm thanh lập thể (stereo audio) với tốc độ 192 bit/s. Nó được dùng để lưu trữ video và âm thanh trên CD-ROM.

Vào những năm 1990, MPEG-2 đã ra đời nhằm đáp ứng các tiêu chuẩn nén video cho truyền hình. MPEG-2 có khả năng mã hoá tín hiệu truyền hình ở tốc độ 3-15Mbit/s và truyền hình độ nét cao ở tốc độ tới 15-30Mbit/s. MPEG-2 cho phép

mã hoá tín hiệu video với nhiều mức độ phân giải khác nhau, chúng có khả năng đáp ứng cho nhiều ứng dụng khác nhau. Nhiều thuật toán tương ứng với nhiều các ứng dụng khác nhau đã phát triển và được tập hợp lại thành một bộ tiêu chuẩn đầy đủ của MPEG. Việc áp dụng toàn bộ các đặc điểm của chuẩn MPEG-2 trong tất cả các bộ mã hoá và giải mã là không cần thiết do sự phức tạp của thiết bị cũng như sự tốn kém về dải thông của đường truyền Vì vậy trong hầu hết các trường hợp ta chỉ sử dụng một phần nhất định trong toàn bộ các đặc điểm của chuẩn MPEG-2, chúng thường được gọi là profiles và levels. Một profile sẽ xác định một thuật toán (điều chỉnh bitstream và độ phân giải màu) và một level sẽ xác định một số tiêu chí bắt buộc cho các tham số của bức ảnh (ví dụ như kích thước ảnh và số lượng bit).

MPEG-4 trở thành một tiêu chuẩn cho nén ảnh kỹ thuật truyền hình số, các ứng dụng về đồ hoạ và video tương tác hai chiều (games, videoconferencing) và các ứng dụng multimedia tương tác hai chiều (World Wide Web hoặc các ứng dụng nhằm phân phát dữ liệu video như truyền hình cáp, Internet video...) vào năm 1999. Ngày nay, MPEG-4 đã trở thành một tiêu chuẩn công nghệ trong quá trình sản xuất, phân phối và truy cập vào các hệ thống video. Nó đã góp phần giải quyết vấn đề về dung lượng cho các thiết bị lưu trữ, giải quyết vấn đề về băng thông của đường truyền tín hiệu video hoặc kết hợp cả hai vấn đề trên.

MPEG không phải là một công cụ nén đơn lẻ mà ưu điểm của nén ảnh dùng MPEG chính là ở chỗ MPEG có một tập hợp các công cụ mã hoá chuẩn, chúng có thể được kết hợp với nhau một cách linh động để phục vụ cho một loạt các ứng dụng khác nhau.

Nén MPEG là sự kết hợp hài hoà của bốn kỹ thuật cơ bản: Tiền xử lý (Preprocessing), đoán trước sự chuyển động của các frame ở bộ mã hoá (temporal prediction), bù chuyển động ở bộ giải mã (motion compensation) và mã lượng tử hoá (quatisation coding). Các bộ lọc tiền xử lý sẽ lọc ra những thông tin không cần thiết từ tín hiệu video và những thông tin khó mã hoá nhưng không quan trọng cho sự cảm thụ của mắt người. Kỹ thuật đoán chuyển động dựa trên nguyên tắc là các ảnh trong chuỗi video dường như có liên quan mật thiết với nhau theo thời gian: Mỗi frame tại một thời điểm nhất định sẽ có nhiều khả năng giống với các frame đứng ngay phía trước và ngay phía sau nó. Các bộ mã hoá sẽ tiến hành quét lần

lượt từng phần nhỏ trong mỗi frame gọi là macro blocks, sau đó nó sẽ phát hiện macro block nào không thay đổi từ frame này tới frame khác. Bộ mã hoá sẽ tiên đoán trước sự xuất hiện của các macro blocks khi biết vị trí và hướng chuyển động của nó. Do đó chỉ những sự thay đổi giữa các khối trong frame hiện tại (motion compesated residual) và các khối được tiên đoán mới được truyền tới bên phía thu. Phía bên thu tức bộ giải mã đã lưu trữ sẵn những thông tin mà không thay đổi từ frame này tới frame khác trong bộ nhớ đệm của nó và chúng được dùng để điền thêm một cách đều đặn vào các vị trí trống trong ảnh được khôi phục.

Như chúng ta đều biết, nén tín hiệu video được thực hiện nhờ việc loại bỏ cả sự dư thừa về không gian (spatial coding) và thời gian (temporal coding). Trong MPEG, việc loại bỏ dư thừa về thời gian (nén liên ảnh) được thực hiện trước hết nhờ sử dụng các tính chất giống nhau giữa các ảnh liên tiếp (Inter-frame techniques). Chúng ta có thể sử dụng tính chất này để tạo ra các bức ảnh mới nhờ vào những thông tin từ những ảnh đã gửi trước nó ("predicted"). Do vậy ở phía bộ mã hoá, ta chỉ cần gửi những bức ảnh có thay đổi so với những ảnh trước, sau đó ta lại dùng phương pháp nén về không gian để loại bỏ sự dư thừa về không gian trong chính bức ảnh sai khác này. Nén về không gian dựa trên nguyên tắc là phát hiện sự giống nhau của các điểm ảnh (pixels) lân cận nhau (Intra-frame coding techniques). JPEG chỉ áp dụng phương pháp nén theo không gian vì nó được thiết kế để xử lý và truyền các ảnh tĩnh. Tuy nhiên nén tín hiệu theo phương pháp của JPEG cũng có thể được dùng để nén các bức ảnh một cách độc lập trong dãy tín hiệu video. ứng dụng này thường được gọi là JPEG động (Motion JPEG). Trong một chu kỳ gửi một dãy các bức ảnh theo kiểu JPEG động, ảnh đầu tiên được nén nhờ sự loại bỏ độ dư thừa về không gian, sau đó các ảnh tiếp theo được nén nhờ sự loại bỏ độ dư thừa về thời gian (nén liên ảnh). Quá trình được lặp đi lặp lại cho một dãy các bức ảnh trong tín hiệu video.

Thuật toán nén MPEG cũng dựa trên phép biến đổi DCT cho các khối ảnh 8x8 picxels để tìm ra sự thừa về không gian một cách có hiệu quả giữa các điểm ảnh trong cùng một bức ảnh. Tuy nhiên, trong trường hợp có mối tương quan chặt chẽ giữa các điểm ảnh trong các bức ảnh kế tiếp nhau tức là trong trường hợp hai bức ảnh liên tiếp có nội dung trùng nhau, kỹ thuật Inter-frame coding techniques sẽ

được dùng cùng với việc tiên đoán sự dư thừa về không gian để tạo thành kỹ thuật tiên đoán bù chuyển động giữa các bức ảnh (Motion compesated prediction between frames). Trong nhiều sơ đồ nén MPEG, người ta thường kết hợp cả việc tiên đoán bù chuyển động theo thời gian và phép biến đổi thông tin theo không gian để đạt hiệu quả nén cao (Hybrid DPCM/DCT coding of video).

Hầu hết các sơ đồ nén MPEG đều dùng kỹ thuật lấy mẫu bổ xung (Subsampling) và lượng tử hoá (Quantization) trước khi mã hoá. Lấy mẫu bổ xung nhằm mục đích để làm giảm kích thước bức ảnh đầu vào theo cả theo chiều ngang và chiều dọc, như vậy sẽ giảm số lượng các điểm ảnh trước mã hoá. Cũng nên nhớ rằng trong một số trường hợp người ta còn lấy mẫu bổ xung theo thời gian để làm giảm số lượng các bức ảnh trong dãy ảnh trước khi mã hoá. Đây được xem như là một kỹ thuật rất cơ bản nhằm loại bỏ sự dư thừa dựa vào khả năng lưu ảnh của mắt người cảm thụ. Thường thường, chúng ta có thể phân biệt sự thay đổi về độ sáng của ảnh (changes in Brightness) tốt hơn so với sự thay đổi về màu (Chromaticity changes). Do đó trước hết các sơ đồ nén MPEG sẽ tiến hành chia bức ảnh thành các thành phần Y (Luminance hay brightness plane) và UV (Chrominance hay color planes) tức là một thành phần về độ sáng và hai thành phần về độ màu. Các tín hiệu video thành phần này sẽ được lấy mẫu (samples) và số hoá (digitised) để tạo nên các điểm ảnh rời rạc theo tỷ lệ 4 : 2 : 2 và 4 : 2 : 0.

Kỹ thuật tiên đoán bù chuyển động được sử dụng như là một trong những công cụ mạnh để làm giảm sự dư thừa về không gian giữa các bức ảnh. Khái niệm về bù chuyển động là dựa trên sự phán đoán hướng chuyển động của các bức ảnh tức là các ảnh thành phần trong dãy video sẽ được thay thế gần đúng. Kỹ thuật tiên đoán bù chuyển động giữa các bức ảnh được xem như là biện pháp để hạn chế bớt các thông số của chuyển động bởi việc dùng các vector chuyển động để mô tả sự dịch chuyển của các điểm ảnh. Kết quả tiên đoán tốt nhất của một điểm ảnh là dựa trên sự tiên đoán bù chuyển động từ một bức ảnh đã mã hoá được truyền phía trước của nó. Cả hai thông số, sai số chuyển động (biên độ) và các vectors chuyển động (hướng chuyển động) đều được truyền tới phía bên nhận. Tuy nhiên do có mối quan hệ tương quan chặt chẽ giữa các điểm ảnh về không gian (trùng về không

gian), một vector chuyển động có thể được dùng cho một khối các điểm ảnh gồm các pixels lân cận nhau (MPEG -1 và MPEG -2 dùng các khối 16 x16 pixels).

Trong MPEG-2, có nhiều phương pháp để tiên đoán sự chuyển động. Ví dụ một khối ảnh có thể được tiên đoán xuôi từ những ảnh đã được truyền trước nó (Forward Predicted), có thể đoán ngược từ những ảnh truyền sau nó (Backward Predicted) hoặc theo cả hai chiều (Bidirectionally Predicted). Các phương pháp dùng để tiên đoán các khối trong cùng một ảnh cũng có thể không giống nhau, chúng có thể thay đổi từ khối nọ sang khối kia. Hơn nữa, hai trường (fields) trong cùng một khối cũng có thể được tiên đoán theo hai cách khác nhau dùng các vector độc lập nhau hoặc chúng có thể dùng chung một vector. Đối với mỗi khối ảnh, bộ mã hoá sẽ chọn các phương pháp tiên đoán thích hợp, cố gắng đảm bảo chất lượng ảnh tốt nhất khi được giải mã trong điều kiện yêu cầu khắt khe về số bit. Các thông số liên quan tới chọn phương pháp tiên đoán cũng được truyền tới bộ giải mã cùng với dự đoán sai số nhằm khôi phục gần chính xác ảnh gốc.

Trong MPEG, có 3 kiểu ảnh khác nhau được dùng để mã hoá cho các khối ảnh. Kiểu ảnh ‘Intra’ (I-pictures) là ảnh được mã hoá một cách độc lập mà không cần tham khảo tới các ảnh khác. Hiệu quả nén tín hiệu đạt được do loại bỏ sự thừa về không gian mà không có yếu tố thời gian tham gia vào quá trình. I-pictures được dùng một cách tuần hoàn để tạo thành các điểm tựa cho dòng dữ liệu trong quá trình giải mã.

Ảnh ‘Predictive’ (P-pictures) có thể sử dụng các ảnh I hoặc P ngay sát phía trước nó để bù chuyển động và chính nó cũng có thể được dùng để tham khảo cho việc tiên đoán các ảnh khác tiếp theo. Mỗi khối ảnh trong P-picture có thể hoặc được mã theo kiểu tiên đoán (predicted) hoặc được mã một cách độc lập (intra-coded). Do sử dụng cả nén theo không gian và thời gian, hiệu quả nén của P-pictures được tăng lên một cách đáng kể so với I-pictures.

Ảnh ‘Bidirectionally-Predictive’ pictures hay B- Pictures có thể sử dụng các ảnh I hoặc P phía trước hoặc phía sau nó cho việc bù chuyển động và do vậy cho kết quả nén cao nhất. Mỗi khối trong B-pictures có thể được tiên đoán theo chiều ngược, xuôi, cả hai hướng hoặc được mã một cách độc lập. Để có thể tiên đoán

ngược từ một bức ảnh phía sau nó, bộ mã hoá sẽ tiến hành sắp xếp lại các bức ảnh

từ thứ tự xuất hiện một cách tự nhiên sang một thứ tự khác của các ảnh trên đường truyền. Do vậy từ đầu ra của bộ mã hoá, B-pictures được truyền sau các ảnh dùng để tham khảo ở phía trước và phía sau của nó. Điều này sẽ tạo ra độ trễ do phải sắp xếp lại thông tin, độ trễ này lớn hay nhỏ là tuỳ thuộc vào số các bức ảnh B-pictures liên tiếp nhau được truyền.

Các ảnh I, P, B-pictures thường xuất hiện theo một thứ tự lặp đi lặp lại một cách tuần hoàn, do đó ta có khái niệm về nhóm các bức ảnh GOP (Group of Pictures). Một ví dụ của GOP ở dạng ảnh tự nhiên xuất hiện theo thứ tự như sau:

B_1 B_2 I_3 B_4 B_5 B_7 B_8 P_9 B_{10} B_{11} P_{12}

Thứ tự xuất hiện của chúng trên đường truyền bị thay đổi do sự sắp xếp lại của bộ mã hoá như sau:

I_3 B_1 B_2 P_6 B_4 B_5 P_9 B_7 B_8 P_{12} B_{10} B_{11}

Cấu trúc của một GOP có thể được mô tả bởi hai tham số: N là số các ảnh trong GOP và M là khoảng cách giữa các ảnh P-pictures. Nhóm GOP này được miêu tả như N = 12 và M = 3.

~~3~~4.3.2.2. Sơ đồ của bộ mã hoá và giải mã dùng MPEG-2

Sơ đồ bộ mã hoá và giải mã MPEG 2 được trình bày trên hình ~~3~~4.~~3~~2.

a. Mã hoá MPEG-2

Quá trình mã hoá cho P pictures và B pictures được giải thích như sau:

Dữ liệu từ các khối ảnh (macroblocks) cần được mã hoá sẽ được đưa đến cả bộ trừ (Subtractor) và bộ đoán chuyển động (Motion Estimator). Bộ đoán chuyển động sẽ so sánh các khối ảnh mới được đưa vào này với các khối ảnh đã được đưa vào trước đó và được lưu lại như là các ảnh dùng để tham khảo (Reference Picture). Kết quả là bộ đoán chuyển động sẽ tìm ra các khối ảnh trong ảnh tham khảo gần giống nhất với khối ảnh mới này. Bộ đoán chuyển động sau đó sẽ tính toán vector chuyển động (Motion Vector), vector này sẽ đặc trưng cho sự dịch chuyển theo cả hai chiều dọc và ngang của khối ảnh mới cần mã hoá so với ảnh tham khảo. Chúng ta lưu ý rằng vector chuyển động có độ phân giải bằng một nửa do thực hiện quét xen kẽ.

Bộ đoán chuyển động cũng đồng thời gửi các khối ảnh tham khảo này mà chúng thường được gọi là các khối tiên đoán (Predicted macroblock) tới bộ trừ để trừ với khối ảnh mới cần mã hoá (thực hiện trừ từng điểm ảnh tương ứng tức là Pixel by pixel). Kết quả là ta sẽ được các sai số tiên đoán (Error Prediction) hoặc tín hiệu dư, chúng sẽ đặc trưng cho sự sai khác giữa khối ảnh cần tiên đoán và khối ảnh thực tế cần mã hoá.

Tín hiệu dư hay sai số tiên đoán này sẽ được biến đổi DCT, các hệ số nhận được sau biến đổi DCT sẽ được lượng tử hoá để làm giảm số lượng các bits cần truyền. Các hệ số này sẽ được đưa tới bộ mã hoá Huffman, tại đây số bits đặc trưng cho các hệ số tiếp tục được làm giảm đi một

cách đáng kể. Dữ liệu từ đầu ra của mã hoá Huffman sẽ được kết hợp với vector chuyển động và các thông tin khác (thông tin về I, P, B pictures) để gửi tới bộ giải mã.

Hình ~~3~~4.~~2~~3: Sơ đồ bộ mã hoá và giải mã dùng MPEG

Đối với trường hợp P-pictures, các hệ số DCT cũng được đưa đến bộ giải mã nội bộ (nằm ngay trong bộ mã hoá). Tín hiệu dư hay sai số tiên đoán được biến đổi ngược lại dùng phép biến đổi IDCT và được cộng thêm vào ảnh đứng trước để tạo nên ảnh tham khảo (ảnh tiên đoán). Vì dữ liệu ảnh trong bộ mã hoá được giải mã luôn nhờ vào bộ giải mã nội bộ ngay chính bên trong bộ mã hoá, do đó ta có thể thực hiện thay đổi thứ tự các bức ảnh và dùng các phương pháp tiên đoán như đã trình bày ở trên.

b. Giải mã MPEG-2

Quá trình khôi phục lại ảnh tại bộ giải mã là hoàn toàn ngược lại. Từ luồng dữ liệu nhận được ở đầu vào, vector chuyển động được tách ra và đưa vào bộ bù chuyển động (Motion Compensator), các hệ số DCT được đưa vào bộ biến đổi ngược IDCT để biến tín hiệu từ miền tần số thành tín hiệu ở miền không gian. Đối với P pictures và B pictures, vector chuyển động sẽ được kết hợp với các khối tiên đoán (predicted macroblock) để tạo thành các ảnh tham khảo.

CHƯƠNG ~~I~~IV: XÂY DỰNG ỨNG DỤNG ĐA PHƯƠNG TIỆN

5.1. C-ác y-êu khi xây dựng một ứng dụng đa phương tiện

Để có được và giữ được sự chú ý của người sử dụng và để cạnh tranh với các sản phẩm khác, một chương trình truyền thông đa phương tiên phải có 3 đặc điểm sau:

- Thông tin, diễn tiến và một "cốt truyện" có khả năng "thúc ép" người sử dụng phải tương tác với chương trình.
- Một tập hợp nhiều loại phương tiện gắn bó với nhau được sắp xếp khéo léo và liền lạc.
- Cơ chế điều hướng linh hoạt, do vậy cho phép người sử dụng duyệt vòng quanh nếu muốn hoặc thâm chí điều chỉnh lai dòng thông tin.

Formatted: Bullets and Numbering

Kết quả là việc tạo ra các sản phẩm truyền thông đa phương tiện hữu hiệu có thể là một quá trình đầy thách thức.

Để bao quát tất cả mọi vấn đề cơ bản, một nhóm phát triển truyền thông đa phương tiện thường gồm nhiều người với những kĩ năng khác nhau gắn với một quá trình phát triển phức tạp nhưng được hoạch định tốt. Các thành viên tham gia một dự án sẽ được trình bày chi tiết trong phần tiếp theo.

45.2. Các thành viên tham gia dự án

Các thành viên tham gia dự án bao gồm:

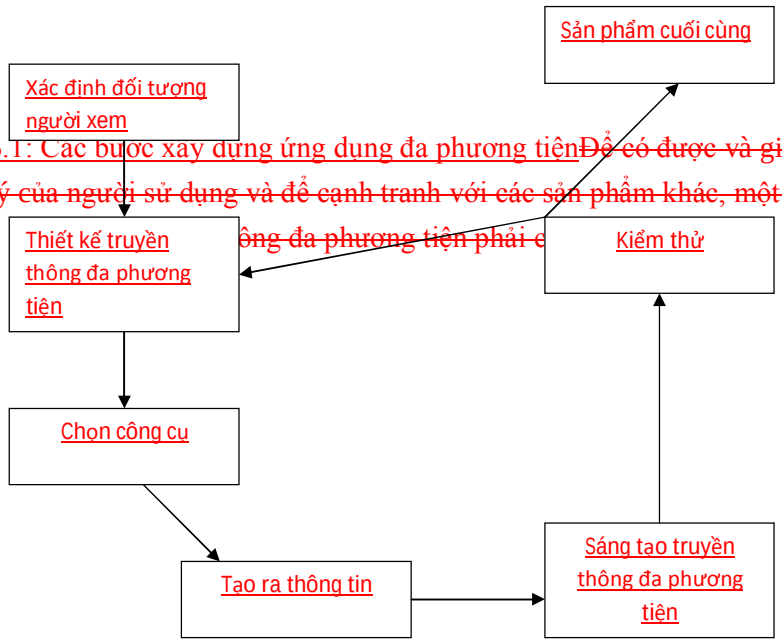
- Người quản lý dự án: Người quản lý dự án đóng vai trò trung tâm trong quá trình xây dựng dự án. Họ là người chịu trách nhiệm chính cho toàn bộ quá trình phát triển và cài đặt một dự án cũng như tất cả các hoạt động thường ngày khác.: ~~Q~~quản lý ngân quỹ, lịch làm việc, quản lý tiến độ, ốm đau của nhân viên, các hoá đơn, tinh thần làm việc của nhóm….Người quản lý dự án có vai trò như là chất keo gắn kết mọi thứ lại với nhau.
- Giám đốc nghệ thuật: Chỉ đạo quá trình tạo ra của tất cả ~~các~~những yếu tố nghệ thuật trong dự án.

- Trưởng bộ phận kĩ thuật: Đảm bảo cho quá trình có tính công nghệ của dự án phải tiến triển và phải thích hợp với tất cả các thành phần và phương tiện của dự án.
- Người thiết kế giao diên: Chỉ đao quá trình phát triển giao diên người sử dụng của sản phẩm
- Người viết kịch bản: Tương tác đan kết nội dung của dự án trong nhiều phương tiện và dạng thức tương tác khác nhau. Một người viết kịch bản tương tác truyền thông đa phương tiện vừa là tác giả vừa là nhà thiết kế tính năng tương tác.
- Chuyên gia xử lý âm thanh: Thiết kế và tạo ra tất cả các âm thanh có trong sản phẩm kể cả các bảng tổng phổ âm nhạc, các đoạn xướng âm, những lời thuyết minh và các hiệu ứng âm thanh và bảo đảm rằng mỗi âm thanh tương tác đúng đắn với tất cả các phương tiện khác.
- Chuyên gia xử lý video: Tao và xử lý các cảnh quay phim, đoan video có sử dung công nghê tương tác của sản phẩm. Video thường là phương tiên phức tạp nhất, tốn nhiều thời gian và tài nguyên nhất để tạo.
- Lập trình viên Multimedia: Thiết kế và tạo ra phần mềm cơ sở để có thể chạy một chương trình truyền thông đa phương tiện và thực hiện các mệnh lệnh của người sử dụng.

Formatted: Bullets and Numbering

5.3. Các bước xây dựng ứng dụng đa phương tiện

Các bước phát triển thông tin đa phương tiện được trình bày trong hình vẽ sau (hình 5.1). Chi tiết về các bước này sẽ được trình bày trong các phần tiếp theo.



Hình 5.1: Các bước xây dựng ứng dụng đa phương tiên~~Để có được và giữ được sự chú ý của người sử dụng và để cạnh tranh với các sản phẩm khác, một chương ông đa phương tiện phải c~~

- ~~Thông tin, diễn tiến và một "cốt truyện" có khả năng "thúc ép" người sử sử dụng phải tương tác với chương trình.~~
- ~~Một tập hợp nhiều loại phương tiện gắn bó với nhau được sắp xếp khéo léo và liền lạc.~~
- ~~Cơ chế điều hướng linh hoạt, do vậy cho phép người sử dụng duyệt vòng quanh nếu muốn hoặc thậm chí điều chỉnh lại dòng thông tin.~~

~~□'ĐINHKết quả là việc tạo ra các sản phẩm truyền thông đa phương tiện hữu hiệu có thể là một quá trình đầy thách thức.~~

~~Để bao quát tất cả mọi vấn đề cơ bản, một nhóm phát triển truyền thông đa phương tiện thường gồm nhiều người với những kĩ năng khác nhau gắn với một quá trình phát triển phức tạp nhưng được hoạch định tốt. Hình minh hoạ phần tổng quan của một quá trình phát triển thông tin truyền thông đa phương tiện. Các phần sau sẽ trình bày chi tiết về mỗi bước của quá trình này.~~

~~Xác định đối tượng người xem~~

5.3.1. Xác định đối tượng người xem

Bởi vì một chương trình truyền thông đa phương tiện có thể cung cấp nhiều loại thông tin khác nhau và có thể được phát triển theo rất nhiều cách khác nhau nên những người tạo ra nó phải hiểu được ai là người xem. Nói cách khác, ai sẽ sử dụng sản phẩm đó? Vấn đề này là yếu tố căn bản nhất mà các nhà phát triển phải giải quyết và nó phải được thảo luận chi tiết một thời gian khá lâu trước khi công việc phát triển thực sự bắt đầu. Để xác định người xem cho sản phẩm của mình, các nhà phát triển sẽ tự hỏi các câu hỏi, chẳng hạn như:

Sản phẩm này sẽ đáp ứng mối quan tâm cụ thể nào và những loại người sử dụng nào có mối quan tâm này? Ví dụ, nếu bạn dự định phát triển một phần hướng dẫn truyền thông đa phương tiện về chủ đề xây boong tàu, bạn nên biết được loại người nào quan tâm đến việc xây boong tàu.

Formatted: Bullets and Numbering

- Nếu bạn phải phát triển một Website cho mục đích bán các phụ tùng xe ô tô, bạn phải lựa chọn xem ai sẽ quan tâm đến việc mua chúng.
- Bạn có thể giả sử điều gì về người xem? Ví dụ, người sử dụng phải có những kĩ năng hay kinh nghiệm gì trước khi sử dụng chương trình? Kĩ năng ở đây bao gồm cả kinh nghiệm với máy tính (hoặc công nghệ cụ thể mà sản phẩm sử dụng để phân phối) cũng như vấn đề mấu chốt mà sản phẩm nói đến.
- Người sử dụng sẽ được gì khi sử dụng chương trình này? Đối với một số loại sản phẩm nhất định, mục tiêu của người sử dụng là để học một cái gì đó. Trong các trường hợp khác, người sử dụng có thể chỉ muốn được giải trí.
- Người sử dụng sẽ chấp nhận bỏ ra bao nhiêu thời gian để khám phá thông tin này? Trong trường hợp của một trò chơi tương tác, người sử dụng có thể sẽ gặp phải các rắc rối đã được dựng sẵn hay có thể bị thử thách nhiều lần trước khi đạt được một mục tiêu cuối cùng. Tuy nhiên, trong trường hợp của một chương trình đào tạo dựa trên máy tính (CBT-Computer based training), người sử dụng có thể sẽ muốn "nhảy" trực tiếp đến thông tin cơ bản.
- Phương tiện nào sẽ chuyển tải tốt nhất thông điệp này đến người sử dụng? Câu trả lời có thể tuỳ vào các mục tiêu và mong muốn của người sử dụng. Trong trường hợp của một chương trình hướng dẫn, lời thoại thuyết minh, các hướng dẫn bằng văn vản, các hình ảnh đồ hoạ sinh động có thể là yếu tố chính. Tuy nhiên, trong một trò chơi thì đoạn video kĩ thuật số, âm thanh nổi, và các nhân vật "có tính người" có thể sẽ là yếu tố cơ bản.
- Phương thức hay các phương thức nào (đĩa mềm, CD-ROM, DVD, mạng Internet quay số, mạng Internet băng rộng, mạng nội bộ) sẽ được dùng để phân phối sản phẩm? Phương thức phân phối xác định kích thước tối đa của sản phẩm. Tốc độ của hệ thống phân phối xác định độ phong phú về phương tiện mà sản phẩm có thể có. Các phương tiện

dùng đĩa đòi hỏi phải xem xét đến hệ điều hành của người sử dụng, các phương tiện dùng Web đòi hỏi phải xem xét đến trình duyệt và cấu hình phần cứng/phần mềm của người sử dụng. Khi một sản phẩm được phân phối liên hệ điều hành (ví dụ, cho cả một hệ thống Windows lẫn Macintosh) thì nhà phát triển phải chọn các loại tập tin và công cụ sáng tạo có tính liên nền.

Sự thực thì danh sách trên vẫn còn ngắn. Các nhóm phát triển có thể tốn hàng tuần hay hàng tháng để cố xác định những người sử dụng của họ, để bắt đầu nắm được mọi mong muốn, nhu cầu và nguyện vọng của người tiêu dùng. Những nhân viên tiếp thị có thể phải được tuyển thêm để phỏng vấn khách hàng tiềm năng hoặc gặp gỡ các nhóm trọng tâm để tìm kiếm phản ứng của người tiêu dùng đối với sản phẩm cạnh tranh.

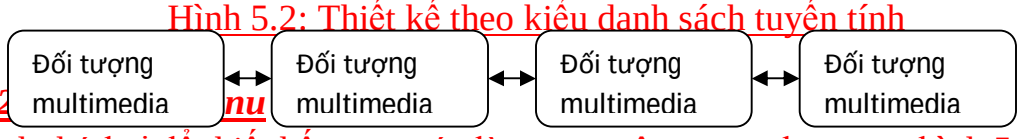
Phần này của quá trình phát triển là phần phổ biến đối với việc phát triển rất nhiều, rất nhiều loại sản phẩm. “Hiểu được khách hàng” là nguyên tắc đầu tiên của quá trình phát triển sản phẩm và là yếu tố chủ chốt đối với sự thành công lâu dài của bất kì sản phẩm nào. Vì lí do này, các trả lời cho các câu hỏi có liên quan đến người xem là các yếu tố quan trọng nhất trong việc “tạo hình” cho sản phẩm cuối cùng.

5.3.2. Sơ đồ thiết kế của các đối tượng multimedia

5.3.2.1. Danh sách tuyến tính

Danh sách tuyến tính là kiểu thiết kế đơn giản nhất. Khi người sử dụng kích chuột, ứng dụng sẽ hiện ra thông tin theo kiểu kế tiếp, mục này tiếp theo mục kia. Mỗi một đối tượng trong danh sách có thể là text, đồ họa, audio clip, video hoặc một đối tượng kết hợp từ nhiều phương tiện khác nhau. Người sử dụng có thể tiến hoặc lùi trên danh sách. Ví dụ minh hoạ về kiểu cấu trúc này được cho trong hình 5.2.

Hình 5.2: Thiết kế theo kiểu danh sách tuyến tính



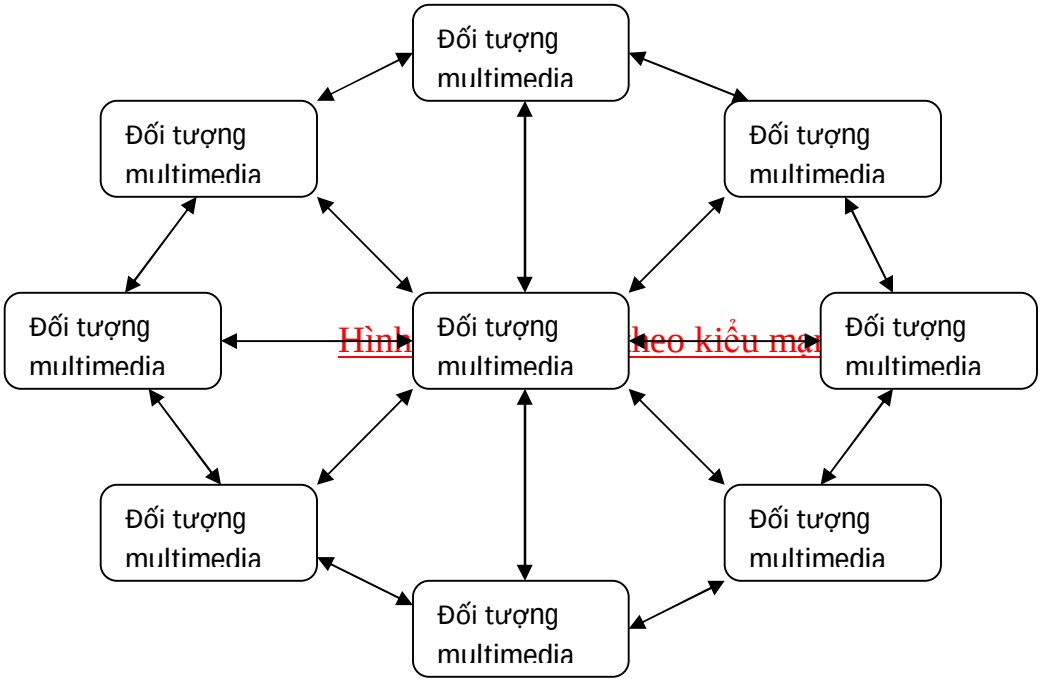
5.3.2.2 nu

Cách thứ hai để thiết kế tương tác là tạo ra một menu như trong hình 5.3. Các mục trong menu có thể hypertext, đồ hoạ, hoặc các đối tượng kết hợp giữa text

và hình ảnh. Khi người sử dụng chọn một mục trong menu, các mục liên kết với nó sẽ xuất hiện và giữ nguyên ở trên màn hình cho đến tận khi người sử dụng kích chuột. Sau đó ứng dụng quay trở về menu để người sử dụng có thể thực hiện một lựa chọn khác.

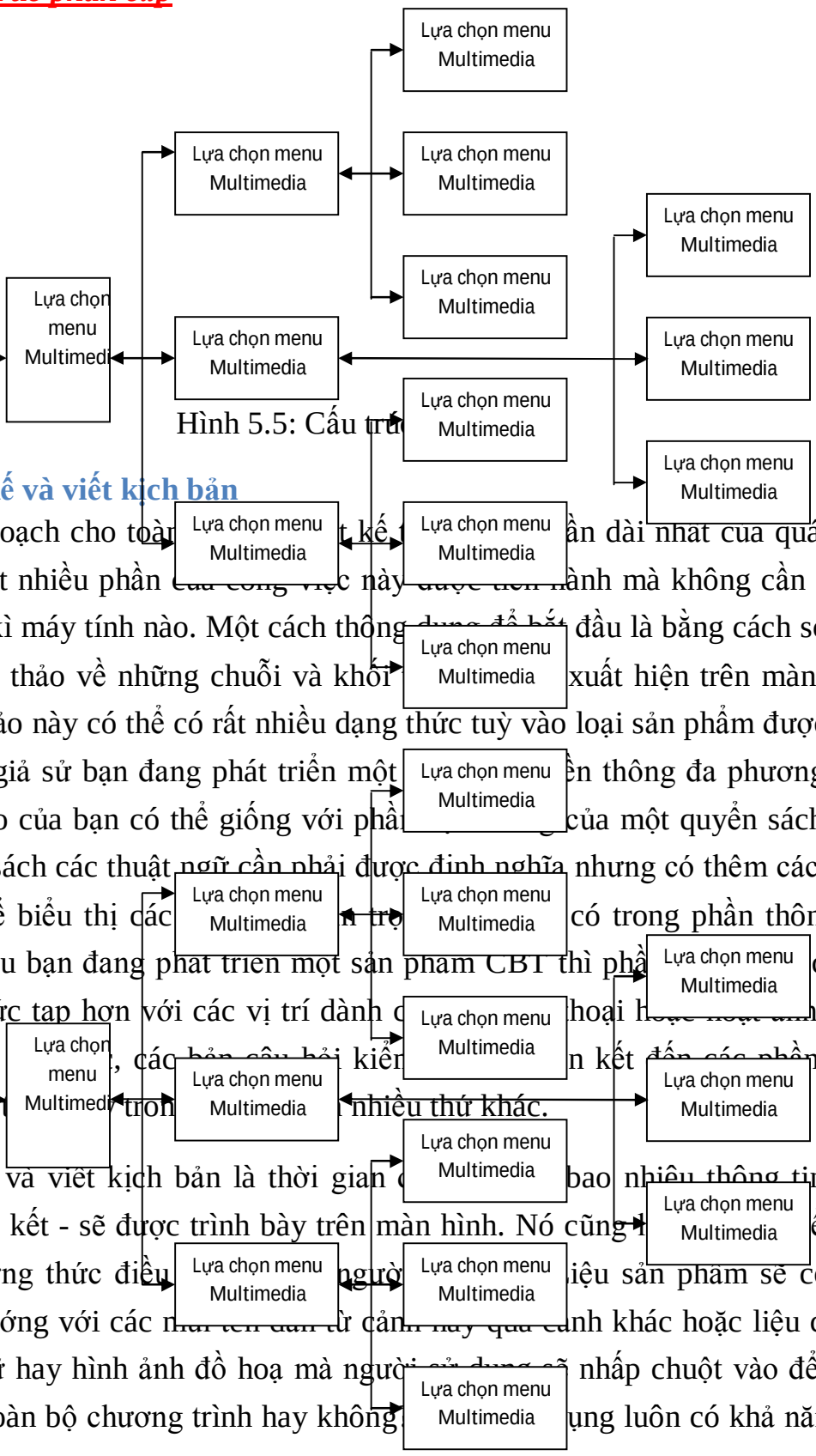
Hình 5.3: Thiết kế theo kiểu menu

5.3.2.3. Cấu trúc mạng



Hình [illegible] theo kiểu mạ[illegible]

5.3.2.4. Cấu trúc phân cấp



Hình 5.5: Cấu trú

5.3.3. Thiết kế và viết kịch bản

Lập kế hoạch cho toà t kế ần dài nhất của quá trình phát triển. Rất nhiều phần của công việc này được tiến hành mà không cần sự trợ gi ất kì máy tính nào. Một cách thông dụng để bắt đầu là bằng cách soạn ra m phác thảo về những chuỗi và khối xuất hiện trên màn hình. D c thảo này có thể có rất nhiều dạng thức tuỳ vào loại sản phẩm được phát triển. Ví dụ, giả sử bạn đang phát triển một ền thông đa phương tiện. Bản phác thảo của bạn có thể giống với phầ của một quyển sách gồm có một danh sách các thuật ngữ cần phải được định nghĩa nhưng có thêm các dòng và mũi tên để biểu thị các có trong phần thông tin. Ngược lại, nếu bạn đang phát triển một sản phẩm CBT thì phầ có thể tương đối phức tạp hơn với các vị trí dành c hoại hoặc hoạt ảnh đóng vai trò là các , các bản câu hỏi kiể n kết đến các phần khác trong chương trìn nhiều thứ khác.

Thiết kế và viết kịch bản là thời gian bao nhiêu thông tin-chữ, hình ảnh, liên kết - sẽ được trình bày trên màn hình. Nó cũng ể thiết lập một phương thức điều người liệu sản phẩm sẽ có một thanh điều hướng với các nhãn tên dẫn từ cảnh này qua cảnh khác hoặc liệu có các đối tượng chữ hay hình ảnh đồ hoạ mà người sử dụng sẽ nhấp chuột vào để nhảy vòng quanh toàn bộ chương trình hay không. ụng luôn có khả năng trở

về một điểm bắt đầu duy nhất hay không? Liệu phần thông tin có thay đổi mà không nhận dữ liệu nhập từ người sử dụng hay không?

Khi một chương trình gồm một số lượng lớn các hoạt ảnh hay nhiều cảnh khác nhau thì phần hỗ trợ tốt nhất là kịch bản. Vốn được các đạo diễn phim sử dụng để sản xuất các chương trình quảng cáo thương mại 30 giây trên truyền hình cho đến các bộ phim dài, "kịch bản" bao gồm các bản tóm tắt của các cảnh và hành động. Lập ra một kịch bản sẽ giúp cho nhà sáng tạo nhận ra các khoảng trống trong logic hoặc các sai sót trong dòng chảy thông tin. Một số chương trình sáng tạo truyền thông đa phương tiện cung cấp các công cụ để vẽ ra và sắp xếp các khung hình của một kịch bản và cũng có các chương trình kịch bản độc lập. Nhiều nhà thiết kế truyền thông đa phương tiện có kinh nghiệm tạo ra các kịch bản chỉ bằng cách đơn giản là sử dụng một chương trình xử lý văn bản hay một chương trình vẽ hình.

5.3.4. Chọn các công cụ, tạo ra thông tin và sáng tạo

Bởi vì truyền thông đa phương tiện bao gồm nhiều loại thông tin khác nhau nên việc tạo ra nó có liên quan đến nhiều loại phần mềm. Tạo ra chữ thường cần có một trình xử lý văn bản; làm việc với các hình ảnh số cần có phần mềm đồ hoạ; sử dụng video cần có chương trình bắt hình video và phần mềm chỉnh sửa; âm thanh cần có phần mềm chỉnh sửa của riêng nó. HTML thường được dùng trong các chương trình truyền thông đa phương tiện tương tác cũng như trong các trang Web cho nên các chương trình hiệu chỉnh HTML là các công cụ quan trọng trong nguồn tài nguyên của nhà phát triển.

Một số phần mềm phổ biến được sử dụng để tạo ra các loại thông tin đa phương tiện:

Bảng 5.1: Các công cụ Painting and Drawing

Canvas	Designer	MacPaint

Charisma	DeskDraw	PixelPaint Pro
ColorStudio	DeskPaint	Professional Draw
Corel Draw	Fractal Design Painter	Studio 1/8/32
Cricket Draw	Harvard Graphics	SuperPaint
Cricket Graph	Illustrator	Windows Draw
Cricket Paint	ImageStudio	
DeltaGraph Pro	MacDraw Pro	

Bảng 5.2: Các công cụ CAD và 3-D

3-D Studio	MacroModel	Swivel 3D
AddDepth	MiniCad+	Three-D
AutoCAD	ModelShop	VersaCAD
ClarisCAD	RayDream Designer	Virtus Walkthrough
Infini-D	Strata Vision	
Life Forms	Super 3D	

Bảng 5.3: Các công cụ tạo hình ảnh

Color it	JagII

ColorStudio	Ofoto
Composer	Photoshop
Digital Darkroom	PhotoStyler
Gallery Effects	Picture Publisher

Bảng 5.4: Các công cụ ORC và TEXT

OmniPage	Typestry
Perceive	TypeStyler
TypeAlign	

Bảng 5.5: Các công cụ tạo âm thanh

Alchemy	Midisoft Studio
AudioShop	Sound Designer II
Audio Trax	SoundEdit Pro
Encore	Turbo Trax
Master Tracks Pro	WaveEdit

Bảng 5.6: Các công cụ tạo video và làm phim

Aminator Pro	Premiere	VideoShop
Elastic Reality	Screen Machine	VideoSpigot
MediaMaker	SuperVideo	Videovision
MetaFlo	VideoFusion	VideoWare HSC
Morph	Video Grafitti	
MoviePak	VideoMachine	

Bảng 5.7: Các công cụ Accessories

Capture	Image Alchemy	PICTpocket
ClipMedia	ImagePals	ResEdit
CompileIt	Kai’s Power Tools	Shoebox
ConvertIt	Kudo Image Browser	SmartPics
DeBabelizer	Media Cataloger	SnapPRO
DiskDoubler	MediaDOCs	StuffIt
Fetch	MediaOganizer	UpDiff
FreezeFrame	MusicBytes	Wraptures
Hijaak	Photo Disc	

5.3.5. Kiểm thử

Việc chương trình phải được những người sẽ sử dụng nó sử dụng thử là mang tính sống còn. Với tác vụ thử này, lập trình viên có thể xác định bất kì điểm sai sót nào và sửa đổi chúng trước khi đưa sản phẩm hoàn tất ra thị trường.

Giống như quá trình thử của bất kì sản phẩm phần mềm nào, việc ta để nhà sáng tạo của chương trình theo dõi người sử dụng duyệt vòng quanh qua sản phẩm là rất có lợi. Loại vấn đề để theo dõi là bất kì vị trí nào trong sản phẩm nơi mà người sử dụng không biết cần phải làm gì tiếp theo? Có phải người sử dụng đang chật vật đọc một đoạn mô tả có cỡ phông quá nhỏ? Liệu có đủ các công cụ điều khiển để cho nếu người sử dụng muốn tiếp tục mà không muốn duyệt qua toàn bộ đoạn trích video hoặc âm thanh thì có thể ngưng đoạn trích đó hay không? Người sử dụng có theo được các đường dẫn định hướng dẫn đến các thông tin mong muốn một cách nhanh chóng không hay là người sử dụng đôi khi bị lạc trong mê cung.

> Trước khi một chương trình sẵn sàng xuất xưởng, nó có thể cần phải qua một vài chu kì thử -và – xem lại sao cho mọi người đều có thể yên tâm với sản phẩm hoàn tất. Trong quá trình hoạch định thì ta phải đưa vào bản kế hoạch đủ thời gian dành cho các chu kì thử. Hầu hết các nhà phát triển phần mềm và các lập trình viên đều thuê các công ty để thử phần mềm hoặc là họ có các phòng thử riêng của họ trong công ty.

Nhà sáng tạo của một chương trình và người sử dụng cuối cùng thường có quan điểm khác nhau. Những gì mà nhà sáng tạo cho là dễ dùng – vì đã thiết kế phần giao diện và dùng nó hàng tuần hay hàng tháng trong quá trình phát triển – thì lại có thể hoàn toàn gây bối rối cho ai đó xem phần giao diện đầu tiên. Nhà sáng tạo phải học cách xem bất kì vấn đề gì mà người sử dụng phát hiện được trong chương trình như là lời phê bình có tính xây dựng. Thử là công việc rất có ích vì ta dễ dàng mất đi cách nhìn của một người xem sau khi quá trình sáng tạo nặng nhọc đã được bắt đầu.

5.3.6. Phân phối thông tin truyền thông đa phương tiện

Một phần quan trọng của quá trình phát triển thông tin truyền thông đa phương tiện là hiểu được cách một sản phẩm được phân phối đến những người sử dụng nó. Hiện tại, thông tin truyền thông đa phương tiện thường được phân phối đến người sử dụng bằng một trong 3 loại phương tiện sau: CD-ROM (hoặc DVD-ROM), mạng Internet hoặc một số loại kết nối mạng hoặc truyền hình. Tất nhiên, mỗi công nghệ phân phối có điểm mạnh và điểm yếu riêng của nó. Mỗi phương pháp phân phối đều có ảnh hưởng đến khả năng của sản phẩm trong việc sử dụng các công nghệ nhất định hay ảnh hưởng đến khả năng của người sử dụng trong việc tương tác và điều khiển thông tin.

Khi các công nghệ phân phối được cải tiến trong những năm tới và khi băng thông không còn là một vấn đề đối với người sử dụng (nhờ vào hệ thống mạng và các kết nối Internet tốc độ nhanh hơn, các công nghệ CD-ROM/DVD-ROM đã được cải tiến và sự tích hợp các công nghệ này với truyền hình), nhiều giới hạn hiện có sẽ biến mất. Sau cùng thì nhiều sản phẩm truyền thông đa phương tiện sẽ hoạt động như nhau không phụ thuộc vào cách chúng đến được với người sử dụng.

5.3.6.1. CD-ROM

Có lẽ cách thức rõ ràng nhất để phân phối thông tin truyền thông đa phương tiện là trên một đĩa compact. Do dung lượng lưu trữ lớn, chi phí thấp và dễ dùng, các đĩa compact đã là sự lựa chọn hiển nhiên lúc ban đầu của nhiều nhà phát triển thông tin truyền thông đa phương tiện, những người cần một cách nào đó để đưa sản phẩm của họ đến tay người tiêu dùng. Các tựa CD-ROM lúc ban đầu thành công và cho thấy rằng các PC và các máy trò chơi có thể hỗ trợ một tập hợp nhiều công nghệ âm thanh và audio, siêu phương tiện và các loại thông tin truyền thông đa phương tiện quan trọng khác.

Bằng cách kết hợp các công nghệ mới chẳng hạn như MPEG, Java, Shockwave và các dạng thức khác cho phép nén các dòng dữ liệu được nhiều hơn, hiệu năng của các sản phẩm trên CD-ROM tiếp tục được nâng cao. Tính theo tương quan, số lượng các sản phẩm có trên CD-ROM vẫn tiếp tục gia tăng với tốc độ rất lớn.

Một điểm mạnh khác của dạng thức đĩa compact là khả năng của nó trong việc tương tác với các công nghệ khác. Ví dụ, ta có thể sử dụng nhiều sản phẩm trên CD trong các môi trường đa người sử dụng, sử dụng trên các mạng và thậm chí kết hợp với các Website riêng biệt hay các nguồn tài nguyên trên Internet. Chẳng hạn như nhiều bộ bách khoa toàn thư trên đĩa đều có đầy các liên kết đến các trang Web, cho phép người sử dụng chuyển đổi dễ dàng từ nguồn tài nguyên này đến nguồn tài nguyên khác.

Một nhược điểm của công nghệ CD là tốc độ tương đối chậm của các ổ đĩa CD-ROM. Mặc dù tốc độ của các ổ đĩa không ngừng gia tăng, chúng vẫn còn chậm hơn nhiều so với các đĩa cứng thông thường. Dung lượng lưu trữ cũng trở thành vấn đề phải quan tâm khi người tiêu dùng đòi hỏi nhiều đặc tính và tính năng hơn trong các sản phẩm truyền thông đa phương tiện của họ. Vì lí do này, một số các sản phẩm mới đã được phát hành trên nhiều đĩa tức là người sử dụng phải ngưng khi đang sử dụng để hoán đổi đĩa. Tuy nhiên, khi nhiều sản phẩm truyền thông đa phương tiện được phát hành trên DVD (và khi nhiều người tiêu dùng sắm các máy tính có ổ đĩa DVD hơn) thì tầm quan trọng của vấn đề lưu trữ hứa hẹn sẽ ít dần.

5.3.6.2. Mạng Internet

Trong vài năm, các chuyên gia đã hình dung được mạng Internet (và phần mở rộng là các mạng riêng lẻ liên kết vào Internet) như là một phương tiện sau cùng để phân phối thông tin truyền thông đa phương tiện. Người tiêu dùng đã từng nghe những hứa hẹn không bao giờ ngưng rằng vì nó hỗ trợ cơ chế tương tác hai chiều giữa người sử dụng và máy chủ, một ngày nào đó mạng Internet sẽ trở thành địa điểm của các trò chơi trực tuyến, địa điểm dành cho mua sắm, giáo dục và các loại hình truyền thông đa phương tiện trực tuyến khác- thậm chí cả thực tế ảo tương tác. Tuy nhiên, mơ ước này vẫn còn bị cản trở bởi hai vấn đề: băng thông bị giới hạn và thiếu các công nghệ hỗ trợ các dòng thông tin truyền thông đa phương tiện. May mắn là cả hai vấn đề này đang ngày càng giảm dần yếu tố quan trọng theo thời gian.

Gần đây người ta đã phát triển một vài công nghệ hỗ trợ thông tin truyền thông đa phương tiện trên Web và cho phép các nhà phát triển nén thông tin âm

thanh, video và đồ hoạ xuống chỉ còn một phần so với kích thước gốc của nó, chia nó thành các gói và phân phối nó trong những gói nhỏ, có thể quản lý được và sau đó có thể được tập hợp lại và phát trên máy PC của người sử dụng. Thông qua các công nghệ gắn thêm mạnh mẽ nhưng có kích thước nhỏ, các nhà phát triển có thể tuỳ biến giao diện trình duyệt để hiển thị hầu như bất kì loại thông tin nào. Rất nhiều trong số những công nghệ này cũng cho phép cơ chế tương tác hai chiều.

Băng thông sẽ không còn là vấn đề nữa vì 2 lí do: Thứ nhất, các nhà thiết kế Web đang sử dụng các công nghệ nén để chắc chắn rằng các trang Web (nhất là các thông tin truyền thông đa phương tiện) có thể được tải và hiển thị, phát lại nhanh hơn bao giờ hết. Các Website cũng sẽ chuyển nhiều hơn các chức năng xử lý văn bản máy chủ sang máy tính của người sử dụng, từ đó cần ít thời gian tải xuống và tải lên hơn và miễn cho máy chủ một số công việc nhất định. Những tiến bộ này sẽ khiến cho việc sử dụng băng thông hiện có được tốt hơn.

Ngoài ra, ngày càng nhiều những người sử dụng Internet chọn dùng các kết nối tốc độ cao. Thông qua những thay đổi này, người tiêu dùng sẽ mở ra một đường truyền rộng hơn để lưu chuyển thông tin khiến cho các sự kiện truyền thông đa phương tiện trực tuyến dễ truy cập hơn bao giờ hết.

Kết quả là, khả năng của các thông tin truyền thông đa phương tiện trực tuyến bùng nổ. Người sử dụng Internet có thể dễ dàng truy cập vào các trò chơi (gồm cả các trò chơi với sự tham gia của hàng ngàn người), các đoạn video âm nhạc, học tập từ xa, xem phim trực tuyến…….Những sản phẩm truyền thông đa phương tiện này sẽ hoạt động trực tuyến với tốc độ cao và đáp ứng nhu cầu của khách hàng tương tự như trên đĩa CD-ROM.

5.3.6.3. Truyền hình

Truyền hình đã từng là chúa tể của các phương tiện phân phối thông tin truyền thông đa phương tiên. Nếu ban có một tivi ở nhà, ban chắc biết được việc chon giữa các chương trình khác nhau dễ như thế nào trong đó mỗi chương trình đều có một tập các hoạt động trực tiếp, âm thanh nói hay âm nhạc, chữ, hình ảnh đồ hoạ, hoạt ảnh và video. Từ góc độ này, việc đánh bại truyền hình trong việc

chuyển tải khối lượng và sự đa dạng của thông tin đến người xem là rất khó khăn.

Tuy nhiên, truyền hình không có tính tương tác. Nó bị giới hạn bởi các loại và khối lượng thông tin phản hồi mà nó có thể nhân được từ người xem bởi truyền hình vốn là một phương tiện một chiều. Các thông tin lưu chuyển từ đài phát đến người sử dụng nhưng không theo chiều ngược lại (cơ chế thay đổi kênh không được tính ở đây). Mãi cho đến thời gian gần đây, người xem vẫn còn gặp khó khăn trong việc phản hồi hoặc không thể phản hồi theo bất kì cách thức có ý nghĩa nào đối với một chương trình truyền hình.

Hiện tại, ta vẫn có truyền hình tương tác nhưng chỉ trong một chừng mực nào đó và phải kết hợp các công nghệ bổ sung vào truyền hình. Ví dụ, bạn có thể sử dụng truyền hình để chơi các trò game tương tác nhưng phải có máy trò chơi và các thiết bi điều khiển kèm theo. Các trò chơi tư bản thân chúng là những phần tách biệt so với chương trình truyền hình mà bạn nhận được qua đường dây anten, dây cáp hay qua đường truyền vệ tinh.

Một trong những tiến bộ mới nhất của quá trình làm cho truyền hình trở nên tương tác là sự tích hợp khả năng kết nối Internet với các chương trình phát hình. Như đã trình bày ở trên, dịch vụ WebTV của Microsoft có một tập các thiết bị đặc biệt có thể kết nối đến tivi của người sử dụng, chuyển đổi nó thành một thiết bi Internet. Do đó, người sử dụng có thể hiển thị chương trình truyền hình bình cũng như các thông tin từ Internet chẳng hạn như các trang Web, thư điên tử và nhiều thứ khác.

Thông tin qua WebTV, một số mạng đã bắt đầu tích hợp các chương trình của chúng với các thông tin đặc biệt chỉ dàng riêng cho những người sử dụng WebTV cho phép người xem tham gia vào chương trình.

Các dich vu thông qua vê tinh khác chẳng hạn như DirectTV và DirectPC đang đi theo hướng của WebTV nhưng hứa hẹn có lượng băng thông rộng hơn thông qua các kênh vê tinh chuyên dung của chúng. DirectDuo, một kết hợp của

dịch vụ DirectTV và DirectPC, có khả năng cho phép người sử dụng kết nối các tivi của ho và các máy tính cá nhân vào dich vu và do đó có thể thưởng thức chương trình phát hình và dịch vụ Internet băng thông rộng, tốc độ cao. Tuy nhiên, không giống như WebTV, những người sử dụng DirectTV không cần phải sử dụng truyền hình của họ để hiển thi các thông tin Internet.

Cuối cùng, các dịch vụ như WebTV và các dịch vụ phát thông tin qua vệ tinh có thể làm cho truyền hình hoàn toàn có tính tương tác và người sử dụng sẽ có thể "đặt" các chương trình và phim ảnh theo nhu cầu, tuỳ biến các lich chương trình của họ, tham gia vào các trò chơi nhiều người chơi và tham gia vào các thông tin trên tivi và thậm chí điều khiển quá trình diễn tiến thông tin của các chương trình riêng biệt (ví dụ, thay đổi cốt truyện của một bộ phim).

~~**2. Các bước xây dựng ứng dụng đa phương tiện**~~

~~**2.1. Lập kế hoạch**~~

~~**a. Lập kế hoạch dự án**~~

~~Lập kế hoạch cho một dự án Multimedia giống như quá trình phân chia tế bào: bức tranh tổng thể của các ý tưởng cho dự án được phân chia thành nhiều pha và sau đó mỗi pha lại được phân nhỏ hơn thành các nhiệm vụ và các khoản mục nhỏ hơn và dễ quản lý hơn. Các nhiệm vụ và các khoản mục này phải được hoàn thành với một khoảng thời gian cho trước. Có một số khối xây dựng của quản lý dự án. Một vài nhiệm vụ là bắt buộc và phải được hoàn thành trước khi các nhiệm vụ khác bắt đầu, vì lập kế hoạch cho các nhiệm vụ trước mắt là quan trọng. Xác định rõ khối lượng thời gian ước tính dành cho mỗi nhiệm vụ, và ghi lại thời gian cho từng nhiệm vụ trên lịch. Đó là kế hoạch cho dự án của bạn.~~

~~**Chú ý:** Ở cuối mỗi pha chúng ta cần thiết lập một mốc thời gian để hoàn thành công việc tiếp theo, và lập hoá đơn dựa trên những công việc đã được hoàn thành trong thực tế, và để đánh giá hoặc kiểm thử, và để nhận được các thông tin phản hồi về cấu trúc. Phụ thuộc vào độ phức tạp của dự án, bạn có thể thiết lập thêm những mốc thời gian ở cuối của mỗi nhiệm vụ.~~

Tất nhiên, cách đơn giản nhất để lập kế hoạch một dự án là sử dụng kinh nghiệm mà bạn tích lũy được từ các dự án tương tự trong quá khứ. Qua thời gian, bạn có thể duy trì và cải tiến khuôn dạng kế hoạch Multimedia của bạn giống như nhóm người bắt đầu đi tìm kiếm vàng. Chỉ cần thêm một chút lúa mạch đen và nước mỗi khi bạn làm một dự án và người khởi đầu tiếp nhận công việc tiếp theo của bạn phân sẽ có thể có nhiều ….

Để lập kế hoạch cho toàn bộ quá trình, bắt đầu với những ý tưởng ban đầu và kết thúc với sự hoàn thành và phân phối của một sản phẩm hoàn thiện. Phác thảo một cách tổng thể về toàn bộ dự án; quá trình bậc thang của việc xây dựng ứng dụng multimedia được minh hoạ trong lược đồ hình 1.1.; sử dụng lược đồ này sẽ giúp bạn triển khai các mục đích của mình trong các pha của dự án. Chú ý đến các vòng lặp cho việc chỉnh sửa dựa trên kết quả kiểm thử.

Ý tưởng: Một cái gì đó thường dễ nhập vào đầu óc của bạn hoặc đầu óc của khách hàng khi nói: "Này, điều này sẽ làm nên một dự án multimedia lớn đấy!". Cảm nhận của bạn về âm thanh và âm nhạc, các hình ảnh ấn tượng, và có thể một đoạn video sẽ giải quyết được một nhu cầu kinh doanh, cung cấp một sản phẩm demo gây chú ý, hoặc tạo ra một công cụ có thể truy cập nhanh cơ sở dữ liệu máy tính. Bạn có thể không quan tâm hoặc cười trong một cuộc họp buồn tẻ, xây dựng một album ảnh tương tác cho những bức ảnh Giáng sinh cho gia đình bạn, hoặc phân phối báo cáo hàng năm cho công ty của bạn trên đĩa cho 40.000 cổ đông. Đây là một vài mục đích mà ở đó multimedia có thể ứng dụng một cách thành công.

- Trình diễn ở màn hình nền
- Hội thảo Video trực tuyến
- Tiếp thị, quảng cáo sản phẩm và trưng bầy sản phẩm
- Các bách khoa toàn thư, tài liệu tham khảo, các tác phẩm âm nhạc, và các hệ thống phục hồi dữ liệu số theo yêu cầu khác
- Các tác phẩm nghệ thuật, các màn trình diễn ở bảo tàng và sở thú
- Các tài liệu phụ đề (chú giải) video và audio

Formatted: Bullets and Numbering

- Các kiốt thông tin tương tác và các hệ thống bán lẻ
- Các hệ thống lưu trữ tài liệu và hình ảnh và các hệ thống quản lý dữ liệu khác
- Các hệ thống quản lý thông tin cá nhân và các hệ thống an ninh và nhận dạng cá nhân
- Các trò chơi, các câu chuyện của trẻ con, và các trò giải trí tương tác
- Các dịch vụ mua bán được phân phối trực tuyến hoặc phân phối qua đĩa CD
- Các khoá đào tạo có sử dụng máy tính tương tác
- Các hệ thống trợ giúp tương tác và hướng dẫn

'DINHMột điều quan trọng bạn cần phải nhớ trong giai đoạn phát triển ý tưởng đó là sự cân đối. Khi bạn đã nghĩ ra ý tưởng của mình, thì tiếp đó bạn phải xét đến tính khả thi của ý tưởng và chi phí cho việc sản xuất và phân phối.

Thực hiện ý tưởng:

- Tính cần thiết của những gì bạn làm? Mục đích và thông điệp của bạn là gì?
- Cách tổ chức dự án của bạn?
- Các thành phần multimedia (văn bản, âm thanh, và hình ảnh) nào là tốt nhất cho việc chuyển tải thông điệp của bạn?
- Bạn đã có tài liệu tham khảo cho dự án mà bạn định làm chưa? như là băng video, âm nhạc, các tài liệu, các bức ảnh, logo, các mục quảng cáo, các tài liệu tiếp thị, và các tác phẩm nghệ thuật khác.
- Ý tưởng của bạn bắt nguồn từ một chủ đề đã có và có thể được cải tiến với multimedia, hay bạn sẽ tạo ra một cái hoàn toàn mới?
- Bạn đã chuẩn bị sẵn sàng phần cứng cho quá trình phát triển dự án của bạn chưa? Mọi thứ đã đầy đủ chưa?
- Không gian lưu trữ mà bạn có là bao nhiêu? bạn thực sự cần bao nhiêu?

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

- Phần cứng nào sẽ sẵn có cho người sử dụng cuối?
- Phần mềm multimedia
- Bạn thực hiện dự án một mình? Có ai giúp đỡ bạn không?
- Bạn có bao nhiêu thời gian dành cho dự án?
- Bạn có bao nhiêu kinh phí dành cho dự án?
- ɔAINH Bạn sẽ phân phối sản phẩm cuối cùng của mình như thế nào?

b. Ước tính chi phí

2.2. Thiết kế và xây dựng

2.2.1.Thiết kế

a. Thiết kế cấu trúc

b. Thiết kế giao diện người dùng

c. Ví dụ minh hoạ

2.2.1.Xây dựng

Formatted: Bullets and Numbering

2.2.1.a.

2.2.2. Kiểm thử

a. Kiểm thử Alpha

b. Kiểm thử Beta

c. Hoàn thiện

2.3. Phân phối

a. Chuẩn bị để phân phối

b.a. Thiết kế các chương trình cài đặt

Formatted: Bullets and Numbering

Danh sách các học liệu mở

Giới thiệu

Hiện tại trên thế giới phong trào xuất bản các cua học mở, miễn phí (Open Course Ware - OCW) ngày càng phát triển mạnh. Các cua học thường được lấy ra từ chương trình giảng dạy của các trường đại học. Đầu tiên là các trường đại học ở Mỹ (tiên phong là MIT), sau đó đến các trường đại học khác ở Mỹ, Nhật, Trung Quốc và Pháp. Phần này chứa danh sách các trường đại học đã công bố OCW. Chúng tôi sẽ thường xuyên cập nhật các trường học tham gia phong trào này. <!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

Danh sách các trường cung cấp học liệu mở

1. Massachusette Institue of Technology - MIT

Website: http://ocw.mit.edu/index.html

MIT là trường học hàng đầu thế giới về công nghệ. MIT đã công bố trên 1000 cua học. Đây là nguồn tài nguyên vô cùng quý giá cho các trường trên toàn thế giới cũng như ở Việt Nam.

2. Các trường đại học công nghệ của Pháp (ParisTech)

Website: http://graduateschool.paristech.org/?langue=EN

ParishTech là tập hợp của 11 trường học công nghệ uy tín nhất tại Pháp. Các trường dẫn đầu về công nghệ trong lĩnh vực của mình. Danh sách các trường bao gồm: École Nationale du Génie Rural, des Eaux et des Forêts (ENGREF) École Nationale des Ponts et Chaussées (ENPC) École Nationale Supérieure d'Arts et Métiers (ENSAM) École Nationale Supérieure de Chimie de Paris (ENSCP) École Nationale Supérieure des Mines de Paris (ENSMP) École Nationale Supérieure des Télécommunications (ENST) École Nationale Supérieure de Techniques Avancées (ENSTA) École Polytechnique (EP).

3. Fulbright Economics Teaching Program OCW tại Việt Nam

Website: http://ocw.fetp.edu.vn

Ngay sau khi MIT công bố OCW, Fulbright School Economics Teaching Program (FETP) tại Việt Nam công bố FETP OpenCourseWare năm 2003.

4. John Hopkins University

Website: http://ocw.jhsph.edu/

5. Keio University

Website: http://ocw.dmc.keio.ac.jp/

6. Utah State University

Website: http://ocw.usu.edu/Index/ECIndex_view

7. Tokyo Institute of Technology

Website: http://www.ocw.titech.ac.jp/index.php?lang=EN

8. Osaka University

Website: http://ocw.osaka-u.ac.jp

9. University of Tokyo

Website: http://ocw.u-tokyo.ac.jp

10. Waseda University

Website: http://www.waseda.jp/ocw/index.html

11. Các trường đại học của Trung Quốc

Website: http://www.core.org.cn/cn/jpkc/index_en.html.

12. Đại học mở Anh - Open University of UK

Gần đây Đại học mở Anh công bố sẽ đưa các tài liệu giảng dạy miễn phí của trường lên mạng. Đại học mở của Anh là một trong các trường cung cấp dịch vụ

đào tạo trên mạng lớn nhất châu Âu. Các bạn đọc thêm tại: **Website**: http://oci.open.ac.uk/pressrelease.html

Hệ thống các từ viết tắt

SGML (Standard Generalised Markup Language)

DTD (Document Type Definition)

RLE (Run Length Coding)

ODA (Office Document Architecture)

PDF (Portable Document Format)

ASCII (American Standard Code for Information Interchange)

MHEG ()

ISO

ITU

Thứ sáu, ngày 24, Tháng 12 , năm 2010

Error!

EBook UBUNTU@TriLe-2008Error!

Cài đặt Ubuntu bằng hình ảnh

Trong thời đại Windows đang thống lĩnh thị trường máy tính dành cho các doanh nghiệp vừa và nhỏ tại Việt Nam với một mức giá khá cao thì việc tìm kiếm một giải pháp tiết kiệm chi phí là việc mà nhiều DN và cả người sử dụng cá nhân muốn hướng tới. Không thể phủ nhận những giá trị mà Windows mang lại cho bạn trong một thời gian dài nhưng giá cả vẫn là rào cản chính ngăn người sử dụng sở hữu chúng một cách hợp pháp. Với mức thu nhập của đa phần người Việt hiện nay thì chi phí để sở hữu một bộ Source-Software đáp ứng yêu cầu công việc vẫn còn khá cao. Nên việc chuyển qua sử dụng các phần mềm mã mở, miễn phí – "Free" là

xu hướng của đa số người dùng trên thế giới. Vậy sao bạn không cài thử bộ phần mềm miễn phí này xem sao?

Chia ổ cứng với HirenBoot CD

Bước 1:Boot từ đĩa HirenBoot CD để tiến hành chia ổ (Bài viết này dùng bản 8.4)

Error!

Bước 2: chọn start từ boot CD và chọn để sử dụng Partition Magic 8.05:

Error!

Error!

Error!

Bước 3 : Xem bảng Partition ở đây sử dụng ổ cứng dung lượng 20GB và đã cài sẵn windows với định dạng NTFS. Bạn muốn sử dụng 5.512 MB cho Ubuntu --> phải resize ổ để lấy chỗ, bước tiến hành resize:

Error!

Error!

Error!

Error!

Error!

Như vậy là ta hiện tại đã có 5.512MB trống để "làm việc" với Linux.

Bước 4: Tạo phân vùng SWAP và EXT3 để làm SWAP và / (root), ở bài viết này máy có 256MB RAM --> vậy bạn dùng 2x256MB=512MB để làm SWAP, phần còn lại sẽ để cho / (root):

Error!

Error!

Bước 5: Tạo phân vùng EXT3 cho / (root) với phần còn lại của ổ cứng:

Error!

Error!

Error!

Như vậy là ta đã có hai phân vùng SWAP và EXT3 cho Linux!!

Bước 6: Ấn apply để chứng thực thay đổi.

Error!

Error!

Bước 7: Kiểm tra lại thay đổi và restart để nhận thành quả.

Error!

Error!

Xong phần thiết lập phân vùng ổ cứng.

**** Tiến hành cài đặt Ubuntu với ổ cứng đã được chia***

Bước 1: Đưa đĩa cài đặt Ubuntu vào máy và tiến hành boot, chọn Start or install Ubuntu.

Error!

Error!

Bước 2: Nháy đúp vào biểu tượng Install để tiến hành thiết lập cài đặt.

Error!

Bước 3: Thiết lập các tuỳ chọn :

1.Chọn ngôn ngữ (ở đây là tiếng Anh).

Error!

2.Tuỳ chọn nơi cư trú

Error!

3. Thiết lập tuỳ chọn bàn phím (chọn tiếng Anh).

Error!

4. Thiết lập tuỳ chọn chia ổ đĩa, phần này chọn manual vì ta đã tự chia ổ bằng HirenbootCD.

Error!

Theo hình sau thì bộ cài đã tự động nhận ra phân vùng SWAP đã tạo bằng HirenbootCD.

Error!

Chọn tiếp để edit phân vùng EXT3 đã được tạo /dev/hda6 và chọn cài phân vùng này vào / (root) theo hình.

Error!

Chọn đánh dấu format phân vùng EXT3 và tiếp tục ấn forward.

Error!

5. Ở phần lựa chọn tiếp nhận thiết lập từ windows thì có thể bỏ chọn vì muốn tạo account từ đầu.

Error!

Tiếp tục là thiết lập account để login:

Error!

6. Xác nhận thiếp lập để cài Ubuntu.

Error!

7. Chờ đến khi xuất hiện màn hình sau :

Error!

8. Sau khi chọn Restart để hoàn tất cài đặt, máy sẽ boot với boot menu của grub:

Error!

Bước 4: Chọn boot vào Ubuntu và login với account đã tạo để có màn hình sau:

Error!

Như vậy là các bước thực hiện đã xong. Các bạn có thể thỏa sức khám phá với Ubuntu vừa được cài đặt.

Chúc các bạn thành công!

CLICK HERE**Error!**

Error!

Error!

Error!

Error!

Error!

3 bước cài đặt Ubuntu từ Windows

Muốn cài đặt Ubuntu, bạn phải mất thời gian phân chia partition, tải file, ghi ra nhiều CD cho tập tin cài đặt, rồi phải cấu hình lại cho hệ điều hành Windows có sẵn trên máy tính để Ubuntu và Windows "hòa thuận" chung một nhà.

Giải pháp đơn giản nhất là dùng Wubi để hỗ trợ cho việc cài đặt Ubuntu.

Wubi *(Windows based Ubuntu Installer)* là tiện ích giúp người dùng cài đặt hệ điều hành mã nguồn mở Ubuntu nhanh chóng từ hệ điều hành Windows. Wubi hỗ trợ các phân hệ của Ubuntu như Kubuntu, Xubuntu, Edubuntu, UbuntuStudio.

3 bước cài đặt Ubuntu

Giao diện Wubi

1. Tải Wubi tại website sourceforge.net hoặc tại đây. Wubi tương thích với hầu hết các phiên bản của hệ điều hành Windows từ Windows 98 đến Windows Vista (chưa hỗ trợ phiên bản 64-bit). Phiên bản Ubuntu mới nhất mà Wubi hỗ trợ là 7.04.

2. Chạy Wubi như những chương trình bình thường khác trong Windows.

3. Chọn mật khẩu cài đặt Ubuntu rồi nhấn ***Install*** để bắt đầu cài đặt tự động.

Sau khi cài đặt, Wubi sẽ thêm vào một tùy chọn khởi động với Ubuntu để người dùng chọn lựa. Ubuntu sẽ được cài đặt trong một tập tin ở phần tập tin hệ thống của Windows (mặc định là: *C:\wubi\disks\system.virtual.disk*).

Tuy vậy, một nhược điểm mà nhóm phát triển Wubi cần lưu ý cho phiên bản kế là dung lượng cài đặt Ubuntu chỉ giới hạn trong 10GB. Người dùng có thể tham khảo hướng dẫn chi tiết qua phần hỗ trợ của Wubi tại đây.

Ngược lại, nếu người dùng đang sử dụng các hệ điều hành Linux, Unix hay FreeBSD thì có thể tải về Lubi tại đây.

Error!

MỘT SỐ ĐIỀU LƯU Ý KHI SỬ DỤNG BỘ GÕ TIẾNG VIỆT TRÊN EDOCMAN - UBUNTU 7.10

I. Trình duyệt

1- Dùng trình duyệt **Mozilla Firefox 2.0.0.6** , **Opera 9.24** để sử dụng **eDocMan ,** qua kiểm tra sơ bộ các năng trong trong chương trình eDocMan đều hiển thị tốt. Hiện
tại chúng tôi chưa phát hiện được lỗi, rất cần test lại.

2- Nếu dùng **IE6** thì không phải kiểm tra, vì đã được thử nghiệm và đã được khuyến cáo dùng.

II. Hiển thị font tiếng Việt trong trình duyệt

Các font chữ được dùng trong **eDocMan** là font **Unicode** . Để **eDocMa** n hiển thị tốt tiếng Việt trong **Mozilla** Firefox, **Opera 9.24** hay **IE** , bạn phải copy các font Unicode cần thiết vào thư mục sau:
/usr/share/fonts/truetype (bạn có thể copy
bộ font Unicode của VietKey mà bạn đã cài trên máy cài Windows).

III. Bộ gõ tiếng Việt trên Ubuntu 7.10

1- Bộ gõ dùng để kiểm tra:

- Bộ gõ đa ngôn ngữ **SCIM** (Smart Common Input Method platform).
- Bộ gõ **xvnkb** phiêu bản 0.2.9a.

2- Đánh giá chung

2.1- Bộ gõ SCIM

- Hỗ trợ nhiều kiểu gõ khác nhau và cho phép sử dụng nhiều ngôn ngữ.
- Các thức xử lý **"không được hay lắm"** trong khi gõ, làm người dùng có vẻ không thích.
- Làm cho nhiều phím chức năng của các ứng dụng không làm việc (việc xử lý mã tiếng Việt làm thay đổi, ảnh hưởng đến các phím mà các ứng dụng đã định nghĩa. Vì
trong các ứng dụng khác nhau sẽ định nghĩa và sử dụng bàn phím khác nhau).
- Có thể gõ được tiếng Việt trong cả **IE** và **Mozilla Firefo** x, **Opera 9.24**
- Nếu chỉ dùng **IE, Mozilla Firefo** x, **Opera 9.24** và **OpenOffice.org** (có thể bị lỗi khi bạn sử dụng một số phím chức năng) thì vẫn có thể chấp nhận được.

2.2- Bộ gõ xvnkb

- Chạy ổn định, không làm ảnh hưởng đến các phím trong các ứng dụng mà tôi kiểm tra (OpenOffice.org, eDocMan...).
- Dễ sử dụng, tuy không phải là bộ gõ đa năng nhưng đối với người dùng bình thường thì rất tốt, chạy ổn định.
- Trong **IE** và **Mozilla Firefo** x, **Opera 9.24** thì chỉ gõ được tiếng Việt trong **Mozilla Firefo** x và **Opera 9.24** (không gõ được tiếng Việt trong **IE**).
- Nếu muốn dùng **xvnkb** thì phải bỏ bộ xử lý tiếng Việt **SCIM .**

Error!

- Bộ gõ **xvnkb** chạy rất tốt trên nhiều ứng dụng, tuy vậy, lưu ý là bạn đừng đặt mật khẩu là tổ hợp có chứa các ký tự dấu (ví dụ: **cafe** , khi hệ thống hỏi mật khẩu bạn gõ
vào **"cafe"** nhưng lại thành **"càe"** nên nếu không để ý bạn không thể đăng nhập được).

Trường hợp bạn chọn giao diện tiếng Việt cho HĐH thì khi đăng nhập không cần lưu ý
vấn đề này.

2.3- Đề xuất

- Nếu các bạn kiểm tra thử khi dùng **Mozilla Firefo** x, **Opera 9.24** đối với **eDocMan** mà không có vấn đề gì thì nên sử dụng bộ gõ **xvnkb** và trình duyệt là **Mozilla Firefo** x hay **Opera 9.24** .
- Nếu bạn dùng **xvnkb** thì bạn phải tắt bộ xử lý ký tự **SCIM** (có thể mỗi lần vào hệ thống thì tiến hành tắt hoặc gỡ bỏ vĩnh viễn, nếu bạn không muốn "ngó ngàng"
đến nó nữa).

Thực nghiệm cho thấy x-Unikey cho phép bỏ dấu tiếng Việt tốt trong các ứng dụng, ngoại trừ OpenOffice. Vì lý do đó mà tôi không đề cập đến x-Unikey ở đây.

2.4- Cách cấu hình để bộ gõ tiếng Việt mỗi khi khởi động đặt chế độ gõ Telex và mã chọn là Unicode (bạn có thể đặt khác đi nếu bạn thích)

Mỗi lần HĐH khởi động thì xvnkb cũng được nạp và chạy, chương trình này có sử dụng nhiều bản tham số, trong đó có một bảng tham số thiết lập các thông tin mặc
định về: giao diện ứng dụng **xvnbk** , kiểu gõ phím, mã ký tự...
Khi **xvnkb** khởi động nó sẽ kiểm tra bảng tham số được thiết lập trong tệp **.xvnkbrc** nằm ở thư mục **"tên_người_sử_dụng"** , nếu không có thì chương trình sẽ sử
dụng các thông số mặc định (nghĩa là sẽ giống như bạn chưa thiết lập).
Để đặt lại, bạn làm như sau:
- Đăng nhập với người dùng là: **root**
- Tại terminal, bạn gõ lệnh: **sudo gedit /root/.xvnkbrc**
để tạo ra tệp **.xvnkbrc** nếu chưa có và soạn vào nội dung sau:

```
# xvnkb (VISC Key) configuration file.
# This file will be automatically updated after each session of xvnkb.
# left: 0 - screenwidth, top: 0 - screenheight --- Icon's position.
# enable: 0 -3 ~ (Off,Vni,Telex,Viqr) --- Allow Input method.
# method: 0 -3 ~ (Off,Vni,Telex,Viqr) --- Current Input method.
# charset: 0-5 ~ (Tcvn,Vni,Viscii,Vps,Utf8) --- Input charset.
# font: fontname --- Display font (All items of xvnkb - flash,icon,menu).
# interface: 0 - English, 1 - Vietnamese.
# hotkey: use Key Symbols (e.g. Alt Shift_L).
left 947
top 722
method 2
enable 2
charset 5
spelling 1
interface 1
docking 0
Error!

font helvetica:size=14:style=bold
hotkey Alt Shift_L
```

- Sau khi bạn sửa xong thì cấu hình bộ gõ **xvnkb** chỉ có tác dụng đối với người dùng **root** . Để cho người dùng **khác root** có cấu hình mong muốn, bạn copy tệp đó vào
thư mục:
/home/tên_người_sử_dụng (tên user)
hoặc tại terminal, gõ: **sudo gedit /home/tên_người_sử_dụng/.xvnkbrc** rồi soạn vào nội dung như trên.

- **Logout** , rồi **login** lại, bạn sẽ thấy điều mình mong muốn.

2.5- Cách gỡ hoàn toàn bộ gõ SCIM (nếu đã cài đặt)

- Chọn **System->Administration ->Synaptic Package Manager**
- Bạn chọn **All** và sau đó chọn **Search** , rồi gõ **SCIM :**
- Khi tìm được, bạn chọn đánh dấu gõ bỏ hết các gói liên quan đến SCIM:

Trỏ chuột vào gói cần gỡ bỏ, chọn **Package->Mark for Removal** hay bấm phím **Delete.** Những gói có thể gỡ bỏ được (tức là đã cài đặt) sẽ có biểu tượng hình chữ nhật
màu xanh bên cạnh tên gói (Package), ví dụ như hình sau:

Error!

- Sau đó chọn **Apply** để gỡ bỏ (nếu hệ thống yêu cầu cho đĩa CD chứa Ubuntu thì bạn chiều nó nhé).

Ghi chú : *Nếu bạn không chọn được các gói cần gỡ bỏ (vì một lý do nào đó), bạn chọn mục tên ứng dụng SCIM ở phần bên trái cửa sổ (hình dưới), rồi chọn:* ***Package-> Lock Version*** *để khoá lại và không sử dụng ứng dụng này nữa.*

IV. Đôi điều về Ubuntu 7.04 và Ubuntu 7.10

1- Khi bạn đã update gói tiếng Việt cho Ubuntu 7.04 , để hiểu thị giao diện tiếng Việt cho HĐH bạn thực hiện:

Chọn: **System->Administration ->Language Support -** > trong mục: **Default Language** , bạn chọn **Vietnamese ->Apply -> OK** .

2- Muốn giao diện trong OpenOffice.org hiển thị tiếng Việt, bạn làm như sau:

- Mở **OpenOffice.org**
- Chọn **Tools->Option...-> Language Settings -> Languages ->** chọn mục **User Interface->** chọn **Vietnamese -> OK .**

Error!

3- Nhiều máy tính, khi bạn khởi động từ đĩa Live CD Ubuntu thì màn hình không thể hiển thị được giao diện đồ hoạ (gần giống như là treo máy, tuy nhiêu không
hẳn thế), nguyên do là việc các trình điều khiển thiết bị đã tích hợp sẵn không tương
thích với cấu hình phần cứng (phần cứng có những vấn đề về tương thích, đặt biệt là
trình điều khiển card video, theo tài liệu hệ thống, trình điều khiển video được tích hợp
trong Ubuntu không phải là tổng hợp tất cả các trình điều khiển video hiệu nay trên thị
trường. Để có thể chạy được trên nhiều máy, chúng đã sử dụng phương pháp "tương

đương" và "ép kiểu"). Khi đó bạn ít có khả năng để tiến hành cài đặt Ubuntu (7.10 Desktop và 7.04 Desktop, các phiêu b ản cũ tôi không đề cập ở đây), nhưng bạn vẫn có
thể sử dụng bản Ubuntu Server để cài đặt. Bản này khi cài đặt không chạy ở chế độ đồ
hoạ, khi cài đặt xong bạn có thể update các gói chứa driver mới nhất và các gói khác
phục vụ cho việc chạy HĐH ở chế độ đồ hoạ (có 2 cách: kết nối internet và cập nhập;
cách 2: cập nhập offline bằng các gói mà bạn đã lấy từ internet về, trường hợp này bạn
chỉ mấy công download từ internet về 1 lần. Chúng tôi đã sử dụng giải pháp này để cài
những máy "khó tính" và kết quả là rất tốt).

4- Một điều cần lưu ý là, khi cài đặt Ubuntu 7.04 thì bạn phải chọn ngôn ngữ mặc định là tiếng Anh , nếu bạn chọn là tiếng Việt thì sẽ gặp lỗi khi cài trình quản lý
khởi động GRUB, nếu bạn thích HĐH hiển thị giao diện tiếng Việt, bạn làm như mục 2
ở trên trong phần này. Đó là hạn chế của Ubuntu 7.04, đối với Ubuntu 7.10 thì vấn đề
này đã được giải quyết, tuy nhiêu trình quản lý khởi động GRUB có vẻ không "thông
minh" lắm đối với việc cài nhiều HĐH trên một máy, chẳng hạn khi cài 5 hệ HĐH trên
cùng 1 máy mà tôi thử (Windows 2003, Fedora, CMC Linux, Redhat AS 4, Ubuntu7.10
Desktop, Ubuntu Server 7.04), khi đó tôi ph ải dùng phương pháp thủ công để tạo dựng
menu cho GRUB thì mới dùng được đủ cả 5 HĐH.

Error!

UBUNTU 7.0.4

CÀI ĐẶT CÁC ỨNG DỤNG CỦA WINDOWS TRÊN UBUNTU

I. Hướng dẫn cài WINE trên Ubuntu.

Để chạy một chương trình Windows trên Linux có thể dùng **wine** . **Wine** không phải
là một dạng mô phỏng như máy ảo mà nó sử dụng các Windows API để chạy ứng dụng.
(trường hợp máy tính bạn không có kết nối internet).

1. Bạn phải download tệp sau (link download ở cuối tài liệu này):
+ **wine_0.9.45~winehq0~ubuntu~7.04 -1_i386.deb**
Nếu báo lỗi, bạn nên cài thêm:
+ linux-libc-dev_2.6.20 -16.32_i386.deb
+ libc6-dev_2.5-0ubuntu14_i386.deb
+ wine_0.9.45~winehq0~ubuntu~7.04 -1_i386.deb
+ wine-dev_0.9.45~winehq0~ubuntu~7.04 -1_i386.deb
2. Chạy tệp trên bằng lệnh (vào thư mục chứa tệp trên nhé):
sudo dpkg -i <tên tệp DEB> (cho từng tệp một)
hay **sudo dpkg -i *.deb**
(cho tất cả các tệp)
Chú ý : - *Bạn có thể nháy đúp chuột vào tệp trên và làm theo hướng dẫn trên màn hình .*
*Sau khi cài, bạn có thể cấu hình **wine** , bằng cách dùng lệnh sau tại cửa sổ terminal:*
winecfg
II. Cài các ứng dụng của Windows trên Ubuntu
1) Điều kiện:
- Trên Ubuntu phải cài wine .
Vậy wine là gì ? Wine tạo cho những chương trình của Window có thể chạy song song với bất kì hệ điều hành nào. Wine là một sự thực thi của thư viện Windows Application Programing Interface (API), ho ạt động như một cầu nối giữa Windos và
Linux. Có thể hiểu Wine như một lớp tương thích, khi một phần mền của Window yêu
cầu thực thi 1 hàm mà Linux không hiểu một cách thông thường, thì Wine sẽ dịch lệnh
của chương trình thành 1 dạng những lệnh tương đương của Linux nhằm giúp cho hệ
thống Linux hiểu và thực thi được. Nếu ta phải truy xuất mã nguồn của những chương

trình Window, Wine có thể cũng được dùng để biên dịch ngược (recompile) chương
trình thành 1 dạng mà Linux có thể hiểu một cách dễ dàng hơn.
- Nơi để cài đặt các ứng dụng của Windows trên Ubuntu là những nơi mà hệ

thống cho phép user (khác **root**) đang làm việc ***có thể ghi được*** (lưu ý **quyền đọc** là **all**
rồi). Mặc định đó là folder (thư mục) bắt đầu ("gốc") ứng với người sử dụng đó và được
khởi tạo trong **/home** , ví vụ: **/nguyenthihien** . Tất cả các thư mục (folder) tạo từ đây thì
user này đều có **quyền ghi/xoá/thêm** ...
- **Cài wine** ? bạn xem **mục I** ở trên.

2) Drive mapping - Ánh xạ các ổ đĩa trong wine

Để một ứng dụng chạy trên môi trường Windows có thể chạy được trong Ubuntu thì phải thông qua **wine** . Khi bạn thực thi một ứng dụng nào của Windows trên ubuntu
thì **wine** tạo ra một môi trường hỗ trợ riêng, đó là các bảng tham số nhằm cung cấp cho
ứng dụng một số thông tin cần thiết. Như ta biết, bảng màu cho màn hình làm việc (Windows Themes/Skins In Wine) ch ẳng hạn, hay các ứng dụng trên windows khi cài
đặt hay đọc ghi dữ liệu đều tham chiếu **theo ổ đĩa** . Mặt khác trong Ubuntu không sử
khái niệm ổ đĩa C:, D:,... Vậy phải làm thế nào ?
Để giải quyết vấn đề này **wine** tạo ra một bảng tham chiếu, chẳng hạn như sau:

Số thứ tự (mapping)	**Windows** **Tương ứng - ánh xạ 1-1** **Linux hoặc Ubuntu**
1	**C:** Drive Mapping **/home/nguyenthihien/.wine/drive_c**
2	**D:** Drive Mapping **/home/nguyenthihien/**
3	**E:** Drive Mapping **/**
4	**F:**

Drive Mapping
/home/
5
Z:
Drive Mapping
/home/nguyenthihien/
2
Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
Nhận xét:
+ Bạn thấy tôi đã khai báo (ánh xạ) **một** thư mục **/home/nguyenthihien** cho tương ứng với **2** ổ trên Windows là **D:** và **Z: .**
+ Như vậy, từ bảng này (giả định để làm căn cứ lập luận) khi bạn cài ứng dụng của Windows trên Ubuntu chỉ được cài trên các ổ **C:, D:, Z:** , với các ổ còn lại bạn sẽ
không ghi được, mặc dù bạn đã tạo ra bảng tham chiếu trên. Điều đó sẽ giải thích hiện
tượng sau đây:
- Khi tôi cài **notes** và chọn cài trên ổ khác với các ổ **C:, D:, Z:** thì sẽ lỗi ngay:
3
Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
- Giả sử tôi chọn nơi cài notes là **Z:** thì **OK** luôn:
4
Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
+ Bạn lưu ý là trong thư mục **/home/<tên_user>/.wine/drive_c** (trên Ubuntu) hay ổ **C:** trên Windows khi bạn cài **wine** sẽ tạo ra 2 thư mục: **Windows** và **Program file** ,
như vậy nó sẽ có sự tương ứng:
C:\ Windows
<---->
/home/<tên_user>/.wine/drive_c /Windows
C:\ Program Files

<-----> **/home/<tên_user>/.wine/drive_c /Program Files**
Quá dễ chịu phải không ?
3) Đọc, ghi trên các ổ đĩa đã ánh xạ trong wine
Nếu bạn có cài **NTFS-3g** thì dù bạn là **user** không phải là root cũng vẫn đọc/ghi được với các phân vùng **NTFS** (đối với phân vùng **FAT** thì hiển nhiên **đọc/ghi** tốt). Tuy
nhiên khi cấu hình đọc ghi các phân vùng **NTFS** bằng **NTFS-3g** , bạn đã ánh xạ các phân
vùng đó thành các thư mục trong **/media** , ví dụ:

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
Số thứ
Phân vùng
Linux hay Ubuntu
tự
NTFS tương ứng - ánh xạ 1-1
1
sda1
<---------->
/media/Win_C
2
sda3
<---------->
/media/Win_D
- Các thư mục **Win_C, Win_D** là những thư mục đã được tạo ra và để ánh xạ tương ứng với các **sda1, sda3** khi cấu hình **NTFS-3g** , bạn chịu khó xem lại tài liệu nhé.
- Do vậy, khi bạn định nghĩa các ổ trong **winecfg** bạn lưu ý là các thư mục này mới cho phép đọc ghi được.
- Để kiểm tra, bạn có thể xem thư mục sau:
/home/nguyenthihien/ .wine /dosdevices
● Những ổ có biểu tượng chiếc khoá là những nơi bạn không ghi vào được.
● Nếu bạn định nghĩa một ổ nào đó trong **winecfg** mà không phải là ổ, thư mục cho phép ghi được thì các ổ đó cũng không ghi được.

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
4) Chạy Notes trên Ubuntu
+ Giải quyết bài toán 1 : Bạn copy **notes** từ máy đang dùng từ **Windows sang Ubuntu** thì cần lưu ý những gì?
- Khi bạn cài **notes** (trên Ubuntu) thì tệp **notes.ini** được mặc định lưu ở t **hư mục Windows** , trong tệp này có tham số chỉ đường dẫn, dẫn tới nơi chứa chương trình **notes .**
Nếu trong thư mục đó không có thì nó tìm ở đâu? Đó là thư mục **chứa notes** , sau đến là
thư mục / **home/<tên_user>** . Như vậy nếu bạn copy sang **Ubuntu** và để vào thư mục
/home/<tên_user>/.wine/drive_c
(tương ứng là **C:**\ đấy !), thì:
● Copy tệp **notes.ini** vào **/home/<tên_user>/.wine/drive_c/windows**
● Mở tệp **notes.ini** và xoá và để lại **6** dòng đầu và sửa lại 2 dòng là:
Directory=C: \notes\data
WinNTIconPath=C: \notes\data\W32
- Nếu bạn sửa 2 dòng trên và thay ổ đĩa là khác **C:** , chẳng hạn là **D:** hay **E:** ... thì **notes** sẽ không chạy được, bạn dễ dàng giải thích được tại sao rồi *(xem mục 2).*
Directory= D: \notes\data
WinNTIconPath= D: \notes\data\W32
- Vậy, để nếu thay **C:** bởi **D:** vào mà **notes** vẫn **chạy "ầm ầm"** thì phải làm thế nào? Có 2 cách giải quyết:

Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
Cách 1:
● Như ta biết (ở trên), ổ **D:** ở đây là thư mục **/home/<tên_user>/** trong Ubuntu (cụ thể là **/home/nguyenthihien).** Cho nên bạn **copy** thư mục **notes** trong **/home/<tên_user>/.wine/drive_c** sang **/home/<tên_user>/**
(tức là
thư mục **/home/nguyenthihien) .**
Cách 2:
● **Định nghĩa một ánh xạ nữa là các ổ không phải là ổ C:** đều trỏ về cùng 1 thư mục **cài notes** trên **Ubuntu** , ví dụ:
Số thứ

Windows tương ứng - ánh xạ 1-1
Linux hay Ubuntu
tự
(mapping)
3
C:
Drive Mapping
/home/nguyenthihien/.wine/drive_c
4
D:
Drive Mapping
/home/nguyenthihien/.wine/drive_c
● Cách thực hiện, tại của sổ termianl bạn gõ lệnh sau:
winecfg
8
Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
Bây giờ thì **OK** rồi. Bạn có thể định nghĩa thêm các ổ đều trỏ về thư mục: **/home/<tên_user>/.wine /drive_c** và khi đó thì bạn vô tư luôn không cần lưu ý khai báo đường dẫn trong tệp **notes.ini** nhé.
+ Giải quyết bài toán 2 : Hiển thị font t **iếng Việt trên Notes.**
- Bạn copy **3 tệp font** hệ thống của **bộ font ABC :**
SSERIFE.FON
VGAFIX.FONT
VGASYS.FON
vào thư mục:
/home/<tên_user>/.wine/windows/fonts
-Nếu bạn là ***root*** thì:
/root/.wine/windows/fonts
Lưu ý: *Nếu chưa có 3 tệp* ***font ABC*** *trên, bạn có thể tải về tại địa chỉ trang web ở cuối tài liệu này.*
5) Cài các ứng dụng của Microsoft Windows trên Ubuntu.
+ Chuyển vào thư mục chứa chương trình cài cần đặt.
+ Tại cửa sổ gõ lệnh, bạn gõ:
wine <tên ứng dụng cần cài>
Nếu thư mục hiện hành không phải là thư mục chứa chương trình thì bạn có thể dùng lệnh sau: **wine /<đường dẫn>/<tên ứng dụng cài đặt>**
6) Cài bộ gõ tiếng Việt trên wine

+ **Nhận xét:** Với mỗi môi trường phải có bộ xử lý tiếng Việt riêng, như vậy để có thể gõ được tiếng Việt trên các ứng dụng Windows phải phải cài bộ gõ **tiếng Việt for**
Windows như **VietKey** hay **Unikey** . Cách cài như sau (tại cửa sổ terminal), gõ:
wine / <đường dẫn>/ <tên ứng dụng cài đặt>
Ví dụ: Giả sử bộ unikey của tôi để tên thư mục Desktop, thì:
wine /home/nguyenthihien/Desktop/ UnikeySetup.exe
+ Sau khi bạn cài bộ xử lý tiếng Việt **Unikey** (bạn có thể chạy các ứng dụng của Windows, chẳng hạn như **notes** và gõ tiếng Việt vô tư nhé).
7 **) Tạo biểu tượng shortcut các ứng dụng của Windows trên Desktop,** ví dụ sau đây minh hoạ phương pháp, bạn có thể mở rộng.
9
Error!

Nguyễn Thị Hiền - Lạng Sơn
Ubuntu 7.0.4 Desktop
+ Trên màn hình **Desktop của ubuntu** , trỏ chuột ra ngoài các đối tương đang có và **bấm nút phải chuột** và chọn: **Create Launcher...**
Khi đó, bạn phải:
- Khai báo tên chương trình vào mục **Name .**
- Chọn kiểu: **Type** (nếu cần, mặc định là ứng dụng rồi).
- **Lệnh (Comamnd)** , dòng phải thật chính xác 100% đấy. Ví dụ:
wine /home/nguyenthihien/.wine/driver_c/notes / notes.exe
(dòng này không thể thiếu nhé).
- **Icon** : Biểu tượng (nếu cần).
- **Comment** : tuỳ ý nhé!
+ Khai báo xong, chọn **OK .**
Toàn bộ các tệp của các chương trình dạng **.DEB** được lưu trên trên trang Web: **http://download.lso.dcs.vn/index.html** của Văn phòng Tỉnh uỷ Lạng Sơn *(soft R-Z, mục Ubuntu)* , các bạn có thể tải về bất kỳ lúc nào. Thời gian có hạn nên việc soạn có thể
vẫn còn nhiều sai sót (tôi đã test nhưng khó có thể kiểm tra được hết những khả năng),
rất mong được sự đóng góp của các bạn. Chúc các bạn gặp nhiều may mắn.
10

Giả sử máy bạn đang sử dụng Windows XP, đang chia ổ cứng (vật lý) thành 3 ổ C, D và E, bạn cần thiết chuyển dữ liệu từ ổ E sang máy khác hoặc sang ổ C, D và dành ổ E cài đặt Ubuntu 7.04.

1. Cho đĩa Ubuntu 7.04 vào ổ CD và khởi động máy tính (chắc chắn rằng máy tính của bạn đã set để boot từ ổ CD-ROM). Từ màn hình xuất hiện, chọn ***Start or install Ubuntu*** và nhấn ***Enter***. Cần phải chờ một thời gian để chương trình chạy.

Error!

2. Sau khi Ubuntu đã chạy xong, màn hình dưới đây sẽ hiện ra, nhấp đúp chuột vào biểu tượng ***Install*** để bắt đầu cấu hình cho Ubuntu.

Error!

3. Màn hình tiếp theo nhắc bạn lựa chọn ngôn ngữ, ở đây tôi chọn English và nhấp chuột vào ***Forward***.

Error!

4. Màn hình tiếp theo sẽ nhắc bạn chọn location, bạn chọn xong và nhấp chuột vào ***Forward***.

Error!

5. Bây giờ bạn phải chọn kiểu bàn phím của bạn. Chọn xong lại tiếp tục nhấp chuột vào ***Forward***.

Error!

6. Mất một chút thời gian để chương trình chuẩn bị ổ đĩa. Tại màn hình xuất hiện, đánh dấu chọn ***Manual*** và nhấp chuột vào ***Forward***.

Error!

7. Tại màn hình tiếp theo là *Prepare partitions*, bạn cần phải thật **cẩn thận**. Lựa chọn ổ đĩa E, thường là ổ đĩa cuối cùng trong danh sách hiện ra, để tạo partition "SWAP" và root của Ubuntu. Đầu tiên là tại SWAP file. Nhấp phải chuột vào ổ đĩa E (là ổ đĩa cuối cùng), chọn Delete partition. Sau đó tiếp tục nhấp phải chuột vào ổ đĩa này (bây giờ là free space), chọn *New partition*. Trong phần *Type for the new partition* chọn *Primary*. Trong ô *New partition size in megabytes* đặt giá trị gấp đôi dung lượng của RAM. Trong phần *Location for the new partition* chọn *Beginning*. Trong ô *Use as*, chọn *SWAP*. Nhấp chuột vào nút *OK*.

Error!

8. Tiếp theo bạn sẽ tạo ổ cứng cho Ubuntu. Nhấp phải chuột vào ổ *free space* và chọn *New partition*. Giữ nguyên giá trị mặc định trong ô *New partition size in megabytes*. Trong phần *Location for the new partition* chọn *End*. Trong ô *Use as*, chọn *ext3*. Trong ô *Mount point*, đánh dấu /. Nhấp chuột vào nút *OK*.

Error!

9. Chọn ổ cứng cuối cùng (có Type là ext3, Mount point là /) và nhấp chuột vào *Forward*.

Error!

10. Tại màn hình tiếp theo sẽ nhắc bạn nếu bạn muốn import các accounts của Windows XP. Nếu cần thì thực hiện, nếu không cần có thể bỏ qua. Nhấp chuột vào *Forward*.

11. Màn hình tiếp theo yêu cầu bạn nhập thông tin cá nhân. Sau khi nhập xong, nhấp chuột vào *Forward*.

Error!

12. Màn hình tiếp theo thông báo cho bạn các thông tin bạn đã cài đặt, nhấp chuột vào nút *Install* để bắt đầu cài đặt. Quá trình cài đặt sẽ diễn ra khá lâu, nhưng ngay lúc này bạn đã có thể thám hiểm Ubuntu được rồi.

Bạn đã hoàn thành cài đặt chạy song song giữa 2 hệ điều hành Windows XP và Ubuntu 7.04.

(Theo Internet)

Error!

UBUNTU 7.0.4

CÀI ĐẶT - GỠ BỎ - BIÊN DỊCH - CHUYỂN ĐỔI DẠNG GÓI CÁC ỨNG DỤNG TRÊN UBUNTU

A. MỞ ĐẦU

Tài liệu này hướng dẫn khi máy của bạn không kết nối với được với Internet, trường hợp nếu đang kết nối với Internet thì mọi việc sẽ khác và sẽ không giống như tài liệu này. Rất mong phần nào giúp được các bạn qua trang viết này.

Để cài đặt và thực hiện các hướng dẫn sau, bạn phải **login** với **account root** .

1) RPM ?

Đóng gói **RPM** , **RPM** Package Management là một trình quản lý gói được sử dụng bởi nhiều Linux Distribution, như **Redhat** , **Suse** , **Mandrake** , … Khi các phần mềm đã được đóng gói dưới dạng **RPM** , người sử dụng chỉ việc download về và cài đặt qua tiện ích của **rpm** . Tuy nhiên có nhiều phần mềm chỉ cung cấp dưới dạng **source code** (**tgz, tar.gz, tar.bz2**). Người dùng có thể sử dụng những **source code** này hoặc người dùng có thể phát triển riêng phần mềm của mình để đóng gói thành gói tin **rpm** và phân phối lại cho cộng đồng sử dụng. Vậy cấu trúc gói tin **rpm** và cách đóng gói chúng như thế nào?

Các gói **RPM** thực chất chỉ chứa các file đã được biên dịch và một số file khác

như file cấu hình, các văn bản của gói phần mềm dạng mã nguồn. File **RPM** nếu được
cài đặt thành công sẽ tạo hệ thống chạy được ngay vì thực chất nó là sự triển khai các
file đã được biên dịch và các file cấu hình, các file văn bản vào các vị trí thích hợp để
phần mềm có thể chạy ngay lập tức. Một gói được đóng dưới dạng RPM có thể coi như
một gói cài đặt dạng **setup.exe** trong Windows.
Quá trình tạo file **RPM** chỉ là việc lựa chọn từ hệ thống file đã được biên dịch của các gói mã nguồn để đưa vào gói **RPM** . Khi đưa gói **RPM** tới nơi khác cài đặt, gói
RPM sẽ tự động thực hiện việc giải bung các file tới các vị trí thích hợp như chính các
file đó được bố trí trên máy đã cài bằng gói mã nguồn. Như phần dưới đây sẽ trình bày,
bước xây dựng **file .spec** là quan trọng nhất trong đóng gói **RPM** vì chính file này hướng dẫn quá trình tạo lập ra file **RPM** . Nó nói cho trình tạo **RPM** biết phải copy các
file nào, thiết lập các thông số cho gói **RPM** ra sao. Trong chính file này, người dùng
cũng có thể can thiệp vào các file và các thư mục sẽ được cài đặt, thiết lập các thông số
cho gói mã nguồn sẽ được được biên dịch và do đó ảnh hưởng tới file **RPM .**
Quy trình đóng gói một gói tin rpm bao gồm:
- *Chuẩn bị mã nguồn (* ***.tar.gz, .tar.bz2*** *),*
- *Cập nhật các bản vá cho các file mã nguồn nếu có,*
- *Tạo file spec,*

Error!

Nguyễn Thị Hiền - VPTU Lạng Sơn
Ubuntu 7.0.4 Desktop
- *Xây dựng gói rpm qua lệnh rpmbuild.*

Cả quá trình này phức tạp nhất và cũng quan trọng nhất là tạo được **file spec** hoạt động đúng và phù hợp với hệ thống, để xây dựng được gói **rpm** hoàn chỉnh.
File spec là một file hướng dẫn cách xây dựng phần mềm và danh sách các file được cài đặt.
Quá trình xây dựng diễn ra bao gồm các bước theo mô tả trong **file spec** . Nếu thành công, quá trình này sẽ tạo ra **3 file** đóng gói:
<tên_gói> -<phiên_bản>.i386.rpm

<tên_gói> -debug-info-<phiên_bản>.rpm
<tên_gói> -<phiên_bản>.src.rpm
Với gói đầu, người sử dụng có thể đem đi cài tại các máy có chương trình **rpm** đã được cài đặt. Việc cài đặt gói này được thực hiện bằng lệnh **rpm -i <tên gói>** và cài đặt
thành công với điều kiện các gói phụ thuộc của nó đã được cài trên máy. Gói thứ hai
dùng để kiểm tra lỗi biên dịch cho gói thứ nhất. Việc cài đặt gói này hay không không
quan trọng lắm tới việc sử dụng phần mềm do gói đầu cài đặt. Với gói thứ ba, người
dùng có thể cài nó và kết quả của việc cài là file mã nguồn và **file SPEC** đã được dùng
để tạo ra gói **.rpm** nói trên. Người sử dụng cuối vẫn có thể biên dịch lại mã nguồn này
và tạo thành gói **.rpm** khác.
Việc phân phối gói **.rpm** dưới dạng gói đầu hay gói thứ ba đều chấp nhận được và người dùng cuối đều có thể sử dụng hai gói này để chạy phần mềm cần cài đặt. Với cách
phân phối theo gói thứ 3, người sử dụng cuối có thể chỉnh sửa thêm một số thông số cho
phù hợp nhu cầu riêng. Điều này đảm bảo nguyên lý của GPL là mã nguồn có thể được
tự do phân phối và chỉnh sửa.
Như vậy, **RPM** là một chuẩn phân phối phần mềm phổ biến và tiện dụng trên nền Linux. Các gói phần mềm có thể đóng gói một cách mềm dẻo thành các gói **RPM** với
các thông số cài đặt và cấu hình khác nhau. Đây cũng là một nhân tố đảm bảo việc tạo
sự đa dạng hóa trong các gói mã nguồn cung cấp cho hệ thống đĩa cài chuyên dụng.
2) DEB ?
Phần mềm mã nguồn mở là những phần mềm cung cấp **source code** cho người dùng. **Source code** này thường được viết bằng các ngôn ngữ lập trình như **C, perl** . Vì
vậy để chạy được, chúng cần phải được biên dịch ra **file binary** bằng trình biên dịch như
GCC, G++, perl , ...
Các file đuôi **.tar.gz, tar.bz2, tgz l** à các file **source code** của phần mềm mã nguồn mở.

Các file đuôi **.rpm, .deb** là bản đóng gói chứa các file **binary** của phần mềm. Việc cài đặt chúng chỉ là giải nén ra các thư mục và chạy (tương tự . **exe** của **Windows**).
Các tệp định dạng **.deb** thường được dùng trên các hệ thống Debian, Kubuntu, Ubuntu.

B. NỘI DUNG

1. Cài đặt và gỡ bỏ phần mềm có tập tin dạng DEB

Khi cài đặt hoặc gỡ bỏ phần mềm, nếu bạn đăng nhập với user **không phải ROOT** , Ubuntu sẽ yêu cầu bạn nhập mật khẩu (pasword) để xác nhận.

a) Cài đặt một phần mềm có dạng đuôi tập tin .deb

- Nếu máy bạn kết nối với Internet thì mọi việc thật là ... mình không cần nói nữa. Trường hợp không kết nối thì bạn copy các tệp . **deb** cần cài đặt về máy rồi tiến hành cài
đặt nhé.

Cách 1 : nháy đúp chuột vào từng tệp cần cài đặt, đợi đến khi xuất hiện một cửa sổ bạn
chọn **Install Package** để tiến hành cài đặt.
Sau khi cài đặt xong, bạn nháy vào nút **Close** để đóng của sổ.

Cách 2 : dùng lệnh (tại cửa sổ Terminal), Applications/Accessories/Terminal.
Cú pháp lệnh TQ: **sudo dpkg -i <đường dẫn/tệp dạng DEB>**
Chú ý:

1. Nếu bạn không muốn phải gõ đường dẫn, bạn dùng lệnh **cd <đường dẫn>** để chuyển vào thư mục chứa các tệp cần cài đặt.

2. Nếu cần cài đặt nhiều gói trong 1 thư mục, bạn chuyển đến thư mục chứa các gói cài đặt và gõ lệnh (nếu bạn không chuyển tới thư mục đó thì phải chỉ đường dẫn tới
các tệp đó): **sudo dpkg -i *.deb** . Khi bạn dùng lệnh này thì không cần để ý đến thứ tự
các gói nữa, hệ thống sẽ cài đặt tất cả các gói **.deb** trong thư mục hiện hành.
Như vậy, đối với những ứng dụng đòi hỏi phải cài nhiều gói, thì bạn sử dụng cách 2 sẽ tiện lợi hơn rất nhiều.

Ubuntu 7.0.4 Desktop

b)Gỡ bỏ (uninstall) một phần mềm theo dạng đuôi tập tin .deb,

Cách 1 : Chọn loại bỏ trong chương trình quản lý phần mềm
ở chế độ đồ hoạ.

- Chọn **Applications -> Add/Remove ->** chọn phần mềm cần cài hay gỡ bỏ:
- Nháy đúp chuột vào tên phần mềm cần gỡ bỏ (chẳng hạn, hình sau):
- Sau đó chọn **Apply**
- Chương trình đưa ra các gói trong ứng dụng cần gỡ bỏ:

Error!

- Bạn chọn **Apply** để đồng ý.

Cách 2: Gõ lệnh trong cửa sổ terminal:

sudo dpkg -r <tên_phần_mềm>

c) Chú ý : Khi bạn có kết nối Internet :

+ Cập nhật tất cả các gói hiện tại:

sudo apt-get update

+ Tìm gói theo từ khóa:

apt-cache search <từ cần tìm-keywords>

+ Lấy thông tin về gói:

apt-cache show <tên chương trình>

+ Cài một gói (chương trình) mới:

sudo apt-get install
<tên_phần_mềm>

+ Dỡ bỏ gói (chương trình):

sudo apt-get remove <tên_phần_mềm>

sudo apt-get remove --purge <tên_phần_mềm>

2. Biên dịch, cài đặt phần mềm từ mã nguồn (source):

Khi mà tất cả các công cụ trên không thể cài đặt được phần mềm bạn cần, hoặc phần mềm bạn cần chỉ ở dạng mã nguồn thì bạn cần biết cách cài một phần mềm từ mã
nguồn như thế nào ?

Error!

Các bước để cài đặt như sau :

- Cài đặt chương trình dịch.
- Lấy mã nguồn từ trang cung cấp mã nguồn từ trang cung cấp mã nguồn.
- Cài đặt các thư viện phần mềm yêu cầu (library dependencies).
- Dịch và cài phần mềm.

C **ụ thể** (tham khảo thêm phụ lục):

B1: Cài đặt chương trình dịch *(máy có nối mạng internet).*

sudo apt-get install build-essential

B2: Lấy mã nguồn từ trang cung cấp mã nguồn

Giải nén: **tar xvzf <tên chương trình dạng .tar.gz>**

B3: Cài đặt các thư viện phần mềm yêu cầu (library dependencies *)* **.**

Thường thì khi bạn cài phần mềm từ mã nguồn, nếu thiếu dependencies, Ubuntu sẽ báo cho bạn biết.

B4: Dịch và cài phần mềm:

B4.1: configure

/<thư mục chứa chương trình>$ **./configure**

B4.2: compile

/<thư mục chứa chương trình>$ **make**

B4.3: install

/<thư mục chứa chương trình>$ **sudo make install**

3. Cài đặt gói ALIEN

Mục đích: Cài gói công cụ này nhằm mục đích hỗ trợ cho việc chuyển đổi định dạng của các tập tin sẽ thực hành dưới đây.

Gồm các bước sau (quy trình sau không cần bạn phải kết nối internet):

1 . Khởi động Ubuntu và đăng nhập với account ROOT.

2 . Copy **10 t** ệp sau vào một thư mục nào đó và tiến hành cài đặt **theo thứ tự** sau (*xem cách cài đặt tại mục 1):*

1- **libbeecrypt6_4.1.2 -6build1_i386.deb**
2- librpm4_4.4.1 -14build1_i386.deb
3- rpm_4.4.1 -14build1_i386.deb
4- dpkg-dev_1.13.24ubuntu6_all.deb
5- gettext_0.16.1 -1ubuntu2_i386.deb
6- intltool-debian_0.35.0+20060710.1_all.deb
7- html2text_1.3.2a -3_i386.deb
8- po-debconf_1.0.8_all.deb

Error!

9- debhelper_5.0.42ubuntu1_all.deb

10- alien_8.65_all.deb

4. Chuyển đổi các tệp dạng: RPM sang DEB

Mục đích : Trên thực tế có nhiều ứng dụng, đặc biệt các driver cho các thiết bị như máy in, máy quyét, camera... hay ở cách dạng cho Windows hoặc cho Linux và
thuộc loại RPM. Vậy để cài đặt các ứng dụng, driver đơn giản trên Ubuntu nhiều khi ta
phải chuyển đổi dạng. Để chuyển đổi được trên máy bạn phải cài gói **ALIEN (phần 1) .**

Cú pháp lệnh :

sudo alien -d <Đường dẫn>/<Tên tệp cần chuyển đổi .RPM>

Ví dụ 1 :

sudo alien -d /home/hien/Desktop / AVerMedia -5-0.35Beta-1.i386.rpm

***Ví dụ 2* :** Đổi tệp driver của máy in Cano LBP -3000 từ dạng RPM sang DEB.

sudo alien -d /root/Desktop/CAPTlinux_1 -1/ cndrvcups -capt-1.10-1.i386.rpm

Kết quả thành tệp: **cndrvcups -capt_1.10-2_i386.deb**

5. Cài đặt Microsoft Windows Fonts (MS fonts) t rên Ubuntu.

Các file word gõ từ Windows sẽ không hiển thị tốt trên Ubuntu do thiếu fonts, để cài
thêm font MS cho Ubuntu có 2 cách như sau :

1. *Cách 1* : Cài fonts bằng tay

Thư mục fonts của Ubuntu là **/usr/share/fonts fonts truetype** có thư mục:
/ **usr/share/fonts/truetype/** , bạn chỉ cần copy các **fonts** của **window** s vào thư mục
/ **usr/share/fonts/truetype/** này là **OK .**

Ví dụ:

Giả sử bạn có thư mục fonts của Windows: **/media/fonts**

+ **cd /media/fonts**

(chuyển vào thư mục này).

+ **sudo cp**

*** /usr/share/fonts/truetype**

(copy tất cả các tệp trong thư mục này
vào thư mục **/usr/share/fonts/truetype** .

2. *Cách 2:* Cài gói **msttcorefonts**

+ Bạn cài các gói sau (địa chỉ tải tệp ở cuối bài này)

- cabextract_1.2 -2_i386.deb

- msttcorefonts_1.8ubuntu1_all.deb

sudo dpkg -i cabextract_1.2 -2_i386.deb msttcorefonts_1.8ubuntu1_all.deb

Error!

Nguyễn Thị Hiền - VPTU Lạng Sơn
Ubuntu 7.0.4 Desktop
Chú ý: Nếu máy bạn nối internet thì dùng lệnh sau:
sudo apt-get install msttcorefonts
Phụ lục: Cài thư viện cho biên dịch các gói phần mềm
1. Bạn phải cài bổ sung các thư viện cơ bản sau:
a) Build-essential:
build-essential_11.3_i386.deb
g++_4%3a4.1.2 -1ubuntu1_i386.deb
g++-4.1_4.1.2-0ubuntu4_i386.deb
libc6_2.3.6 -0ubuntu20_i386.deb
libc6_2.4-1ubuntu12_i386.deb
libstdc++6 -4.1-dev_4.1.2-0ubuntu4_i386.deb
Bằng lệnh: dpkg -i *.deb
b) Xorg-dev
libdmx-dev_1%3a1.0.2 -2build1_i386.deb
libexpat1-dev_1.95.8-3.4build1_i386.deb
libfontconfig1 -dev_2.4.2-1ubuntu1_i386.deb
libfontenc-dev_1%3a1.0.4 -1_i386.deb
libfs-dev_2%3a1.0.0 -4ubuntu2_i386.deb
libice-dev_2%3a1.0.3 -1build1_i386.deb
libsm-dev_2%3a1.0.2 -1build1_i386.deb
libstdc++6 -4.1-dev_4.1.2-0ubuntu4_i386.deb
libxau-dev_1%3a1.0.3 -1_i386.deb
libxaw7-dev_2%3a1.0.3 -2build1_i386 .deb
libxaw-headers_2%3a1.0.3 -2build1_all.deb
libxcomposite -dev_1%3a0.3.1 -1_i386.deb
libxcursor-dev_1%3a1.1.8 -1_i386.deb
libxdamage -dev_1%3a1.0.3 -3_i386.deb
libxdmcp-dev_1%3a1.0.2 -1_i386.deb
libxevie-dev_1%3a1.0.2 -1_i386.deb
libxext-dev_2%3a1 .0.3-1build1_i386.deb
libxfixes-dev_1%3a4.0.3 -1_i386.deb
libxfont-dev_1%3a1.2.7 -1ubuntu1_i386.deb
libxft-dev_2.1.12-1_i386.deb
libxi-dev_2%3a1.1.0 -1build1_i386.deb
libxinerama -dev_2%3a1.0.1 -4build1_i386.deb
libxkbfile-dev_1%3a1.0.3 -2_i386.deb
libxkbui1_1%3a1.0.2 -2_i386.deb

libxkbui-dev_1%3a1.0.2 -2_i386.deb
8
Error!

Nguyễn Thị Hiền - VPTU Lạng Sơn
Ubuntu
7.0.4 Desktop
libxmu-dev_2%3a1.0.2 -1ubuntu2_i386.deb
libxmu-headers_2%3a1.0.2 -1ubuntu2_all.deb
libxmuu-dev_2%3a1.0.2 -1ubuntu2_i386.deb
libxpm-dev_1%3a3.5.6 -1_i386.deb
libxrandr-dev_2%3a1.2.0 -3ubuntu1_i386.deb
libxrender-dev_1%3a0.9.1 -3_i386.deb
libxres-dev_2%3a1.0.1 -2_i386.deb
libxss-dev_1%3a1.1.0 -1_i386.deb
libxt-dev_1%3a1.0.5 -1_i386.deb
libxtrap-dev_2%3a1.0.0 -3build1_i386.deb
libxtst-dev_2%3a1.0.1 -3build1_i386.deb
libxv-dev_2%3a1.0.1-3ubuntu2_i386.deb
libxvmc1_2%3a1.0.2 -0ubuntu2_i386.deb
libxvmc-dev_2%3a1.0.2 -0ubuntu2_i386.deb
libxxf86dga -dev_2%3a1.0.1 -2_i386.deb
libxxf86misc -dev_1%3a1.0.1 -2_i386.deb
libxxf86vm-dev_1%3a1.0.1 -2_i386.deb
x11proto-bigreqs-dev_1%3a1.0.2 -0ubuntu4_all.deb
x11proto-composite-dev_1%3a0.3.1 -1ubuntu2_all.deb
x11proto-core-dev_7.0.10-1_all.deb
x11proto-damage-dev_1%3a1.1.0 -1build1_all.deb
x11proto-dmx-dev_1%3a2.2.2 -3ubuntu3_all.deb
x11proto-evie-dev_1%3a1.0.2 -4ubuntu1_all.deb
x11proto-fixes-dev_1%3a4.0 -0.1ubuntu2_all.deb
x11proto-fontcache-dev_0.1.2-4ubuntu1_all.deb
x11proto-fonts-dev_2.0.2-5ubuntu1_all.deb
x11proto-gl-dev_1.4.8-1_all.deb
x11proto-input-dev_1.4.1-1_all.deb
x11proto-kb-dev_1.0.3-2ubuntu1_all.deb
x11proto-randr-dev_1.2.1-1_all.deb
x11proto-record-dev_1.13.2-4ubuntu1_all.deb
x11proto-render-dev_2%3a0.9.2 -4ubuntu1_all.deb
x11proto-resource-dev_1.0.2-4ubuntu1_all.deb

x11proto-scrnsaver-dev_1.1.0.0 -1_all.deb
x11proto-trap-dev_3.4.3-5ubuntu1_all.deb
x11proto-video-dev_2.2.2-4ubuntu1_all.deb
x11proto-xcmisc-dev_1.1.2-4ubuntu1_all.deb
x11proto-xext-dev_7.0.2-5ubuntu1_all.deb
x11proto-xf86bigfont-dev_1.1.2-4ubuntu1_all.deb
x11proto-xf86dga-dev_2.0.2-4ubuntu1_all.deb
9
Error!

Nguyễn Thị Hiền - VPTU Lạng Sơn
Ubuntu
7.0.4 Desktop
x11proto-xf86dri-dev_2.0.3-4ubuntu1_all.deb
x11proto-xf86misc-dev_0.9.2-4ubuntu1_all.deb
x11proto-xf86vidmode -dev_2.2.2-4ubuntu1_all.deb
x11proto-xinerama-dev_1.1.2-4ubuntu1_all.deb
xorg-dev_1%3a7.2 -0ubuntu11_all.deb
xserver-xorg-dev_2%3a1.2.0 -3ubuntu8_i386.deb
xtrans-dev_1.0.3-1_all.deb
zlib1g-dev_1%3a1.2.3 -13ubuntu4_i386.deb
c) Gcc xlibs -dev libxft-dev:
libexpat1-dev_1.95.8-3.4build1_i386.deb
libfontconfig1 -dev_2.4.2-1ubuntu1_i386.deb
libfreetype6 -dev_2.2.1-5ubuntu1.1_i386.deb
libice-dev_2%3a1.0.3 -1build1_i386.deb
libsm-dev_2%3a1.0.2 -1build1_i386.deb
libx11-dev_2%3a1.1.1 -1ubuntu3_i386.deb
libxau-dev_1%3a1.0.3 -1_i386.deb
libxdmcp-dev_1%3a1.0.2 -1_i386.deb
libxext-dev_2%3a1.0.3 -1build1_i386.deb
libxft-dev_2.1.12-1_i386.deb
libxi-dev_2%3a1.1.0 -1build1_i386.deb
libxmu-dev_2%3a1.0.2 -1ubuntu2_i386.deb
libxmu-headers_2%3a1.0.2 -1ubuntu2_all.deb
libxmuu-dev_2%3a1.0.2 -1ubuntu2_i386.deb
libxpm-dev_1%3a3.5.6 -1_i386.deb
libxrandr-dev_2%3a1.2.0 -3ubuntu1_i386.deb
libxrender-dev_1%3a0.9.1 -3_i386.deb
libxt-dev_1%3a1.0.5 -1_i386.deb

libxtrap-dev_2%3a1.0.0 -3build1_i386.deb
libxtst-dev_2%3a1.0.1 -3build1_i386.deb
libxv-dev_2%3a1.0.1 -3ubuntu2_i386.deb
x11proto-core-dev_7.0.10-1_all.deb
x11proto-input-dev_1.4.1-1_all.deb
x11proto-kb-dev_1.0.3-2ubuntu1_all.deb
x11proto-randr-dev_1.2.1-1_all.deb
x11proto-record-dev_1.13.2-4ubuntu1_all.deb
x11proto-render-dev_2%3a0.9.2 -4ubuntu1_all.deb
x11proto-trap-dev_3.4.3-5ubuntu1_all.deb
x11proto-video-dev_2.2.2-4ubuntu1_all.deb
x11proto-xext-dev_7.0.2-5ubuntu1_all.deb
x-dev_7.0.10-1_all.deb

Error!

Nguyễn Thị Hiền - VPTU Lạng Sơn
Ubuntu 7.0.4 Desktop
xlibs-dev_1%3a7.2 -0ubuntu11_all.deb
xtrans-dev_1.0.3-1_all.deb
zlib1g-dev_1%3a1.2.3 -13ubuntu4_i386.deb
Chú ý :
1. Nếu máy tính bạn đang kết nối Internet. Từ cửa sổ terminal, bạn gõ các lệnh sau:
sudo apt-get install build-essential
sudo apt-get install xorg-dev
sudo apt-get install gcc xlibs-dev libxft-dev
2. Bây giờ bạn có thể biên dịch các gói chương trình cho dưới dạng mã nguồn, ví dụ như bộ gõ tiếng Việt xvnkb: **xvnkb-0.2.9a.tar.bz2** ...
Toàn bộ các tệp của các chương trình dạng **.DEB** được lưu trên trên trang Web:
http://download.lso.dcs.vn/index.html
(Soft R-Z, mục Ubuntu) của Văn phòng Tỉnh
uỷ Lạng Sơn, các bạn có thể tải về bất kỳ lúc nào. Thời gian có hạn nên việc soạn có thể
vẫn còn nhiều sai sót (tôi đã test nhưng khó có thể kiểm tra được hết những khả năng),
rất mong được sự đóng góp của các bạn. Chúc các bạn gặp nhiều may mắn.

Error!

CÀI ĐẶT OFFLINE INTERNET EXPLORER 6 TRONG UBUNTU DESKTOP 7.1 0

Cài đặt trình duyệt web **Internet Explorer** (IE) trong Ubuntu rất đơn giản nếu máy tính của bạn có kết nối internet, nh ưng hiện nay, theo quy định, những máy trạm trong hệ thống mạng diện rộng khối Đảng khôn g được đồng thời kết nối internet, giải pháp cho vấn đề tr ên là gì, mời bạn tham khảo bài viết dưới đây.

Download các gói cài đặt (**wine_7.10** , **ies4linux-2.0.5, .ies4linux)** *(chú ý, gói cài đặt này đã được sửa 1 chút cho phù hợp với việc cài đặt offline)* .

Bạn tiến hành các bước sau:

Bước 1 . Copy các tệp đã tải về vào máy tính cài Ubuntu, giải nén để có thư mục **wine_7.10, ies4linux-2.0.5.**

Copy tệp **.ies4linux.tar.gz** vào thư mục **/home/ten_nguoi_dung** , giãn nén *(nháy phải chuột vào tệp, chọn* **Extract here**), bạn sẽ có thư mục **/home/ten_nguoi_dung/.ies4linux** *(chú ý: để tránh bị lỗi, bạn cần copy tệp, rồi giãn nén tại đúng thư mục này)* .

Trường hợp bạn không thấy tệp, thư mục nói trên, bạn cần chọn chế độ hiển thị file ẩn (Ctrl + H) .

thư mục

/home/ten_nguoi_dung

phải chuột, chọn

Extract here

Bước 2. Khởi động **Terminal** (Chọn **Applications -> accessories ->**

Terminal).

Bước 3 . Cài **wine và cabextract** *(nếu cài rồi thì bỏ qua bước này)* .

- Dùng lệnh: **cd /<đường dẫn>** để chuyển đến thư mục **wine_7.10 .**

Error!

- Gõ lệnh **sudo dpkg -i *.deb**

Bước 4 . **Cài đặt IE6**

- Chuyển đến thư mục **ies4linux-2.0.5** , lệnh: **cd /<đường dẫn> .**
- Bạn gõ lệnh ./ies4linux, để hệ thống cài đặt IE6.
- Với câu hỏi: Do you want to install IE 5.5 SP2 too? [y / n], And do you want to install IE 5.01 SP2? [y / n], bạn gõ " **y** " hoặc " **n** " rồi gõ Enter, tuỳ theo việc bạn có muốn cài thêm IE 5.5 , 5.01 hay không.
- Gõ Enter để chấp nhận "Default is EN -US. Hit enter to keep it or choose a different one:"
- Is that ok for you? (To configure adv anced options type n) [y / n] , bạn

gõ " **y** " rồi gõ Enter để xác nhận.

Bước 5 . Sau khi hoàn tất việc cài đặt, trên Desktop sẽ xuất hiện biểu tượng internet Explorer 6.0 (và IE5,01, 5,5 nếu bạn chọn cài), các thao tác mở, cấu hình IE tương tự như bạn vẫn thực hiện trên Windows.

Chúc các bạn thành công.

Nguyễn Thị Hiền, *Email: nguyenthihienls@gmail.com*

Error!

CHIA SẺ TÀI NGUYÊN GIỮA UBUNTU VÀ WINDOWS TRONG MẠNG LAN

A. Dịch vụ Samba và Network File System

1. Dịch vụ Network File System

Network File System (NFS) do công ty Sun Microsystems tạo ra với mục đích dùng để chia sẻ các tập tin và thư mục giữa những hệ điều hành UNIX. Với NFS, khi một tập tin hoặc thư mục được dùng chung, nó gần như trở thành một phần hệ thống của người dùng thay vì có mặt trên máy ở xa. Ví dụ nếu người dùng có một máy Linux chứa đầy hệ thống tập tin gồm các trò chơi thì NFS sẽ cho phép người dùng thiết lập hệ thống tập tin game này để nó xuất hiện trên máy của người dùng như là một phần cấu trúc thư mục chuẩn. Mỗi khi truy cập khu vực chứa game, người dùng sẽ đi qua mạng để đến máy khác mà nhờ có NFS nên chẳng có gì khó khăn.

NFS có thể sử dụng cho nhiều kiểu mạng khác nhau nhưng thực tế nó được thiết kế để làm việc với TCP/IP và hiện nay NFS vẫn được sử dụng phổ biến trên các mạng TCP/IP. Do nhiều người ưa chuộng nên NFS đã hình thành trên các hệ điều hành khác để có thể dùng chung thư mục trên các mạng đa chủng loại.

Bên trong hệ điều hành Linux và UNIX, NFS sẽ hoạt động ở chế độ ngang hàng. Điều này có nghĩa máy tính của người dùng có vai trò như một máy khách của dịch vụ NFS trên một máy khác và là máy phục vụ cho những máy khác trên mạng hoặc đồng thời đóng cả hai vai trò.

2. Dịch vụ Samba

Các hệ thống Linux sử dụng giao thức TCP/IP trong kết nối mạng, trong khi đó hệ điều hành của Microsoft sử dụng một giao thức kết nối mạng khác - giao thức Server Message Block (SMB), giao thức này sử dụng NetBIOS để cho phép các máy tính chạy Windows chia sẻ các tài nguyên với nhau trong mạng cục bộ. Để kết nối tới các mạng lớn, bao gồm cả những hệ thống Unix, Microsoft phát triển Common Internet File System (CIFS), CIFS vẫn sử dụng SMB và NetBIOS cho mạng Windows. Có một phiên bản của SMB được gọi là Samba, Samba cho phép các hệ thống Unix và Linux kết nối tới mạng Windows. Các hệ thống Unix/Linux có thể sử dụng các tài nguyên trên hệ thống Windows,

đồng thời nó cũng chia sẻ tài nguyên trên hệ thống cho máy tính Windows. Gói phần mềm Samba có chứa hai daemon dịch vụ và nhiều chương trình tiện ích. Một daemon là *smbd* cung cấp các dịch vụ tập tin và in ấn cho các hệ thống khác có hỗ trợ SMB. Một daemon là *nmbd* cung cấp chức năng phân giải tên NetBIOS và hỗ trợ dịch vụ duyệt thư mục.
Error!

B. Cấu hình chia sẻ files giữa các máy tính cài Ubuntu và Windows trong cùng một mạng LAN.

I. Trên máy cài Windows:

e Bạn cấu hình chia sẻ thư mục như bình thường giữa các máy cài Windows trong mạng LfN (Nháy phải chuột vào thư mục, chọn Sharing and security).

II. Trên máy cài hệ điều hành Ubuntu

1. Cài đặt samba, NFS (nếu cần)

ghi bạn chọn hiệ thống /juản lk /Danh mục dùng chungl sẽ xuất hiện màn hình đề nghị cài đặt dịch vụ *(nếu dịch vụ NFS và SMB chưa được cài đặt trước đó, việc chọn cài riêng SMB hay cả SMB và NFS là tùy mục đích của bạn, giả sử tôi cài 2 dịch vụ trên)* .

e Nếu máy tính cài Ubuntu của bạn có kết nối internet, bạn chọn hInstall servicesl để cài đặt.

e Nếu máy tính của bạn không có kết nối internet, bạn tải gói cài đặt NFS và SMB tm địa chn dưới đâyo

http://download.lso.dcs.vn/softr_z.html#u

p Copy tệp tải về vào máy cài Ubuntu, sau khi giãn nén, bạn sẽ có thư mục hchiaseq.rsl

p ghởi động Terminal, dùng lệnh chuyển vào thư mục hchiaseq.rsl

p Gt lệnh dưới đây để cài đặto

sudo dpkg -i *.deb

2. Sửa tên nhóm máy tính (nếu cần)

e Chọn h **Hệ thống /Quản lý /Danh mục dùng chung** l, bạn chọn tab hThuộc tính chungl, gt tên nhóm vào mục hMiền/Nhóm làm việcl . Nháy vào nút hĐóngl.

Chú ý o

e Tên nhóm máy tính mặc định trong Ubuntu là **mshome .**

u
Error!

e Bạn có thể cấu hình tại máy cài Windows hoặc tại máy cài Ubuntu sao cho tên nhóm tại các máy tính trùng nhau. Nếu tên nhóm trong Ubuntu không

trùng với tên nhóm trong mục Workgroup của máy cài Windowsv tại máy cài Windows bạn có thể không nhìn thấy máy tính cài Ubuntuv khi đó bạn phải gt địa chn IP của máy cài Ubuntu để kết nối.
e Nếu máy tính bạn không phải là máy phục vụ WINS thì không tích chọn mục đó.
3. Đặt mật khẩu người dùng Samba (cần chia sẻ file thuộc quyền người dùng nào, thì bạn đặt mật khẩu samba cho người dùng đó).
p ghởi động Terminal, gt lệnh sauo
sudo smbpasswd -a <ten_nguoi_dung>
p Gt mật khẩu sau dòng lệnho hNew SMB passwordl, rồi ấn phím wNTwx
p Gt lại chính xác mật khẩu đã đặt sau dòng hxetype New SMB passwordl rồi ấn phím wNTwx
Chú ý :
+ Tên tài khoản của người dùng trên Ubuntu trùng với tên tài khoản của người dùng Samba (tức là **Ubuntu_name** trùng **smb_name**). Trong khi đó trên nhiều hệ thống Linux khác thì tên tài khoản Samba có thể trùng với tên tài khoản hệ thống, nhiều tên tài khoản Samba có thể tham chiếu đến cùng một tên tài khoản hệ thống.
+ ghi cần khởi động lại dịch vụ samba, bạn dùng lệnh sauo
sudo /etc/init.d/samba restart
4. Cấu hình chia sẻ thư mục
e Bạn có thể vào hiệ thống /juản lk /Danh mục dùng chungl, rồi sử dụng phương pháp kéo thả thư mục, hoặc nháy vào nút hThêml để chọn thư mục cần chia sẻ. Nhưng theo tôi cách tiện lợi nhất là cần chia sẻ thư mục nào, bạn nháy phải chuột vào thư mục đó và chọn hDanh mục dùng chungl
e Xuất hiện màn hình chia sẻ, bạn chọn
p Chia sẻ quao Mạng Windows (SMB)
y
Error!

p Têno Bạn có thể đặt lại tên chia sẻ của thư mục đã chọn, gt thêm phần chú thích (nếu muốn).
p Nếu bạn bz dấu tích ở ô hchn đọcl thì tại máy tính kết nối, bạn có quyền **xem và sửa** nội dung bên trong thư mục đã chia sẻ, nếu để dấu tích tại ô đó, tại máy tính kết nối, bạn không có quyền sủa nội dung thư mục đã chia sẻ.
p Lựa chọn xong bạn nháy vào hĐồng kl
e Nháy phải chuột vào thư mục, chọn hThuộc tínhl, bạn có thể gán lại quyền cho người dùng, đặt lại hình tượng cho thư mục... (nếu muốn).
C. Hướng dẫn truy nhập tài nguyên giữa máy cài HĐH Windows và máy

cài HĐH Ubuntu .

1. Tại máy cài Windows

e Bạn truy nhập vào máy cài Ubuntu bình thường như giữa các máy tính cài Windows.

p Mở My Network Place, chọn nhóm, chọn máy cài Ubuntu.

p ioặc vào Start/xun, gt {{dia|chi|IP|may|Ubuntu, rồi ấn wNTwx

e Xuất hiện hộp thoại hConnect to May|Ubuntul, bạn gt các mục như sau.

p **User name** o Bạn gt vào tên người dùng trong Ubuntu (người dùng đã chia sẻ thư mục).

p **Password:** Bạn gt mật khẩu samba mà bạn đã đặt cho người dùng đó

p Tích vào ô h **Remember my password** l nếu muốn lưu lại mật khẩu. Sau đó chọn Og.

e Sau khi kết nối, xuất hiện các thư mục đã chia sẻ trên máy cài Ubuntu.

2. Tại máy cài Ubuntu

e Bạn chọn hNơi/Mạngl

}

Error!

Nguyễn Thị Hiền-

Lạng Sơn

Ne Xuất hiện các máy tính hiện thời đang có kết nối với máy tính của bạn.

Nếu không thấy máy tính cần kết nối, bạn nháy đúp vào hMạng Windowsl, chọn nhóm mạng, sau đó chọn máy tính cần mở.

e Xuất hiện các ổ đĩa và các thư mục đã chia sẻ trên máy cài Windows.

Chú ý o Đối với những ổ đĩa chia sẻ có kk hiệu C~, F~... để truy nhập được phải thza mãn điều kiệno

e Máy cài iĐi Windows phải là Windows Server (ví dụ Windows Server ussy).

e Bạn biết mật khẩu của user fdministrator.

Nếu việc kết nối không thành công, bạn cần chú k kiểm tra những phần mềm tường lửa, diệt virus, spyware đang cài trên máy Windows xem có chức năng chặn kết nối hay không, (ví dụo symantec wndpoint Protection rr).

Ngoài việc chia sẻ File, bạn còn có thể chia sẻ máy in để dùng chung giữa các máy cài Windows và Ubuntu trong cùng mạng LfN, các bạn hãy thử xem nhé.

eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

CHÚ Ý KHI SỬ DỤNG LỆNH WINE TRÊN UBUNTU

Chú ý 1. Thư mục .wine có thuộc tính ẩn, vì vậy, để nhìn thấy thư mục này bạn phải
chọn chế độ hiển thị thư mục ẩn trong view. (**View/Show Hidden files**)

Chú ý 2. Khi trong tên tệp, thư mục có dấu cách.

1. Giả dụ tôi log in vào Ubuntu vơi tên user: **nguyenthihien.**

Trong thư mục **/home/nguyenthihien/UD_win** có chứa tệp **Portable WinRar.v.3.71.Final.exe**
(có dấu cách giữa **Portable** và **WinRar)**

2. Khi tôi chạy lệnh hoặc tạo **shortcut** trên Desktop với dòng **Lệnh (Comand),** chính xác là:

wine /home/nguyenthihien/UD_win/Portable WinRar.v.3.71.Final.exe

3. Thì **Portable WinRar** không chạy, mặc dù lệnh đã gõ rất chính xác.

4. Lỗi ở đây là trên tên tệp **"Portable WinRar.v.3.71.Final.exe"** có 1 **dấu cách**.
Và Ubuntu chỉ hiểu đoạn tên tệp (gồm cả đường dẫn) viết liền trước dấu cách, cụ thể là: **"/home/nguyenthihien/UD_win/Portable"**

5. Phát hiện lỗi rồi thì việc sửa thật đơn giản, mình sửa lại tên tệp, bỏ đi dấu cách, **"PortableWinRar.v.3.71.Final.exe",** dòng **Lệnh (Comamnd),** trong shortcut sửa lại thành:

wine /home/nguyenthihien/UD_win/PortableWinRar.v.3.71.Final.exe

Bây giờ thì chạy **winrar portable** "ngon lành".

Chú ý 3: Cách gõ đường dẫn trong lệnh wine, cách 2.

1. Khi cài ứng dụng của windows trong thư mục **Program Files** (như mặc định) **trên Ubuntu.**
Bạn chú ý tên thư mục **"Program Files",** cũng có dấu cách, nhưng nếu bạn sửa tên thư mục này thì không ổn,
thư mục cài chương trình đã được ghi vào bảng tham số. (bạn chạy lệnh **wine RegEdit** thì có thể xem, sửa
thông tin giống như khi bạn dùng lệnh **RegEdit** trong windows).

Không được sửa tên thư mục **"Program Files"**, nhưng có dấu cách mà gõ lệnh như bình thường
thì không được, vậy phải làm sao?

2. Khi sử dụng lệnh **wine,** còn có 1 cách gõ đường dẫn khác, tương tự như lệnh trong DOS, *(tương tự thôi, không phải giống nhé)* cụ thể như sau:

Sau lệnh wine bạn gõ tên tệp (bao gồm cả đường dẫn) theo quy tắc:

- Bạn sử dụng địa chỉ theo các ổ đĩa đã được ánh xạ trong **wine.**
- Dùng 2 dấu xược ngược \\ tại vị trí ngăn cách giữa ổ đĩa, tên thư mục, tên tệp.
- Nếu trong tên tệp, thư mục có dấu cách thì gõ vào trước dấu cách đó 1 dấu xược ngược \

Ví dụ: /home/ten_nguoi_dung/.wine/Driver_C/Program Files

tương ứng với: **C:\\Program\ Files**

3. Ví dụ minh hoạ:

Ví dụ 1: Giả sử tôi copy tệp "**Portable WinRar.v.3.71.Final.exe**" vào trong thư mục **/home/nguyenthihien/.wine/Driver_C/Program Files**

Để chạy tệp đó, tôi có thể dùng lệnh sau:

wine C:\\Program\ Files\\Portable\ WinRar.v.3.71.Final.exe

Ví dụ 2: Trường hợp như tại **chú ý 2**, tôi có tệp như sau:

/home/nguyenthihien/UD_win/Portable WinRar.v.3.71.Final.exe

Nhưng tôi không muốn sửa tên tệp, tôi kiểm tra phần ánh xạ các ổ đĩa trong **wine** thư mục **/home/nguyenthihien** được ánh xạ tương ứng với ổ **Z:** Để chạy tệp, tôi có thể dùng lệnh sau:

wine Z:\\UD_win\\Portable\ WinRar.v.3.71.Final.exe

Và ứng dụng của bạn chạy ngon rồi, phải không bạn? Chúc các bạn thành công.

(Nguyễn Thị Hiền-Lạng Sơn)

Error!

UBUNTU 7.x

THIẾT LẬP TÀI KHOẢN-GỬI NHẬN THƯ

SAO LƯU - PHỤC HỒI THƯ ĐIỆN TỬ TRONG EVOLUTION

Ubuntu 7.x (7.04 và 7.10) đã cài đặt sẵn tiện ích gửi nhận thư điện tử Evolution, với giao diện tiếng Việt, thân thiện và đặc biệt là rất dễ sử dụng. Evolution hỗ trợ đầy đủ các công cụ sao lưu, phục hồi, rất hữu ích khi bạn cần lưu những thư quan trọng, lưu sổ địa chỉ... phòng khi phải cài lại hệ điều hành, hay khi bạn muốn chuyển thư, sổ địa chỉ... từ máy tính này sang máy tính khác. Bài viết dưới đây hướng dẫn sử dụng Evolution trong trường hợp bạn đã chọn giao diện tiếng Việt trong Ubuntu 7.x.

I. KHỞI ĐỘNG Evolution

Bạn chọn <Ứng dụng /Mạng /Thư tín Evolution>, hoặc chọn biểu tượng hình phong bì thư trên Bảng điều khiển.

II. THIẾT LẬP TÀI KHOẢN THƯ

Khi khởi động Evolution lần đầu tiên, chương trình cho phép bạn thực hiện một vài thao tác cấu hình rất đơn giản để thiết lập một tài khoản thư điện tử. Những lần chạy Evolution sau đó, bạn chọn mục **<Sửa /Tuỳ thích>** khi muốn sửa chữa hoặc thiết lập tài khoản thư điện tử mới. Các bước thiết lập 1 tài khoản thư điện tử như sau:

1. Trong hộp thoại **<cấu hình thư>,** bạn nháy nút **<Tới>** để bắt đầu.
2. Hộp thoại **<Nhận dạng>** xuất hiện, bạn gõ các thông tin cần thiết, chú ý gõ chính xác địa chỉ thư (ví dụ: địa chỉ thư của tôi là nthien@lso.dcs.vn), rồi chọn nút **<Tới>.**

Error!

3. Trong hộp thoại **<Nhận thư>** bạn chọn kiểu máy phục vụ **<POP>.**
- Máy phục vụ: Bạn gõ vào tên chính xác máy chủ thư của đơn vị, Ví dụ: 10.138.0.1.
- Tên người deng, mặc định hệ thống đã hiển thị sẵn tên người deng (là những ký tự phía bên trái chữ @ trong địa chỉ thư của bạn), nếu không chính xác, bạn kiểm tra lại địa chỉ thư bạn gõ đã đúng hay chưa.
- Ban có thể chọn kiểu <bảo mật>, <kiểu xác thực> theo ý muốn. sau đó nháy vào nút **<Tới>.**
4. Trong mục **<Tuỳ chọn nhận>,** bạn tích vào các ô muốn chọn, rồi nháy vào nút **<Tới>.**
f. Trong hộp thoại **<Gửi thư>,** bạn chọn Kiểu máy phục vụ là <gMTh>
- **Máy phục vụ** : Bạn gõ vào tên chính xác máy chủ thư của đơn vị, Vi: 10.138.0.1.
- hhần tên người deng, bảo mậtj tương tự như đã nêu trong hộp thoại **<Nhận thư>.**
2
Error!

k. Hộp thoại **<Quản lý tài khoản>** xuất hiện, bạn có thể sửa tên tul ý, hoặc chỉ đơn giản là chọn <Tới>
7. Bạn **chọn <Áp dụng>** để hoàn tất việc thiết lập 1 tài khoản thư điện tử.

III. GỬI THƯ

1. Gửi thư không có tệp đính kèm.

- Mở chương trình Thư tín Evolution (nếu chưa mở).
- **Bước 1** : Chọn nút <Mới> để tạo thư mới.
3
Error!

- **Bước 2** : miền địa chỉ người nhận thư vào ô <Cho>, (bạn cần gửi thư cho ai).
- **Bước 3** : nõ chủ đề thư, nội dung thư (nếu cần)
- **Bước 4:** Nháy vào nút <nửi> để gửi thư.

Chú ý:
- Bạn có thể gõ vào địa chỉ người nhận, hoặc nháy vào nút <Cho> để chọn địa chỉ trong gổ địa chỉ.
- Bạn nháy vào nút **<Gửi/Nhận>,**
mỗi khi cần đoy thư gửi đi
đến máy chủ hoặc khi cần nhận thư mới từ máy chủ về.

2. Gửi thư có đính kèm tệp

- Từ **Bước 1** đến **Bước 3** bạn thực hiện như phần gửi thư không có tệp đính kpm.

- **Bước 3a** : **Đính kèm tệp :**

q Bạn nháy vào nút <mính kpm> trên thanh công cụ, (có kpm theo biểu tượng hình chiếc ghim cài).

q ruất hiện hộp thoại <Chpn đồ đính kpm>. Bạn chọn đến thư mục chsa tệp. rồi nháy đúp chuột vào tệp cần đính kpm (hoặc nháy đơn chuột để chọn tệp -> nháy nút <đính kpm>)

4

Error!

q ruất hiện tệp mà bạn đã đính kpm theo thư.

f

Error!

- **Bước 4:** Nháy vào nút **<Gửi>** để gửi thư.

IV. ĐỌC THƯ

Bạn nháy vào nút **<Gửi/Nhận>** để nhận thư mới (nếu có).

- Bạn chọn mục chsa thư cần đọc (ví dụ: Hộp đến, mã gửij)
- Nháy đúp để mở thư cần đọc.
- gau khi đọc xong, bạn nháy vào dấu r (hoặc chọn <Tập tin / móng>) để đóng thư.

*** Lưu tệp đính kèm thư.**

- Bạn chọn <tưu> (hoặc <tưu hết> nếu có 2 tệp đính kpm trở lên) để lưu tệp đính kpm.
- ruất hiện hộp thoại <tưu đính kpm dạng>, bạn nháy nút <tưu> để lưu tệp.

- Chú ý :

q Bạn có thể đặt lại tên tệp (nếu cần).

q Nếu không muốn lưu tệp ở thư mục đã được chọn sẵn. Bạn nháy vào <iuyệt tìm thư mục khác> để chọn lại nơi lưu tệp.

k

Error!

V. SAO LƯU-PHỤC HỒI TRONG EVOLUTION

1. Sao lưu-phục hồi thư điện tử

**Sao lưu:*

- Bước 1: Bạn chọn những thư cần sao lưu

- Bước 2: Chọn <Tập tin /tưu thư>
- Bước 3: ruất hiện hộp thoại lưu thư,
q Bạn gõ tên tệp lưu thư vào ô <Tên>
q Mặc định tệp của bạn su được chsa trong thư mục <Màn hình nền (iesktop)>. Nếu muốn lưu tệp trong thư mục khác bạn nháy chuột vào nút <iuyệt tìm thư mục khác> để chọn.
q Nháy chuột vào nút <lưu>.
**Phục hồi thư đã lưu.*
- Bước 1: Bạn chọn <Tập tin /Nhập>, nhấn nút <Tới> trong màn hình chào mừng.
- Bước 2: Bạn chọn kiểu bộ nhập: <Nhập 1 tập tin riêng lv> rồi nháy nút <Tới>
- Bước 3: Chọn tên tập tin lưu thư cần phục hồi, nháy đúp vào tên tập tin cần chọn. Chọn kiểu tập tin là <Berkeley Mailbox (mbox)>, nháy nút <Tới>

- Bước 4: Chọn thư mục đích chsa thư cần phục hồi, rồi nháy <Tới>
- Bước f: Nháy vào nút <Nhập>, toàn bộ thư cần phục hồi của bạn su được xuất hiện tại thư mục mà bạn đã chọn tại bước 4.

2. Sao lưu-phục hồi sổ địa chỉ

**Sao lưu:*
- Bạn chọn mục <tiên lạc> để mở sổ địa chỉ
- Chọn <Tập tin /tưu sổ địa chỉ dạng VCard>
- Các bước tiếp theo bạn thực hiện tương tự như khi bạn lưu thư.

**Phục hồi sổ địa chỉ*

Các bước phục hồi sổ địa chỉ tương tự như khi bạn phục hồi thư, lưu ý bạn chọn tệp tin lưu sổ địa chỉ có đuôi là <.vcw, gcrd> và chọn kiểu tập tin là <Vcard>. mịa điểm nhập là tên sổ địa chỉ do bạn chọn, mặc định là sổ <cá nhân>.

Nguyễn Thị Hiền-Lạng Sơn

3. Sao lưu-phục hồi Evolution (công cụ Mxy, chỉ có trong phiên bản Ubuntu 7.10).
- gử dụng công cụ này bạn có thể sao lưu-phục hồi tất cả mọi tiện ích có trong Evolution, gồm cả thư điện tử, sổ địa chỉ, cầu hình tài khoản, ghi nhớ...

- Cách sử dụng rất đơn giản, khi cần sao lưu, bạn chọn <Tập tin /Thiết lập sao lưu>, đặt lại tên tệp nếu muốn (mặc định là evolution-backup.tar.gz), mặc định tệp sao lưu su được lưu trong thư mục <màn hình nền (iesktop)>, bạn có thể chọn nơi khác tul ý. Bạn nháy vào nút <lưu>, sau đó chọn <Có> để chấp nhận.
- Bạn chọn <Tập tin /Thiết lập phục hồi> khi muốn phục hồi Evolution, tìm đến tệp tin đã tạo khi sao lưu (evolution-backup.tar.gz), nháy đúp để mở tệp và chọn <Có> để chấp nhận việc phục hồi.

Ngoài ra, còn có rất nhiều tính n{ng, công cụ khác rất tuyệt trong Evolution đang chờ bạn khám phá.

}

Hướng dẫn cài đặt LAMP trên Ubuntu cho người mới bắt đầu

Bài viết này sẽ hướng dẫn cho bạn cách cài đặt một hệ thống LAMP. LAMP bao gồm *L*inux, *A*pache, *M*ySQL, *P*HP. Hướng dẫn này chủ yếu dành cho những người chỉ có một chút kiến thức trong việc sử dụng Linux.

Cài đặt Apache

Để bắt đầu chúng tôi sẽ hướng dẫn cài đặt Apache.

1. Mở phần Terminal (***Applications*** > ***Accessories*** > ***Terminal***)

2. Copy/Paste dòng mã sau vào Terminal và nhấn phím enter:

sudo apt-get install apache2

3. Terminal sẽ hỏi mật khẩu của bạn, nhập nó vào và nhấn enter.

Kiểm tra Apache

Để chắc chắn mọi thứ đã được cài đặt chính xác, chúng ta sẽ tiến hành kiểm tra Apache để đảm bảo nó hoạt động đúng cách.

1. Mở trình duyệt và sau đó nhập địa chỉ web sau đây vào ô địa chỉ:

http://localhost/

2. Bạn sẽ thấy một thư mục có tên là apache2-default/. Mở thư mục đó ra, bạn sẽ nhận được thông báo là "*It works!*" và bạn đã thành công.

Cài đặt PHP

Tiếp theo chúng ta sẽ tiến hành cài đặt PHP 5.

Bước 1: Mở lại phần Terminal (***Applications*** > ***Accessories*** > ***Terminal***)

Bước 2: Copy/Paste dòng lệnh sau vào Terminal và nhấn enter:

sudo apt-get install php5 libapache2-mod-php5

Bước 3: Hợp lệ để PHP làm việc và tương thích với Apache và chúng ta phải khởi động lại nó. Nhập vào câu lệnh sau trong Terminal để thực hiện điều này:

sudo /etc/init.d/apache2 restart

Kiểm tra lại PHP

Để đảm bảo không có vấn đề gì phát sinh đối với PHP, hãy kiểm tra lại nó bằng các bước sau:

Bước 1: Trong Terminal, copy và paste dòng lệnh sau rồi nhấn enter:

sudo gedit /var/www/testphp.php

Câu lệnh này sẽ mở một file có tên là *phptest.php*.

Bước 2: Copy/Paste dòng lệnh sau vào file *phptest*:

Bước 3: Lưu và đóng file lại

Bước 4: Mở trình duyệt web của bạn và nhập vào địa chỉ sau:

http://localhost/testphp.php

Bạn sẽ thấy giao diện sau:

Error!

Việc cài đặt cả Apache và PHP đã thành công!

Cài đặt MySQL

Cuối cùng là việc cài đặt MySQL

Bước 1: Lại tiếp tục mở lại Terminal và đưa vào dòng lệnh sau:

sudo apt-get install mysql-server

Bước 2 (không bắt buộc): Để các máy tính khác trong mạng xem được server mà bạn đã tạo, đầu tiên là bạn phải chỉnh sửa "Bind Address". Bắt đầu bằng việc mở Terminal để sửa file *my.cnf*.

gksudo gedit /etc/mysql/my.cnf

Tại dòng

bind-address = 127.0.0.1

đổi địa chỉ **127.0.0.1** thành địa chỉ IP của bạn

Bước 3: Đây là bước quan trọng, nhập dòng lệnh sau vào Terminal:

mysql -u root

Và copy/paste dòng lệnh sau:

mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('yourpassword');

(Hãy thay đổi **yourpassword** bằng mật khẩu mà bạn chọn)

Bước 4: Giờ chúng ta sẽ tiến hành cài đặt chương trình phpMyAdmin, đây là một công cụ đơn giản để chỉnh sửa cơ sở dữ liệu của bạn. Copy/paste dòng lệnh sau vào Terminal:

sudo apt-get install libapache2-mod-auth-mysql php5-mysql phpmyadmin

Sau khi đã cài đặt mọi thứ, bước tiếp theo cần thực hiện là làm cho PHP có thể làm việc cùng với MySQL. Để thực hiện điều này, chúng ta cần mở file php.ini bằng cách nhập vào dòng lệnh sau:

gksudo gedit /etc/php5/apache2/php.ini

Trong file này, chúng ta cần bỏ dấu chú thích ở dòng lệnh sau bằng cách bỏ đi dấu chấm phẩy đầu dòng (**;**):

;extension=mysql.so

Thay đổi nó thành như sau:

extension=mysql.so

Giờ thì bạn có thể khởi động lại Apache và hoàn thiện toàn bộ quá trình cài đặt!

sudo /etc/init.d/apache2 restart

Hồng Ngân

TỰ ĐỘNG SAO LƯU DỮ LIỆU TRONG UBUNTU 7.04 &7.10

An toàn dữ liệu là một trong những vấn đề luôn được mọi người sử dụng máy tính đặc biệt quan tâm, có rất nhiều nguyên nhân dẫn đến việc bạn có thể mất đi những dữ liệu quý giá của mình, ổ cứng chứa dữ liệu bị bad, sự cố phần mềm, thậm chí do chính bạn xoá nhầm dữ liệu...

Sao lưu dữ liệu là một giải pháp cực kỳ hữu hiệu để giải quyết vấn đề nêu trên. Bài viết dưới đây sẽ giới thiệu với các bạn phần mềm **sbackup**, một trong những công cụ giúp bạn thực hiện việc **sao lưu dữ liệu một cách tự động**, định kỳ, trong hệ điều hành Ubuntu 7.x.

I. Cài đặt sbackup

1. Nếu máy tính của bạn có kết nối internet.

Bạn khởi động Terminal (Chọn **Applications-> accessories -> Terminal**), gõ lệnh sau:

sudo apt-get install sbackup

2. Nếu máy tính của bạn không có kết nối internet, bạn ra dịch Interent.

để tải gói cài đặt về cài offline.

Bạn nháy đúp vào tệp sbackup_0.10.3-0.1_all_7.04.deb (đối với Ubuntu 7.04), hoặc sbackup_0.10.4_all_7.10.deb (đối với Ubuntu 7.10), rồi chọn <Install Package> để cài đặt.

II. Cấu hình sbackup

- Sbackup là công cụ sao lưu, phục hồi hệ thống, và đương nhiên, chúng ta hoàn toàn có thể sử dụng công cụ này để thực hiện việc sao lưu dữ liệu tự động.

- Để khả năng lựa chọn cấu hình được mở rộng hơn, bạn nên đăng nhập với account <ROOT>.

- Chọn <Hệ thống/Quản lý/Simple Backup Config>, bạn sẽ thấy xuất hiện màn hình <backup Properties>. Tôi sẽ lần lượt giới thiệu với các bạn nội dung và cách cấu hình từng mục (tab), có 6 tab.

1. General: có 3 sự lựa chọn cách sao lưu.

- Nếu bạn chỉ sử dụng sbackup để sao lưu hệ thống và bạn không muốn phải mất công thiết lập cấu hình, thì bạn chọn <Use recommended backup setting>.

- Lựa chọn <Use custom backup setting> cho phép bạn tuỳ ý thiết lập tất cả các cấu hình cần thiết. ***Sau đây tôi xin giới thiệu với các bạn cách sử dụng tuỳ chọn này để thiết lập tác vụ sao lưu dữ liệu tự động.***

- Nếu bạn không muốn lập lịch sao lưu tự động, mỗi lần sao lưu là do bạn

tự thao tác, thì bạn chọn <Manual backups only>.

Error!

2. Include: Tab này cho phép bạn lựa chọn danh sách các thư mục, các
tệp mà bạn muốn sao lưu. Mặc định là những thư mục hệ thống cần sao lưu.

- Bạn nháy vào <Add file>, <Add directory> để chọn nguồn là tệp, thư
mục chứa dữ liệu cần sao lưu.

- Khi cần loại bỏ những tệp, thư mục trong danh sách, bạn nháy đơn chuột
vào tên tệp, thư mục (để chọn) rồi nháy vào nút <gỡ bỏ>.

Error!

Ví dụ: Tôi loại bỏ 4 thư mục có sẵn theo mặc định của chương trình, và thêm vào thư mục </home/hien/Documents> là thư mục mà tôi lưu toàn bộ văn
bản mà mình soạn thảo.

3. Exclude:

- Path: Khi bạn chọn 1 thư mục trong tab <**Include>** thì tất cả tệp và các
thư mục con (nếu có) chứa trong thư mục đó đều được sao lưu. Nhưng nếu bạn
thấy 1 (hoặc 1 vài) tệp, thư mục trong đó không cần thiết phải sao lưu, thì bạn
lựa các tệp, thư mục đó vào danh sách trong tab này.

Cách thêm, loại bỏ tệp, thư mục trong danh sách tương tự như mục trên.

Error!

Ví dụ: trong thư mục </home/hien/Documents> có thư mục <luu-tam>,
tôi không muốn sao lưu thư mục này, vì vậy, **tôi chọn th ư mục**
</home/hien/Documents/luu-tam> vào danh sách trong tab <**Exclude>**.

- Tương tự như vậy, bạn chọn những kiểu loại trừ sao lưu khác trong mục

<file type>, <Regex>, <Max size>,

4. Destination: là thư mục đích, nơi chưa dữ lưu sao lưu của bạn.

Mặc định, thư mục đích là </var/backup>, nhưng bạn hoàn toàn có thể lựa
chọn thư mục khác, bạn cũng có thể chọn sao lưu trên mạng qua SSH hoặc FTP

Ví dụ: Nếu bạn muốn chọn thư mục đích nằm ngoài phân vùng
cài Ubuntu, phòng trường hợp hệ điều hành gặp sự cố.

- Bạn chọn <User custom local backup directory>, nháy vào ô lựa chọn
thư mục, bạn chọn mục <khác> để xuất hiện màn mình <select the destination
folder>, bạn chọn phân vùng, chọn thư mục đích, rồi nháy nút <Mở> để chấp
nhận.

5. Time: Tại đây bạn có thể đặt lịch sao lưu hằng ngày, giờ, tuần, tháng
hoặc tuỳ theo lựa chọn riêng của bạn.

6. Purging: Tuỳ chọn <Enable purging of old and incomplete backups>
cho phép bạn lựa chọn việc tự động xoá những backup cũ hoặc chưa hoàn thành.

- Bạn chọn <Simple cutoff> để xoá tất cả những backup sau 1 số ngày
nhất định (do bạn đặt).

- Bạn chọn <Logarithmic> để giữ lại một backup từ hôm qua, tuần trước,
tháng trước, năm trước và xoá những backup khác
Error!

*** Sau khi đã hoàn tất việc cấu hình**, bạn nháy nút <Lưu>, sẽ xuất hiện
thông báo <Configuration save successful>.

*** Nếu muốn thực hiện tác vụ sao lưu ngay**, bạn nháy nút <Backup
now>, xuất hiện thông báo <A backup run is initated in the backgrount. The
process ID is:....>,

*** Nếu muốn thực hiện tác vụ sao lưu ngay**, bạn nháy nút <Backup
now>, xuất hiện thông báo <A backup run is initated in the backgrount. The
process ID is:....>, bạn chọn <Đóng>

* Bạn nháy vào nút <Đóng> để kết thúc việc cấu hình.

III. Sử dụng dữ liệu đã sao lưu.

- Dữ liệu của bạn sẽ được **tự động sao lưu** theo chu kỳ mà bạn đã lập lịch
hoặc khi bạn nháy vào nút <Backup now>.

- Mở vào thư mục đích, bạn sẽ thấy một hoặc một số thư mục có tên
tương tự như sau <2007-12-15_19.49.01.602189.hien-desktop.ful>, mở thư
mục, bạn thấy tệp chứa dữ liệu được sao lưu <files.tgz>.

- Khi cần sử dụng dữ liệu đã sao lưu:

+ Bạn có thể giãn nén tệp <files.tgz> bằng trình giải nén của Ubuntu hoặc
bằng winrar để lấy dữ liệu.

+ Hoặc bạn chọn <Hệ thống/Quản lý/Simple Backup restore> để khôi
phục dữ liệu.

Bây giờ thì bạn có thể yên tâm lướt trên diễn đàn, trong khi dữ liệu của

bạn đã có anh bạn **sbackup** chăm lo sao lưu theo định kỳ. Phần mềm còn rất
nhiều tính năng thú vị khác đang chờ bạn khám phá, các bạn hãy tìm hiểu thêm
nhé.

Chúc Bạn thành công!

HƯỚNG DẪN

CÀI BỘ GÕ TIẾNG VIỆT TRÊN UBUNTU DESKTOP

I. MỞ ĐẦU

Hướng dẫn sau chỉ áp dụng trên bản Ubuntu Desktop. Đối với bản Ubuntu Server,

khi bạn cài xong nếu muốn cài GNOME thì chạy lệnh sudo aptget install ubuntu

desktop hoặc cài KDE thì sudo aptget install kubuntudesktop. Nếu Nếu muốn cài

KDE và bỏ qua các gói mở rộng, có thể dùng lệnh sau: sudo aptget install kdebase

kdm xwindowsystemcore.

Bài viết này hướng dẫn bản Ubuntu desktop download từ trên mạng, với bản

Ubuntu của phòng mã nguồn mở của Sở Bưu chính viễn thông TP. HCM thì đã tích hợp sẵn

Openoffice và bộ gõ tiếng Việt.

Bộ gõ tiếng việt là của công ty VISC mà tác giả chính là Đào Hải Lâm đã được

biên dịch sẵn mà bạn chỉ việc nháy chuột cài đặt và không phải làm gì thêm, bạn thấy

thích không ?

Khi bạn muốn cài đặt phần mềm mới cho Ubuntu, thường dựa vào những công cụ

sẵn có sau:

· Add/Remove… (cái này đơn giản nhất, giống Add/Remove trong Control Panel

của Windows)

· apt (chạy từ cửa sổ dòng lệnh, khá tiện dụng nếu đã dùng quen)

· synaptic (cái này gần như trình Add/Remove nhưng rất mạnh)

· Cài đặt trực tiếp từ gói phần mềm, hoặc biên dịch từ mã nguồn

1. Phần mềm trên Linux được phân phối thế nào?

Trên Windows phần mềm thường được phân phối ra dưới dạng file cài đặt .msi

hoặc .exe thì trên Linux cũng gần tương tự như vậy, có điều trên Linux có nhiều hình

thức hơn thôi. Phần mềm cho Linux thường có ở những nơi sau:

· Trong bộ đĩa cài đặt (thường với những bản phân phối lớn như Redhat, openSuse,

Mandriva…

· Trên trang web của nhà sản xuất (người dùng thường phải tự download về và

thường có sẵn hướng dẫn cài đặt cho từng hệ thống)

· Trên các repository (gọi tắt: repo) là các nơi chứa phần mềm tập trung trên mạng

dành riêng cho một hệ thống nào đó. Ubuntu và Debian sử dụng repo nhiều nhất,

kế đến là Fedora và openSuse. Mọi phần mềm đều được chứa tại repo và khi nào

người dùng cần thì phần mềm sẽ được tải về từ repo rồi cài đặt lên máy. Rất tiện

lợi trong việc cập nhật phần mềm.

Các gói phần mềm có thể được lưu ở dạng file chạy được (như file setup.exe

thường thấy trên Windows, chúng thường là trình cài đặt riêng của nhà sản xuất) hoặc ở

định dạng phân phối dành riêng mà phổ biến nhất là .RPM và .DEB (các gói phần mềm

này có thể cài đặt dễ dàng và gần như đã thành chuẩn chung cho việc phân phối phần

mềm). Phần mềm cũng có thể được phân phối dưới dạng mã nguồn (nhất là phần mềm

nguồn mở), người dùng phải tự biên dịch trên máy rồi cài đặt (thường chỉ áp dụng với

những phiên bản mới nhất của phần mềm nhỏ, mất ít thời gian biên dịch, hoặc khi chưa

có bản deb hay rpm tương ứng).

2. RPM và DEB là gì ?

RPM (Redhat package manager) và DEB (Debian software package) là hai định

dạng file chuyên dùng cho phân phối phần mềm. Chúng giống như định dạng file nén

mà trong đó chứa tất cả nhưng file chạy và cấu hình của phần mềm, thông tin về phần

mềm, nhà sản xuất, những yêu cầu về hệ thống… Hệ điều hành Linux sẽ có một phần

mềm chuyên dùng để cài đặt các gói phần mềm dạng này (giải nén, chuyển các file của

phần mềm vào đúng chỗ, cấu hình cho phần mềm…) và nói chung thì phân phối phần

mềm kiểu này rất dễ cài đặt.

RPM thường được dùng trong các hệ thống tương tự Redhat như:

Fedora, openSuse,… còn DEB lại được dùng trên các hệ thống của Debian gồm

Debian, các họ nhà Ubuntu… Khó có thể nói cái nào tốt hơn cái nào, chỉ biết là

cả hai đều rất đơn giản và dễ dùng.

Mỗi file RPM hoặc DEB chỉ chứa một phần mềm hoặc một phần nào đó của phần

mềm. Vì vậy thường khi cài một phần mềm phải cài đặt kèm theo 1, 2 hay thậm chí cả

chục gói khác. Chúng ít khi chứa toàn bộ thư viện (vì số lượng thư viện dùng chung là

khá lớn) nên đôi khi xảy ra tình trạng không thể cài đặt do thiếu một gói nào đó (thuộc

về một chương trình khác chẳng hạn). Chương trình cài đặt bao giờ cũng kiểm tra xem

toàn bộ gói cần thiết đã được cài đặt trước chưa, nếu thiếu một gói nào đó, quá trình cài

đặt sẽ dừng lại. Công việc này gọi là “check dependency”.

Chính vì sự ràng buộc đó nên chúng ta mới cần đến những phần mềm hỗ trợ cài

đặt. Những phần mềm này sẽ tự động tải về hoặc tìm tất cả những gói có liên quan rồi

lần lượt cài đặt chúng theo đúng thứ tự. Nhờ đó mà mọi việc cài đặt sẽ đơn giản hơn

nhiều. Trước đây việc cài đặt một phần mềm rất vất vả và có thể cài mãi không được vì

không biết thư viện bị thiếu của nó nằm trong file RPM nào.

Sau đâu là hướng dẫn cài bộ gõ tiếng Việt (bộ cài đặt chỉ duy nhất có 1 tệp sau:

"xvnkb0.2.9autf_i386.deb". Bạn tải về tại **đây**).

II. Hướng dẫn cài đặt

b1) Copy tệp xvnkb0.2.9autf_i386.deb và máy tính của bạn có cài Ubuntu (nếu

trên máy bạn chưa có).

b2) Nháy đúp chuột vào tệp xvnkb0.2.9autf_i386.deb,

Và đợi cho đến khi xuất hiện một cửa sổ bạn chọn Install Package để tiến hành

cài đặt.

b3) Khi cài xong bạn khởi động lại máy tính.

Ở góc dưới bên phải màn hình sẽ có biểu tượng của bộ

gõ, bạn hãy đặt lại bảng mã và kiểu gõ cho phù hợp với

nhu cầu.

Chúc Bạn thành công!

+ v.v...

Error!

6- Cài Opera 9.24 trên Ubuntu 7.10

+ Điều kiện là bạn phải có 2 tệp sau:

- libqt3-mt_3.3.8really3.3.7 -0ubuntu5.2_i386.deb

- opera_9.24 -20071015.6 -shared-qt_en_i386.deb

+ Tại terminal, gõ:

sudo dpkg -i libqt3-mt_3.3.8really3.3.7 -0ubuntu5.2_i386.deb

sudo dpkg -i opera_9.24 -20071015.6-shared-qt_en_i386.deb

Lê Anh Tài -Lạng Sơn

TÌNH HUỐNG:

Bạn mở tài liệu có sẵn và trong tài liệu đó bạn sử dụng font **.Vntime**... (theo TCVN3 hay... những font 1 byte) và nếu trên **Ubuntu** của bạn không có font theo chuẩn đó thì văn bản không hiển thị được. Tương tự đối với các font Vni.... Vậy phải làm thế nào bây giờ ?

CÁCH GIẢI QUYẾT:

1. Tìm các nguồn font mà bạn cần cho văn bản có thể hiển thị được.

2. Bạn hãy copy các font một byte (ABC, Vietkey-[trong Vietkey có cả font theo TCVN3 và font Unicode], Vni...) vào thư mục sau:**/usr/share/fonts/truetype**

Error!

HIỆN TƯỢNG UBUNTU KHÔNG TỰ ĐỘNG NHẬN THIẾT BỊ CẮM QUA CỔNG USB:

1-Khi bạn cắm ổ USB hay máy in vào máy tính đang chạy HĐH Ubuntu nhưng thấy đèn trên ổ USB sáng (ở đây giả định là ổ thì vẫn tốt, làm việc bình thường trên HĐH khác).

2-Hay khi bạn cắm máy in qua cổng USB mà không thấy nhận được hay báo là có thiết bị mới cắm vào.

CÁC GIẢI QUYẾT:

1. Bạn kiểm tra xem có ổ USB hay thiết bị khác (máy in chẳng hạn, tôi cắm LBP-3000) cắm vào và máy tính nhận ra không. Dùng lệnh sau tại của sổ terminal:

lsusb

kết quả (ví dụ):

Bus 003 Device 001: ID 0000:0000
Bus 002 Device 004: ID 0000:0000
Bus 002 Device 003: ID 062a:0000 Creative Labs Optical Mouse
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000

2. Đối với ổ USB thì bạn có thể dùng lệnh mount để ánh xạ ổ đó với 1 thư mục bạn tạo ra trong thư mục **media**. Ở đây tôi sử dụng lệnh modprobe cho việc nhận dạng thiết bị cắm qua cổng USB. Tại cửa sổ terminal, bạn gõ lệnh sau:

sudo modprobe -r ehci_hcd

3. Kiểm tra kết quả nhận dạng:

lsusb

Bus 003 Device 001: ID 0000:0000
Bus 002 Device 004: ID 058f:6387 Alcor Micro Corp.
Bus 002 Device 003: ID 062a:0000 Creative Labs Optical Mouse
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000

(tôi đã cắm ổ USB vào máy tính đang chạy Ubuntu, lưu ý là nếu bạn cắm xong thiết vào cổng usb rồi khởi động lại HĐH thì hướng dẫn trên đây là không cần thiết, vì khi đó hệ thống đã nhận được rôi!)

Ví dụ sau đây tôi vừa cắm ổ USB và máy in Canon LBP-3000

Bus 003 Device 001: ID 0000:0000
Bus 002 Device 007: ID 04a9:266a Canon, Inc.
Bus 002 Device 006: ID 062a:0000 Creative Labs Optical Mouse
Bus 002 Device 005: ID 058f:9254 Alcor Micro Corp. Hub
Bus 002 Device 004: ID 058f:6387 Alcor Micro Corp.
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000

THAM KHẢO LỆNH MODPROBE:

NAME

modprobe - program to add and remove modules from the Linux Kernel

SYNOPSIS

modprobe [-v] [-V] [-C config-file] [-n] [-i] [-q] [-Q] [-o modulename] [modulename] [module parameters ...]
modprobe [-r] [-v] [-n] [-i] [modulename ...]
modprobe [-l] [-t dirname] [wildcard]
modprobe [-c]

DESCRIPTION

modprobe intelligently adds or removes a module from the Linux kernel: note that for convenience, there is no difference between _ and - in module names. modprobe looks in the module directory /lib/modâ?ules/â?˜uname -râ?˜ for all the modules and other files, except for the optional /etc/modprobe.conf configuration file and /etc/modprobe.d directory (see modprobe.conf(5)). All files in the /etc/modâ?probe.d/arch/ directory are ignored.

Note that this version of modprobe does not do anything to the module itself: the work of resolving symbols and understanding parameters is done inside the kernel. So module failure is sometimes accompanied by a kernel message: see dmesg(8).

modprobe expects an up-to-date modules.dep file, as generated by depmod (see depmod(8)). This file lists what other modules each module needs (if any), and modprobe uses this to add or remove these dependencies automatically. See modules.dep(5)).

If any arguments are given after the modulename, they are passed to the kernel (in addition to any options listed in the configuration file).

OPTIONS

-v --verbose

Print messages about what the program is doing. Usually modâ?â?probe only prints messages if something goes wrong.

This option is passed through install or remove commands to other modprobe commands in the MODPROBE_OPTIONS environment

variable.

-C --config

This option overrides the default configuration file (/etc/modâ?probe.conf or /etc/modprobe.d/ if that isnâ?™t found).
This option is passed through install or remove commands to other modprobe commands in the MODPROBE_OPTIONS environment variable.

-c --showconfig

Dump out the configuration file and exit.

-n --dry-run

This option does everything but actually insert or delete the modules (or run the install or remove commands). Combined with -v, it is useful for debugging problems.

-i --ignore-install --ignore-remove

This option causes modprobe to ignore install and remove comâ?mands in the configuration file (if any), for the module on the command line (any dependent modules are still subject to comâ?mands set for them in the configuration file). See modâ?â?probe.conf(5).

-q --quiet

Normally modprobe will report an error if you try to remove or insert a module it canâ?™t find (and isnâ?™t an alias or install/remove command). With this flag, modprobe will simply ignore any bogus names (the kernel uses this to opportunistiâ?cally probe for modules which might exist).

-Q --silent

As -q with the addition that all warnings and errors are also silenced.

-r --remove

This option causes modprobe to remove, rather than insert a modâ?ule. If the modules it depends on are also unused, modprobe will try to remove them, too. Unlike insertion, more than one module can be specified on the command line (it does not make sense to specify module parameters when removing modules).
There is usually no reason to remove modules, but some buggy modules require it. Your kernel may not support removal of modâ?ules.

-V --version

Show version of program, and exit. See below for caveats when run on older kernels.

-f --force

Try to strip any versioning information from the module, which might otherwise stop it from loading: this is the same as using both --force-vermagic and --force-modversion. Naturally, these checks are there for your protection, so using this option is dangerous.

This applies to any modules inserted: both the module (or alias) on the command line, and any modules it depends on.

--force-vermagic

Every module contains a small string containing important inforâ? mation, such as the kernel and compiler versions. If a module fails to load and the kernel complains that the "version magic" doesnâ?™t match, you can use this option to remove it. Naturally, this check is there for your protection, so this using option is dangerous.

This applies to any modules inserted: both the module (or alias) on the command line, and any modules it depends on.

--force-modversion

When modules are compiled with CONFIG_MODVERSIONS set, a section is created detailing the versions of every interface used by (or supplied by) the module. If a module fails to load and the kerâ? nel complains that the module disagrees about a version of some interface, you can use "--force-modversion" to remove the verâ? sion information altogether. Naturally, this check is there for your protection, so using this option is dangerous.

This applies any modules inserted: both the module (or alias) on the command line, and any modules it depends on.

-l --list

List all modules matching the given wildcard (or "*" if no wildâ? card is given). This option is provided for backwards compatiâ? bility: see find(1) and basename(1) for a more flexible alternaâ? tive.

-a --all

Insert all module names on the command line.

-t --type

Restrict -l to modules in directories matching the dirname given. This option is provided for backwards compatibility: see find(1) and basename(1) or a more flexible alternative.

-s --syslog

This option causes any error messages to go through the syslog

mechanism (as LOG_DAEMON with level LOG_NOTICE) rather than to standard error. This is also automatically enabled when stderr is unavailable.

This option is passed through install or remove commands to other modprobe commands in the MODPROBE_OPTIONS environment variable.

--set-version

Set the kernel version, rather than using uname(2) to decide on the kernel version (which dictates where to find the modules). This also disables backwards compatibility checks (so modâ?â? probe.modutils(8) will never be run).

--show-depends

List the dependencies of a module (or alias), including the modâ? ule itself. This produces a (possibly empty) set of module filenames, one per line, each starting with "insmod". Install commands which apply are shown prefixed by "install". It does not run any of the install commands. Note that modinfo(8) can be used to extract dependencies of a module from the module itself, but knows nothing of aliases or install commands.

-o --name

This option tries to rename the module which is being inserted into the kernel. Some testing modules can usefully be inserted multiple times, but the kernel refuses to have two modules of the same name. Normally, modules should not require multiple insertions, as that would make them useless if there were no module support.

--first-time

Normally, modprobe will succeed (and do nothing) if told to insert a module which is already present, or remove a module which isnâ?™t present. This is backwards compatible with the modutils, and ideal for simple scripts. However, more compliâ? cated scripts often want to know whether modprobe really did something: this option makes modprobe fail for that case.

BACKWARDS COMPATIBILITY

This version of modprobe is for kernels 2.5.48 and above. If it detects a kernel with support for old-style modules (for which much of the work was done in userspace), it will attempt to run modprobe.moduâ?â? tils in its place, so it is completely transparent to the user.

Error!

Quản lý các tập tin
Di chuyển / liệt kê các tập tin
Tập tin và thư mục
Nội dung các tập tin
pwd
hiển lên tên thư mục đang làm việc với
cp *file1 file2*
chép *file1* sang *file2*
cat *file*
xuất hiện nội dung của tập tin *file* trên màn
hình ở dạng mã ASCII
cd
di chuyển sang thư mục « /home/ *người_dùng »*
cp *file* / *thưmục*
chép *file* vào thư mục « *thưmục »*
more *file*
xuất hiên nội dung của tập tin *file* trên màn
cd ~/Desktop
di chuyển sang thư mục
cp -r *thưmục1 thưmục2*
chép toàn bộ nội dung của thư mục
hình theo chế độ từng trang một : ấn phím
« /home/người_dùng/ Desktop »
rsync -a *thưmục1 thưmục2*
« *thưmục1 »* sang thư mục « *thưmục2 »*
« Enter » để xuống 1 dòng ; ấn phím « Space »
để sang thêm 1 trang ; ấn phím « q » để thoắt.
cd ..
di chuyển sang thư mục cha (ngay trên thư mục hiện
mv *file1 file2*
chuyển tên tập tin *file1* thành tên *file2*
hành)
less *file*
« less » giống như « more », nhưng cho phép
mv *thưmục1 thưmục2*
chuyển tên *thưmục1* thành *thưmục2*
dùng phím [Page Down]
cd /usr/apt
di chuyển sang thư mục « /usr/apt »
mv file thưmục

chuyển tập tin *file* vào thư mục
head -n *file*
xuất hiện số n dòng đầu tiên của tập tin *file*
ls -l *Thưmục*
liệt kê danh mục tập tin trong thư mục *Thưmục* một
thưmục
dir -l *Thưmục*
cách chi tiết
tail -n *file*
xuất hiện số n dòng cuối cùng của *file*
mv file1 thưmục/file2
chuyển *file1* vào thư mục *thưmục* đồng
ls -a
liệt kê tất cả các tập tin, kể cả các tập tin ẩn
(thường
thời đổi tên tập tin thành *file2*
vi *file*
soạn tập tin *file* dùng trình soạn vi
dir -a
có tên bắt đầu bằng một dấu chấm)
mkdir *thưmục*
tạo ra thư mục *thưmục*
nano *file*
soạn tập tin *file* dùng trình soạn nano
ls -d
liệt kê tên các thư mục nằm trong thư mục hiện hành
mkdir -p *thưmục1/thưmục2*
tạo ra thư mục cha *thưmục1* và thư mục
dir -d
gedit *file*
soạn tập tin *file* dùng trình soạn gedit
con *thưmục2* cùng lúc
ls -t
xếp lại các tập tin theo ngày đã tạo ra, bắt đầu bằng
grep *chuỗi file*
xuất hiện các dòng chứa nội dung *chuỗi* trong
rm *file*
xóa bỏ tập tin *file* trong thư mục hiện
dir -d
những tập tin mới nhất

tập tin *file*
hành
ls -S
xếp lại các tập tin theo kích thước, từ to nhất đến nhỏ
grep -r *chuỗi*
tìm nội dung *chuỗi* trong tất cả các tập tin
rmdir *thưmục*
xóa bỏ thư mục trống mang tên *thưmục*
dir -S
nhất
thưmục
trong thư mục mang tên *thưmục*
rm -rf *thưmục*
xóa bỏ thư mục mang tên *thưmục* với
ls -l | more
liệt kê theo từng trang một, nhờ tiện ích « more »
lệnh > file
ghi kết quả của lệnh *lệnh* trong tập tin *file*
tất cả các tập tin trong đó *(force)*
lệnh >> file
bổ sung kết quả của lệnh *lệnh* ở phần cuối của
ln -s *file liênkết*
tạo ra một liên kết mang tên *liênkết* đến
Quyền truy cập tập tin
tập tin *file*
tập tin *file* (nối tắt)
Nén và giải nén tập tin
chown *tênngườidùng file*
xác định người chủ của tập tin *file* là
find *thưmục* -name *file*
tìm tập tin mang tên *file* trong thư mục
người dùng mang tên
thưmục kể cả trong các thư mục con
tar xvf archive.tar
giải phóng các tập tin có trong tập tin
« *tênngườidùng* »
« archive.tar », đồng thời hiển thị các tên
diff *file1 file2*
so sánh nội dung của 2 tập tin hoặc của
chown -R *tênngườidùng*

xác định người chủ của thư mục
tập tin
2 thư mục
thưmục
thưmục, kể cả các thư mục con (-R) là
tar xvfz archive.tar.gz
giải nén các tập tin có trong tập tin
người dùng « *tênngườidùng* »
« archive.tar.gz » dùng « gzip » và « tar »
chgrp *nhóm file*
chuyển tập tin *file* thành sở hữu của
tar jxvf archive.tar.bz2
giải nén các tập tin có trong tập tin
nhóm người dùng mang tên *nhóm*
« archive.tar.bz2 » dùng « bzip » và
chmod u+x *file*
giao (+) quyền thực hiện (x) tập tin *file*
« tar »
cho người dùng (u)
tar cvf archive.tar *file1*
tạo ra một tập tin *archive.tar* chứa các tập
chmod g-w *file*
rút (-) quyền ghi (w) *file* của nhóm (g)
file2
tin *file1* , *file2*
chmod o-r *file*
rút (-) quyền đọc (r) tập tin file của
tar cvfz archive.tar.gz
tạo một tập tin « archive.tar.gz » dùng
Tờ ghi nhớ
thưmục
« gzip » để chứa toàn bộ thư mục *thưmục*
những người dùng khác (o)
gzip file.txt
tạo tập tin nén « file.txt.gz »
chmod a+rw *file*
giao (+) quyền đọc (r) và ghi (w) *file*
ubuntu
cho mọi người (a)
gunzip file.txt.gz

giải nén tập tin « file.txt »
GNU / Linux
chmod -R a+rx *thưmục*
giao (+) quyền đọc (r) và vào bên
bzip2 file.txt
tạo tập tin nén « file.txt.bz2 »
trong thư mục (x) *thưmục* , kể cả tất cả
Bản gốc : 08/2006
các thư mục con của nó (-R), cho tất
Bản dịch : 01/2007
bunzip2 file.txt.bz2
giải nén tập tin « file.txt »
cả mọi người (a)
Error!

Quản trị hệ thống
Gói phần mềm
giải quyết các gói phụ thuộc)
/etc/apt/sources.list
tập tin xác định nguồn các kho phần
dpkg -c *paquet.deb*
liệt kê nội dung của gói *paquet.deb*
Cơ bản
mềm để tải xuống nhằm cài mới hoặc
cập nhật hệ thống
dpkg -I *paquet.deb*
hiển thị thjng tin của gói *paquet.deb*
sudo *command*
thực hiện lệnh *command* với tư cách
người siêu dùng (root)
Chú ý : cần cài các gói phần mềm apt-file, alien và deborphan nếu
apt-get update
cập nhật danh sách các gói phần mềm
muốn dùng chúng.
gksudo *command*
giống với sudo nhưng dùng cho các
căn cứ vào các kho phần mềm có trong
ứng dụng đồ hoạ
tập tin *sources.list*
Mạng máy tính

sudo -k
chấm dứt chế độ dùng lệnh có chức
apt-get upgrade
cập nhật các gói phần mềm đã cài rồi
/etc/network/interfaces
thjng tin cấu hình của các bộ phần
năng của người siêu dùng
giao diện (interfaces)
apt-get dist-upgrade
nâng cấp phiên bản hbuntu đang có
uname -r
cho biết phiên bản của nhân Linux
đến phiên bản mới tiếp theo
uname -a
hiện thị tên của máy tính trong mạng
(hostname)
shutdown -h now
khởi động lại máy tính ngay lập tức
apt-get install *soft*
cài phần mềm *soft* đồng thời giải quyết
các gói phần mềm phụ thuộc
ping *địa chỉIP*
thử nối mạng đến máy có địa chl IP
lsusb
liệt kê các thiết bị usb hoặc pci có mặt
lspci
trong máy tính
apt-get remove *soft*
loại bỏ phần mềm *soft* cing như tất cả
ifconfig -a
hiển thị thjng tin về tất cả các giao
các gói phần mềm trực thuộc
diện mạng đang có
time *command*
cho biết thời gian cần thiết để thực
hiện xong lệnh *command*
apt-get remove --purge *soft*
loại bỏ phần mềm *soft* kể cả tập tin cấu
ifconfig *eth0 địa chỉIP*
xác định địa chl IP cho giao diện cạc

hình của phần mềm *soft*
mạng *eth0*
command1 | command2
chuyển kết quả của lệnh *command1*
làm đầu vào của lệnh *command2*
apt-get autoclean
xoá bỏ các bản sao chép của những gói
ifdown *eth0*
ngưng hoạt động giao diện cạc mạng
phần mềm đã bị loại bỏ
ifconfig *eth0* down
eth0
clear
xoá màn hình của cửa sổ « Thiết bị
cuối » (terminal)
apt-cache dumpavail
hiện thị danh sách các gói phần mềm
ifup *eth0*
kích hoạt giao diện cạc mạng *eth0*
đang có
ifconfig *eth0* up
apt-cache search *soft*
cho biết danh sách các gói phần mềm
poweroff -i
ngưng hoạt động tất cả các nối mạng
Tiến trình (Processus)
có tên, hoặc có phần mj tả, chứa chuki
route add default gw *địa chỉ*
xác định địa chl IP của máy làm
soft
ps -ef
hiện thị tất cả các tiến trình đã đưec thực hiện
IP
cổng dmn đến bên ngoài mạng cục bộ
(*pid* et *ppid)*
apt-cache show *soft*
hiện thị phần mj tả của gói phần mềm
route del default
bỏ địa chl IP mặc định để ra khỏi
soft

ps aux
hiện thị chi tiết các tiến trình
mạng cục bộ
apt-cache showpkg *soft*
hiện thí các thjng tin của gói phần
ps aux | grep *soft*
hiện thị các tiến trình liên quan đến chưfng khởi
Phân vùng ổ cứng
mềm *soft*
động *soft*
/etc/fstab
chứa các thjng tin về các ổ cứng và hệ
apt-cache depends *soft*
liệt kê các gói phần mềm cần thiết cho
kill *pid*
báo chấm dứt tiến trình mang số *pid*
thống tập tin đưec gắn tự dộng
gói phần mềm *soft*
kill -g *pid*
yêu cầu hệ thống chấm dứt tiến trình *pid*
fdisk -l
hiện thị các phân vùng tích cực
apt-cache rdepends *soft*
liệt kê các gói phần mềm cần đến gói
xkill
chấm dứt một ứng dụng theo dạng đồ hoạ (ấn
phần mềm *soft*
mkdir /media/diskusb
tạo thư mục để gắn hệ thống tập tin của
chuột vào cửa sổ của ứng dụng)
thiết bị *diskusb*
apt-file update
cập nhật thjng tin căn cứ vào danh
sách nguồn phần mềm trong tập tin
mount /media/cleusb
gắn hệ thống tập tin *diskusb*
sources.list
umount /media/cleusb
tách ra hệ thống tập tin *diskusb*
apt-file search *file*

xác định tập tin *file* thuộc gói phần
mềm nào
mount -a
gắn, tách ra hoăc gắn lại tất cả các
mount -a -o remount
ổ/thiết bị có trong tập tin « /etc/fstab »
Tờ ghi nhớ
apt-file list *soft*
liệt kê các tập tin có trong gói phần
mềm *soft*
fdisk /dev/hda1
tạo mới và bỏ phân vùng trên ổ cứng
IDE thứ nhất
deborphan
liệt kê các gói phần mềm « mồ cji »
ubuntu
mkfs.extn /dev/hda1
tạo một hệ thống tập tin « extn » trên
alien -di *paquet.rpm*
chuyển phần mềm *paquet.rpm* thành
phân vùng « /dev/hda1 »
GNU / Linux
gói phần mềm dạng Debian *paquet.deb*
mkfs.vfat /dev/hda1
tạo một hệ thống tập tin « fatn2 » trên
Bản gốc : 08/2006
(-d) và thực hiện cài đặt lujn (-i)
phân vùng « /dev/hda1 »
Bản dịch : 01/2007
dpkg -i paquet.deb
cài đặt phần mềm paquet.deb (khjng

Reset Ubuntu/Gnome về cấu hình mặc định

Sau khi cài đặt Ubuntu các bạn có thể làm rất nhiều thứ để khám phá nó. Thay đổi các theme, chỉnh sửa các thiết lập bàn phím, màn hình. Nhưng có thể 1 lúc nào đó sẽ xảy ra trục trặc, Ubuntu làm việc không như bạn mong muốn. Và bạn cũng khộng nhớ việc gì đã dẫn đến lỗi đó. Có thể bạn sẽ tốn rất nhiều thời gian với Google để biết được cách khắc phục lỗi đó. Nhưng có lẽ tốt nhất bạn vẫn còn 1 cách đó là cài đặt lại Ubuntu. Đùa thôi với các thay đổi thông số của Gnome bạn vẫn có thể trả về thiết lập mặc định giống như lúc mới vừa cài lại máy mà vẫn giữ được các dữ liệu trong thư mục Home và các chương trình cài đặt.

(Cách này chỉ có thể sửa lại thông số mặc định cho Gnome khi bạn thay đổi. Những vấn đề về card màn hình, xserver… có thể không thể khắc phục bằng cách này).

Nếu bạn Login vào màn hình giao diện không được các bạn có thể login vào bằng Failsafe Terminal (Trong lựa chọn Option->Session của màn hình đăng nhập). Hoặc có thể sử dụng tổ hợp phím Ctrl + Atl + F1 để vào Terminal và đăng nhập vào. Sau đó chạy lệnh này

rm -rf .gnome .gnome2 .gconf .gconfd .metacity

(Bạn không nên chạy trong Recovery Mode vì nếu xài tài khoản root thì cũng chỉ xóa những thiết lập của Root mà thôi :D)

Quay lại màn hình đăng nhập bình thường bằng phím Ctrl + Alt + F7.

Trường hợp của mình thì không thể nào gõ các phím số cũng như phần bàn phím bên phía NumLock được. Nhưng user khác vẫn gõ được. Lỗi này sau 1 ngày mình VNC cái máy (hic hic nhà làm nên ko vào phòng được). Sau khi xài cách này thì máy trở lại hoạt động bình thường.

Sử dụng Internet với tốc ghi trên Modem bằng Ubuntu.

Sơ lược về ý tưởng

Đôi lúc bạn sẽ gặp rắc rối lúc config Port Forwarding cái zoom X4 và quản lý cái Host của mình bằng cái D-Link. Vì vậy mình chuyển qua sử dụng Bridge mode để kết nối Internet. Lúc đầu tìm hiểu về Bridge mode mình cũng gặp khá nhiều trục trặc và vô tình mình phát hiện ra là có thể tạo ra nhiều PPP interfaces với 1 account. Mình thử Ping các IP của các Interface đó ttl trả về đều là 64 đều từ máy Linux mà ra hết. Tiếp theo mình thử sử dụng 2 máy để kết nối PPP tới ISP cả 2 máy đều có thể download được Full đường truyền. Từ đó mình có ý định sử dụng Load Balancing để chia tải cho các kết nối PPP và tăng tốc kết nối Internet. Thật ra ngay lúc đó mình cũng chỉ biết Load Balancing là chia tải chứ chưa thật sự biết nó là gì. Sau nửa ngày trời lục lọi trên Internet xem xét nhiều Software mình thấy Load Balancing chỉ hiệu quả khi tạo nhiều kết nối dùng để download hoặc upload thôi nếu cũng sử dụng 1 kết nối thì tốc độc vẫn bình thường và ứng dụng thích hợp nhất cho nó là Torrent. Mình cũng phát hiện rằng trong chính Ubuntu đã có chức năng này.

Các bạn có thể tìm hiểu nhiều hơn về định tuyến (route) trên Linux tại http://lartc.org nếu các bạn quan tâm về định tuyến thì tài liệu này có thể rất có ích.

Nhận xét của mình

Mình chỉ mới thử cái này trên Viettel và Ubuntu còn Fedora có hướng dẫn thử cho một người nhưng làm không thành công. Nếu tốc độ kết nối của bạn cũng bằng với tốc độ Downstream và Upstream trong Modem ghi thì không nên thử vì cũng không cải thiện thêm. Còn nếu muốn dùng Home N và tận hưởng tốc độ Home C thì bài viết này sẽ giúp bạn. Mình hi vọng Viettel sẽ cho chạy thả giàn trong mấy ngày tết qua tết sẽ Fix lỗi này lại vì lỗi này rất dễ Fix. Nếu nhiều người

sử dụng cách này có thể sẽ gây lỗi tràn DSLAM, IP của Viettel vì vậy mình mong các cao thủ không nên làm quá tay.

Các bước tiến hành

Đọc hết bài viết rồi mới thử nhé coi chừng chết giữa đường không vào Net được đâu.

Đầu tiên các bạn phải cài đặt kết nối theo kiểu PPP ở chế độ Bridge.

Ở chế độ Bridge thì chính Ubuntu sẽ làm nhiệm vụ kết nối với ISP. Trên Windows thì không thể tạo nhiều kết nối WAN được nhưng Linux thì có thể.

Sau khi đã dùng lệnh pppoeconf để cài đặt Internet bạn có thể xài lệnh

pon dsl-provider

để tạo thêm kết nối

(Để disconnect thì xài lệnh poff dsl-provider)

Bạn tạo chừng 5 kết nối thêm. Sau đó phải xoá bản default rote đang chạy. Bằng lệnh

sudo ip route del default

Chạy 6-7 lần gì cho chắc ăn để có thể xoá hết.

Lúc này xài lệnh ifconfig để xem xem bạn đang có bao nhiêu ppp connect. Nếu có tới ppp5 thì bạn đang có 6 connect.

Sau đó sử dụng lệnh ip route để tạo một bảng định tuyến mới.

gateway=$(ifconfig ppp0 | grep ‘inet addr:’ | cut -d: -f3 | awk ‘{ print $1}’)

sudo ip route add default scope global nexthop via $gateway dev ppp0 weight 1 nexthop via $gateway dev ppp1 weight 1 nexthop via $gateway dev ppp2 weight 1 nexthop via $gateway dev ppp3 weight 1 nexthop via $gateway dev ppp4 weight 1 nexthop via $gateway dev ppp5 weight 1

lúc này xài lệnh ip route để xem bản định tuyến của bạn ra sao.

Nếu có dạng giống giống

117.5.128.1 dev ppp0 proto kernel scope link src 117.5.130.181
117.5.128.1 dev ppp1 proto kernel scope link src 117.5.134.51
117.5.128.1 dev ppp2 proto kernel scope link src 117.5.134.52
117.5.128.1 dev ppp3 proto kernel scope link src 117.5.134.54
117.5.128.1 dev ppp4 proto kernel scope link src 117.5.134.55
117.5.128.1 dev ppp5 proto kernel scope link src 117.5.134.57
117.5.128.1 dev ppp6 proto kernel scope link src 117.5.134.58
117.5.128.1 dev ppp7 proto kernel scope link src 117.5.134.59
117.5.128.1 dev ppp8 proto kernel scope link src 117.5.134.60
117.5.128.1 dev ppp9 proto kernel scope link src 117.5.134.62
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.2
169.254.0.0/16 dev eth0 scope link metric 1000
default
nexthop via 117.5.128.1 dev ppp0 weight 1

nexthop via 117.5.128.1 dev ppp1 weight 1
nexthop via 117.5.128.1 dev ppp2 weight 1
nexthop via 117.5.128.1 dev ppp3 weight 1
nexthop via 117.5.128.1 dev ppp4 weight 1
nexthop via 117.5.128.1 dev ppp5 weight 1
nexthop via 117.5.128.1 dev ppp6 weight 1
nexthop via 117.5.128.1 dev ppp7 weight 1

Thì bạn đã thành công rồi. Bây giờ chỉ việc download nhiều file 1 lúc thử xem.

Mình có thử làm một Script dùng để Load Balancing luôn bạn phải chạy nó. Điều kiện là phải tạo bridge mode ở bài viết trước nhé. (Open -> Run In Terminal -> nhập password vào)

Error!

Đây là đoạn Script Loadbalancing

```
##########################################
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 1
sudo pon dsl-provider
sleep 3
sudo ip route del default
sudo ip route del default
sudo ip route del default
sudo ip route del default
sudo ip route del default
sudo ip route del default
sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 0.5
```

sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 0.5
sudo ip route del default
sleep 3
gateway=$(ifconfig ppp0 | grep ‘inet addr:’ | cut -d: -f3 | awk ‘{ print $1}’)
sudo ip route add default scope global nexthop via $gateway dev ppp0 weight 1 nexthop via $gateway dev ppp1 weight 1 nexthop via $gateway dev ppp2 weight 1 nexthop via $gateway dev ppp3 weight 1 nexthop via $gateway dev ppp4 weight 1 nexthop via $gateway dev ppp5 weight 1
##
Chú ý ở dòng gateway là dấu ‘ ở dưới dấu ” thẳng đứng không phải dấu ` đâu nhé. Post lên đây nó bị đổi.

Sử dụng phím tắt trong Ubuntu

1. ‘ Alt‘ + ‘ F1 ‘ - Mở ‘ Applications Menu‘ cái này thật sự hữu ích vì hồi đó giờ không biết nếu không có chuột thì làm sao để vào mấy Menu ở trên được..

2. ‘ Alt‘ + ‘ F2 ‘ - ‘ Run Application‘ giống kiểu Windows - R nhưng xịn honw.

3. ‘ Print Screen ‘ - Nút này chắc ai cũng biết.

4. ‘ Alt‘ + ‘ Print Screen ‘ - Chụp ảnh màn hình ở cửa sổ đang sử dụng

5. ‘ Ctrl‘ + ‘ Alt‘ + ‘ right arrow ‘ - Di chuyển sang workspace phải.

6. ‘ Ctrl ‘ + ‘ Alt ‘ + ‘ left arrow‘ - Di chuyển sang workspace trái.

7. ‘ Ctrl ‘ + ‘ Alt ‘ + ‘ up arrow‘ - Di chuyển sang workspace trên

8. ‘ Ctrl ‘ + ‘ Alt ‘ + ‘down arrow‘ - Di chuyển sang workspace dưới.

9. ‘ Ctrl‘ + ‘ Alt ‘ + ‘ D‘ - Thu nhỏ tất cả các cửa sổ.

10. ‘ F1‘ - Trợ giúp.

Khi không kết nối với LAN, Ubuntu chạy chậm kinh khủng.

Nếu cài đặt không cẩn thận bạn có thể gặp vấn đề sau.

Nếu máy bạn không kết nối với 1 Switch hoặc 1 Modem hoặc 1 máy khác thì khi khởi động máy sẽ vào rất chậm. Các chương trình đều chạy chậm mặc dù CPU và ổ cứng không chạy nhiều.

Vấn đề này do cấu hình kết nối mạng đấy. Mặc định mỗi chương trình khi khởi động đều ping đến Hostname nhưng do trong file /etc/hosts lại khác với host name vì vậy không ping được dẫn đến sự chậm trễ. Bạn có thể sửa tại file /etc/hosts nhưng nếu không bạn có thể vào:

System->Administration->Network

Ở Tab General là Host name của máy. Ở Tab Hosts sẽ lưu địa chỉ tương ứng với hostname.

Bạn có thể thay đổi chúng để giống nhau. Nhưng thường nên thay đổi ở Tab Hosts. Ở địa chỉ 127.0.0.1 và 127.0.1.1 phần Alias bạn phải điền chính xác host name của bạn vào. Sau đó khởi động máy lại và bạn sẽ thấy nó không còn Delay nữa.

Tạo một file backup Server trên Ubuntu bằng rsync

Việc backup dữ liệu quả thật là rất quan trọng. Hôm qua mình phải xử lý 1 cái máy ổ cứng nó đòi tiền bao nhiêu dữ liệu trong đó mém mất. Vì vậy mình nghĩ ngay đến phải làm 1 Server để backup những dữ liệu quan trọng. Thông thường để backup qua mạng bạn có thể sử dụng một FTP Server và một Client Software ở trên đó. Tuy nhiên cách đó thì không tối ưu bởi dữ liệu không được nén lại. Nếu bạn sử dụng nasbackup kết hợp với rsync làm Server thì bạn sẽ có một giải pháp sao lưu hiệu quả. Thường thì Backup Server phải nằm khác nơi với máy kia (tránh trường hợp cháy nổ).

Trong bài này mình hướng dẫn bạn Backup các Windows PC trên Ubuntu Server:

Tại Backup Server

Các bạn thiết lập một rsync Server bằng cách sau.sudo apt-get install rsync (ở Ubuntu 7.10 rsync đã được cài mặc định)

Sau đó cần thay đổi file cấu hình của rsync. Username là user mà bạn muốn sử dụng để backup. Bạn nên tạo 1 user riêng để làm việc này.

sudo gedit /etc/rsyncd.conf

Thay đổi file đó với nội dung

[usernamebackup]

path = /home/username/backup

comment = Backup

uid = username

gid = username

read only = false

auth users = username
secrets file = /etc/rsyncd.secrets
Thay đổi quyền trên file cấu hình
sudo chmod 644 /etc/rsyncd.conf
Tạo một file chứa username và mật khẩu
sudo gedit /etc/rsyncd.secrets
với nội dung username:password
Username và password của User dùng để backup.
Việc quan trọng là phải bật server lên bằng cách
sudo gedit/etc/default/rsync
và đổi thành RSYNC_ENABLE=true
Sau đó restart rsync lại
sudo /etc/init.d/rsync restart
Nếu muốn cho rsync chạy mỗi lần khởi động thì bạn thêm dòng
rsync stream tcp nowait root /usr/bin/rsync rsyncd –daemon
vào file /etc/inetd.conf
Tại máy cần backup
Các bạn chỉ cần cài chương trình Nasbackup
http://sourceforge.net/project/showfiles.php?group_id=107470
Các thông số để cài đặt với server ở trên
Sharename sẽ là usernamebackup
Username và Password là cái bạn đã thiết lập.
IP có thể chọn là IP của máy nội bộ hoặc domain nếu backup qua mạng Internet các bạn phải cài đặt Port Forwarding ở cổng 873 .
##
Nếu bạn muốn sao lưu một máy sử dụng Ubuntu thì có thể sử dụng chương trình sbackup. Chương trình này rất dễ sử dụng và cài đặt. Có thêm chức năng backup lên FTP server nữa.

KHÁM PHÁ UBUNTU 7.0.4

Error!

Xin giới thiệu với các bạn những thủ thuật cơ bản để chinh phục sự "hơi lạ lạ" đó.

Bạn tải về tại **đây** (dạng file PDF)

Cài đặt AntiVirus trên Ubuntu

Bất kỳ hệ thống nào tham gia vào mạng Internet cũng cần đến sự hỗ trợ của các phần mềm antivirus nhằm bảo đảm tính an toàn. Với các hệ điều hành Microsoft Windows, chúng ta đã rất quen thuộc và thành thạo với Norton, McAfee, Trend Micro…Còn với Ubuntu, những phần mềm antivirus đang được xếp hàng đầu có thể kể đến là AVG Free, Avast, ClamAV…

AVG AntiVirus Free

AVG Free là một trong những giải pháp antivirus miễn phí nổi tiếng nhất dành cho người sử dụng ở phạm vi gia đình (home users). Với những tính năng như tự động cập nhật cơ sở dữ liệu virus một cách nhanh chóng, sử dụng đơn giản, chiếm ít tài nguyên hệ thống, tự động phát hiện virus… phần mềm này đã và đang trở thành một công cụ an toàn và tin cậy đối với các hệ thống máy tính. Bài viết hướng dẫn các bước cài đặt, cấu hình và sử dụng AVG Free trên Ubuntu-7.04. Ngoài ra, bạn đọc cũng có thể hiểu được cách thức cài đặt và sử dụng ***avast!*** và ***ClamAV***.

Để cài đặt AVG Free, chúng ta thực hiện các bước như sau:

1. Download AVG Antivirus Free Edition (.deb) về Desktop của máy tính Ubuntu.

Thực hiện thao tác này bằng cách truy cập vào địa chỉ:

http://free.grisoft.com/, chọn tab **Downloads**. Ở mục **Free Downloads**, chọn **AVG Anti-Virus Free Edition 7.5 for Linux**. Cuối cùng, chọn **Debian based distributions (Debian, Ubuntu)**.

Sau khi hoàn thành thao tác download, file cài đặt **avg75fld-r49-a1130.i386.deb** với kích thước ~ 41.9 MB sẽ được lưu về Desktop của máy tính theo mặc định. Tuy nhiên, chúng ta hoàn toàn có thể thay đổi vị trí lưu trữ từ Desktop sang một thư mục bất kỳ trên hệ thống của mình ngay khi trình duyệt bắt đầu download.

2. Cài đặt AVG Free vào hệ thống

Di chuyển vào thư mục chứa file cài đặt:

root@ln01:~# cd /home/tthai/Desktop

Tiến hành cài đặt với lệnh:

root@ln01:/home/tthai/Desktop# dpkg -i avg75fld-r49-a1130.i386.deb

3. Cấp quyền để các user trên Ubuntu có thể cập nhật virus

Cấp quyền thực thi để các user có thể chạy được chương trình AVG Free Update:

root@ln01:~# chmod 777 /opt/grisoft/avg7/bin/avgupdate

Cấp quyền ghi để cho phép chương trình AVG Free Update có thể đọc ghi được các file cần thiết trong thư mục */opt/grisoft/avg7/var/run*:

root@ln01:~# chmod 777 /opt/grisoft/avg7/var/run

Cấp quyền ghi để cho phép chương trình AVG Free Update có thể đọc ghi được các file cấu hình cũng như download các bản cập nhật virus về thư mục */opt/grisoft/avg7/var/update*:

root@ln01:~# chmod 777 /opt/grisoft/avg7/var/update

Đến bước này, bạn đã hoàn thành việc cài đặt và có thể bắt đầu với AVG Free bằng cách vào menu **Applications** > **Accessories** > **AGV for Linux Workstation**.

Nhấn nút **OK** trên cửa sổ License để bắt đầu sử dụng chương trình antivirus này.

Màn hình chính của AVG Free tương tự như dưới đây. Bạn có thể kiểm tra virus (test), xem kết quả kiểm tra (test results) và cập nhật cơ sở dữ liệu virus (update) bằng cách thực hiện các chức năng **Test**, **Test Results** và **Update**.

Bên cạnh đó, nếu muốn cấu hình để AVG Free tự động kiểm tra và cập nhật virus, chúng ta vào menu **Service** > **Program settings**.

- Để hệ thống kiểm tra virus tự động, bạn thay đổi các thông số thích hợp ở mục **Scheduler** > **Test schedule**.

Tại cửa sổ này, bạn chỉ định thời gian kiểm tra hàng ngày, hàng tuần, hay hàng tháng và vào lúc mấy giờ. Đồng thời, cũng cần chỉ định những thư mục nào sẽ được tự động kiểm tra.

- Để hệ thống cập nhật virus tự động, bạn thay đổi các thông số thích hợp ở mục **Scheduler** > **Update schedule**.

Tại cửa sổ này, bạn chỉ định thời gian cập nhật hàng ngày, hàng tuần, hay hàng tháng và vào lúc mấy giờ.

Clam AntiVirus - ClamAV

Bên cạnh AVG AntiVirus Free, bạn còn có ClamAV. Đây cũng là một chương trình antivirus dành cho các hệ điều hanh Unix/Linux. Mục đích chính của trình này là tích hợp với Mail server để thực hiện chức năng *attachment scanning*. Đồng thời, bạn cũng có thể sử dụng ClamAV cho mục đích phòng chống virus nhờ vào các cơ sở dữ liệu virus đi kèm.

Để cài đặt ClamAV, bạn thực hiện các lệnh sau:

root@ln01:~# apt-get update

root@ln01:~# apt-get install clamav

Hệ thống tự động dò tìm và chuẩn bị các thư viện liên quan. Khi dòng "**Do you want to continue [Y/n]?**" xuất hiện, bạn bấm phím **Y** để bắt đầu tiến trình cài đặt.

Khi các bước cài đặt đã hoàn tất, ClamAV sẽ chạy ngầm trên Ubuntu. Để quét virus tại một thư mục, bạn thực hiện lệnh:

root@ln01:~# clamscan -r /*đường-dẫn-đến-thư-mục*

Ví dụ: **root@ln01:~# clamscan -r /mydir**

avast! AntiVirus

Bạn cũng có thể lựu chọn avast! để phục vụ khả năng phòng chống virus trên hệ thống Ubuntu của mình.

Thao tác cài đặt rất đơn giản, bạn download gói cài đặt về thư mục hiện thời trên máy tính Ubuntu bằng lệnh:

root@ln01:~# wget http://files.avast.com/files/linux/avast4workstation_1.0.8-2_i386.deb

Tiếp theo, chạy lệnh cài đặt:

root@ln01:~# dpkg -i ./avast4workstation_1.0.8-2_i386.deb

Sau khi hoàn thành các bước cài đặt, bạn cần vào website http://www.avast.com/eng/download-avast-for-linux-edition.html, nhập địa chỉ email cùng thông tin liên quan đến cá nhân (tên, địa chỉ) để đăng ký một dãy khóa (registration key) nhằm kích hoạt phần mềm avast! trước khi sử dụng. Sau khi đăng ký xong, dãy khóa sẽ được gửi về địa chỉ email của bạn.

Cấu hình và sử dụng

Đưa avast! vào menu *Applications* bằng thao tác sau:

root@ln01:~# cd /usr/lib/avast4workstation/share/avast/desktop

root@ln01:/usr/lib/avast4workstation/share/avast/desktop# ./install-desktop-entries.sh install

Từ menu **Applications** > **Accessories**, bạn chọn **avast! Antivirus**. Trong màn hình *Registration* hiện ra, bạn sao chép dãy khóa đã đăng ký ở trên trong hộp thư của mình vào và bấm nút **OK**.

Trong màn hình chính của avast!, bạn dễ dàng thực hiện các thao tác phòng chống virus cho hệ thống Ubuntu của mình.

Trước khi sử dụng avast!, bạn nên cập nhật cơ sở dữ liệu virus bằng cách bấm nút **Update database**. Thao tác này nhằm đảm bảo avast! trên máy tính của bạn đã cập nhật cơ sở dữ liệu virus đến ngày hiện tại.

avast! cho phép bạn lựa chọn thư mục quét virus ở ba trường hợp: *Home directory*, *Entire system* và *Selected folders*. Bạn có thể thực hiện thao tác quét từ cấp độ đơn giản (*Quick*) đến phức tạp (*Thorough*).

Ngoài ra, menu **Tools** > **Preferences** cho phép bạn thay đổi cấu hình và tùy biến để avast! hoạt động một cách phù hợp với sở thích cá nhân của mình.

Trên đây là những chỉ dẫn nền tảng và căn bản nhất về cách tiếp cận với các phần mềm antivirus trên Ubuntu. Hy vọng rằng bài viết sẽ đem đến cho bạn đọc những gợi ý đơn giản và dễ hiểu để có thể thực thi cài đặt và cấu hình trên hệ thống Ubuntu của mình.

Theo *QTM*

Chia sẻ các file giữa Windows và Linux

Máy tính chạy Windows của bạn được cài đặt khởi động kép với Ubuntu Linux và sử dụng luân phiên hai hệ điều hành này. Tuy nhiên vấn đề ở đây là tất cả các file của bạn đều sử dụng partition NTFS trên hệ điều hành Windows, chính vì vậy Ubuntu không thể nhìn được các partition này, dù bạn có làm gì đi chăng nữa. Đó là vì Microsoft muốn hệ thống file NTFS có được độ bảo mật cao (không giống như làm cách làm việc của FAT32). Vậy phải thực hiện gì để có thể khắc phục được vấn đề này?

Có ba giải pháp nhanh và dễ dàng có thể giải quyết vấn đề này: NTFS-3G, Samba, và NTFS for Linux. NTFS-3G là một driver cho phép người dùng Linux có thể truy cập vào các ổ đĩa NTFS đã được cài đặt trên cùng một máy tính. Gutsy Gibbon distro mới của Ubuntu gồm có driver trong Synaptic Package Manager. Samba (tìm thấy thông qua Synaptic) được thiết kế để cung cấp các dịch vụ file và máy in cho tất cả các máy khách SMB, gồm có Microsoft Windows. Nó thực hiện như một tiện ích mạng, trong thực tế gắn ổ đĩa NTFS của bạn vào mạng Linux. NTFS for Linux là một công cụ tuyệt vời cho các nhà quản lý CNTT, phiên bản pro của nó còn cho phép bạn thực hiện cả các công việc đọc và ghi một cách đơn giản.

Bước 1: Sử dụng trình duyệt file

Sau khi cài đặt Samba hoặc NTFS-3G, sử dụng File Browser của Ubuntu để tìm đến partition NTFS mà bạn muốn làm việc sau đó kích đúp vào để mở nó.

Error!

Bước 2: Kiểm tra các thuộc tính của ổ đĩa

Hộp thoại Volume Properties trong Ubuntu thể hiện rằng thư mục này đã được định dạng là NTFS.

Error!

Bước 3: NTFS for LINUX

Tiện ích của Windows nổi tiếng, phần mềm Paragon (www.paragon-software.com/products.htm) phân phối NTFS for Lunix, công cụ dành cho dân CNTT ($149.95), gói tính năng đầy đủ ($29.95), hoặc một download miễn phí trên mạng. Phiên bản miễn phí cho phép truy cập vào các partition của Linux nhưng chỉ có chức năng đọc.

Error!

Bước 4: Phía Windows: LINUX READER và EX2 IFS

Hai chương trình này cung cấp khả năng truy cập vào Linux từ bên trong Windows. Linux Reader từ DiskInternals (có trong ảnh) cho phép bạn có thể truy cập ở chế độ chỉ đọc và chỉ sử dụng chương trình xem của nó, trong khi đó Ex2 IFS cung cấp cả truy cập đọc và ghi từ Windows Explorer. Tuy nhiên trước khi cài đặt Ex2 IFS, bạn hãy đọc trang khắc phục sự cố của site, trang này sẽ liệt kê một số vấn đề có thể xảy ra thu thập từ một số kinh nghiệm. Cả hai đều có khả năng bảo vệ partition của Lunix, bỏ qua bảo mật, chính vì vậy bạn cần phải có kiến thức về vấn đề này trước khi cài đặt.

Error!

Theo *PcMag*

Hiển thị hình nền Ubuntu Desktop ngay sau khi đăng nhập

Các bạn dùng Ubuntu Desktop hẳn đã quen với việc khi đăng nhập, sau khi gõ vào username và password thì hiện ra một màn hình màu nâu sáng (tông màu Human của Ubuntu) trong lúc chờ GDM load desktop lên.

Error!

Ta có thể thay đổi màu bằng cách chỉnh sửa file gdm.conf, nhưng nếu bạn muốn hiển thị ngay hình nền desktop của mình chứ không phải là những màu đơn sắc này thì những hướng dẫn trong bài viết này sẽ giúp bạn làm được điều đó. Đặc biệt khi làm thủ thuật này bạn sẽ có cảm giác khởi động vào giao diện nhanh hơn.

1. Mở cửa sổ terminal dòng lệnh bằng menu Application> Accessories> Terminal

2. Trước tiên ta cần cài đặt thêm chương trình xloadimage bằng dòng lệnh

sudo apt-get install xloadimage

3. Tạo một đoạn script để load hình nền desktop lên ngay sau khi đăng nhập

sudo gedit /etc/gdm/PostLogin/Default

Chép và dán đoạn mã sau vào:

```
#!/bin/sh
#
# Note that output goes into the .xsession-errors file for easy debugging
#
# Extract the wallpaper filename
WALLPAPER="`cat ~/.gconf/desktop/gnome/background/%gconf.xml | sed -n -e 'N
s/^[ \t]*\(.*\)<\/stringvalue>.*$/\1/ip'`"
# Check if the wallpaper file exists. If yes - draw it, if no - use primary background color
if [ -e "$WALLPAPER" ] && [ -f "$WALLPAPER" ] ; then
xsetbg -onroot "$WALLPAPER"
else
PRIMARY_COLOR="`cat ~/.gconf/desktop/gnome/background/%gconf.xml | sed -n -e 'N
s/^[ \t]*\(.*\)<\/stringvalue>.*$/\1/ip'`"
xsetroot -cursor_name left_ptr -solid "$PRIMARY_COLOR"
fi
exit 0
```

Đoạn script này sẽ kiểm tra thiết lập ảnh nền, và dùng chương trình 'xsetbg' để vẽ lên cửa sổ gốc. Nếu không có ảnh nền được thiết lập, nó sẽ tô màn hình bằng màu nền desktop.

4. Cấp quyền thực thi cho đoạn script

sudo chmod +x /etc/gdm/PostLogin/Default

5. Bước cuối cùng là vô hiệu hoá file /etc/gdm/PreSession/Default. Đây là file đảm nhiệm việc thiết lập màu cho cửa sổ gốc (chẳng hạn màu Human), được thực thi sau các script đặt trong PostLogin. Ta chỉ cần làm nó biến đi bằng cách đổi tên, chẳng hạn thành Default.bak:

sudo mv -v /etc/gdm/PreSession/Default /etc/gdm/PreSession/Default.bak

Bây giờ hãy logout, login vào lại và xem sự khác biệt!

6. Trong trường hợp bạn muốn khôi phục lại các cài đặt gốc, hãy dùng hai lệnh sau:

sudo rm /etc/gdm/PostLogin/Default

sudo mv /etc/gdm/PreSession/Default.bak /etc/gdm/PreSession/Default

Thủ thuật giúp server Ubuntu Linux của bạn an toàn

Khi là quản trị viên hệ thống, một trong những nhiệm vụ trọng yếu của bạn là xử lý các vấn đề bảo mật server. Nếu server của bạn được kết nối Internet, bạn nên đặt nó trong vùng xung đột. Nếu đó chỉ là một server nội bộ, bạn vẫn cần xử lý (có thể là một cách ngẫu nhiên) những đối tượng nguy hiểm, các nhân viên chống đối hay gã kế toán nào đó muốn đọc trộm e-mail bí mật của sếp.

Thông thường Ubuntu Server rất an toàn. Ubuntu Server Team - nhóm sản xuất các phiên bản update bảo mật văn phòng - đã thực hiện lần lột xác thành công nhất trong lịch sử ngành công nghiệp bảo mật với Ubuntu Server. Ubuntu không được gắn với chính sách cổng mở. Có nghĩa là sau khi bạn cài đặt, để chế độ desktop hay server cho Ubuntu xong, mặc định sẽ không có chương trình ứng dụng nào chấp nhận kết nối đến internet. Giống như Ubuntu desktop, Ubuntu Server sử dụng cơ chế sudo trong quản trị hệ thống, tránh sử dụng tài khoản gốc. Các bản update bảo mật còn được bảo hành ít nhất 18 tháng sau khi phát hành (một số bản lên đến 5 năm như Dapper) và hoàn toàn miễn phí.

Trong phần này chúng tôi muốn bàn về vấn đề bảo mật file hệ thống, các giới hạn nguồn hệ thống, xử lý các bản ghi và an ninh mạng. Nhưng bảo mật trong Linux là một đề tài khó và rộng lớn nên chúng tôi chỉ xin cung cấp cho các bạn một số cách giải quyết xung đột cơ bản. Để trở thành một quản trị viên tốt, bạn nên quan tâm tới vấn đề này và học hỏi thêm từ các nguồn khác mà chúng tôi sẽ cung cấp trong bài.

Quản trị tài khoản người dùng

Nhiều khía cạnh quản trị người dùng của hệ thống Linux được thực hiện nhất quán trên các phân phối của nó. Trước đây, hãng Debian cung cấp một số tiện ích như mã lệnh useadd, giúp bạn quản trị dễ dàng hơn. Sau này Ubuntu kế thừa đầy

đủ mô hình quản trị người dùng của Debian. Chúng ta sẽ không đi sâu vào chi tiết của Debian mặc dầu nó được coi là mô hình chuẩn trong quản trị người dùng. Các bạn muốn tìm hiểu thêm có thể tham khảo tại website của O'Reilly. Vấn đề chúng ta quan tâm ở đây là sự khác biệt của Ubuntu với mô hình chuẩn: sudo.

Ubuntu không cho phép đặt mặc định root, administrator, account. Nó có cách xử lý lợi ích bảo mật khá hay và một số phương án giảm cấp đáng kinh ngạc. Đó là văn bản hoá tất cả trong các trang chính của file gốc sudo_root.

Trong quá trình cài đặt, bạn thêm vào người dùng nào thì mặc định người dùng đó sẽ được đặt trong nhóm admin và có thể dùng sudo để thực hiện các nhiệm vụ quản trị hệ thống. Sau khi thêm tên người dùng mới vào hệ thống, bạn có thể đưa họ vào nhóm admin bằng câu lệnh:

$ sudo adduser username admin

Nếu muốn loại một người nào ra khỏi nhóm admin, đơn giản bạn chỉ cần đặt lệnh deluser thay thế adduser.

Một điều bạn nên chú ý là sudo không chỉ cung cấp quyền truy cập thư mục gốc. Nó còn có thể điều khiển các quyền nhỏ bên trong, chẳng hạn như việc ra lệnh: "chỉ cho phép người dùng này thực thi 3 câu lệnh với các đặc quyền của superuser"

Tài liệu mô tả các quyền này nằm trong trang "sudoers" nhưng nó khá khó hiểu. Bạn chỉ cảm thấy rõ ràng hơn đôi chút khi đọc đến phần ví dụ của nó, tài liệu này cung cấp hầu hết các tình huống bạn cần dùng đến sudo. Khi đã thực sự hiểu, đơn giản bạn chỉ cần chạy câu lệnh:

$ visudo

Ở đây bạn phải cẩn thận. Cơ sở dữ liệu sudoers, nằm trong "/etc/sudoers" không mở được bằng một trình soạn thảo. Bởi vì một trình soạn thảo không thể kiểm tra được cú pháp.

Nếu bạn làm rối cơ sở dữ liệu sudoers, có thể bạn sẽ phải tự mình tra tìm dữ liệu mà không thể trở thành người quản trị được.

Bảo mật hệ thống file

Mô hình bảo mật file được chuẩn hoá trong hầu hết các hệ thống tựa Unix và được gọi là mô hình POSIX. Mô hình này có 3 quyền truy cập file và thư mục mở rộng cho: người sở hữu, nhóm và các đối tượng khác. Tất cả đều được thực hiện giống nhau tại bất kỳ phân phối Linux nào. Đó là lý do vì sao chúng ta không tập trung phân tích kỹ vấn đề này. Các bạn có thể tham khảo thêm tại các trang "chmod" và "chown" trong phần trợ giúp của Linux hoặc trên Internet.

Bây giờ chúng ta sẽ tập trung vào việc phân vùng bảo mật thông qua các tuỳ chọn lắp ghép, một vấn đề quan trọng cần chú ý khi xử lý bảo mật hệ thống. Việc phân vùng sẽ có tác động mạnh nếu được dùng thích hợp. Khi giải thích cách thức phân vùng hệ thống chúng tôi đã nhấn mạnh ưu điểm của Linux trong việc cung cấp các thư mục "/home", "/tmp", "/var" cho các phân vùng riêng. Các thư mục

này đề cập đến cách dùng các tuỳ chọn đặc biệt khi ghép các phần vùng vào hệ thống file.

Nhiều tuỳ chọn lắp ghép là kiểu hệ thống file phụ thuộc. Nhưng những tuỳ chọn chúng ta xét đến không phải loại này. Chúng ta có một số tuỳ chọn sau:

nodev: Một hệ thống file lắp ghép với tuỳ chọn nodev sẽ không cho phép sử dụng hay tạo các file "device" đặc biệt. Chẳng có lý do tốt đẹp nào khi cho phép hệ thống file biên dịch các ổ đặc biệt block, character vì như thế tức là cho phép chúng tạo ra các nguy hiểm bảo mật tiềm ẩn.

nosuid Các file trong Unix nói chung và trong Linux nói riêng đều có thể được đánh dấu bằng cờ để cho phép một người nào đó thực thi file bằng quyền của người khác hay nhóm khác, thông thường là của người quản trị hệ thống. Cờ này được gọi là setuid (suid) hay cờ nhị phân setgid bit. Nó cũng cho phép thực thi file bên ngoài thư mục chứa các mã nhị phân hệ thống không cần thiết, làm giảm độ an toàn. Nếu một người dùng được quyền sử dụng thì anh ta có thể tạo hoặc lấy một cờ nhị phân suid theo cách chọn riêng. Sau đó có thể sử dụng hệ thống một cách hiệu quả.

noexec: nếu một hệ thống file được đánh dấu cờ là noexec, người dùng sẽ không thể chạy bất kỳ chương trình thực thi nào nằm trong nó.

noatime cờ này nói rằng hệ thống file không giữ bản ghi lần truy cập cuối cùng của các file. Nếu sử dụng một cách bừa bãi có thể khiến giảm an toàn hệ thống. Vì nó giới hạn thông tin ghi sự cố bảo mật. Cờ này cũng cung cấp các lợi ích thực thi cho bất kỳ kiểu dùng nào. Bạn nên dùng trên các phân vùng, nơi bảo mật cân bằng với tốc độ.

Quyết định sử dụng tuỳ chọn lắp ghép nào trong phân vùng nào là một kỹ thuật cao. Bạn sẽ thường xuyên phải phát triển các tham chiếu khi trở nên quen thuộc hơn với cơ chế quản trị. Dưới đây là kiểu lựa chọn cơ bản các bạn có thể tham khảo. Tất nhiên các bạn có thể lựa chọn kiểu khác, nhưng nên bắt đầu bằng kiểu cơ bản này:

• /home-nosuid, nodev
• /tmp-noatime, noexec, nodev, nosuid
• /var-noexec, nodev, nosuid

Giới hạn nguồn hệ thống

Mặc định Linux sẽ không sử dụng bất kỳ giới hạn nguồn nào trong các tiến trình của người dùng. Điều này có nghĩa là bất kỳ người dùng nào đều được tự do lấp đầy bộ nhớ làm việc trên máy, hoặc sinh ra các tiến trình lặp vô hạn, trả lại hệ thống không dùng được trong vài giây. Giải pháp khắc phục là thiết lập một số giới hạn nguồn bằng cách chỉnh sửa file "/etc/security/limits.conf":

$ sudoedit /etc/security/limits.conf

Các thiết lập đều được giải thích trong các comment bên trong file. Các bạn nên dùng ít nhất là giới hạn "nproc" hoặc cũng có thể là "as/data/_memlock/rss".

Mẹo nhỏ: một ví dụ giới hạn nguồn real-life

Chúng tôi mới chỉ giới thiệu sơ lược về các giới hạn như thế nào trên các server sản xuất. Dưới đây là cấu hình server đăng nhập chung của Bộ môn khoa học máy tính, trường đại học Harvard, Hoa Kỳ:

as 2097152

_____

data 131072

_____

memlock 131072

_____

rss 1013352

_____

hard nproc 128

Các giới hạn này quy định người dùng có thể sử dụng 128 tiến trình, với không gian địa chỉ lớn nhất là 2GB, kích thước dữ liệu nhỏ nhất và địa chỉ được khoá trong bộ nhớ là 128MB, giới hạn kích thước tập hợp lưu trú lớn nhất là 1GB.

Các file bản ghi hệ thống

Khi là một quản trị viên hệ thống, các file bản ghi log là một trong số những người bạn tốt nhất của bạn. Nếu bạn theo dõi các file này một cách thường xuyên, cẩn thận, bạn sẽ phát hiện được lỗi sai trong hệ thống ngay khi nó vừa xuất hiện. Do đó bạn có thể giải quyết được hầu hết mọi vấn đề trước khi chúng kịp phát sinh.

Đáng tiếc, khả năng quan tâm tới các file log này ngày càng giảm. Vì thế các quản trị viên thường chỉ sử dụng phần mềm thực hiện tiến trình log, cảnh báo họ một số sự kiện nào đó, hoặc ghi các tuỳ chọn riêng của họ theo một số ngôn ngữ như Perl và Python.

Các bản ghi log thường nằm trong thư mục "/var/log". Sau khi server của bạn chạy được một lúc, bạn sẽ thấy có rất nhiều phiên bản file log cũ đang tăng lên trong thư mục này. Nhiều trong số chúng được nén trong chương trình nén gzip (với đuôi mở rộng là ".gz").

Dưới đây là một số file log cần chú ý:

*

/var/log/syslog – file log hệ thống thông thường

*

/var/log/auth.log – các file log thẩm định hệt thống

*

/var/log/mail.log -- các file log thư hệ thốngsystem

*

/var/log/messages – các tin nhắn log thông thường

*

/var/log/dmesg – tin nhắn bộ đệm chuông ở nhân kernel, thông thường từ khi khởi động hệ thống.

Hộp công cụ Toolbox Log

Khi xem lại các file log, có một vài công cụ lựa chọn mà bạn phải sử dụng thuần thục. Phần cuối của các tiện ích được in ra đặt mặc định là mười dòng cuối cùng của file, đây là tùy chọn gọn nhỏ cho biết thông tin về lần cuối cùng truy cập vào file log.

$ tail /var/log/syslog

Với tham số -f, phần đuôi được đưa vào theo mẫu dưới, nó sẽ mở các file và thể hiện sự thay đổi trên màn hình cho bạn biết.

Các file z.grep, zcat, zless cũng hoạt động giống như các file tương ứng không có chữ "z" ở đầu. Các file này là kiểu file nén của gzip. Ví dụ, để lấy ra danh sách các dòng trong tất cả file log nén có từ "warthog" bạn chỉ cần cung cấp câu lệnh sau:

$ zgrep -i warthog /var/log/*.gz

Hộp công cụ Toolbox của bạn xử lý các log phát triển theo kinh nghiệm và dựa trên các tham chiếu của bạn nhưng bạn nên tìm kiếm trong apt-cache các file log trước.

Một chút về bảo mật mạng

Quản trị bảo mật mạng là một thành phần khác, được hệ điều hành cung cấp theo mảng khá rộng. Giữa Ubuntun và các mô hình phân phối khác của Linux không có sự khác nhau nhiều lắm.

Câu lệnh iptables là phần mặt trước tới các bảng tường lửa rất mạnh của Linux. Thật không may, thao tác xử lý với iptables có thể khó hơn nhiều nhất là khi bạn đang cố gắng thiết lập các chính sách firewall tổng hợp. Câu lệnh dưới đây xoá tất cả các gói dữ liệu đến từ một tên miền xấu:

$ sudo iptables -A INPUT -s www.slashdot.org -j DROP

Các tài liệu hướng dẫn, các cách thức thực hiện và các bài báo về iptables có trên Internet với số lượng lớn và hệ thống trang chính cung cấp thông tin chi tiết về các tuỳ chọn thích hợp. Bạn nên bỏ ra một chút thời gian học về iptables vì nó sẽ cho phép bạn cài đặt chế độ bảo mật an toàn trên bất kỳ cơ chế Linux nào và sẽ dễ dàng hơn khi học về các hệ thống tường lửa OS khác.

Những điểm cần chú ý cuối cùng về bảo mật

Trong bài này chúng ta mới chỉ lướt qua các vấn đề bề mặt của bảo mật hệ thống. Mặc dù chúng tôi đã cố gắng cung cấp cho các bạn các gợi ý hay về điểm bắt đầu và nơi có thể học hỏi thêm. Nhưng thật sự là không có một hệ thống bảo mật hoàn hảo nào cả. Bảo mật không có nghĩa là xoá bỏ được hoàn toàn các vi phạm, mà chỉ là làm cho chúng trở nên khó bị khai thác, khó bị tấn công. Định nghĩa này có thể bị thay đổi dễ dàng. Bởi nó còn phụ thuộc vào kẻ tấn công. Nếu kẻ tấn công là một đứa trẻ bụi đời, sống trong tầng hầm, nhai bánh pizza lạnh thì

nó có thể chán nản, dễ dàng bỏ cuộc nếu hàng rào an ninh của bạn quá an toàn. Nhưng nếu bạn đang giữ các thông tin bí mật đắt giá thì cho dù hệ thống bảo mật có an toàn đến đâu vẫn có thể bị phá vào một ngày nào đó. Bởi hoạt động phá hoại lúc này xuất phát từ quan điểm giá cả, lợi nhuận của kẻ tấn công.

Bảo mật cũng khá rõ ràng, vì nó được phát triển như là một khái niệm trong khoa học máy tính. Muốn bảo mật thật tốt đòi hỏi phải thực sự hiểu sâu về các hoạt động bên trong hệ thống máy tính. Tuy nhiên cũng sẽ chẳng có cải tiến đáng kể nào nếu bạn hiểu sâu về nó mà không biết bắt đầu từ đâu. Các bạn có thể bắt đầu ngay từ hôm nay, theo những tham khảo ở trên, và dùng nó để nâng cao kiến thức bảo mật sau này của bạn.

(Theo Computerworld)

Đây là bộ gõ tiếng Việt dùng cho hệ điều hành Ubuntu, dung lượng 1,8MB. Để cài đặt, bạn chỉ việc click đôi chuột lên tập tin vừa mới tải về và chọn Install Package. Nếu được yêu cầu, bạn cần khai báo tài khoản đăng nhập vào hệ thống đã tạo trước đó (tài khoản khi cài đặt Ubuntu). Khi quá trình cài đặt hoàn tất, bạn khởi động lại máy để bộ gõ có hiệu lực.

Lúc này, trên thanh tác vụ nằm phía trên màn hình xuất hiện thêm một biểu tượng mới của SCIM. Để gõ được tiếng việt, bạn cần mở ứng dụng muốn nhập liệu (các thành phần trong bộ OpenOffice.org chẳng hạn). Sau đó click chuột lên biểu tượng SCIM, nhấp chọn ngôn ngữ là Vietnamese và chọn kiểu gõ tùy theo ý thích của bạn.

Bạn tải về tại đây.

Error!

Anh, em thân mến !!

Có lẽ có rất nhiều anh em khi đọc những dòng viết này vẫn còn thắc mắc không hiểu tại sao tôi lại gọi công việc đóng gói Ebook là một "kỹ nghệ ".

Vâng, đối với tôi công việc tạo nên những cuốn Ebook đúng là một kỹ nghệ. Để đóng được một cuốn Ebook thực sự hay, thật sự lôi cuốn người đọc không hề dễ dàng như một số người trong chúng ta vẫn tưởng chút nào. Việc làm này đòi hỏi phải có kỹ thuật, thủ thuật khéo léo để Ebook tiện lợi đối với mọi đối tượng mà chúng ta hướng đến, mang Ebook của ta làm đến với mọi người mà không gặp bất cứ một rào cản nào về kỹ thuật công nghệ, điều này khiến chúng ta giống như một

kỹ sư thiết kế vậy. Ngoài ra nó còn đòi hỏi chúng ta phải biết cảm nhận được sở thích của đối tượng mà chúng ta hướng tới, mang lại cho người đọc những thứ họ quan tâm, hy sinh thời gian công sức để đóng góp cho xã hội giống như là một nghệ sĩ thật thụ.

Vâng, tôi nghĩ rằng, có lẽ chúng ta có thể gọi một người đóng Ebook là một nghệ nhân. Tác phẩm của họ được nhào nặn ra bởi chính tài năng, niềm cảm xúc thăng hoa, tâm huyết với xã hội. Tác phẩm của họ có thể không to lớn về vật chất hay về tinh thần nhưng nó đang hàng ngày hàng giờ đóng góp vào việc xây dựng một nền tư tưởng học tập tiến bộ, một cách giải trí đầy hữu ích cho chúng ta.

Vâng, đã có rất nhiều người như vậy. Đang âm thầm cống hiến cho cuộc sống. Còn bạn thì sao? Bạn có dám hi sinh vài giờ chơi Game ra để làm một việc có ích không? Mỗi ngày, tốn một ít thời gian để gửi mơ ước đến thế hệ tương lai không ?

Câu trả lời tôi dành cho các bạn !!!

Các bạn hãy cùng với chúng tôi viết lên cuộc sống, **Ebook Team của thegioiebook.com** !!!!

Đây là cuốn Ebook hướng dẫn các bạn đóng gói Ebook từ A -Z. Chỉ cần có tâm huyết là bạn sẽ làm được ngay bất kể bạn là ai. Chúng tôi hướng dẫn các bạn tạo Ebook dưới 2 định dạng chính CHM và PDF

langtulangthang, phamtienvuong - TGE Team - www.thegioiebook.com

-- Tuyển nhân sự cho Ebook Team --

Anh, em nhã giám !!!

Trong thời đại tin học bùng nổ, Internet không còn là trong giấc mơ của mọi người. Ebook đang dần dần trở thành một thứ không thể thiếu với chúng ta. Có những người đang âm thầm tưng ngày, từng giờ đóng góp cho Xã hội bằng những cuốn sách nhỏ nhoi đó. Còn chúng ta thì sao ??? Câu trả lời tôi dành cho các bạn.

Các bạn sẵn sàng hy sinh vài giờ chơi Game để làm chút việc có ích cho cuộc sống hay không??? Mỗi ngày dành một chút thời gian để gửi gì đó cho thế hệ tương lai. Để sau này sẽ có người vẫn nhớ đến bạn, dù nhỏ nhoi nhưng đáng làm lắm chứ !!!

Dù bạn là ai, nếu các bạn không ngại, hãy tham gia với chúng tôi để cùng nhau vẽ nên cuộc sống !!!

*** Quyền lợi được hưởng :**

- Được hưởng toàn bộ quyền lợi của một VIP account, truy nhập được vào Vip Center, Request bất cứ cái gì (tất nhiên là trừ những thứ cấm)
- Được cung cấp Acount để vào một số thư viện trên Net như NetLibrary chẳng hạn
- Trong tương lai sẽ có Site riêng cho cho Team, chỉ post sách do Team làm, các Team sẽ có quyền update sách ở đây
- Được hưởng những quyền lợi mà chỉ TGE mới có trong tương lai (cái này đang trong kế hoạch bí mật)
- Được sáng tạo hết sức để góp phần xây dựng Team và toàn TGE, được giúp đỡ để hoàn thành những dự án của riêng bản thân.
- Sẽ là lựa chọn hàng đầu nếu TGE thiếu nhân lực quản lý (MOD)

*** Trách nhiệm:**

- Làm việc hết khả năng mà bạn có để xây dựng các kế hoạch của Team cũng như là làm Ebook
- Tuân thủ nội quy của Ebook Team
- Phải chịu mọi trách nhiệm nếu vi phạm các quy định cũng như là vô trách nhiệm với công việc.

*** Các vị trí cần tuyển:**

- **Ebook Seacher:**

+) **Công việc chính** của nhóm là tìm kiếm tài nguyên trên Net cung cấp cho các thành viên khác đóng sách. Nhận yêu cầu tìm kiếm thông tin cần thiết của các thành viên đóng gói sách để tìm kiếm.

+) Yêu cầu: Sử dụng tốt các công cụ tìm kiếm, có kinh nghiệm lướt Web, có nhiều thời gian trên Net, biết phân tích thông tin, biết nắm bắt thực tế để khai thác những loại sách. Qua phỏng vấn và 2 tuần thử thách trong Team

+) **Liên lạc:** Bạn liên lạc với YM: **du_hi_vuong** hoặc PM: **thesirius114** để sắp xếp thời gian cùng nói chuyện.

- **Ebook Design:**

+) **Công việc chính:** Thiết kế bìa sách cho các Ebook do Team đóng gói. Nhóm này có trách nhiệm theo dõi việc tìm kiếm tài nguyên, khi có một tài nguyên về Ebook ngay lập tức người trong nhóm phải Design bìa để kịp cho việc đóng gói. Ngoài ra nhóm có nhiệm vụ Design bìa theo yêu cầu của Teamer đóng những sách không có trong kho tài nguyên.

+) Yêu cầu: Có một chút khiếu thẩm mỹ, sử dụng tốt các Tools Design, chăm chỉ và sáng tạo. Qua phỏng vấn và 2 tuần thử thách trong Team

+) Liên lạc: Bạn liên lạc với YM: **du_hi_vuong** hoặc PM: **thesirius114** để sắp xếp thời gian cùng nói chuyện.

- **Ebook Maker:**

+) Công việc chính là tự tìm kiếm thông tin để đóng gói Ebook (hiện chưa đủ nhân lực để tìm đủ nguồn) hoặc đóng gói theo các nguồn tài nguyên được cung cấp. Có thể gửi yêu cầu tìm kiếm thông tin và yêu cầu làm bìa đến 2 trên nhóm khác.

+) Yêu cầu: Có tâm huyết với công việc,biết chút ít về máy tính, chăm chỉ, chịu khó, có thêm chút tư duy nắm bắt thông tin để khai thác các loại sách khác nhau thì càng tốt ...Sẽ được hướng dẫn đóng gói thử Ebook để kiểm tra khả năng. 2 tuần thử thách trong Team

+) Liên lạc: Gửi 2 cuốn Ebook bạn làm trực tiếp tại Topic này để kiểm tra (**1 định dạng PDF – 1 định dạng CHM – Download Ebook hướng dẫn tại link bên dưới).** Có thể liên lạc với YM: **langtult_vn** hoặc PM: **langtulangthang** nếu cần thiết.

langtulangthang

-- Nội quy Ebook Team --

I – Nội quy chung:

- Đoàn kết thân ái với mọi thành viên trong Team, chấp hành tốt quy định của 4rum. Không chia bè kết phái gây mất đoàn kết trong Team
- Không có những lời lẽ khiêu khích miệt thị lẫn nhau. Tôn trọng ý kiến và công việc của nhau.
- Không được phép tiết lộ những thông tin bên trong Team ra bên ngoài. Nhất là những kế hoạch có ý nghĩa trong việc phát triển TGE trong tương lai.
- Mọi thành viên đều có quyền góp ý và phê bình thẳng thắn đối với Leader và Deputy Leader về cách làm việc của Team và người trong Team.
- Mọi thành viên đều có thể tự do sáng tạo, đóng góp ý kiến cho việc phát triển Team cũng như là forum trong tương lai.
- Mọi thành viên đều có quyền đòi hỏi những quyền lợi mà mình xứng đáng được nhận.
- Nếu có vấn đề gì (cá nhân hoặc tập thể) dẫn đến không hoàn thành được công việc phải báo cho Leader hoặc Deputy Leader biết để giải quyết.
- Tất cả mọi người trong Team đều phải tuân thủ các nội quy trên dù người đó là bất kỳ ai LEADER, DEPUTY LEADER, MOD, SMOD hay ADMIN
- Tất cả đều hướng tới một mục đích xây dựng một Ebook team vững mạnh, đóng góp sức mình cho tương lai.

II – Nội quy làm việc :

- Nếu bạn không hoàn thành trách nhiệm của mình trong tháng thứ 1 sẽ bị đưa vào danh sách nhắc nhở (trừ khi bạn có lý do và được sự cho phép của Leader)
- Nếu bạn không hoàn thành trách nhiệm của mình trong tháng thứ 2 sẽ bị loại bỏ khỏi nhóm và tước bỏ toàn bộ các quyền lợi ...

- Ngoài công việc do cá nhân các thành viên tự thực hiện như đã được nêu trong "Hướng dẫn và phân công làm việc trong Ebook Team". Các thành viên sẽ phải làm các công việc do **Leader** và **Deputy Leader** giao cho (trừ trường hợp có lý do thích đáng)
- Các Mod và Smod sẽ được nới lỏng công việc trong Ebook Team để có thời gian dành cho việc quản lý và phát triển forum

III - Quy định trách nhiệm:

- Hình phạt nhẹ nhất là cảnh cáo
- Nặng nhất là sẽ ban nick vĩnh viễn
- Áp dụng cho tất cả mọi thành viên của Ebook Team
- Trường hợp không nghiêm trọng sẽ do Leader quyết định – Trường hợp đặc biệt nghiêm trọng sẽ lấy biểu quyết của cả Team

Mọi con người khi sinh ra đều có quyền bình đẳng. Trong đó có quyền học luật, tôn trọng luật và thi hành luật. Không gì có thể làm thay đổi được những quyền đó.

langtulangthang

-- Ebook làm mẫu --

Đây là những cuốn sách được đóng gói khá kỹ càng, bạn có thể xem để tham khảo và tùy biến.Giúp bạn định hình được một phần công việc đóng Ebook. Cố gắng làm sao để Ebook của bạn làm ra vừa tiện lợi, vừa có thẩm mỹ và giá trị nội dung (**Click** vào tên sách để **Save** vào máy của bạn).

Ebook về định dạng CHM:

- **Sống thiền** - Ebook này là dạng không có **Navigation Pane** - Sử dụng **Bookmark**

- **Kỹ nghệ đóng gói Ebook -** Là cái bạn đang đọc đó **Error!**

sử dụng **Navigation Pane**

Ebook về định dạng PDF:

- **Cánh đồng bất tận** - Ebook trình bày khá đẹp mắt, có ảnh minh họa

Ebook về định dạng HTML: Ebook này chỉ đưa ra để các bạn tham khảo mà thôi tôi chưa có thời gian viết TUT hơn nữa loại sách náy khá lỉnh kỉnh.

- **Ức Trai thi tập** - Xây dựng bằng Soft **Adobe Robo Help.** Ebook không đánh tiêu đề có dấu, chỉ sử dụng **Hyperlink** để làm mục lục.

Chúc các bạn thành công !!!

Error!

-- Thiết lập Tiếng Việt cho WinXP --

Anh em thân mến! Để có thể làm được tiêu đề tiếng Việt cho Ebook, anh em buộc phải bắt WinXP của chúng ta hỗ trợ cật lực cho tiếng Việt. Sau đây là bài hướng dẫn thiết lập. Anh em chú ý làm theo từng bước một nhé, nếu không khi viết tiêu đề tiếng Việt sẽ bị lỗi nhìn như tiếng Ả Rập ấy **Error!**

- Start menu\Settings\Control Panel\Regional & Language Options

+ **Tab Languages** => đánh dấu chọn **Install file for complex script => OK**

Lúc này nếu trong quá trình cài Win bạn không thiết lập môi trường tiếng Việt thì khi nhấn OK nó sẽ bắt bạn chèn đĩa WinXP vào.

Error!

+ **Tab Regional Options** => chọn **Vietnamese/Vieetnam** như hình dưới

Error!

+ Tab Advanced: chọn **Vietnamese**

Error!

+ **Tab Languages => Details**

Tab Settings: bổ sung "kiểu nhập" **Vietnamese** => **chọn làm mặc định** (như hình dưới)

Error!

Tab Advanced: Click chọn **extend support**

Error!

-- Các công cụ làm Ebook --

1, Unikey 4.0

- Bộ gõ tiếng Việt, dùng để soạn thảo và viết tiêu đề cho **Ebook**. **[Click Here]**

2, PocketCHM 5.9:

- Dùng để tạo Import các bài viết thành **Ebook .CHM**. **[Click Here]**

3, pdfFactory Pro 3.0:

- Dùng để Import các bài viết thành **Ebook .PDF [Click Here]**

4, Foxit Reader

- Dùng để đọc các **File PDF** không cần cài đặt **[Click Here]**

5, Smiles:

- Trang trí các bài **TUT** thêm sinh động [Click Here]

-- Tạo bài viết bằng FrontPage --

Ở đây tôi sẽ hướng dẫn các bạn sử dùng **FrontPage** một cách cơ bản nhất để viết các bài viết sau đó **Import** thành file **CHM**.
FrontPage thực ra giao diện soạn thảo cũng chẳng khác Word là mấy. Chúng ta chỉ cần chú ý một số thứ để đến lúc **Import** file CHM của chúng ta sẽ đẹp và không bị lỗi ảnh.
Sau đây tôi xin giới thiệu qua một số thủ thuật cho các anh em lần đầu làm quen với FrontPage

1. Chèn ảnh:

Muốn ảnh khi **Import** thành file CHM không bao giờ bị lỗi bạn không nên dùng cách copy-paste mà hãy: Chọn **Menu Insert -- Picture - From File**

Error!

Chọn ảnh muốn Insert rồi nhấn Ok là xong. Làm cách này bạn sẽ không bao giờ bị lỗi ảnh khi **Import** thành file CHM. Đây là kinh nghiệm sương máu đó.
Lưu ý: ảnh tốt nhất là nên để chung thư mục với file html bạn đang soạn thảo và định dạng **png** sẽ cho một bức ảnh tốt nhất

2. Chèn nền : (BackGround)

Để chèn ảnh nền cho bài viết của bạn, bạn Click phải chuột vào trang soạn thảo, chọn **Page Properties**, lúc đó bảng **Properties** sẽ hiện ra:

Error!

Bạn chuyển sang **Tab Formating** , click chọn **Background Picture** , nhấn vào **Browse** để chọn ảnh. Sau đó nhấn **OK** là được.

3. Chèn Java Script:

Bạn chẳng cần là một tay Design chuyên nghiệp vẫn có thể chèn Java vào để bài viết thêm sinh động tạo cảm quan cho người đọc
Lúc này, bạn nhấn vào **Tab Code** (Front Page 2000 là HTML) sau đó chèn đoạn Java vào sau khóa **Body**

Error!

Ví dụ ở đây là tôi chèn đoạn Code để chạy Window Media Player ....
Chèn Flash vào cũng tương tự như vậy. Theo tôi bạn đừng chèn những đoạn Java quá rối mắt sẽ làm mất cảm quan của quyển sách ...

4. Làm Book Mark

Bookmark giống như là ta viết mục lục cho một cuốn sách vậy. Nhấn vào đó là chuyển đến đoạn bài viết ta muốn đọc.
Để làm BookMark cũng không khó lắm.
Ở đây tôi sẽ làm Ví dụ cho bạn thấy: Tôi sẽ làm một nút khi bạn nhấn vào sẽ chuyển về phần 1 của bài viết này:
Đầu tiên bạn viết tiêu đề cho bookmark. **Về đầu** chẳng hạn. Bạn chuyển đến đoạn bạn muốn **BookMark** hướng tới (ở đây tôi chọn là **Chèn ảnh**) bôi đen nó bạn nhấn **Ctrl + G** (FP 2000 là vào **Edit - Bookmark**) bạn đánh tên cho **Bookmark** đó, sau đó nhấn **OK**.
Tiếp theo bạn bôi đen cái tiêu đề **Bookmark**, cái tôi vừa chọn là **Về đầu** đó. Nhấp phải chuột chọn **HyperLink** lúc này một bảng mới hiện ra:

Error!

Bạn nhấn vào nút Bookmark, chọn cái bookmark mà bạn vừa đặt đó (ở đây của tôi là **Chèn ảnh**). Nhấn OK là xong.
Bây giờ bạn thử nhấn vào đây xem thế nào nhé: **Về đầu**
Đối với file CHM dạng ko có menu Index, Contents thì làm Bookmark là việc bắt buộc
6. Xem thử:
Bạn nhấn vào **Preview** để xem thử rồi **Save** lại nhé ....
Chú ý: Khi Save bạn chọn Change Title - đánh **Title** bằng tiếng Việt có dấu, bộ gõ **Unikey** - bảng mã **Vietnamese Local CP 1258.** làm thế để sau này khi thiết lập rồi bạn khỏi phải đánh lại tiêu đề cho bài viết trong **PocketCHM.**

-- Hướng dẫn đóng gói file CHM --

1. Tại sao dùng CHM ?

+Tính phổ biến: Bất kỳ máy nào cài Windows đều chạy tốt CHM mà không cần cài thêm bất kỳ chương trình nào khác, hình như các hệ điều hành khác (Linux,MacOSX) cũng chạy được CHM. Do đó CHM phổ biến hơn rất nhiều các định dạng khác.
+Gọn nhẹ, dễ chia sẻ: Cùng 1 nội dung nhưng dạng CHM có dung lượng nhỏ hơn khá nhiều so với các định dạng khác, do vậy chia sẻ nhanh chóng hơn (ở VN đa số vẫn là thuê bao internet Dial Up)
+ Dễ làm, dễ tùy biến: Có thể làm ebook dạng CHM rất dễ dàng với PowerCHM hoặc VisualCHM, tùy biến dễ dàng.
+ Dễ sử dụng
Vì những đặc tính như trên mà trong đa số trường hợp bạn nên làm ebook dạng CHM
Để phóng to chữ trong ebook CHM bạn giữ phím Ctrl+ lăn phím cuộn (MouseWheel)

2. Một số nguyên tắc khi làm ebook dạng CHM

+ không nên có quá 25 chủ đề chính, quá nhiều chủ đề sẽ dẫn đến 1 số chủ đề không được xem >>giảm tính hiệu quả của ebook. Chủ đề từ 26 trở đi sẽ ít được để ý đến.
+ Kkông nên có quá 25 chủ đề con...
+ Một chủ đề (hoặc chủ đề con) không nên có quá 25 bài viết, nếu nhiều hơn 25 ta nên chia vào các chủ đề con như Phần 1, Phần 2 chẳng hạn.
+ Nên đánh số thự tự thống nhất cho tòan ebook, với số thứ tự <10 nên thêm một số 0 đằng trước: 01,02,...,09. Và nếu số chủ đề chính <10 cũng nên thêm một số 0 đằng trước để cho thống nhất, không lủng củng. Việc đánh số thứ tự giúp cho khi import vào CHM tất cả các chủ đề và bài viết sẽ xuất hiện đúng như số thứ tự của nó mà ta không cần phải làm thủ công. Việc đánh số cũng giúp bạn đọc dễ dàng theo dõi ebook, trao đổi về các bài viết,...

+ Các chủ đề con và bài viết không nên để lẫn lộn nhau trong 1 chủ đề chính, như thế cấu trúc của ebook sẽ rất lủng củng, ta phải xếp các bài viết vào các chủ đề con khác.

3. Hướng dẫn Import thành định dạng CHM bằng PocketCHM

Bạn chạy chương trình PocketCHM ở phiên bản 6.2 tên là FlyHelp. Giao diện chính của chương trình hiện ra:

Error!

Vùng 1: Chứa các nút sẽ hiện ra phía trên của **File CHM** bạn tạo ra, cái này là tùy vào cuốn Ebook bạn định xây dựng.
Vùng 2: Chứa các công cụ để bạn thiết lập khi I**mport** vào. Gồm các nút định dạng **Drag and Drop** (kéo và thả), 2 nút hình chữ A-Z đó là để sắp xếp theo thứ tự tăng hoặc giảm. 2 mũi tên cuối cùng là để Undo ...
Vùng 3: Là nơi đặt giao diện Menu Ebook khi làm ra. Nếu bạn Import vào **Contents** thì là dạng phân cấp dạng cha con. **Index** là không phân cấp.
Bên phải là các Menu điều khiển: **Import Folder, Import File**, **tạo Folder cha, tạo folder con, xóa, di chuyển bài viết, thay đổi Font cho Toc, thay đổi Icon, thay đổi màu nền Toc.**
Vùng 4: Các của sổ giao diện để kéo thả vào vùng 3, **Preview** để xem file vừa **Imporrt** ....
Vùng 5: Đây là thứ quyết định giao diện vùng **Contents**
Tiếp theo để **Import** bạn chọn vào **Import Folder** (hình folder có dấu cộng màu xanh), chọn đường dẫn đến Folder đó nhấn Ok để **Import** ra. Như thế bạn sẽ thấy đươc hình sau:

Error!

Nếu trong thư mục bạn có các file thừa thì cứ nhấn **Ctrl** bôi đen tất các những file thừa sau đó nhấn vào dấu X màu đỏ để xóa đi, chỉ để lại những bài viết và các thứ cần thiết mà thôi.
Bạn chọn các nút xuất hiệnsẽ xuất hiện trên file và các kiểu thể hiện cho phù hợp (ở vùng 2 và 5).
Chọn **Setting - HTML Help Properties**
- Mục **General** : Điền Title cho sách của bạn, chọn Default Topic (cái này mặc định Topic sẽ xuất hiện mỗi khi chạy file CHM)

Error!

Lưu ý nhất là phần **Language,** chỉ khi nào chúng ta thiết lập tiếng Việt hiển thị như hình trên thì mới viết được tiêu đề tiếng Việt cho Ebook.
- Các mục khác thì tùy bạn chỉnh sửa để có được một giao diện cảm quan nhất.
Nhấn OK để hoàn thiện việc chỉnh sửa.

Tiếp theo là việc gõ tiêu đề tiếng Việt. Bạn phải dùng **Unikey** với bảng mã **Vietnamese Local CP 1258** để gõ tiêu đề có dấu cho các bài viết (cần thiết lập chế độ tiếng Việt cho Windows XP).
Chú ý: Lúc gõ và lúc hiển thị không được đẹp lắm hoặc lộn xộn nhưng khi mở file CHM thì chữ tiếng Việt có dấu rất chuẩn.
Nếu như có rất nhiều tiêu đề thì ta chỉ cần copy tiêu đề từ danh sách chủ đề và bài viết vào từng tiêu đề của ebook là ngon lành ngay.
Sau khi gõ tiêu đề có dấu xong rồi hãy click menu **Tools >> Compile to CHM** để compile ra ebook.
Bây giờ thì ngồi hưởng thành quả lao động của mình !!!

-- Hướng dẫn tạo file PDF bằng pdfFactory Pro --

Hiện nay có khá nhiều chương trình có thể giúp chúng ta tạo nên các tài liệu này, đặc biệt là phần mềm của hăng Adobe như: Acrobat, Indesign,... Thế nhưng, nếu như bạn có một đống tài liệu thực hiện trên file của Microsoft Word và muốn chuyển sang thành tài liệu PDF cho dễ dàng chia sẻ? Thật vất vả nếu như bạn cứ phải lặp đi lặp lại công việc Copy và Paste. Hay là bạn muốn viết hoặc đóng một Ebook PDF nhưng chả biết gì về các thao tác phức tạp của các phần mềm nặng trình trịch của Adobe.

Tất cả sẽ được giải quyết với **pdfFactory,** nhanh chóng, tiện lợi, dễ dàng, môi trường soạn thảo là Word quá quen thuộc. Còn gì mà không không lựa chọn phải không nào.

Sau khi cài đặt pdfFactory, bạn hãy mở file Word vừa đánh xong muốn chuyển thành file PDF ra. Nhấn **Ctrl + P** hay là click vào biểu tượng máy in trên thanh công cụ. Cửa sổ in sẽ hiện ra:

Error!

Bạn chọn **Name** của máy in là **pdfFactory Pro** tiếp theo là bạn nhấn OK để tiến hành in, đợi một chút để chương trình tiến hành in, cửa sổ **pdfFactory** sẽ hiện ra

Error!

*** Các Tab ***

About: Bạn chú ý vào đây mà **Register** cho Soft

Preview: Xem trước tài liệu sau khi in ra.

Font: Bạn có thể chọn gửi kèm Font chữ của trọng tài liệu ở file PDF hay là không bằng cách nhấn vào nút **Embed al**l hay **Embed none**. Nếu như bạn muốn chia sẻ file PDF trên mạng th́ bạn nên bỏ qua chức năng này để cho file PDF nhỏ hơn.

DOC Info: Chứa các thông tin của tài liệu khi in ra như tên, tác giả, ...

Security: Bước này thực sự quan trọng nếu như bạn muốn đưa file lên mạng mà không muốn bị người khác lấy mất. Bạn đánh dấu tích vào mục "Use PDF Security" và thực hiện một số tùy chọn theo yêu cầu của ḿnh: bạn nên mã hóa ở 128-bit hay cao hơn để chắc rằng tài liệu của ḿnh khó bị lấy cắp mất. Bạn có thể không cho phép in, xem, sửa hay thiết đặt chế độ Master Password để sau này có thể thực hiện chỉnh sửa nếu muón.

Link: Bạn có thể thay đổi kiểu dáng thể hiện các liên kết cho các bài text có chứa các liên kết sao cho phù hợp với tài liệu tại phần này.

Bookmark: Bạn không nên đánh dấu vào phần này, bởi khi in ra dưới dạng tài liệu sẽ chứa thêm cả đường dẫn của file tài liệu ban đầu được in ra.

Setting: Một số thiết đặt khác cho tài liệu như thông báo cho bạn biết nếu tài liệu sớm hơn một giá trị bạn đặt ra, nơi save file in ra, ... Bạn chú ư phần PDF level bạn nên đặt giá trị cao nhất trong đó để tài liệu có thể đạt kích thước nhỏ nhất, và hăy đánh dấu vào **Allow** "**Master Password**"...." nếu cần sử dụng chức năng bảo mật này.

***** Các Button *****

View PDF: Xem thử dưới dạng file PDF tài liệu bạn đang làm

Save: Lưu thành file PDF và share cho mọi người

Send: Gửi cho người khác qua đường Mail

Vậy là bạn đã hoàn toàn nắm được cách thức tạo một file PDF rồi ... Hãy làm thử đi nào !!!

-- Viết Comment và tạo ảnh bìa Ebook --

Một câu hỏi đặt ra là tại sao chúng ta phải viết **Comment và design bìa Ebook** ?

Viết **Comment** cho cuốn Ebook của bạn chính là viết những lời giới thiệu, bình luận về cuốn Ebook. Có thể nói, một cuốn sách không có Comment là một cuốn sách không hoàn hảo. Bạn nên nhớ rằng, trên Net có thể có vài chục cuốn Ebook có nội dung giống như bạn đang làm, đang viết. Vậy khác biệt ở đâu?? Khác biệt chính là ở chỗ Ebook của bạn có một Comment đem lại những nội dung chính, một vài câu bình luận của cuốn Ebook.

Nó chính là sự khác biệt về khả năng tổng hợp và tư duy cảm nhận của từng người khi làm Ebook (đóng ko thì ai chả đóng được). Khi một người tiếp xúc với bất cứ cái gì mới, họ đều muốn nắm bắt tổng thể nó, tìm hiểu kỹ về nó trước khi đưa ra quyết định sau cùng. Người đọc Ebook cũng vậy, họ sẽ tìm hiểu xem mình sẽ được những gì khi đọc cuốn sách đó. Chắc bạn muốn Ebook mình viết ra có nhiều người đọc chứ ...**Comment** chính là giải pháp quảng bá tốt nhất hình ảnh cuốn sách của bạn.

Tạo bìa Ebook chính là chúng ta thể hiện cái thần của cuốn sách. Chỉ cần người đọc nhìn cái bìa họ có thể cảm nhận được ngay Ebook đó nói về vấn đề gì. Tất nhiên đây là lĩnh vực mỹ thuật đồ họa, tôi cũng ko đủ giỏi để bàn về vấn đề này. Cái này là do tư duy của từng người mà thôi. Nó cũng không đòi hỏi bạn phải quá giỏi về thứ này, một bức họa chau chuốt chưa chắc đã là một bức họa có thần. Chỉ cần chúng ta phác họa được phần nào vấn đề là được. Ví dụ:

Error!

Chính **Comment** và bìa **Ebook**, sẽ là thứ thể hiện được khả năng tư duy của bạn và tạo ra cái khác biệt với những Ebook cùng nội dung khác.

Tôi tin rằng các bạn sẽ làm được. Chúng ta hãy cùng cố gắng.

-- Hướng dẫn Upload lên Freewebtown.com ---

Freewebtown là trang cho đăng kí host miễn phí hiện nay (hình như cho 10Gb đó) và dễ đăng kí.

Tôi xin được viết 1 bài viết hướng dẫn cách đăng kí và upload files lên www.freewebtown.com

Bước 1: Đầu tiên bạn vào www.freewebtown.com

Error!

Chọn hình **John Us Now** ở bên góc trên phía trái

Nếu bạn đã có acc thì điền use và pass sau đó Login nhé

Bước 2: Khi bạn chọn **Join us Now** thì bảng này hiện ra

Chú ý: Các bạn chỉ cần điền thông tin vào những ô màu đỏ

Error!

Bạn điền tên tài khoản mà bạn cần lập vào ô " **Use Name** "

Điền pass và xác nhận lại pass vào 2 ô tiếp theo

Error!

Điền code mà site đó cung cấp vào ô **" Enter the code shown "**

Và nhớ đánh dấu vào ô của **" Terms of Services"** nhé

Sau đó ấn **Submit** để khởi tạo cho mình acc nhé

Bước 3: Đăng ngập với **use** vừa khởi tạo

Đây là giao diện khi bạn đăng nhập vào **freewebtown**

Error!

Bạn chọn vào " **File Manager** " ở bên tay trái nhé

Error!

Bạn chỉ cần để ý đến " **Single Uploader** " mà thôi bởi vì nếu bạn chọn " **Java Multi Image Uploader**" thì bạn cần phải cài **Java** vào mới **upload** được.

Error!

Bạn chọn **Browse** để lựa chọn file cần upload rồi chọn **Upload Files** để bắt đầu quá trình up file nhé

Bước 4: Đợi 1 thời gian để trình duyệt upload file cho bạn

Error!

Và file bạn up đã xong và hiện ra rồi

Bạn có thể click ngay vào file đó để biết link down về hoặc bạn có thế làm cách sau : Click chuột phải vào file và chọn **Propertites** để biết **link** của file đó

Error!

Lưu ý: Nếu sau khi up load file xong mà trình duyệt thông báo là **"Cannot open service"** thì bạn **Refesh** lại sẽ thấy file của bạn vừa up

Chúc các bạn may mắn và thành công !

-- Hướng dẫn upload tại MediaFire --

Bài viết này tôi sẽ hướng dẫn các bạn đăng kí vào up file lên host free là :http://www.mediafire.com/

Bước 1: Vào địa chỉ trang http://www.mediafire.com/ để đăng kí cho mình 1 acc free

Giao diện của site này hiện ra như sau:

Error!

Các bạn hãy click vào " **Create a Free Account** " để tạo cho mình 1 tài khoản nhé .Còn nếu có account rồi bạn hãy **click** vào **login** để đăng nhập nhé

Sau đó có bảng hiện ra các bạn hãy điền địa chỉ **email và pass** rồi click chọn **Create a Free Account**

Error!

Và rồi có thông báo như vậy nè,là các bạn có 1 acc free và bắt đầu uplaod file rồi đó

Error!

Bước 2: Trở về với giao diện để up file nhé

Error!

Bạn chọn vào " **Browse** " để lựa chọn file cần up .Nếu bạn muốn up nhiều file cùng 1 lúc thì chọn ở chỗ " **I want to upload ..file**" đó nhé

Error!

Lựa chọn file xong rồi Open để tiếp tục

Bước 3: Sau khi chọn xong thì các bạn đợi để nó up file cho bạn.Tùy thuộc vào dung lượng file mà thời gian chờ đợi của bạn nhanh hay chậm

Error!

Nó hiện ra thông báo như này là đã xong rồi đó

Error!

Bước 4: Nếu muốn chia sẽ link thì bạn copy link ở **Download link** để chia sẻ file hoặc bạn cũng có thể chọn ở " **Forum link code** " để chia sẻ link

Thế là xong rồi đó bạn ạ.Thật đơn giản phải không

Chúc các bạn thành công !

-- Upload dữ liệu lên box.net --

Bạn băn khoăn không biết phải chọn host nào để up file rồi chia sẽ cho bạn bè .
Bạn hãy đăng kí tài khoản free ở www.box.net (đăng ký rất dễ dàng không đòi hỏi nhiều) và bài TUT này hướng dẫn bạn up file nên host đó.
Đăng nhập với tài khoản của mình vừa đăng ký tại www.box.net

Error!

Login bình thường
Một cửa sổ mới hiện ra với các tab tác vụ, bạn Click vào Tab Upload ở phía trên

Error!

Nếu bạn muốn tạo folder để up + chia sẻ thì chọn vào **Create a new folder**
Còn nếu ko bạn hãy chọn vào **Upload new file**
Tôi xin hướng dẫn các bạn lập 1 folder mới .Click vào **Create a new folder**

Error!

Bạn đặt tên cho **folder** đó >Tôi đặt là **Ebook**
Sau đó **Click Ok** để chuyển sang bước tiếp theo
Bạn thấy **Folder Ebook** hiện ra rồi đúng ko .Bạn hãy **click** vào **Folder Ebook** nhé.

Error!

Sau đó click chọn **Upload new file** để bắt đầu **up file** nào

Error!

Hãy click vào **Add files** nhé rồi lựa chọn đường dẫn tới file cần up hoặc kéo thả file cần Up vào khung cửa sổ

Error!

Chọn tên file sau đó **Ok**
Bạn đã thấy file hiện nên ở cửa sổ **Files** rồi chứ (ở đây là file HN.chm mà tôi chọn)
Nếu muốn add thêm bạn lại chọn vào **Add files**
Còn ko muốn up thêm thì bạn chọn vào **Upload** nhé

Error!

Ngồi chờ 1 lúc để nó upload file nhé
Tùy dung lượng mà up nhanh hay chậm
Đó ! File đã đã up xong rồi kìa > bây giờ chỉ cần chia sẻ là xong
Bạn nhìn thất mũi tên xổ xuống ở khung của file ko
Hãy click vào đó và chọn **Get public link**

Copy link đó để gửi cho bạn bè là **Ok** rồi đó

Chúc các bạn thành công !

Sổ tay Xử lý sự cố

Phiên bản 1.0

Sau các e-Book: Sổ tay Tổng hợp, Sổ tay Pokemon, Sổ tay WarCraft, Software Handbook (Sổ tay phần mềm), eBook MultiMedia,... thì giờ đây, B00DF đã hoàn thành phiên bản đầu tiên của Sổ tay Xử lý sự cố và là eBook thứ 3 làm theo chuẩn B00DF_eBook_Black. E-Book này sưu tầm các bài viết được sưu tầm từ nhiều nguồn khác nhau, bàn về việc phòng bệnh và chữa bệnh cho máy tính, một số hiểu biết và thủ thuật dùng cho máy tính. Vì các bài viết được sưu tầm từ nhiều nguồn, một số bài được đăng trên báo, lại không tìm được link để download (chưa có điều kiện tìm) nên B00DF phải đánh lại bằng tay vì thế nên có thể còn nhiều thiếu sót, mong các bạn thông cảm và bổ sung. Hi vọng cuốn Sổ tay Xử lý sự cố này sẽ trở thành một cẩm nang hoàn hảo cho máy tính của bạn.

B00DF

boodf2@yahoo.com

Hướng dẫn sử dụng PocketCHM

Thực ra đã có rất nhiều bài hướng dẫn về việc sử dụng PocketCHM để làm eBook đầy đủ từ “mầm non” đến “chuyên nghiệp”

. Bài viết này của B00DF để cho vui thôi, với lại khả năng của B00DF Studio còn hạn chế (xếp vào loại gà

).

Để cụ thể hóa những công đoạn làm eBook với PocketCHM, chúng ta sẽ làm luôn một eBook (hoành tráng!

). Ở đây sẽ là eBook đóng gói phần cuối tập 59 và phần đầu tập 60 của truyện tranh Thám tử lừng danh Conan (hàng mới nhập!

)

Đầu tiên ta cần phải có tài liệu cần thiết (có rồi!), sắp xếp theo từng mục mà ta muốn làm trong eBook (biết rùi!

), ...hic hic, thôi chuyển qua giai đoạn thực hiện luôn!

Đây là mặt mũi thằng PocketCHM (chà trông sáng sủa dữ!

)

Trước hết ta tổng hợp tài liệu thành một định dạng thống nhất (HTML cũng được mà MHT cũng được, nhưng để MHT cho tài liệu, tranh ảnh chúng nó hợp nhất vào một nhà, dễ quản lý

). Sau đó, nhìn ở khung bên phải của PocketCHM ta thấy có ba thẻ đó là Resource Explorer (duyệt vị trí của các tài liệu), Preview (Xem trước mặt mũi chúng nó), TOC/Index Entry Properties (Tạo chỉ mục cho chúng nó). Phù! Giải lao tí đã nào!

Nào bây giờ chúng ta tiếp tục! Mở lại PocketCHM lên, chọn vào thư mục chứa tài liệu.

Trước tiên để tài liệu có "hộ khẩu" trong Sổ tay, ta phải "làm nhà" cho tài liệu

. Bạn chọn vào nút có hình cuốn sách và một dấu đỏ ở thanh công cụ dọc theo khung bên trái

hoặc có thể chọn Menu Edit \ New Book. Sau đó chỉ việc "đánh số nhà" cho căn hộ mới xây này (đặt tên đó

). Chẳng hạn như:

Các bạn thấy đó, hai mục "Tap 59" và "Tap 60" nằm bên trong mục "Noi dung". Để làm được như vậy các bạn dùng hệ thống các nút di chuyển

. Nút lên xuống dùng để thay đổi thứ tự sắp xếp của các mục còn nút sang phải để đưa một mục vào trong một mục nằm trên nó, nút sang trái để lôi nó ra

, đối với các tài liệu khi cho vào rồi cũng vậy.

Sau khi có nhà rồi, bạn tống lũ tài liệu kia vào nhà

. Đối với PocketCHM cũng như nhiều chương trình tạo file Compiled HTML Help (CHM) khác, thao tác này chỉ đơn giản là “kéo và thả” vào chỗ cần thiết, dễ như ăn bánh

. Đến đây bạn có thể vào Preview xen thử xem các tài liệu ổn chưa:

Hoặc bạn có thể nhập tài liệu bằng cách nhấn vào một trong hai nút trên cùng của thanh công cụ nằm dọc theo khung nội dung bên trái. Nút

cho ta nhập cả một thư mục tài liệu còn nút

cho phép nhập một hoặc nhiều tài liệu nào đó.

Ổn định hàng ngũ xong, bạn cần đổi tên cho các tài liệu này (tên file MHT lúc ban đầu chỉ nên đặt ngắn gọn thôi cho nó đỡ mọc cánh bay mất khỏi đầu

, đến khi vào eBook rồi mới đặt lại cho chính xác). Bạn có thể chọn vào page cần đổi tên và thực hiện một trong những cách sau:

- Menu Edit \ Rename
- Nhấn chuột phải \ Rename
- Nhấn F2

Xong rùi! Bây giờ bạn có thể xuất ra rồi, nhưng thực tế không ai xuất eBook ngay ra lúc này cả, con phải trang trí nữa chứ!

. Sau đây là giới thiệu sơ bộ về các tùy chọn:

- : Thằng này nằm ở thanh công cụ dọc theo khung bên trái (hic hic, có cái câu này mà nói lại mãi, gọi là thanh công cụ thôi cho nó gọn
-). Nhấn vào thằng này thì hiện ra :
  Đây là hộp thoại Select Icon cho ta thay đổi biểu tượng của các mục.
- : Hai thằng này nằm dưới cùng thanh công cụ đó. Thằng trên cho đổi màu font chữ của bảng nội dung còn thằng dưới đổi loại font, cỡ font,..

Bây giờ nhìn xuống dưới ta sẽ thấy thanh công cụ sau :

- Nút đầu tiên (Position) cho ta thay đổi vị trí các thẻ của bảng nội dung (Phía trên, phía dưới, dọc theo bên trái)

- Nút thứ hai (Float) Tạo ra một khung cửa sổ cho bảng nội dung giúp ta thoải mái kéo thằng này đi như thế này:
- Nút thứ ba (Border) hiện đường biên quanh bảng nội dung.
- Nút thứ tư (Rootline) hiện hoặc ẩn đường nối của những mục chính (những thằng nằm ngoài cùng đó
-).
- Nút thứ năm (PlusMinus) Hiện hoặc bỏ các dấu cộng - trừ ở bên trái các mục.
- Nút thứ sáu (Line) Hiện hoặc bỏ các đường nối giữa các mục (Nên để cái này để thây được sự phân cấp rõ ràng hơn, xem chúng nó có cùng cha cùng mẹ hay không
-)
- Nút thứ bảy (Select) Sorry hen! Cái này B00DF cũng thấy khó hiểu hén: Hiện sự lựa chọn ngay cả khi thẻ nội dung không được chọn.
- Nút thứ tám (Track) Tự động kéo các mục lựa chọn
- Nút cuối cùng (Expand) Nếu nút này được chọn thì khi ta đọc eBook, chọn chủ đề nào đó thì các chủ đề còn lại đều chui vào nhà đi ngủ
- , chỉ có chủ đề được chọn mới mở ra thôi.

  Bây giờ ngước mắt nhìn lên trên, chỗ ngay dưới thanh menu ấy
  , các bạn sẽ nhìn thấy thanh công cụ này:
  Nếu các bạn chọn nút nào trong thanh này thì nút đó sẽ hiện ra ở Toolbar trong eBook sau khi các bạn xuất eBook ra. Ngay dưới đó là:
  Bây giờ thử liệt kê tính năng mà thanh này đem lại.
  Các nút cơ bản:
  Các nút còn lại thì ... xem tiếp đây sẽ rõ
  :
- Settings : Chọn vào đây để mở bảng thiết lập các thuộc tính của file CHM sẽ tạo

  Nhãn General, thiết lập tên thằng eBook
  , tên file log ghi lỗi trong quá trình biên dịch, chủ đề mặc định sẽ nhìn thấy đầu tiên khi eBook được mở ra (Ngoài ra còn có thể nhấn chuột phải vào chủ đề đó, chọn Set as Default Topic
  ), ngôn ngữ của eBook.
  Nhãn Compiler, thiết lập các thuộc tính biên dịch của chương trình như tạo chỉ mục nhị phân,...

Nhãn Window Styles, thiết lập các thuộc tính của cửa sổ eBook gồm có: Ẩn – hiện các nút phóng to thu nhỏ, luôn đặt cửa sổ eBook lên trên các cửa sổ khác, canh tiêu đề eBook sang phải, không thay đổi kích thước cửa sổ eBook. Ngoài ra còn có thể chọn vị trí mặc định, có lưu lại vị trí của eBook hay không, phù... rắc rối...
Nhãn Tri Pane thiết lập thuộc tính của bảng nội dung và thanh công cụ của eBook. Về bảng nội dung, ta có thể cho hiện hoặc không hiện các thẻ (nên ẩn những thằng nào không cần thiết đi cho gọn
), chỉnh kích cỡ bảng hoặc ẩn luôn cả bảng nội dung. Về thanh công cụ thì chỉ có tùy chọn ẩn hay hiện chữ miêu tả chức năng của nút trên thanh công cụ và ẩn thanh công cụ đi.
Cuối cùng là nhãn Toolbar, thiết lập cụ thể hơn chức năng cho thanh công cụ. Chúng ta có thể chọn các nút cần thiết (Cái này dùng thiết lập luôn ở ngoài tiện hơn
, có nói ở phía trên rùi!), chọn trang chủ cho eBook (khi nhấn vào nút Home sẽ chạy đến trang này
). Phía dưới là tùy chọn hiển thị menu và 2 địa chỉ nhảy nhanh tới
.
Thế là xong “em” Settings. Bây giờ đến “em CHM Explorer
” và “ID Mapper
”. Khi chọn hai em này sẽ hiện thêm hai thẻ ở khung bên phải:
Hai thẻ này để xem file CHM, nhập file Header,... thôi mệt quá!
, cái này chắc cũng chẳng mấy khi đụng tới (chính xác thì B00DF chưa đụng tới lần nào!
) Thế nên ta tạm dừng lại ở đây. Ấy suýt quên, còn nút cuối
sẽ hiện lên cái bảng sau khi ta nhấn vào (lắm bảng thế...
) :
Thấy tiêu đề cái bảng chắc các bạn cũng hiểu (cái tên nói lên tất cả mừ
). Đây chắc là lọc file để nhập vào PocketCHM, cả thư mục nữa. Loại file mặc định là HTML (Thì vốn eBook là Compiled CHM Help mà!
).
Thế là xong hết phần giới thiệu sơ bộ (Hic, sơ bộ mà dài và chi tiết wé!
). Sau bao nhiêu công lao vất vả, giờ ta biên dịch..! Trước khi biên dịch ta có thể đặt lại tiêu đề một lần nữa cho eBook
, sau đó nhấn Compile và ... nhào vô

. (Nếu eBook nặng quá thì phải è cổ ra mà chờ!
)
He he! Xong rồi! Đây là kết quả thử nghiệm (đâu...đâu...?)
:

Thế là xong hết rùi đó! Cái bây giờ cần là:

- 1 ý tưởng
- Tài liệu cần thiết
- Sự kiên nhẫn (Quan trọng hén !
-)

Chào thân ái và quyết thắng !

B00DF

boodf2@yahoo.com

Ảnh hưởng của các lỗ hổng bảo mật trên internet

Tuy nhiên, có phải bất kỳ lỗ hổng bảo mật nào cùng nguy hiểm đến hệ thống hay không? Có rất nhiều thông báo liên quan đến lỗ hổng bảo mật trên mạng Internet, hầu hết trong số đó là các lỗ hổng loại C, và không đặc biệt nguy hiểm đối với hệ thống. Ví dụ, khi những lỗ hổng về sendmail được thông báo trên mạng, không phải ngay lập tức ảnh hưởng trên toàn bộ hệ thống. Khi những thông báo về lỗ hổng được khẳng định chắc chắn, các nhóm tin sẽ đưa ra một số phương pháp để khắc phục hệ thống.

Trên mạng Internet có một số nhóm tin thường thảo luận về các chủ đề liên quan đến các lỗ hổng bảo mật đó là:

- **CERT (Computer Emergency Reponse Team)**: Nhóm tin này hình thành sau khi có phương thức tấn công Worm xuất hiện trên mạng Internet. Nhóm tin này thường thông báo và đưa ra các trợ giúp liên quan đến các lỗ hổng bảo mật. Ngoài ra nhóm tin còn có những báo cáo thường niên để khuyến nghị người quản trị mạng về các vấn đề liên quan đến bảo mật hệ thống. Địa chỉ Web site của nhóm tin: http://www.cert.org

- **CIAC (Department of Energy Computer Incident Advisory Capability):** tổ chức này xây dựng một cơ sở dữ liệu liên quan đến bảo mật cho bộ năng lượng của

Mỹ. Thông tin của CIAC được đánh giá là một kho dữ liệu đầy đủ nhất về các vấn đề liên quan đến bảo mật hệ thống. Địa chỉ web site của CIAC : http://ciac.llnl.org

- **FIRST (The Forum of Incident Response and Security Teams):** Đây là một diễn đàn liên kết nhiều tổ chức xã hội và tư nhân, làm việc tình nguyện để giải quyết các vấn đề về an ninh của mạng Internet. Địa chỉ Web site của FIRST: http://www.first.org. Một số thành viên của FIRST gồm:

- **CIAC**

- **NASA Automated Systems Incident Response Capability.**

- **Purdue University Computer Emergency Response Team**

- **Stanford University Security Team**

- **IBM Emergency Response Team**

CÁC BIỆN PHÁP PHÁT HIỆN HỆ THỐNG BỊ TẤN CÔNG:

Không có một hệ thống nào có thể đảm bảo an toàn tuyệt đối; bản thân mỗi dịch vụ đều có những lỗ hổng bảo mật tiềm tàng. Đứng trên góc độ người quản trị hệ thống, ngoài việc tìm hiểu phát hiện những lỗ hổng bảo mật còn luôn phải thực hiện các biện pháp kiểm tra hệ thống xem có dấu hiệu tấn công hay không. Các biện pháp đó là:

- Kiểm tra các dấu hiệu hệ thống bị tấn công: hệ thống thường bị treo hoặc bị crash bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân về phần cứng hay không, nếu không phải phần cứng hãy nghĩ đến khả năng máy bị tấn công

- Kiểm tra các tài khoản người dùng mới trên hệ thống: một số tài khoản lạ, nhất là uid của tài khoản đó = 0

- Kiểm tra xuất hiện các tập tin lạ. Thường phát hiện thông qua cách đặt tên các tệp tin, mỗi người quản trị hệ thống nên có thói quen đặt tên tập tin theo một mẫu nhất định để dễ dàng phát hiện tập tin lạ. Dùng các lệnh ls -l để kiểm tra thuộc tính setuid và setgid đối với những tập tinh đáng chú ý (đặc biệt là các tập tin scripts).

- Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình login, sh hoặc các scripts khởi động trong /etc/init.d, /etc/rc.d ...

- Kiểm tra hiệu năng của hệ thống. Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống như ps hoặc top ...

- Kiểm tra hoạt động của các dịch vụ mà hệ thống cung cấp. Chúng ta đã biết rằng một trong các mục đích tấn công là làm cho tê liệt hệ thống (Hình thức tấn công DoS). Sử dụng các lệnh như ps, pstat, các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.

- Kiểm tra truy nhập hệ thống bằng các account thông thường, đề phòng trường hợp các account này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm sóat được.

- Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ như /etc/inetd.conf; bỏ các dịch vụ không cần thiết; đối với những dịch vụ không cần thiết chạy dưới quyền root thì không chạy bằng các quyền yếu hơn.

- Kiểm tra các phiên bản của sendmail, /bin/mail, ftp; tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng của dịch vụ sử dụng

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

&ksvthdang(HCE)

Làm sao để cải thiện kết nối mạng không dây Wifi

Kết nối mạng không dây Wifi (Wireless Fidelity) đã trở thành một trong những cách thức truy cập Internet và chia sẻ dữ liệu thông dụng nhất hiện nay. Đối với nhiều công ty, thậm chí nó còn đóng vai trò sống còn trong phương thức kinh doanh của họ. Với người dùng gia đình, nó giải quyết vấn đề chia sẻ kết nối băng thông rộng với chi phí hợp lý nhất. Hiện tại wifi được chia làm 3 chuẩn chính thông dụng bao gồm:

- 802.11a: Đây là chuẩn 54Mbps hoạt động ở tần số 5Ghz. Nó sử dụng thiết bị

riêng rất đắt tiền. Một số món đồ chơi mạng trên thị trường hiện nay được đóng dấu tương thích chuẩn này nhưng thực tế chỉ có khả năng kết nối hòa mạng chứ không phát huy được những đặc điểm thế mạnh riêng.
- 802.11b: Chuẩn B với số lượng người dùng đông đảo nhất hiện nay do khả năng tương thích rộng và giá thành thấp. Tần số hoạt động ở mức 2.4Ghz và băng thống 11Mbps.
- 802.11g: Đây là phiên bản mới nhất của dòng 802.11x hiện nay, so với chuẩn B, khoảng cách sử dụng của G không bằng nhưng lại có băng thông lớn hơn nhiều do có khả năng áp dụng công nghệ đa kênh (đạt mức 108Mbps hoặc hơn tùy thiết bị). Các linh kiện mạng không dây chuẩn G thế hệ mới đều tương thích ngược với chuẩn B.
Khoảng cách sử dụng của các thiết bị Wifi hiện tại có thể lên tới 150m trong điều kiện lý tưởng nhưng trong thực tế chỉ dưới 50m mà thôi. Những yếu tố có thể gây ảnh hưởng đối với khoảng cách phát sóng có rất nhiều ví dụ như tường, từ trường, vật liệu kim loại, anten … Bài viết này sẽ đưa ra một vài chi tiết giúp bạn cải thiện kết nối không dây của mình.
A. Chọn lựa và sắp xếp thiết bị hợp lý:
1. Sử dụng một Routermới: Dĩ nhiên đây là cách thức đơn giản nhất để nâng cấp chất lượng sóng không dây. Bạn nên làm điều này nếu như thiết bị đang sử dụng đã có tuổi thọ trên 2 năm. Trong những trường hợp như vậy, thiết bị mới đôi khi tăng cường diện tích sử dụng lên gần gấp đôi.
- Ưu điểm:
+ Việc thay đổi khá dễ dàng, đa số các thiết bị mới đều hỗ trợ Wizard dạng HTML cho phép người dùng thiết lập thông số rất nhanh chóng để tương thích với mạng hiện hành.
+ Giá cả thiết bị mới không đắt so với hiệu năng chúng mang lại.
+ Một số thiết bị có những công nghệ cao cấp ví dụ như NetGear WPN824 với RangeMax có thể tự động gia tăng diện tích phủ sóng hoàn toàn tự động.
- Nhược điểm:
+ Đôi khi bạn phải nâng cấp toàn bộ các thiết bị thành phần trong mạng như Adapter, Accesspoint, Router… để tận dụng được những công nghệ mới.
+ Không phù hợp cho môi trường với nhiều vật cản ví dụ như các tòa nhà cao tầng.
2. Sử dụng thêm một Router nữa với chức năng Access Point:
Với giải pháp này, bạn sẽ tắt chức năng Router của thiết bị và chỉ sử dụng tính năng phát sóng không dây của nó. Mô hình trong hình dưới đây là một ví dụ.
- Ưu điểm:
+ Chi phí thấp, bạn có thể sử dụng bất cứ Router nào còn dư hoặc mua một chiếc mới rẻ tiền để sử dụng.
- Nhược điểm:
+ Các nhà sản xuất không chính thức hỗ trợ cho kiểu hình mạng này.

+ Những thiết bị Router không được thiết kế phục vụ cho chức năng này nên đôi khi hiệu năng làm việc có thể không tối ưu.
+ Chỉ thích hợp cho những mạng đơn giản, tải nhẹ. Không phù hợp với máy chủ game hay cơ sở dữ liệu lớn.
+ Khá rắc rối để cài đặt. Người dùng phải có kiến thức cơ bản về mạng.
3. Kết hợp sử dụng cáp:
Bạn có thể chạy dây cáp LAN thông thường để vượt qua những đoạn môi trường ngắn nhưng bất lợi cho sóng wifi ví dụ như các bức tường dày hay từ tầng này qua tầng khác của một tòa nhà.
- Ưu điểm:
+ Chi phí rất thấp.
+ Hiệu quả cho những môi trường nhạy cảm sóng vì tín hiệu mạng chỉ truyền đi trong dây điện, không phát ra bên ngoài.
+ Tính bảo mật tốt cho người dùng.
+ Dây mạng nếu được đặt sẵn trong tường sẽ không ảnh hưởng nhiều đến mỹ quan nội thất.
+ Làm việc tốt với những điểm mù mà tín hiệu Wifi không đến được.
- Nhược điểm:
+ Phụ thuộc vào chất lượng dây và tín hiệu điện rất dễ bị nhiễu.
4. Thêm Access Point:
Thêm một Access Point là cách hiệu quả nhất để cải tiến mạng không dây của bạn. Nó tốt hơn so với việc sử dụng Router thay thế ở bước 2.
- Ưu điểm:
+ Có thể phủ sóng diện tích cách xa Router chính mà không cần phải tiếp tín hiệu ở khoảng giữa.
+ Hiệu năng cao, tính năng bảo mật tốt.
- Nhược điểm:
+ Thiết lập khá rắc rối.
+ Sử dụng AccessPoint với vai trò của thiết bị nối tiếp tín hiệu sẽ không đảm bảo được vấn đề hiệu năng tối đa.
5. Thay thế Anten:
Đây là giải pháp đơn giản nhất và đôi khi lại hiệu quả nhất. Những loại Anten cao cấp có thể cải thiện chất lượng tín hiệu rất nhiều. Một số loại đặc biệt có thể tăng cường phủ sóng tới vài KM. Tất nhiên những giải pháp gia đình hoặc văn phòng không cần thiết phải mạnh như vậy nhưng vẫn đủ sức đảm đương diện tích cả tòa nhà.
- Ưu điểm:
+ Anten sử dụng tốt cho những khoảng diện tích rộng lớn nối tiếp nhau.
+ Hiệu quả cho cả môi trường trong nhà lẫn ngoài trời.
+ Giải pháp tối ưu cho mạng giữa nhiều tòa nhà gần nhau.

- Nhược điểm:
+ Hầu hết các loại Anten chỉ sử dụng được với những thiết bị thiết kế riêng cho nó.
+ Để lắp đặt Anten hiệu quả, bạn phải nghiên cứu kĩ môi trường và đôi khi phải nhờ cậy tới các chuyên gia.
+ Khi mưa hoặc có sét, tín hiệu có thể bị ngắt hoặc tốc độ chậm đi. Nếu kết nối mang tính sống còn, bạn nên chuẩn bị các giải pháp phòng bị.
B. Đặt thiết bị ở vị trí tốt nhất:
Khi tiến hành đặt thiết bị phát sóng không dây cũng như các thành phần liên quan, bạn phải luôn chú ý ba điểm sau:
+ Đặt Anten ở vị trí tốt với góc phù hợp.
+ Tránh các vật cản vật lý có thể chặn sóng.
+ Tránh xa các thiết bị gây nhiễu khác.
Nếu mạng nội bộ của bạn có nhiều thiết bị không dây, trước khi bạn di chuyển bất cứ thứ gì hãy xác định thứ nào sẽ chịu tải nhiều nhất. Điều này rất quan trọng đối với việc tối ưu hóa. Hầu hết các nhà sản xuất đều có những công nghệ riêng để tăng cường khoảng cách phủ sóng của thiết bị nhưng trên thực tế những thiết bị nằm càng xa điểm phát sóng sẽ có tốc độ kết nối càng chậm đi. Chính vì thế hãy đặt những chiếc router, accesspoint hay bất kì thiết bị nào chịu tải lớn ở vị trí gần trung tâm mạng nhất.
1. Chọn vị trí cho Anten:
Router Wifi, AccessPoint, Adapter Wifi gửi và nhận tín hiệu thông qua anten, có những sản phẩm (chủ yếu phục vụ môi trường di động) sử dụng anten ngầm. Tuy nhiên đại đa số các thiết bị Wifi đều có anten ngoài. Do đó vị trí Anten đóng vai trò quyết định đối với hiệu năng làm việc của một thiết bị wifi. Khi thiết lập vị trí Anten, bạn phải tuân theo những nguyên tắc sau đây:
+ Hạn chế tối thiểu những vật cản giữa các anten của thiết bị wifi. Từ anten này hãy cố gắng tìm vị trí để bạn có thể nhìn thấy các anten thiết bị khác khác là lý tưởng nhất.
+ Đặt ở vị trí cao hơn hẳn các vật cản.
+ Đặt cách xa các bề mặt kim loại như ống nước, tủ… tối thiểu 60cm.
+ Tránh xa các khối nước lớn như bể cá, tủ lạnh hay bộ tản nhiệt nước.
+ Anten thường có điểm mù ở dưới chân nó, chính vì thế bạn không nên đặt nó ngay trên các thiết bị nhận tín hiệu.
+ Nếu bạn sử dụng các thiết bị wifi từ cả tầng trên dưới lẫn xung quanh, hãy chỉnh anten thành góc 45 độ so với phương ngang.

Một số Router Wifi có nhiều anten để tăng cường sóng ví dụ như dòng RangeMAx của Netgear với 3 anten. Trong trường hợp này, bạn hãy đặt anten chính vuông góc 90 độ với mặt đất, mỗi anten bên nằm ở góc 45 độ và 135 độ tương ứng. Với những tòa nhà hẹp, anten có thể đặt ở vị trí nằm ngang 180 độ. Nhớ chú ý không để các đầu anten quá gần nhau.

2. Chống nhiễu:
Vật liệu - Khả năng chặn sóng
Tường khô ráo, gỗ dán <20%
Thủy tinh, cửa trong nhà 30-60%
Gốm sứ, bê tông, gạch 90-95%
Khối lượng nước/kim loại lớn. 100%
- Không đặt gần cửa sổ nếu bạn không có nhu cầu liên lạc với tòa nhà bên cạnh. Cửa số là đường vào cho rất nhiều các loại sóng không cần thiết từ bên ngoài.
- Đặt cách xa anten của thiết bị khỏi các nguồn phát sóng khác đặc biệt là những thiết bị sử dụng tần số từ 2.4Ghz tới 2.5Ghz. Những nguồn nhiễu thông thường bao gồm:
+ Máy vi tính và máy fax.
+ Máy photocopy, điện thoại di động.
+ Lò vi sóng.
C. Tối ưu hóa thiết bị:
Một trong những thông số ít được chú ý liên quan trực tiếp đến hiệu năng làm việc của các thiết bị wifi chính là số kênh tần. Mục đích chính của bạn là tìm ra được kênh tín hiệu tốt nhất để tránh các sóng gây nhiễu từ mạng khác hoặc các thiết bị có tính chất phát sóng radio. (Với thiết bị chuẩn 802.11a hay a/g thì việc chọn kênh không chiếm vai trò quan trọng).
Nếu bạn chỉ sử dụng mạng gia đình đơn giản và hàng xóm không có ai sử dụng Wifi, bạn có thể sử dụng bất cứ kênh nào cũng được. Tuy nhiên những rắc rối sẽ xảy ra khi bạn rơi vào một trong những trường hợp sau đây:
+ Bạn muốn tăng cường khả năng phủ sóng của mạng.
+ Bạn có nhiều Router hoặc AccessPoint phát sóng không dây buộc phải dùng nhiều kênh tần khác nhau.
+ Bạn không phải là người duy nhất trong khu vực sử dụng mạng Wifi.
Việc tăng cường tín hiệu mạng không dây hoàn toàn khác với việc bạn cho thêm bóng đèn vào một căn phòng để làm nó sáng lên. Những thiết bị phát sóng mạnh như Router, AccessPoint sẽ trực tiếp gây ảnh hưởng lẫn nhau trong khoảng cách gần. Bạn cần phải đặt chúng xa nhau và đặc biệt là thiết lập để mỗi mạng lưới sử dụng một kênh tần khác biệt.
Đối với mạng thuộc chuẩn 802.11b/g, có tất cả 11 kênh cho những thiết bị không dây. Những thiết bị sản xuất cho thị trường Châu Âu sẽ hỗ trợ 13 kênh. Khi xảy ra tranh chấp tín hiệu khiến cho mạng bị chập chờn, bạn có thể chọn một trong các kênh chính không bị chồng chéo tin hiệu lên nhau là 1,6,11 (1,7,13 cho Châu Âu) hoặc số kênh càng cách xa nhau càng tốt. Như vậy bạn sẽ có thể sử dụng tới 3 mạng không dây độc lập trong cùng một không gian diện tích.
Nếu như ở gần bạn có một mạng không dây nào đó, chẳng có gì ngạc nhiên nếu nó đã sử dụng kênh 1 và 11 vì đó là thiết lập mặc định của phần lớn các thiết bị phát

sóng Wifi. Tuy nhiên thật đáng buồn là bạn không thể tránh được việc bị xung đột tín hiệu một cách triệt để vì giao thức không giây B/G chỉ có 3 kênh chính không chồng chéo như đã nói ở trên. Chính vì thế nếu trong cùng một khu vực có từ 4 mạng không dây khác nhau trở lên, vấn đề "va chạm" sẽ trở nên càng trầm trọng hơn. Đặc biệt khi bạn và người hàng xóm của mình mỗi người đều vừa có một Router và một Accesspoint Wifi thì chắc chắn cả hai sẽ phải chịu những tác động không tốt đẹp gì. Giải pháp tối ưu nhất cho vấn đề này đó là bạn hãy chủ động bàn bạc với chủ nhân của mạng "hàng xóm" để cùng tìm ra những tùy chọn thích hợp nhất ví dụ như kênh tần 1 và 8 cho bạn, 5 và 11 cho người kia. Bạn cũng có thể đặt Router và Access Point của mình về phía xa để giảm thiểu những tín hiệu mà hàng xóm của bạn không muốn "nhìn thấy". Ngoài ra, anten phát sóng có hướng cũng là một trong những giải pháp bạn có thể xem xét.
Khi có nhiễu, tốc độ mạng sẽ bị giảm đi đáng kể chính vì vậy, đôi khi nếu việc giảm nhiễu không thực sự hiệu quả, bạn có thể giảm tải cho mạng không dây và hạn chế khối lượng dữ liệu được phát đi. Trong những môi trường có nhiều thiết bị với khả năng sinh sóng radio, bạn nên sử dụng dây cáp mạng cho những kết nối truyền tải nhiều thông tin nhất. Ngoài ra bạn cũng có thể xem xét phương án nối mạng thông qua đường dây điện bằng một số thiết bị chuyên dụng ví dụ như dòng Powerline của Netgear. Việc bật tùy chọn SSID Broadcast cũng là một trong những yếu tố tăng tải. Mặc dù nó giúp cho các thiết bị nhanh chóng nhận ra luồng tín hiệu mạnh nhất nhưng điều đó cũng đồng nghĩa cho phép những thiết bị không mong muốn ở gần khu vực bạn kết nối ké hoặc tự động "xin phép" kết nối vài lần trong một giây dù được hay không được phép. Chính vì thế nếu bạn chỉ có nhu cầu sử dụng cá nhân, hãy tắt SSID Broadcast và đổi tên SSID mặc định thành giá trị khác.
Cuối cùng, hai tính năng bảo mật WEP và WPA mặc dù giữ cho thông tin trong mạng không bị mất trộm nhưng thực tế đôi khi chúng cũng góp phần "rùa bò" cho tốc độ mạng không dây. Tắt chúng đi sẽ tăng băng thông cho mạng nhưng cũng để lộ sơ hở cho những tay hacker. Bạn không nên làm điều này trừ khi có những biện pháp an ninh riêng hoặc lý do đặc biệt nào đó.
D. Kiểm tra hiệu quả thiết bị:
Bạn có thể tiến hành kiểm tra sơ lược hoặc kĩ càng tùy ý, tuy nhiên rõ ràng sau khi thực hiện bất cứ thay đổi nào, bạn sẽ muốn kiểm tra xem hiệu năng có khác biệt gì hay không. Hãy chú ý rằng khi thử nghiệm, bạn nên tạo ra một môi trường giống với thực tế ví dụ như bật lò vi sóng, nhờ ai đó nói chuyện điện thoại di động… trong khu vực phủ sóng wifi.
Sau đây là một vài phương thức thử nghiệm thông dụng:
1. Thử xem nó có làm việc không:
Đây là cách rẻ tiền và nhanh chóng nhất. Tất cả những gì bạn cần làm chỉ là bật thiết bị lên, xem xem nó có hoạt động không và hiệu năng có vừa ý bạn hay không

mà thôi. Nếu có, bạn chẳng cần làm gì thêm cả.
2. Kiểm tra sức sóng bằng công cụ phần mềm:
Mỗi thiết bị wifi đều được cài đặt kèm một tiện ích phần mềm theo dõi độ mạnh của tín hiệu và luồng dữ liệu. Thường thì chúng là một thanh ngang với các màu xanh, vàng, đỏ. Khi mức trạng thái ở màu xanh chứng tỏ thiết bị đang nhận được luồng tín hiệu rất mạnh và băng thông tốt, khi bạn di chuyển xa khỏi Router hay Access Point, tín hiệu sẽ dần giảm xuống và chỉ còn mức vàng. Khi tín hiệu mạng yếu đi, băng thông sẽ tự động giảm xuống nhưng kết nối vẫn được duy trì. Khi mức trạng thái chỉ còn ở vạch đỏ, bạn sẽ bắt đầu gặp trục trặc như rớt mạng, tín hiệu không ổn định, dữ liệu truyền chập chờn.
Bạn có thể nhận rõ hiệu quả mạng wifi của mình theo cách này thông qua việc đi loanh quanh trong khu vực phát sóng với một thiết bị wifi di động trong tay như điện thoại, pocketPC hay laptop.
3. Kiểm tra khoảng cách giữa hai nguồn phát:
Hai Router hoặc AccessPoint có cùng kênh tần khi đặt càng gần nhau sẽ càng dễ bị nhiễu. Bạn hãy sử dụng một món đồ chơi wifi di động và thiết lập kết nối với một trong hai thiết bị phát rồi di chuyển trong khoảng 2m tính từ anten. Kích hoạt chế độ dò để tìm các luồng tín hiệu mạng. Nếu bạn nhìn thấy thiết bị khác xuất hiện chung kênh tần, bạn hãy thực hiện 1 trong 3 cách sau:
+ Di chuyển một trong hai thiết bị phát ra xa.
+ Tắt một trong hai thứ.
+ Thay đổi kênh tần của Router hoặc AccessPoint.
4. Kiểm tra tính ổn định dữ liệu:
Thanh trạng thái cho phép bạn đo khối lượng dữ liệu truyền qua mạng không dây nhưng nó không thể báo cáo với bạn có bao nhiêu dữ liệu bị thất lạc trong quá trình vận chuyển và bị buộc phải gửi lại. Khi những gói dữ liệu nhỏ thường xuyên bị mất (ví dụ trong môi trường nhiễu) thì tốc độ mạng sẽ chậm, đôi khi hỏng hóc các file và độ trễ sẽ tăng lên cao. Thông thường tỉ lệ dữ liệu bị đi lạc trong một mạng nội bổ chỉ được phép nằm trong khoảng 1% đến 2% mà thôi. Để kiểm tra thông số này (Packet Loss), bạn làm như sau:
+ Từ màn hình Desktop của Windows, bạn mở Start > Run > nhập vào “cmd” (không có dấu ngoặc kép) rồi nhấn Enter. Cửa sổ dòng lệnh Command sẽ xuất hiện.
+ Bạn gõ vào “ping x.x.x.x –t” trong đó x.x.x.x là địa chỉ IP của Router, AccessPoint hoặc một thiết bị thành viên mạng mà bạn muốn kiểm tra (Ví dụ: ping 192.168.1.133 –t”). Nhấn Enter.
+ Sau thao tác này, máy tính sẽ gửi liên tục tín hiệu kiểm tra tới thiết bị mỗi giây. Khi có gói dữ liệu đi lạc, dòng thông báo “Request Time Out” sẽ hiện ra.
+ Khi cần dừng phép thử lại, bạn nhấn Ctrl+C và đóng cửa sổ Command.

5. Xem xét băng thông:
Đây là một bước khá quan trọng để xác định hiệu quả mạng không dây vì mục đích cuối cùng của bạn vẫn là gửi nhận dữ liệu. Bạn có thể sử dụng nhiều công cụ để thực hiện công việc này ví dụ như module Network/Lan Bandwidth trong bộ tiện ích Sandra của Sisoftware.
Nhìn chung với sức phát triển mạnh mẽ như hiện nay của mạng không dây, việc một ngày nào đó mọi đoạn dây lằng nhằng biến mất khỏi văn phòng cũng như căn nhà của bạn không có gì đáng ngạc nhiên. Những nhược điểm cố hữu của Wifi như tốc độ chậm hay độ trễ cao đã và đang được giải quyết khá triệt để. Nhiều công nghệ mới ra đời điển hình như MIMO của Airgo Network đã nâng tốc độ kết nối vượt mức 200Mbps và trong tương lai sẽ còn cao hơn nữa. Giá thành của các thiết bị mạng không dây hiện nay đã giảm xuống mức chấp nhận được. Chỉ chưa tới 100 USD, bạn đã sở hữu một router Wifi loại tốt với đầy đủ các tính năng mới nhất cho công việc của mình. Hãy mạnh dạn đến với công nghệ mới và cảm nhận sự khác biệt.

Một cách phòng chống DoS !

Để chống DOS có rất nhiều cách, lúc trước Server bạn Vũ cũng bị DOS . Vũ có viết 1 ứng dụng nhỏ bằng C++\Linux . Và thấy khá hiệu quả, các bạn có thể sử dụng.
NOTE: Cách này chỉ dùng được khi bạn sở hữu server riêng, và webserver phải là apache .

1. Phân tích nguyên lý làm việc của Aapche trong việc lưu log file :
+ Mọi user khi vào 1 website, apache sẽ ghi lần access đó vào file access_log trong folder apache\log . Chý ý là nếu website của bạn có nhiều Image thì mỗi Image cũng được tạo 1 access trên apache. Đều này có nghĩ là nếu site của bạn bao gồm 1 trang html và 3 image thì trên access_log sẽ có 4 record.
+ Bình thường, 1 IP chỉ có thể access tối đa 100 lượt/giây. Trường hợp này đặt giã định Web bạn có ít hơn 20 image, các file CSS . . . ., con số 100 này chỉ là tương đối.
+ Nếu trong 1 giây, 1 website bi truy cập đến cở 1000 lượt/s thì xem như bị DOS.
2. Cách làm việc của chương trình.
+ Bạn viết 1 ứng dụng, định kỳ 5 phút sẽ đọc file log 1 lần.
+ Giả sữ trung bình, 1 giây trên toàn server có 10000 lượt truy cập (tất cả các site trên server). vả kích thước file access_log mỗi giây tăng 100KB. Vậy 5 phút sẽ là 600KB.
+ Nếu sau năm phút, số MB tăng đột biến,cở 1MB , thì xem như server đang bị DOS. Khi đó bạn cho phân tích cú pháp trong file log. Nếu thấy 1 domain (vysa.jp) bị gọi nhiều lần trong 1 giây (1000 lần) . thì tiến hành LOCK IP đó lại, kg cho apache trả lời request IP đó, bằng cách DENY Ip đó trên .htaccess . Chú ý khi phân

tích file LOG, hãy tắt Apache đi, sau khi song thi open nó lên lại .

Dĩ nhiên các số liệu Vũ đưa ra chỉ là tương đối, bạn có thể tùy biến cho phù hợp với yêu cầu của server mà bạn dùng bạn .
Quangvu (ddth.com)

Cách diệt virus Vlove đang hoành hành

Cộng đồng Internet Việt Nam đang chứng kiến một cơn "hồng thủy" mới từ virus nội có tên Vlove, lây lan lan qua dịch vụ tin nhắn nhanh Yahoo Messenger phổ biến nhất hiện nay. Virus gửi IM cho toàn bộ danh sách friends mà chủ nhân hoàn toàn không biết về việc này.

Tin nhắn (message) phát tán virus có nội dung đa dạng:

http://fun.nguoiiu.com/y/local1.hta Tang ban tam thiep ne`...,
http://fun.nguoiiu.com/funny/ Vui qua ne
http://fun.nguoiiu.com/funny/ Vao day nhe... Chuc vui ve!

Khi nhận được message này người dùng tuyệt đối không click vào link, hãy bỏ qua
Trong trường hợp đã nhiễm bị nhiễm virus này, bạn thực hiện các bước sau:

1. Download các công cụ cần thiết:

- Tải phần mềm Hijackthis để quản lý các chương trình khởi động cùng Windows.

- Load phần mềm Killbox để delete các file mà windows không cho phép.
2. Chạy Hijackthis:

Click vào Do a system scan and save a logfile (hình 1)

Những vùng có được khoanh đỏ (hình 2) là các key do virus tạo ra bạn hãy check vào tất cả các key đó sau đó chọn fix checked để gỡ bỏ chúng. (hình 3).

Các bạn tìm và click chọn vào các key sau:

R1 – HKCU\Software\Microsoft\Internet Exlplorer\Main,Default_Page_URL = http://fun.nguoiiu.com/life/

R1 - HKCU\Software\Microsoft\Internet Exlplorer\Main,SearchPage= http://fun.nguoiiu.com/life/

R0 - HKCU\Software\Microsoft\Internet Exlplorer\Main,Start Page = http://fun.nguoiiu.com/life/

R1 - HKCU\Software\Microsoft\Internet Exlplorer\Main,First Home Page = http://fun.nguoiiu.com/life/

R1 - HKCU\Software\Microsoft\Internet Exlplorer\Main,Window Title = Power by MTVC

O4 – HKCU\..\Run: (System32) C: Windows\System32.exe

O4 - HKCU\..\RunOnce: (Windows) C: (Windows\System32\victory.jse

O11 – Options Group: (International) International*

3. Xóa file bằng Killbox:

Bạn cần delete các file sau:

C:\WINDOWS\system32.exe (hình 4)

C:\WINDOWS\system32\victory.jse

Kent(HCE)

Bảo mật cho các máy tính của một tổ chức

(Security Article Series -Bài viết hướng dẫn cách thức để bảo vệ cho các Computer của một tổ chức. Thích hợp cho những ai quan tâm đến Network Security.)

Một trong những yếu tố quan tâm hàng đầu trong việc Thiết kế Security một hệ thống thông tin đó là kiểm soát chặt chẽ tất cả Computer của tổ chức. Vì chúng là nơi cất giữ tài sản thông tin có giá trị của tổ chức. Attacker có thể trực tiếp tấn công thẳng vào Computer và lấy đi những dữ liệu quý báu.

Việc xác định những mối đe dọa và những lỗ hỗng ở tất cả computer trong tổ chức là điều thiết yếu và cấp bách (Quan tâm đến Security cho Computer kể từ lúc mua, cho đến khi cất chúng vào kho - life Cycle)

Hầu hết các loại Computer nếu không có những kẽ hở thiếu an toàn về vật lý, thì bản thân hệ điều hành cũng có thể phơi bày những tử huyệt, những miếng mồi ngon cho attacker. Security Admin phải đảm bảo an toàn và cập nhật đầy đủ các miếng vá lỗi và thiết lập hệ thống phòng thủ trong suốt quá trình "sống" của Computer.

Xác định những rủi ro và những mối đe dọa Computer.

Bảo mật suốt chu kì "sống" của một computer:

Vòng đời của một computer trải qua những giai đoạn sau:

• Tiến hành cài đặt: Trong suốt quá trình tiến hành cài đặt Hệ điều hành và Ứng dụng, sự xâm nhập của Virus, và những lỗi cấu hình có thể là nguy cơ trực tiếp cho Computer. Chú ý setup password cho tài khỏan built-in ADMINISTRATOR tại

giai đoạn này theo đúng chính sách đặt password của tổ chức. Chúng ta có thói quen không tốt ở giai đoạn này là set password null (không đặt pssword) !

• Xác lập chính sách bảo mật chuẩn (baseline security) theo quy định an toàn thông tin của tổ chức sau khi hoàn thành cài đặt mỗi Computer

• Bảo mật cho các Computer có vai trò đặc biệt. ví dụ Web server , Database Server. Căn cứ trên chính sách bảo mật chuẩn, các security admin cần tăng cường hơn nữa các xác lập bảo mật đối với các Computer đặc biệt này nhằm tạo một hệ thống được bảo vệ tối đa có thể đương đầu với các kiểu tấn công đa dạng và phức tạp từ phía attackers.

• Cập nhật security cho tất cả ứng dụng phát sinh lỗi trên Computer (thông thường sẽ update các Service packs, securiry updates..) Đây là điều bắt buộc để nâng cao hơn nữa baseline security đã được thiết lập

• Tạm biệt Computer: Kết thúc vòng đời, giờ là lúc đem chiếc Computer này vào kho làm kỉ niệm hoặc giải phong một nó cho một ai đó cũng cần phải security, attacker có thể lấy những thông tin còn sót lại trên HDD, hoặc các thiết bị Media khác để khai thác những thông tin còn sót lại này.

Tầm quan trọng của việc bảo mật cho Computer

Những cuộc tấn công từ bên ngoài:

Khi một admin cài đặt software trên một computer mới, một Virus có thể lây nhiễm vào Computer trước khi Admin này cài service pack bảo vệ hệ thống. Virus này sẽ khai thác lỗ hổng đã xác định, và cài tiếp vào hệ thống một chú Trojan Horse (ví dụ như Bo 2k). Admin hoàn thành việc cài software và đưa vào sử dụng mà không hề biết rằng Computer có thể đã nằm trong tầm kiểm soát của một attacker ngoài hệ thống Mạng của tổ chức !

Hiểm họa từ bên trong:

Admin chọn cách cài đặt cho các Computer của tổ chức là cài đặt từ xa và không cần phải theo dõi trong suốt quá trình cài đặt (unattended Installation) , cách cài đặt này nhanh chóng và tỏ ra rất "professional". Trong suốt quá trình cài đặt operating system qua Mạng này, tài khỏan Local administrator của các máy được cài đặt được chuyển qua Mạng dưới dạng Clear-text (không mã hóa). Một nhân viên có chút trình độ về hệ thống và Network, thúc đẩy bởi những động cơ bất hợp pháp có thể cài các công cụ nghe lén và thâu tóm thông tin chuyển đi trên Mạng, đặc biệt là các Local Administrator Password (nếu admin Mạng đang tiến hành cài đặt qua Mạng cho Computer của sếp và password chuyển qua Mạng dưới dạng cleart-text thì nguy to…vì dữ liệu của các Manager rất important và hầu hết có giá trị economic..). Đây là một trong rất, rất nhiều những nguy cơ attack từ bên trong Mạng nội bộ.

Những mối đe dọa phổ biến:

Mặc dù những kĩ thuật bảo mật được trang bị trên các Computer, thế nhưng rủi ro lại đến từ yếu tố con người và những kẽ hở trong quy trình làm việc với Computer.

Ví dụ như attacker có thể lấy thông tin từ Đĩa cứng, hoặc truy cập vào máy tính qua các ứng dụng (không cài đặt các bản vá lỗi), mà nhân viên sử dụng, đặc biệt là những ứng dung connecting với Internet như Chat, Internet Browser, E-mail…

Thiết kế Security cho các Computer

Những phương thức chung secure Computer

Tiến hành cài đặt an toàn ngay từ ban đầu cho Hệ điều hành và các Ứng dụng theo

hướng dẫn:

Thực thi các cấu hình bảo mật mặc định cho HDH và ứng dụng
Chỉ cài đặt những ứng dụng và dịch vụ cần thiết trên các Server (ví dụ: nkhông cài lung tung các ứng dụng và triển khai những dich vụ không cần thiết trên Mail, Web server của tổ chức..)
Xác lập bảo vệ cho tất cả các tài khỏan mặc định của hệ thống (ví dụ: tài khoản mặc định Administrator nên được rename vì tên này ai cũng biết, và set password phức hợp, sẽ có tác dụng lớn để đối phó với attacker trong những cuộc tấn công dạng Brute force password)
Những file cài đặt cho HDH và application phải an toàn, phải được xác nhận (digitally sign) từ nhà cung cấp, có thể dùng nhiều utility để kiểm tra vấn đề này , ví dụ Sign verification…
Tiến hành cài đặt phải là những Người có đủ độ tin cậy trong tổ chức.
Nên cô lập Mạng trong quá trình cài đặt . Tạo một Network riêng dành cho việc cài đặt nếu phải cài đặt HDH, ứng dụng qua Mạng (ví dụ dùng dịch vụ RIS của Microsoft..), điều này là thiết yếu và tăng sự an toàn, có thể chống được sự lây nhiễm Virus từ bên ngoài hoặc các Built-in account như Administrator được tạo ra qua Mạng từ các unattended installation scripts không bị thâu tóm.. các CD cài đặt HDH, ứng dụng nên tích hợp đầy đủ các Service packs, security updates (vá lỗi ngay trong quá trình cài đặt)

Làm thế nào để cấu hình các xác lập chuẩn bảo mật cho một tổ chức (Security baseline)

Trước khi triển khai Computer cho tổ chức, cần xác định các security baseline. Các security admin có thể triển khai những security baseline này trong suốt quá trình cài đặt hoặc sau đó. Trên Microsoft Windows 2000 và Microsoft Windows XP, các admin có thể taọ và triển khai các security templates để đạt được những yêu cầu bảo mật cần thiết.

Tuân thủ những hướng dẫn sau để tạo security baseline cho các Computer

Tạo một chính sách security baseline cho các Computer theo đúng những quy định của tổ chức về an toàn thông tin phục vụ cho các quy trình nghiệp vụ. Chính sách này phải đảm bảo an toàn cho Computer, HDH và các ứng dụng nghiệp vụ…

Ví dụ: chính sách chỉ định rằng tất cả HDH trong tổ chức phải chống được kiểu tấn công SYN-ACK (synchronize acknowledge) denial of service (DoS) tấn công từ chối dịch vụ. Một chính sách tốt cũng hình dung được vai trò của Computer cần bảo vệ..

2. Tạo sẵn các security templates mẫu, cho phép chỉnh sửa. Ví dụ để bảo vệ HDH chống lại SYN-ACK attacks, có thể đơn giản thêm vào Registry những giá trị mong muốn nhằm thay đổi cách thức vận hành của TCP/IP stack trong giao tiếp Mạng với các Computer khác, như vậy có thể chống được những cuộc tấn công kiểu này.

3. vận hành thử và Kiểm tra các security templates này. Mỗi security template được triển khai sẽ không có các yếu tố gây cản trở HDH, các dich vụ khác, hoặc

xung đột với các ứng dụng

4. Triển khai các security templates cho Computer thông qua những công cụ như command Secedit Group Policy, hoặc tự động hóa triển khai cho hàng loạt Computer thông qua các Group Policy của Active Directory Domain (GPO)

Security cho các Computer có vai trò đặc biệt như thế nào.

Admin sẽ cài đặt những Ứng dụng và những dịch vụ phụ thuộc vào vai trò của những Computer đó.

Như vậy những Computer đặc biệt này cần có những Security baseline tương đối khác nhau để phù hợp với dịch vụ đang vận hành.

Ví dụ: Web server chạy dịch vụ Internet Information Services (IIS) cho phép hàng ngàn truy cập mỗi ngày từ Internet với những mối nguy hiểm luôn rình rập. Ngược lại thì một File server sẽ không chạy dịch vụ IIS và chỉ có thể truy cập bởi những user trong mạng nội bộ . Thiết kế bảo mật cho các Computer có vai trò đặc biệt đòi hỏi có kinh nghiệm và am hiểu chi tiết về những ứng dụng và dịch vụ mà chúng đang vận hành. Ví dụ một Windows 2000 administrator có thể không có những kiến thức để hiểu được cách hoạt động của một database server như Microsoft SQL Server 2000, cho dù nó được cài đặ trên một Windows 2000.

Phải đảm bảo những cá nhân chịu trách nhiệm thiết kế bảo mật cho những Server này có những hiểu biết cần thiết và kinh nghiệm đáp ứng được các yêu cầu bảo mật cua tổ chức. Và cũng đảm bảo rằng tổ chức chúng ta có những chính sách sẵn sàng, quản lý bảo mật cho các server ày khi chúng thay đổi vai trò hoạt động. ví dụ File Server được triển khai lại thành một Web server.

Những Phương pháp chung để áp dụng Security Updates (cập nhật security)

Có thể dùng những phương pháp sau để tiến hành cập nhật security cho các Computer trên Mạng.

Dùng tính năng Windows Update: Để scan Computer, đảm bảo rằng tất cả security updates mới nhất, các thành phần liên quan đến Windows (Windows components) , và các driver cho thiết bị đã được cài đặt. Để sử dụng Windows Update phải là

thành viên của nhóm Administrators. Nếu phải scan nhiều máy trên Mạng từ một location, có thể sử dụng tool: MBSA (Microsoft Baseline Security Analyzer) của hãng Shavlik, một partner của Microsoft. Hoặc chuyên dụng hơn và cung cấp giải pháp scan bảo mật toàn diện có thể dùng GFI Languard network security scanner của GFI, rất phổ biến với Admin.
Office Update: Scan và cập nhật những secuirty mới nhất cho bộ sản phẩm Microsoft Office. Vá lỗi cho các sản phẩm này cũng là một việc rất quan trong mà các Security admin cần chú ý. Chỉ thành viên nhóm Administrators mới được dùng tính năng này
Dùng Group Policy: Nếu triển khai security updates cho hàng loạt các Computer trong môi trường Active directory domain, các admin sẽ sử dụng các chính sách của Domain hoặc GPO cho các OU trong Domain. Khi dùng Group Policy, User không cần phải làm bất cứ động tác nào vì thông qua Active Directory service, Group Policy có thể thực hiện hoàn toan 2 tự động
Dùng dịch vụ Microsoft Windows Software Update Services (WSUS/SUS): Server cài đặt dịch vụ này, được xem là trung tâm phân phối các security updateas cho các Computer trên Mạng. Admin có thể cấu hình trên các Computer để tự động download security updates hoặc lập lịch biểu (scheduling) download từ WSUS server này
Dùng tính năng Feature Pack (Microsoft Systems Management Server (SMS) Update Services Feature Pack) có trong dịch vu SMS: Bao gồm Wizard hướng dẫn đóng gói các Security updates và triển khai chúng đến các Computer thông qua kho lưu trữ Software Inventory.
New Horizons VietNam (New Horizons Computer Learning centers Viet Nam)
Ho Viet Ha
Instructor Team Leader
Email: hvha@newhorizons.com.vn

(Security Article Series -Bài viết hướng dẫn cách thức để bảo vệ cho các Computer của một tổ chức. Thích hợp cho những ai quan tâm đến Network Security.)

Một trong những yếu tố quan tâm hàng đầu trong việc Thiết kế Security một hệ thống thông tin đó là kiểm soát chặt chẽ tất cả Computer của tổ chức. Vì chúng là nơi cất giữ tài sản thông tin có giá trị của tổ chức. Attacker có thể trực tiếp tấn công thẳng vào Computer và lấy đi những dữ liệu quý báu.

Việc xác định những mối đe dọa và những lỗ hỗng ở tất cả computer trong tổ chức là điều thiết yếu và cấp bách (Quan tâm đến Security cho Computer kể từ lúc mua, cho đến khi cất chúng vào kho - life Cycle)

Hầu hết các loại Computer nếu không có những kẽ hở thiếu an toàn về vật lý, thì bản thân hệ điều hành cũng có thể phơi bày những tử huyệt, những miếng mồi ngon cho attacker. Security Admin phải đảm bảo an toàn và cập nhật đầy đủ các miếng vá lỗi và thiết lập hệ thống phòng thủ trong suốt quá trình "sống" của Computer.

Xác định những rủi ro và những mối đe dọa Computer.

Bảo mật suốt chu kì "sống" của một computer:

Vòng đời của một computer trải qua những giai đoạn sau:

• Tiến hành cài đặt: Trong suốt quá trình tiến hành cài đặt Hệ điều hành và Ứng dụng, sự xâm nhập của Virus, và những lỗi cấu hình có thể là nguy cơ trực tiếp cho Computer. Chú ý setup password cho tài khỏan built-in ADMINISTRATOR tại giai đoạn này theo đúng chính sách đặt password của tổ chức. Chúng ta có thói quen không tốt ở giai đoạn này là set password null (không đặt pssword) !

• Xác lập chính sách bảo mật chuẩn (baseline security) theo quy định an toàn thông tin của tổ chức sau khi hoàn thành cài đặt mỗi Computer

• Bảo mật cho các Computer có vai trò đặc biệt. ví dụ Web server , Database Server. Căn cứ trên chính sách bảo mật chuẩn, các security admin cần tăng cường hơn nữa các xác lập bảo mật đối với các Computer đặc biệt này nhằm tạo một hệ

thống được bảo vệ tối đa có thể đương đầu với các kiểu tấn công đa dạng và phức tạp từ phía attackers.

• Cập nhật security cho tất cả ứng dụng phát sinh lỗi trên Computer (thông thường sẽ update các Service packs, securiry updates..) Đây là điều bắt buộc để nâng cao hơn nữa baseline security đã được thiết lập

• Tạm biệt Computer: Kết thúc vòng đời, giờ là lúc đem chiếc Computer này vào kho làm kỉ niệm hoặc giải phong một nó cho một ai đó cũng cần phải security, attacker có thể lấy những thông tin còn sót lại trên HDD, hoặc các thiết bị Media khác để khai thác những thông tin còn sót lại này.

Tầm quan trọng của việc bảo mật cho Computer

Những cuộc tấn công từ bên ngoài:

Khi một admin cài đặt software trên một computer mới, một Virus có thể lây nhiễm vào Computer trước khi Admin này cài service pack bảo vệ hệ thống. Virus này sẽ khai thác lỗ hổng đã xác định, và cài tiếp vào hệ thống một chú Trojan Horse (ví dụ như Bo 2k). Admin hoàn thành việc cài software và đưa vào sử dụng mà không hề biết rằng Computer có thể đã nằm trong tầm kiểm soát của một attacker ngoài hệ thống Mạng của tổ chức !

Hiểm họa từ bên trong:

Admin chọn cách cài đặt cho các Computer của tổ chức là cài đặt từ xa và không cần phải theo dõi trong suốt quá trình cài đặt (unattended Installation) , cách cài đặt này nhanh chóng và tỏ ra rất "professional". Trong suốt quá trình cài đặt operating system qua Mạng này, tài khỏan Local administrator của các máy được cài đặt được chuyển qua Mạng dưới dạng Clear-text (không mã hóa). Một nhân viên có chút trình độ về hệ thống và Network, thúc đẩy bởi những động cơ bất hợp pháp có thể cài các công cụ nghe lén và thâu tóm thông tin chuyển đi trên Mạng, đặc biệt là các Local Administrator Password (nếu admin Mạng đang tiến hành cài đặt qua

Mạng cho Computer của sếp và password chuyển qua Mạng dưới dạng cleart-text thì nguy to…vì dữ liệu của các Manager rất important và hầu hết có giá trị economic..). Đây là một trong rất, rất nhiều những nguy cơ attack từ bên trong Mạng nội bộ.

Những mối đe dọa phổ biến:

Mặc dù những kĩ thuật bảo mật được trang bị trên các Computer, thế nhưng rủi ro lại đến từ yếu tố con người và những kẽ hở trong quy trình làm việc với Computer.

Ví dụ như attacker có thể lấy thông tin từ Đĩa cứng, hoặc truy cập vào máy tính qua các ứng dụng (không cài đặt các bản vá lỗi), mà nhân viên sử dụng, đặc biệt là những ứng dung connecting với Internet như Chat, Internet Browser, E-mail…

Thiết kế Security cho các Computer

Những phương thức chung secure Computer

Tiến hành cài đặt an toàn ngay từ ban đầu cho Hệ điều hành và các Ứng dụng theo hướng dẫn:

Thực thi các cấu hình bảo mật mặc định cho HDH và ứng dụng
Chỉ cài đặt những ứng dụng và dịch vụ cần thiết trên các Server (ví dụ: nkhông cài lung tung các ứng dụng và triển khai những dich vụ không cần thiết trên Mail, Web server của tổ chức..)
Xác lập bảo vệ cho tất cả các tài khỏan mặc định của hệ thống (ví dụ: tài khoản mặc định Administrator nên được rename vì tên này ai cũng biết, và set password phức hợp, sẽ có tác dụng lớn để đối phó với attacker trong những cuộc tấn công dạng Brute force password)
Những file cài đặt cho HDH và application phải an toàn, phải được xác nhận

(digitally sign) từ nhà cung cấp, có thể dùng nhiều utility để kiểm tra vấn đề này , ví dụ Sign verification…
Tiến hành cài đặt phải là những Người có đủ độ tin cậy trong tổ chức.
Nên cô lập Mạng trong quá trình cài đặt . Tạo một Network riêng dành cho việc cài đặt nếu phải cài đặt HDH, ứng dụng qua Mạng (ví dụ dùng dịch vụ RIS của Microsoft..), điều này là thiết yếu và tăng sự an toàn, có thể chống được sự lây nhiễm Virus từ bên ngoài hoặc các Built-in account như Administrator được tạo ra qua Mạng từ các unattended installation scripts không bị thâu tóm.. các CD cài đặt HDH, ứng dụng nên tích hợp đầy đủ các Service packs, security updates (vá lỗi ngay trong quá trình cài đặt)

Làm thế nào để cấu hình các xác lập chuẩn bảo mật cho một tổ chức (Security baseline)

Trước khi triển khai Computer cho tổ chức, cần xác định các security baseline. Các security admin có thể triển khai những security baseline này trong suốt quá trình

cài đặt hoặc sau đó. Trên Microsoft Windows 2000 và Microsoft Windows XP, các admin có thể tạo và triển khai các security templates để đạt được những yêu cầu bảo mật cần thiết.

Tuân thủ những hướng dẫn sau để tạo security baseline cho các Computer

Tạo một chính sách security baseline cho các Computer theo đúng những quy định của tổ chức về an toàn thông tin phục vụ cho các quy trình nghiệp vụ. Chính sách này phải đảm bảo an toàn cho Computer, HDH và các ứng dụng nghiệp vụ…

Ví dụ: chính sách chỉ định rằng tất cả HDH trong tổ chức phải chống được kiểu tấn công SYN-ACK (synchronize acknowledge) denial of service (DoS) tấn công từ chối dịch vụ. Một chính sách tốt cũng hình dung được vai trò của Computer cần bảo vệ..

2. Tạo sẵn các security templates mẫu, cho phép chỉnh sửa. Ví dụ để bảo vệ HDH chống lại SYN-ACK attacks, có thể đơn giản thêm vào Registry những giá trị mong muốn nhằm thay đổi cách thức vận hành của TCP/IP stack trong giao tiếp Mạng với các Computer khác, như vậy có thể chống được những cuộc tấn công kiểu này.

3. vận hành thử và Kiểm tra các security templates này. Mỗi security template được triển khai sẽ không có các yếu tố gây cản trở HDH, các dich vụ khác, hoặc xung đột với các ứng dụng

4. Triển khai các security templates cho Computer thông qua những công cụ như command Secedit Group Policy, hoặc tự động hóa triển khai cho hàng loạt Computer thông qua các Group Policy của Active Directory Domain (GPO)

Security cho các Computer có vai trò đặc biệt như thế nào.

Admin sẽ cài đặt những Ứng dụng và những dịch vụ phụ thuộc vào vai trò của những Computer đó.

Như vậy những Computer đặc biệt này cần có những Security baseline tương đối khác nhau để phù hợp với dịch vụ đang vận hành.

Ví dụ: Web server chạy dịch vụ Internet Information Services (IIS) cho phép hàng ngàn truy cập mỗi ngày từ Internet với những mối nguy hiểm luôn rình rập. Ngược lại thì một File server sẽ không chạy dịch vụ IIS và chỉ có thể truy cập bởi những user trong mạng nội bộ . Thiết kế bảo mật cho các Computer có vai trò đặc biệt đòi hỏi có kinh nghiệm và am hiểu chi tiết về những ứng dụng và dịch vụ mà chúng đang vận hành. Ví dụ một Windows 2000 administrator có thể không có những kiến thức để hiểu được cách hoạt động của một database server như Microsoft SQL Server 2000, cho dù nó được cài đặ trên một Windows 2000.

Phải đảm bảo những cá nhân chịu trách nhiệm thiết kế bảo mật cho những Server này có những hiểu biết cần thiết và kinh nghiệm đáp ứng được các yêu cầu bảo mật cua tổ chức. Và cũng đảm bảo rằng tổ chức chúng ta có những chính sách sẵn sàng, quản lý bảo mật cho các server ày khi chúng thay đổi vai trò hoạt động. ví dụ File Server được triển khai lại thành một Web server.

Những Phương pháp chung để áp dụng Security Updates (cập nhật security)

Có thể dùng những phương pháp sau để tiến hành cập nhật security cho các Computer trên Mạng.

Dùng tính năng Windows Update: Để scan Computer, đảm bảo rằng tất cả security updates mới nhất, các thành phần liên quan đến Windows (Windows components) , và các driver cho thiết bị đã được cài đặt. Để sử dụng Windows Update phải là thành viên của nhóm Administrators. Nếu phải scan nhiều máy trên Mạng từ một location, có thể sử dụng tool: MBSA (Microsoft Baseline Security Analyzer) của hãng Shavlik, một partner của Microsoft. Hoặc chuyên dụng hơn và cung cấp giải

pháp scan bảo mật toàn diện có thể dùng GFI Languard network security scanner của GFI, rất phổ biến với Admin.
Office Update: Scan và cập nhật những secuirty mới nhất cho bộ sản phẩm Microsoft Office. Vá lỗi cho các sản phẩm này cũng là một việc rất quan trong mà các Security admin cần chú ý. Chỉ thành viên nhóm Administrators mới được dùng tính năng này
Dùng Group Policy: Nếu triển khai security updates cho hàng loạt các Computer trong môi trường Active directory domain, các admin sẽ sử dụng các chính sách của Domain hoặc GPO cho các OU trong Domain. Khi dùng Group Policy, User không cần phải làm bất cứ động tác nào vì thông qua Active Directory service, Group Policy có thể thực hiện hoàn toan 2 tự động
Dùng dịch vụ Microsoft Windows Software Update Services (WSUS/SUS): Server cài đặt dịch vụ này, được xem là trung tâm phân phối các security updateas cho các Computer trên Mạng. Admin có thể cấu hình trên các Computer để tự động download security updates hoặc lập lịch biểu (scheduling) download từ WSUS server này
Dùng tính năng Feature Pack (Microsoft Systems Management Server (SMS) Update Services Feature Pack) có trong dịch vu SMS: Bao gồm Wizard hướng dẫn đóng gói các Security updates và triển khai chúng đến các Computer thông qua kho lưu trữ Software Inventory.
New Horizons VietNam (New Horizons Computer Learning centers Viet Nam)
Ho Viet Ha
Instructor Team Leader
Email: hvha@newhorizons.com.vn

Chính sách an toàn Account cho Computer (Security Account Policies)

Ở phần trước tôi đã giới thiệu những phương thức chung để bảo vệ máy tính của một tổ chức. Phần tiếp theo này tôi sẽ trình bày những phương thức cụ thể theo trình tự, từ quá trình setup hệ thống, vận hành hệ thống dựa trên những chính sách an toàn từ basic cho đến những kĩ năng advance mà các Security Admin cần quan tâm để áp dụng vào việc xây dựng các quy trình an toàn thông tin cho tổ chức. Phần trình bày này tôi xin đề cập đến vấn đề an ninh account (account security) và cách thức tạo account an toàn nhằm đối phó với những kiểu tấn công rất phổ biến

và hiệu quả dưới sự trợ giúp của những công cụ phù thủy…

Chính sách về account và cách thức tạo account nghèo nàn là con đường dễ dàng nhất cho attacker, như vậy những hình thức bảo mật khác được áp dụng vào hệ thống như trang bị các công cụ chống maleware (prevent virus, worm, spyware, ad-ware..), triển khai hệ thống phòng thủ Mạng (Firewall) cũng sẽ không có tác dụng nào đáng kể, vì Admin quá thờ ơ trong cách thức tạo account và đưa ra chính sách tạo account chứa đựng nhiều rủi ro này.

Yêu cầu xác định các chính sách tạo password mạnh và đưa ra được chiến lược an toàn account áp dụng vào an toàn thông tin của tổ chức là vấn đề mang tính cấp bách.

A. Làm thế nào để tạo và quản lý Account an toàn

Những yếu tố dưới đây sẽ cho chúng ta thấy cách thức tạo và quản lý Account sao cho an toàn

Account phải được bảo vệ bằng password phức hợp (password length, password complexity)
Chủ sở hữu account chỉ được cung cấp quyền hạn truy cập thông tin và dịch vụ cần thiết (không thiếu quyền hạn mà cũng không thể để thừa)
Mã hóa account trong giao dịch trên Mạng (kể cả giao dịch trong Mạng nội bộ)
Lưu trữ account an toàn (nhất định database lưu giữ tai khoản phải được đặt trên những hệ thống an toàn và được mã hóa)
Huấn luyện nhân viên, những người trực tiếp sử dụng Computer cách thức bảo mật account tránh rò rĩ (attacker có thể lợi dụng mối quan hệ với nhân viên hoặc giả danh bộ phận kĩ thuật hỗ trợ xử lí sự cố hệ thống từ xa để khai thác), hướng dẫn cách thức thay đổi password khi cần thiết và tránh tuyệt đối việc ghi lại account trên các stick-notes rồi gián bừa bãi trên Monitorhoặc Keyboard..), Khóa (lock) ngay Computer khi không sử dụng, mặc định trên các máy tính thường cũng có chính sách tự động lock computer sau môt thời gian không sử dụng, để giúp cho những nhân viên hay quên tránh được lỗi bảo mật sơ đẳng (lỗi này giống như việc ra khỏi nhà mà không khóa cửa)

Những người tạo và quản lý account (đặc biệt là những account hệ thống – System accounts, và account vận hành, kiểm soát các dịch vụ - service accounts) cho toàn bộ tổ chức là những người được xem là AN TOÀN TUYỆT ĐỐI.
Disable những account tạm thời chưa sử dụng, delete những account không còn sử dụng.
Tránh việc dùng chung Password cho nhiều account
Khóa (lock) account sau một số lần người sử dụng log-on không thành công vào hệ thống.
Có thể không cho phép một số account quản trị hệ thống và dịch vụ, không được log-on từ xa (remote location log-on), vì những hệ thống và dịch vụ này rất quan trọng và thông thường chỉ cho phép được kiểm soát từ bên trong (internal Network), nếu có nhu cầu quản trị và support từ xa Security Admin vẫn dễ dàng thay đổi chính sách để đáp ứng nhu cầu.
Các Security admin khi log-on vào Server chỉ nên dùng account có quyền hạn thấp, khi cần quản trị hay vận hành các dịch vụ, mới nên dùng account System hoặc Service (ví dụ Microsoft Windows hỗ trợ command run as thông qua run as service để cho phép độc lập quản trị các thành phần của hệ thống, các dịch vụ mà không cần phải log-on vào máy ban đầu bằng account admin). Điều này giúp chúng ta tránh được các chương trình nguy hiểm đã lọt vào máy tính chạy với quyền admin, khi đó các admin thật sự của Computer sẽ gặp nhiều rắc rối.
Vá tất cả những lỗ hỗng hệ thống để ngăn chặn các kiểu tấn công "đặc quyền leo thang" (bắt đầu lọt vào hệ thống với account thông thường và sau đó leo thang đến quyền cao nhất)
Trên đây là những phần trực quan nhất mà Admin Security cần hình dung cụ thể khi thiết kế chính sách bảo mật account (account security policies). Một trong những chính sách bảo vệ hệ thống cần phải xem xet kĩ lưỡng nhất nhưng thông thường dễ lơ là thậm chí là coi nhẹ, mà sự thực hầu hết các con đường xâm nhập vào hệ thống đều qua khai thác Credentials (có được thông tin account), attacker nắm được vulnerabilities (yếu điểm) này, nên lợi dụng khai thác rất hiệu quả.

B. Phân tích và thiết kế các chính sách an toàn cho account.

<u>Phân tích những rủi ro và xác định các mối đe dọa đối với account:</u>
Account cho một User sẽ xác định những hành động mà User đó có thể thực hiện.
Việc phân loại account sẽ chỉ ra những cấp độ bảo vệ thích hợp khác nhau.
Các account trên hệ thống sẽ nhận được 2 loại quyền cơ bản:

User rights (Quyền hệ thống): Là loại đặc quyền mà User được hệ thống cho phép thực thi những hành động đặc biệt (ví dụ: Quyền Backup Files Và Folders, thay đổi thời gian hệ thống, shutdown hệ thống…)

Trên Windows các bạn có thể type command secpol.msc tại RUN, để open Local Security Settings\ local policies\ User rights assignment là nơi xác lập các User rights của hệ thống
Permissions (Quyền truy cập): Được kiểm soát bởi DACLs (Discretionary access control lists) của hệ thống, được phép truy cập vào các File/Folder hay Active Directory objects (trong Domain) (ví dụ User A được quyền Read/Modify đối với Folder C:\Data, User B được Full Control đối với OU Business..)
Chú ý trong việc cấp phát Permission cho account, nên đưa account vào Group để dễ kiểm soát, tránh việc phân quyền mang tính cá nhân cho một account nào đó. Điều này tăng cường khả năng kiểm soát account, vì khi số lượng account của hệ thống (Local hay Domain) tăng lên thì việc tổ chức này tạo sự an toàn và dễ kiểm soát hơn.
Những kẽ hở từ Account có thể tạo cơ hội cho attacker:

Password:
Password quá yếu (độ dài password quá ngắn, các kí tự đơn giản, lấy ngày tháng năm sinh, tên những bộ phim, địa danh, nhân vật nổi tiếng , đặt cho password).
Dùng cùng password cho nhiều account. password được dán bừa bãi lên Monitor/Keyboard, hoặc lưu password vào một text file không bảo vệ.
Chia sẽ password hệ thống của mình cho bạn đồng nghiệp…

Cấp phát đặc quyền:
Cấp phát đặc quyền Administrator cho các User.
Các services của hệ thống không dùng Service account.
Cấp phát User right không cần thiết cho account.
Việc sử dụng account:
Log-on vào máy với account Administrators khi thi hành những tác vụ thông thường.
Tạo những User account cho phép quyền quản trị các tài khoản khác. Kích hoạt những tài khoản không còn được sử dụng (ví dụ nhân viên đã nghỉ việc, tài khỏan vẫn được lưu hành trên hệ thống..)
Thiết kế chính sách tạo Password đáp ứng bảo mật cho Account:
Chính sách tạo password sao cho an toàn thực sư là một trong những yếu tố chính để bảo vệ tài khoản. Chính sách này bao gồm các yếu tố chính như sau:
Thời gian tối đa sử dụng password (maximum password age): Hạn sử dụng tối đa của password trước khi user phải thay đổi password. Thay đổi password theo định kì sẽ giúp tăng cường an toàn cho tài khoản
Thời gian tối thiểu password phải được sử dụng trước khi có thể thay đổi (minimum password age). Admin có thể thiết lập thờigian này khoảng vài ngày, trước khi cho phép user thay đổi password của họ.
Thực thi password history: Số lần các password khác biệt nhau phải sử dụng qua, trước khi quay lại dùng password cũ. Số Password history càng cao thì độ an toàn càng lớn.
Chiều dài password tối thiểu (minimum password length) cần phải đặt. Càng dài càng an toàn
Password phải đạt yêu cầu phức hợp: không chỉ về độ dài mà còn về độ phức hợp của các kí tự đặt password (ví dụ bạn có thể thấy sự khác biệt giữa password và P@ssW0rd)
Khi dùng password phức hợp cần quan tâm:
Không sử dụng họ và tên
Chứa ít nhất 6 kí tự
Có thể đan xen chữ hoa,(A..Z) thường (a..z), và các kí tự đặc biệt như:
!@#$%^&*()
Account lockout: Sẽ bị khóa tài khoản trong một thời gian nhất định, nếu như sau một số lần log-on không thành công vào hệ thống. Mục đích của chính sách này nhằm ngăn chặn các cuộc tấn công dạng brute force vào account để dò password.
Trên đây là những vấn đề cốt lõi trong việc tạo và quản lý Account sao cho an toàn, nhằm đáp ứng các yêu cầu khắt khe trong chính sách an toàn thông tin của tổ chức và đối với các Security Admin thiết nghĩ vấn đề này không nên chễnh mãng hoặc thờ ơ, vì đây là "ngõ vào" đầu tiên mà attacker luôn ưu tiên trong việc thăm dò, khai thác yếu điểm của hệ thống.

New Horizons VietNam (New Horizons Computer Learning Centers VietNam)
Ho Viet Ha
Instructor Team Leader Email: hvha@newhorizons.com.vn

Bảo vệ máy tính trên Internet

Thực hiện: Lê Thu

Chỉ cần kết nối máy tính vào Internet thì ngay lập tức sẽ có kẻ tìm cách đột nhập vào máy tính của bạn. Trước đây, khi đột nhập thành công vào một chiếc máy tính nào đó, vi rút máy tính chỉ tìm cách ăn cắp thông tin có trong máy. Ngày nay, không chỉ vậy, máy tính của bạn còn bị vi rút sử dụng làm bàn đạp tấn công vào các hệ thống máy tính khác.

Muốn hệ thống máy tính của mình vững chắc thì không thể sử dụng chỉ một giải pháp mà cần phải phối hợp nhiều biện pháp khác nhau: Luôn cập nhật bản sửa lỗi cho Windows và phần mềm ứng dụng, cấu hình lại cho trình duyệt, cài đặt phần mềm chống vi rút và luôn cập nhật thông tin vi rút mới nhất. Sử dụng tường lửa (firewall) để giám sát cả hai chiều thông tin (từ máy tính đi ra và từ ngoài vào). Và cuối cùng, đừng quên cài đặt thêm các tiện ích phòng chống chương trình "gián điệp" (spyware) xâm nhập. Thật may, tất cả các công cụ trên đều có sẵn và miễn phí.

Cập nhật bản sửa lỗi

Đa số các phần mềm ứng dụng, nhất là các sản phẩm do Microsoft sản xuất, đều có tính năng tự động cập nhật bản sửa lỗi qua Internet. Cơ chế này trong thời gian qua đã chứng minh tác dụng hữu ích của nó trong việc hạn chế thiệt hại cho người sử dụng (khi một lỗ hổng trong phần mềm bị phát hiện và lợi dụng).

Trong hệ thống máy tính chạy Windows XP đã cài phiên bản SP2, thủ tục để hệ thống tự động cập nhật bản sửa lỗi mới nhất như sau: nhấn phải biểu tượng My Computer, chọn menu Properties.Automatic Updates, trong màn hình System Properties đánh dấu chọn ở mục có nhãn Automatic (recommended), khai báo

khoảng thời gian máy tính thực hiện chức năng này (thường chọn giá trị mặc định), cuối cùng nhấn OK. Với các phần mềm bảo vệ máy tính như chống vi rút và tường lửa cũng tương tự, bạn chỉ cần kết nối máy tính vào Internet và kích hoạt chức năng tự động cập nhật là xong, các công việc còn lại phần mềm sẽ tự động đảm nhiệm. Với các phần mềm không có chức năng tự động cập nhật thì cũng có menu để người dùng khởi động chế độ cập nhật bản sửa lỗi mới nhất từ website của nhà sản xuất.

Giải pháp bắt buộc

Nếu như cách đây vài năm bạn có thể tự tin vào kinh nghiệm hay kiến thức tin học của mình để tự ngăn ngừa máy tính bị xâm nhập bất hợp pháp, thì giờ đây biện pháp này không còn hiệu quả. Vi rút máy tính hay đúng hơn là các chương trình máy tính nguy hiểm đã tìm được vô số cách rất hợp pháp để "âm thầm" xâm nhập vào máy tính mà bạn không hề cảm nhận thấy sự khác biệt. Do đó, để an toàn và tiện lợi, nên chọn một phần mềm chống vi rút nào đó giúp bạn bảo vệ máy tính.

Năm ngoái, phần mềm PC-cillin Internet Security của Trend Micro được chọn là phần mềm chống vi rút được ưa chuộng nhất. Hiện tại có một số sản phẩm miễn phí làm việc rất hiệu quả, ví dụ như: AVG Free Edition của Grisoft (hình 1), hay Avast 4 Home Edition của Alwil... các sản phẩm này cũng có tính năng tự động cập nhật thông tin vi rút mới từ website của nhà sản xuất.

Tinh chỉnh browser

Internet Explorer của Microsoft là trình duyệt phổ biến nhất hiện nay và cũng là trình duyệt hỗ trợ công nghệ ActiveX. Một ActiveX nhúng vào trang web sẽ được phép tải về, cài đặt rồi hoạt động trên bất cứ máy tính nào truy cập đến trang web có ActiveX. Đây chính sơ hở để vi rút, chương trình gián điệp... tập trung lợi dụng.

Khắc phục điểm yếu này, Microsoft đã phát hành bản vá lỗi SP2 dành cho Windows XP, nhưng cứ bịt xong lỗ rò này thì lỗ hổng khác lại bị phát hiện. Một điểm khác đáng quan tâm là các bản sửa lỗi mới nhất chỉ chú trọng cho các hệ thống Windows XP còn khác hệ thống Windows khác như Windows Me, 98... thì không được Microsoft quan tâm cung cấp kịp thời.

Để phòng tránh bị cài đặt các ActiveX nguy hiểm, bạn có thể chuyển sang dùng trình duyệt khác (tham khảo bài "Những thế lực mới trên web" – TGVT tháng 2/2005, ID: A0502_74). Nếu vẫn muốn tiếp tục sử dụng IE, bạn nên vô hiệu hóa chức năng hỗ trợ ActiveX của IE, thủ tục thực hiện như sau: Vào Tools.Internet Options.Security.Custom Level, chọn mục có nhãn Run ActiveX controls and plug-ins, đánh dấu chọn mục Disable, rồi nhấn OK, Yes, OK (xem hình 2).

Khi muốn cho phép tính năng ActiveX của website (như Windows Update của Microsoft), bạn khai báo địa chỉ website vào danh sách các địa chỉ web an toàn (Trusted Sites). Thủ tục thực hiện như sau: Vào Tools.Internet Options.Security, chọn Trusted Sites tiếp theo nhấn nhãn Sites và nhập các địa chỉ website được coi là an toàn. Bỏ đánh dấu chọn ở mục có nhãn Require server verification (https:) for all sites in this zone, cuối cùng nhấn OK.

Phối hợp tường lửa

Tường lửa là công cụ bảo vệ máy tính chống lại sự xâm nhập bất hợp pháp trong môi trường Internet bằng cách quản lý toàn bộ các cổng dịch vụ Internet theo yêu cầu của người sử dụng. Một tường lửa vững chắc không đơn thuần là ngăn chặn hiệu quả mọi sự xâm nhập từ bên ngoài mà còn phải còn phải theo dõi được toàn bộ các ứng dụng đang hoạt động trong máy tính và phát hiện được ngay khi có hiện tượng một ứng dụng nào đó tìm cách liên lạc ra bên ngoài thông qua đường truyền Internet (đa số các chương trình spyware, trojan... sử dụng phương thức này để bí mật gửi thông tin ăn cắp được).

Phần mềm tường lửa có sẵn trong Windows XP chỉ giám sát được sự xâm nhập từ Internet vào máy tính chứ không ngăn chặn được các phần mềm "gián điệp" trong máy tính liên lạc ra bên ngoài. Trên thị trường có một số phần mềm tường lửa tốt và miễn phí như Kerio Personal Firewall, Outpost Firewall Free, Sygate Personal Firewall, hay ZoneAlarm.

Nếu bạn sử dụng đường truyền Internet tốc độ cao thì nên ưu tiên chọn mua modem ADSL có sẵn chức năng tường lửa để hệ thống máy tính được bảo vệ bằng tường lửa phần cứng lẫn phần mềm. Tường lửa phần cứng ngăn chặn hữu hiệu mọi

sự tấn công từ ngoài Internet vào hệ thống máy tính, không làm lộ địa chỉ IP của máy tính ra ngoài như vậy máy tính của bạn trở nên "vô hình" trong thế giới Internet. Tuy nhiên tường lửa phần cứng không thể phát hiện được phần mềm nào trong máy tính đang tìm cách liên lạc ra thế giới bên ngoài. Việc kết hợp cả hai giải pháp giúp bảo vệ hệ thống máy tính tốt hơn.

Chống spyware

Spyware là thuật ngữ chỉ các chương trình máy tính "lén lút" theo dõi mọi hành vi sử dụng Internet của người dùng để ăn cắp các thông tin cá nhân (mật khẩu đăng nhập mạng, số tài khoản...) hay phát tán các địa chỉ web với mục đích quảng cáo.

Tương tự như đối với vi rút, muốn tránh spyware thì chúng ta phải cài đặt các phần mềm tiêu diệt spyware. Chọn phần mềm chống spyware tốt cũng là cả một vấn đề, bạn có thể tham khảo bài giới thiệu các công cụ diệt spyware miễn phí tốt nhất trong số tháng 4/2005 (ID: A0504_91).

Hiện nay, hai phần mềm diệt spyware tốt nhất (và miễn phí) là Ad-Aware SE và Spybot Search & Destroy. Để phát hiện spyware, 2 phần mềm này tiến hành quét đĩa cứng và Registry để vô hiệu hóa các spyware nguy hiểm. Spybot Search & Destroy còn chạy thường trực trong bộ nhớ máy tính để giám sát các hành vi tìm cách thay đổi nội dung Registry để thông báo cho người sử dụng kịp thời can thiệp. Ngoài ra, bạn cũng có thể sử dụng hai công cụ miễn phí của Javacool Software gồm: SpywareBlaster ngăn chặn spyware dạng ActiveX tự cài đặt vào máy tính và SpywareGuard kiểm tra các tập tin tải về từ Internet để phát hiện có spyware.

Khác với các phần mềm diệt vi rút, bạn có thể cài đặt thoải mái các phần mềm chống spyware trên cùng một máy để khai thác tính năng tốt nhất trong từng phần mềm mà không bị xung đột. Tuy nhiên, để tiêu diệt "triệt để" các phần mềm "gián điệp" đã xâm nhập được vào trong máy tính, bạn nên dùng phần mềm HijackThis. HijackThis có khả năng rà soát tất cả các thành phần bổ sung (add-on) đã được tích hợp vào trình duyệt đang cài trong máy cùng các thông tin liên quan của add-on lưu trong Registry và ghi lại vào một tập tin nhật ký, nhiệm vụ của bạn là duyệt nội dung tập tin này để tìm ra những add-on không cần thiết để loại bỏ hay vô hiệu hóa (hình 3). Tuy nhiên, HijackThis không phân biệt được add-on nào có hại, add-on

nào không, vì vậy nếu vô tình vô hiệu hóa một add-on quan trọng có thể làm cho máy tính của bạn "quờ quạng". Để biết chính xác add-on nào là quan trọng, cần thiết hay có ích cho hệ thống, bạn nên tham khảo thông tin tại các diễn đàn chuyên về sử dụng HijackThis, ví dụ như Merijn.org (www.spywareinfo.com/~merijn/).

Lê Thu
PC World Mỹ 5/2005

KHẮC PHỤC KỸ THUẬT ANTI-DDOS BẰNG FIREFOX

- Không cần phải dài dòng, nhìn bức hình trên, hẳn có lẽ các bạn đã biết tôi muốn đề cập đến vấn đề gì ! Đó chính là kỹ thuật anti-ddos mà hầu hết các website, diễn đàn hiện nay (điển hình là diễn đàn VietDown trong hình minh hoạ trên) đều sử dụng (nhằm tăng tính bảo mật, tránh bị tin tặc tấn công, v.v...).
- Mặt tốt của kỹ thuật này thì không có gì để bàn cãi, nhưng mặt trái của vấn đề thì cũng nghiêm trọng không kém. Dù muốn dù không, bạn cũng phải công nhận rằng, khi dạo qua các trang web có sử dụng kỹ thuật anti-ddos, bạn sẽ phải:
+ Mất nhiều thời gian hơn (do quá rờm rà, hỡ 1 tí là nó lại trở ra màn hình bên ngoài trang (có dòng click here .... hoặc Enter Forum (như trên)), v.v...).
+ Không thể lưu bài (tôi nói là không thể, chứ không phải là khó khăn (chỉ 1 số rất ít trường hợp hiếm hoi là bạn có thể lưu mà thôi).
- Riêng vấn đề thứ 2 (lưu bài) là vấn đề hết sức bức xúc. Bởi dù bạn có dùng trình duyệt nào đi chăng nữa (Internet Explorer, Opera, FireFox, v.v...) thì kết quả vẫn như nhau (1 file HTML với nội dung rỗng !).

- May thay, vấn đề này có thể khắc phục với trình duyệt **FireFox kết hợp với extension** có tên là RefControl

1. Chuẩn bị:
- Trình duyệt web Mozilla FireFox (1.5 trở lên) (FF)
- Extension RefControl (RC)

2. Tiến hành:
- Sau khi đã tải & cài đặt thành công extension RC cho FF, bạn sẽ thấy có 1 biểu tượng nhỏ xuất hiện dưới thanh status (hình 2 tờ giấy)

- ***Yêu cầu đặt ra:*** vượt qua màn hình anti-ddos của diễn đàn VietDown (http://www.vietdown.org/)
- Giả sử, tôi đang đứng tại màn hình anti-ddos, khi click vào dòng Enter Forum địa chỉ trên thanh address sẽ chuyển từ http://www.vietdown.org/ thành http://vietdown.org/vbb/index.php
 như vậy, rõ ràng là http://vietdown.org/vbb/index.php mới chính là trang thật. Bạn hãy để ý phần http://vietdown.org/vbb
- Click phải vào biểu tượng của RC RefControl Options for This Site ...

- Cửa sổ RefControl Site Properties xuất hiện. Bạn điền các thông số như sau:

+ Site: <trang đầu> (tức tên miền của diễn đàn (theo mặc định). Thông thường, chương trình sẽ tự động dò & xác định phần này cho bạn.
+ Custom: <trang cuối> (tức trang chủ thật sự của diễn đàn). Bạn gõ vào (phần tôi bảo bạn lưu ý bên trên): http://vietdown.org/vbb
- Nhấn OK để thoát ra ngoài đóng trang VietDown đang mở vào lại (http://vietdown.org/vbb) kết quả:
- Bạn sẽ càng ngạc nhiên hơn, khi trước đây, nếu bạn lưu bài kết quả thu được chỉ là 1 file HTML trắng toát, thì giờ đây, toàn bộ nội dung trang cần lưu sẽ được lưu lại triệt để.
- Ngoài ra, nếu bạn áp dụng thủ thuật này với những diễn đàn có sử dụng kỹ thuật anti-ddos khác, kết quả cũng sẽ tương tự.

3. Thay lời kết:
- Lại thêm 1 bằng chứng nữa cho thấy FireFox hoàn toàn xứng đáng với ngôi vị dẫn đầu trong số các trình duyệt web. Không những nhanh, thân thiện, mà lại còn đa năng, phải không bạn ? Vậy sao bạn không thử ngay trình duyệt tuyệt với này & tự mình khám phá những extension tuyệt vời "có 1 không 2" như RefControl này ?!

Lương Thiên Khôi
zeromanltk@gmail.com

10h15-10/08/2006: bắt đầu
10h55-10/08/2006: kết thúc

Loại bỏ "tận gốc" phần mềm gián điệp

Thực hiện: Minh Xuân

Máy tính của tôi bị nhiễm một phần mềm gián điệp (spyware) có khả năng tự sao chép lại ngay cả khi tôi đã xóa nó khỏi Windows Registry. Ngoài ra, tôi cũng đã sử dụng tất cả công cụ diệt spyware sưu tầm được nhưng kết quả vẫn vậy.

Nếu đã quét kiểm tra hệ thống bằng các chương trình phòng chống spyware mà vẫn không đạt được kết quả mong muốn, bạn hãy thử dùng tính năng System Restore của Windows (chú ý là Windows 2000 không có System Restore). Bạn nhấn Start.Programs.Accessories.System Tools.System Restore. Chọn Restore my computer to an earlier time, nhấn Next, chọn một cột mốc khôi phục hệ thống (Restore Point) gần đây nhất trên lịch được hiển thị, sau đó thực hiện theo các nhắc nhở.

Nếu System Restore không giải quyết được vấn đề, bước tiếp theo khởi động lại máy tính và ấn trước khi màn hình chuyển độ phân giải khi Windows được nạp vào hệ thống. Trong trình đơn vừa xuất hiện, bạn chọn Safe Mode with a Command Prompt, sau đó chọn hệ điều hành của mình. Tại dấu nhắc lệnh, bạn gõ vào lệnh C:\windows\system32\restore\rstrui.exe, ấn và thử chạy System Restore từ đây.

Nếu máy tính vẫn nhiễm spyware sau khi sử dụng những biện pháp trên, tôi khuyên bạn nên nhờ trợ giúp từ các chuyên gia. Hãy liên hệ với bộ phận hỗ trợ kỹ thuật của các hãng sản xuất phần mềm bảo mật, biết đâu một trong số họ có thể đề xuất cho bạn một giải pháp phù hợp.

Để tham khảo ý kiến cộng đồng, trước hết bạn cần tải về tiện ích miễn phí HijackThis (find.pcworld.com/56218) và khởi chạy tiện ích này để tạo một bản báo cáo mang đậm chất kỹ thuật về những hành xử đáng ngờ của hệ điều hành Windows trong hệ thống mà bạn đang sử dụng (Hình 1). Sau đó, bạn chép báo cáo này lên một trong các diễn đàn trên mạng với thành viên là những người cũng từng gặp phải trường hợp tương tự chẳng hạn TechSoup (find.pcworld.com/56219) và Spyware Varrior (http://www.spywawarrior.com/).

Hình 1: Sử dụng HijackThis tạo báo cáo về các phần mềm nguy hại có trong hệ thống.

Nếu tất cả các biện pháp trên đều thất bại, bạn hãy sao lưu các thư mục dữ liệu của mình và chuẩn bị định dạng lại đĩa cứng, sau đó khôi phục hệ thống từ một bản sao lưu đầy đủ. Nếu không có bản sao lưu của ổ đĩa, bạn phải cài lại Windows, cài đặt và cập nhật phần mềm chống spyware, và phục hồi dữ liệu từ bản sao lưu. Bạn cần tham khảo bài viết "Move All of Your Valuable Data to a New Partition" (find.pcworld.com/56220) để xem danh sách các thư mục thường chứa dữ liệu. Thay vì di chuyển các thư mục này (như thủ thuật trong bài viết trên đề nghị), bạn nên chép chúng vào đĩa CD, DVD hoặc đĩa cứng ngoài.

Dĩ nhiên, việc định dạng lại và khôi phục đĩa cứng sẽ dễ dàng hơn nếu bạn sử dụng một chương trình sao lưu có các tính năng phục hồi dữ liệu sau khi gặp thảm họa tốt. Các chương trình sao lưu và khôi phục như True Image của Acronis (50 USD, find.pcworld.com/56223) và Norton Save & Restore của Symantec (70 USD, find.pcworld.com/56224) đều xuất sắc trong việc khôi phục đĩa cứng, cho phép bạn phục hồi toàn bộ đĩa cứng từ một sao lưu trước khi máy tính bị nhiễm bệnh.

Liệt kê nhanh danh sách trình điều khiển thiết bị
Bạn cần biết những trình điều khiển thiết bị (driver) nào đang chạy trong máy tính và cái gì khởi động chúng? Công cụ Device Manager của Windows sẽ cung cấp đầy đủ chi tiết về một driver cụ thể, nhưng điều đó không giúp ích gì cho bạn nếu muốn có được một cái nhìn tổng quan về tất cả driver có trong hệ thống. Trong Windows XP Pro và Vista, bạn có thể dễ dàng xem thông tin của tất cả driver, dù đang chạy hay không: Chọn Start.Programs.Accessories.Command Prompt. Tại dấu nhắc lệnh, bạn gõ vào lệnh driverquery /v /fo csv > dr.csv rồi ấn . Sau đó, cũng tại dấu nhắc lệnh, gõ dr.csv và ấn . Báo cáo này sẽ được mở ra bằng Microsoft Excel hoặc chương trình bảng tính mà bạn đã thiết lập mặc định sử dụng.

Nếu không có một công cụ sao lưu hệ thống tốt, bạn hãy cài đặt lại Windows bằng đĩa phục hồi hay Windows CD bán kèm theo hệ thống của mình. Trước khi cài đặt, bạn hãy chọn phương án có khả năng phá hủy mọi thứ trên đĩa cứng (một ý tưởng tốt nhưng chỉ trong trường hợp riêng này mà thôi). Bạn cũng sẽ phải thiết lập lại kết nối Internet cũng như cài đặt lại tất cả trình điều khiển thiết bị và trình ứng dụng trên đĩa cứng. Bạn có thể tham khảo hướng dẫn cài đặt lại Windows XP tại địa chỉ find.pcworld.com/56221.

Cuối cùng, khi Windows và các chương trình của bạn đã yên vị, bạn còn phải cập nhật tất cả tiện ích bảo mật và sau đó thực hiện quét kiểm tra virus bản sao lưu các thư mục dữ liệu trước khi di chuyển các dữ liệu cũ này về lại đĩa cứng.

Minh Xuân
PC World Mỹ 4/2007

Sơ cứu hộp thư bị "đóng băng"

Thực hiện: Song Đặng

Bỗng một ngày đẹp trời nào đó, bạn không thể truy xuất hộp thư điện tử của mình bằng tiện ích Microsoft Outlook, hoặc nếu được thì tác vụ tải nội dung thư về từ máy chủ dịch vụ liên lục "gãy gánh" giữa đường mỗi khi bạn cố thử lại tác vụ này bằng cách nhấn liên tục vào nút Send/Receive trên thanh trình đơn. Hãy bình tĩnh, rất có thể hộp thư của bạn đang bị nghẽn bởi ai đó đã vô tình gửi cho bạn một (hay nhiều) thư điện tử có dung lượng các tập tin đính kèm quá lớn. Thông thường, hầu hết dịch vụ thư điện tử hỗ trợ tổng dung lượng tối đa cho một hộp thư là 10MB.

Trên thực tế, toàn bộ thư điện tử được gửi đến tài khoản của bạn được sắp xếp theo dạng hàng đợi (queue) trên máy chủ dịch vụ và chúng sẽ được tiện ích Outlook tải

về theo nguyên tắc "đến trước - ra trước" (FIFO - First In First Out). Nếu chẳng may, thư điện tử gây ra hiện tượng tắc nghẽn lại nằm ở những vị trí đầu tiên thì bạn

không tài nào biết được còn có bao nhiêu thư nữa ở đằng sau và sẽ rất phiền toái nếu đó là những thư điện tử quan trọng mà bạn cần trả lời gấp cho khách hàng, đối tác hay lãnh đạo.

Có một giải pháp khá đơn giản để "hóa giải" tình trạng này là bạn đừng yêu cầu Outlook tải về toàn bộ nội dung của các thư điện tử từ máy chủ dịch vụ, thay vào đó là yêu cầu chỉ tải về phần tiêu đề (header) của mỗi thư. Bạn nhấn chuột vào nút mũi tên hướng xuống ở ngoài rìa nút Send/Receive, một trình đơn phụ sẽ xuất hiện, bạn chọn tài khoản hộp thư cần truy xuất và chọn Download Inbox Headers. Ngay lập tức, toàn bộ danh sách thư hiện có trên máy chủ sẽ xuất hiện, kèm theo là thông tin về dung lượng tập tin đính kèm. Khi này, các thư vẫn còn lưu trên máy chủ dịch vụ và công việc tiếp theo của bạn là đặt "mã lệnh" tương ứng cho mỗi thư.

Hình 1

Để tải về một thư, bạn nhấn chuột phải lên tiêu đề thư đó, chọn Mark to download Message(s) hay Delete để xóa thư đó (Hình 1). Lặp lại cách đánh dấu với các thư còn lại. Sau đó, bạn thực hiện các thao tác tương tự như khi tải về tiêu đề thư, nhưng lần này là chọn Process Marked Headers. Bằng cách này, Outlook sẽ được chỉ dẫn cụ thể cần thực hiện tác vụ tải về những thư nào và xóa trực tiếp trên máy chủ dịch vụ những thư nào dựa trên mã đánh dấu mà người dùng đã dán lên mỗi thư điện tử.

DÈ CHỪNG OUTLOOK

Bạn bị khách hàng phàn nàn tại sao không trả lời thư điện tử mà họ đã gửi cho bạn trong tuần vừa qua, hay không nhận được thư điện tử từ người đồng nghiệp đang làm việc ở một văn phòng chi nhánh khác cho dù hai người này đều khẳng định đã gửi thư đi. Hãy tìm chúng ở hộp thư rác (Junk Email).

Hình 2

Trước vấn nạn thư rác, Microsoft đã cung cấp cho Outlook tính năng Junk Email để hạn chế đến mức tối đa những thư điện tử "không mời mà đến" lọt vào hộp thư chính của bạn. Tuy nhiên, cũng có không ít trường hợp, Junk Email nhận dạng lầm những thư điện tử của bạn bè, khách hàng, người thân là thư rác và ngay tức khắc "quẳng" chúng vào hộp thư Junk Email. Nếu không ngại đọc và xóa thư rác mỗi ngày, bạn hãy tắt tính năng này: trong Outlook, chọn Tools.Options, ở thẻ Preferences, nhấn Junk Email, ở thẻ Options, đánh dấu tùy chọn No Automatic Filtering và nhấn OK để kết thúc.

Song song với giải pháp tình thế đó, bạn còn có thể "thỏa hiệp" với Outlook bằng cách tạo ra một danh sách địa chỉ email người gửi an toàn (Safe Sender). Trong Outlook, bạn chọn Tools.Options, ở thẻ Preference, chọn Junk Email. Tiếp đến, ở thẻ Safe Senders, bạn đánh dấu 2 tùy chọn ở phía cuối hộp thoại là Also trust e-mail from My Contacts và Automatically add people I e-mail to the Safe Senders List. Bằng cách này, Outlook sẽ xem các địa chỉ thư điện tử có trong danh bạ liên lạc Contacts của bạn và những địa chỉ thư điện tử mà bạn gửi đi là những địa chỉ an toàn (không phải là địa chỉ phát tán thư rác). Ngoài ra, bạn cũng có thể bổ sung các địa chỉ thư điện tử khác vào danh sách Safe Senders (Hình 2).

Cần lưu ý, bạn nên thường xuyên kiểm tra hộp thư Junk Email vì tính năng "lọc" thư rác của Outlook nhiều khả năng sẽ tiếp tục nhận dạng lầm các thư điện tử có nguồn gốc rõ ràng nhưng lại không có tên trong danh sách Safe Sender, cũng như vô tình có những thuộc tính nào đó tương đồng với đặc điểm nhận dạng thư rác của Junk Email.

Song Đặng

Bảo vệ PC khi chưa có bản vá

Thực hiện: Nguyễn Lê

Kẽ hở ngày zero (zero-day) tạo nên tình trạng dễ bị tấn công của phần mềm mà nhà sản xuất chưa kịp vá lỗi. Tuy nhiên vẫn có cách giữ an toàn cho máy tính của

bạn trong thời gian "trống" này.

1. Từ bỏ Internet Explorer 6. Một trong những hành động tốt nhất mà bạn có thể làm để cải thiện độ an toàn khi lướt web là tống khứ trình duyệt đầy lỗi tai tiếng của Microsoft. Dĩ nhiên, không có chương trình nào tuyệt đối an toàn; nhưng IE 6 dễ bị tấn công hoặc vì bản thân nó vốn "ốm yếu", hoặc vì có số lượng người dùng đông đảo nên trở thành mục tiêu hấp dẫn. Hãy nâng cấp lên IE 7 hay dùng trình duyệt khác thay thế như Firefox hay
Opera.

2. Thử các chương trình khác thay thế cho những mục tiêu thường bị tấn công zero-day. Chẳng hạn dùng chương trình Foxit thay cho Adobe Reader và OpenOffice thay cho MS Office.

3. Thiết lập chế độ cập nhật tự động cho Windows và các chương trình khác khi có thể. Các lỗi nghiêm trọng thường vẫn là mục tiêu tấn công ngay cả sau khi đã có bản vá, do tin tặc biết nhiều người không thèm vá lỗi. Để kiểm tra và thay đổi thiết lập Windows Update, nhấn Automatic Updates trong Control Panel. Để hệ thống luôn cập nhật, bạn nên chọn Download updates for me, but let me choose when to install them.

Các chương trình khác cũng có thể thiết lập cập nhật tự động. Ví dụ, trong Firefox, vào Tools.Options.Advanced, và chọn mục Update (nên chọn mặc định Ask me what I want to do). Với Adobe Reader, bạn cần kiểm tra thủ công các bản cập nhật trong menu Help, rồi nhấn nút Preferences.

4. Sử dụng chương trình chống virus hay bảo mật có khả năng phân tích thông minh hay theo hành vi để bổ trợ cho phần mềm chống virus dựa trên thông tin nhận dạng truyền thống.

Các bản vá không dập tắt các cuộc tấn công zero-day nhưng các bản cập nhật cần cho việc bảo vệ PC.

5. Sử dụng firewall của Windows XP hay của một hãng nào đó. Firewall giúp ngăn chặn các đoạn mã phá hoại (sâu - worm) có thể quét máy tính của bạn để tìm các lỗ hổng chưa được vá và đột nhập. Để kiểm tra xem firewall của Windows XP có được kích hoạt hay chưa, vào Control Panel, mở Security Center và nhấn liên kết Windows Firewall. Hầu hết router băng rộng đều có chức năng firewall.

6. Sử dụng chương trình ngăn chặn như DropMyRights để bổ trợ phần mềm chống virus hay bảo mật. Hiện có nhiều công cụ tiện ích, cả miễn phí và có phí, thay đổi cách thức vận hành các chương trình dễ bị tấn công để giới hạn vùng ảnh hưởng nếu xảy ra tấn công zero-day.

7. Cập nhật thông tin. Trang chuyên đề "Bảo mật" của Thế Giới Vi Tính Online cung cấp tin tức mới nhất về các mối đe dọa bảo mật, các hướng dẫn an toàn và các bài nhận xét về sản phẩm bảo mật. Ngoài ra còn có các nguồn thông tin tốt khác như website eEye Zero-Day Tracker (research.eeye.com) và blog Security Fix (http://blog.washingtonpost.com/securityfix/).

Nguyễn Lê
PC World Mỹ 04/2007

Thu hồi Email đã gởi trong MS Outlook

Có lúc nào đó bạn đã gởi đi một Email nhưng bất chợt "thôi chết rồi gởi lộn địa chỉ rồi" và bạn muốn lấy lại email đó. Nếu bạn sử dụng Microsoft Outlook hãy làm theo cách này :

1. Vào Sent Items
2. Chọn cái mail mà bạn đã gởi nhầm (click vào nó)

3. Trong cái cửa sổ của mail đó bạn vào Action trên thanh Menu và chọn tiếp Recall This Message
4. Bạn sẽ có hai lựa chọn hãy chọn Delete unread copies of this message

(c) ghost1982@updatesofts.com

Sử dụng và diệt các loại trojan nè

Lang thang trên mạng mới tìm đc mấy cái nên box lên cho anh em xem nè:

1.Đầu tiên là con Trojan Hooker
Sau khi bạn tải con này về ,các bạn chạy tập tin Hkconf.ini các bạn đặt thuộc tính cho
file này như sau
Số 1 là đặt thuộc tính enable cho tính chất đó
Số 0 là đặt thụôc tính disable cho tính chất đó

kill = 1 ;kill itself?
Ví dụ nếu bạn chọn kill=1 thì nó sẽ tự kill nó,còn nếu chọn 0 thì nó sẽ không tự kill nó

Nhưng mấy cái dó không quan trọng cái quan trọng là phần host đây là cai server mà thông qua đó con Trojan đó sẻ gửi thư về cho ta

sendmail host
host=mx4.mail.yahoo.com

Phần host= bạn có thể cho nó bằng các Host tôi đưa ra đây (không biết có cái nào không còn hoạt động không nữa , vì mấy cái này hoạt động bất thường lắm ,lâu rồi tôi chưa thử nên không biêt ,nếu anh em ai biết cái nào còn hoạt động tốt thì Post lên cho anh em xài)

SMTP đây :
mx2.mail.yahoo.com
hoac mx4.mail.yahoo.com
hoac mta45.mail.yahoo.com
hoac hcm-mail-prepaid.vnn.vn==> tot day
hoac mta-v13.level3.mail.yahoo.com
hoac isp-mta.fpt.vn
hoac mta469.mail.yahoo.com ===>rat tot

Nhân dây tôi cũng giải thích cho các bạn rõ Smtp (Simple Mail Transfer Protocol) là gì :đây là một giao thức đưa trên TCP/IP được sử dụng để upload thư của người dùng lên mail Server,nói đơn giàn hơn smtp
giống như là anh đưa thư vậy ,có đia chỉ rồi nhưng không có anh đưa thư ,thì thư

cũng không được chuyển đến địa chỉ đó được ,smtp cũng vậy phải có nó thì các thông tin mới được gủi về hộp mail của mình.

Đay cũng là cách để Bomb mail luôn đó (Post=25)
Và phần quan trọng không kém là phần điền địa chỉ thư để mà con Trojan còn gũi thư về cho ta nữa chứ

mailto - your email
mailto=bạn diền dịa chỉ của bạn vào chỗ này
Thư của bạn được gủi về hộp thư của bạn với chủ đề

subject of message
subj=đây là chủ dề mà bạn sẽ nhận dược khi con Trojan gửi thư về cho bạn

name of exec
exename=hsys.exe ===> dây là tập tin mà con Trojan sẽ chạy ngay trong máy của Victim
Bạn cũng có thể dổi tên tập tin này

reg_path=
====>đây là hướng dẫn dễ con trojan ghi tên nó vào Registry để mỗi lần khởi động máy thì nó tự động chạy ===>bạn cũng có thể thay đỗi hướng dẫn

À Quên một cái cũng rất là quan trọng ,là nếu ở dòng cuối cũng của file Hkconf.ini nếu ở trên là dòng
S5 thì bạn thêm vào dòng cuối cùng là S6=logon còn nếu là dòng trên là S12 th2i bạn thêm vào S13=logon

Xong bạn save file Hkconf.ini này lại rồi chạy file config.bat ,xong bạn gửi file hooker.exe
cho victim đi là xong
Nói chung phần này không khó các bạn có thể tự đọc và làm lấy ,dể tôi chuyển sang các con khác

2.Tôi xin nói về con Barok
Con này sủ dụng rất là dễ
Bạn download về xong rồi chạy file setup.exe
Sau đó bạn nhập vào nut Open Server mở tập tin server.exe
Rất đơn giản
Trong phần file name bạn dặt tẹn vidu là Barok thì sau này nó sẽ tự ghi vào máy

victim với cái tên là Barok.exe
Phần out going mail server bạn diền phần Smtp như tôi dã nói ở trên
Phần destination diền emal của bạn vào
Xong bạn save lại rồi
gủi file server.exe cho victim thế là xong

3.Sau đây là tôi chỉ cho các bạn xài con Kuang2keyloggeras
Cách sử dụng cũng giống như con Barok khi download về rồi đầu tiên bạn chạy file K2as_sự.exe hiện ra một giao diện nhập vào nút Open chọn file K2logas và mở file nảy ra
bạn điện những thu cần thiết vào(smtp,email như tôi đã nói ở trên)
phần source address bạn điện địa chỉ nào cũng được
Con phần bên phải là các thiết lập tuy bạn chọn để con này sẽ gửi về cho bạn những
gì bạn yêu cầu như có lưu phím mở rộng hay là để thời gian máy ngày con trojan gửi thư
về cho bạn
Nói chung bạn đánh dấu chọn hết cho chắc ăn
xong bạn save lại và gửi file K2logas cho victim là xong
4.Con Kuang2 cũng sử dụng giống như con Kuang2keyloggeras mà thôi
5.Bây giờ tới nơi đến con Keylog:===> à mà con này hình như bác người_dân_đường_hanoi đã nói nhiều
rồi thì phải ,thôi thì các bạn từ tìm lấy mà đọc nhẹ ,nói chung máy con này cách sự dùng cũng giống nhau mà thôi
Những túi thấy con Keylog5 này không hay một chút nào,theo tôi thì con Hooker là hay nhất
6.Cách dùng Cyn2.1 để gần Trojan vào file mp3,jpg,đọc v.v...
Những làm cách nào để gửi Trojan cho Victim???
chẳng lẽ attach con Trojan vào thu rồi gửi đi à ,không được đâu các bác à vì hotmail và
yahoo nó phát hiện được vì thế khi download về victim sẽ phát hiện ra ngày
Cách khắc phục là các bác nên gửi trojan khi đang chất với victim rồi send Trojan cho nó
Thế là tốt rồi
Những có cách hay hơn là các bác nên đình con trojan vào một file ví dụ như file.đọc
.jpg hay là file gì đó để cho Victim khỏi nghi ngờ
Tôi thường sử dụng Cyn2.1 để gần trojan
Các bác download về rồi chạy file

C_Client.exe sẽ hiện ra một giao diện khá là đẹp ,bạn chọn thế File Joiner
Trong phần First Executable bên phải là nút để mở bạn chọn con Trojan nào mà muốn
attach vào
Second file là file mà bạn sẽ đình con Trojan vào (ví dụ Victim là tháng con trai nào đó thì nên đình
cho nó một cái hình Séc,rồi nói là "tạo có một cái hình Séc mày mò ra mà xem ,đẹp làm "
mà tháng con trai nào mà cha thích xem hình chữ ,như thế sắc xuất thành công là cao làm do hihihi
Con victim là con gái thì để quá gửi cho nó cái anh của LeoDicapiro,hay Brad Pitt hay Justin
Timberlake gì gì đó hihi 90% là nó đình con Trojan cái chắc)
Sau khi chọn xong 2 file rồi các bác nhấn vào Joiner File (ở bên phải của giao diện do)thế là các bác sẽ có 1 file cố định kém
Trojan ,file này sẽ có tên là 101.exe ,các bạn đổi tên của file này rồi gửi cho Victim
(====>nói tới đây thì tôi nhỏ tới một điều là: tôi muốn hỏi mọi người là có ai biết cách thay đổi Icon của tập tin không ,tối thứ mọi cách rồi mà cha được , ai biết chỉ giun tôi đi cảm ơn nhiều)
8)Meo xem thu mới của victim : xem xong rồi thu vẫn giống như lúc chưa đọc
Khi đọc đóng trên chắc các bác sẽ cuối tôi là để thế mà cũng nói,những ở đây điều tôi muốn
nói là khi có thư một cái mail mới thì cái Subject của bức thư dám đến đúng không ????những khi ta đọc thư
xong rồi thì nó sẽ tự động trắng ra (để đánh dấu lả tả đã đọc rồi) và như thế khi victim mở hộp thư
của mình ra họ sẽ phát hiện là có người đọc thư của mình rồi
Do đó tôi chỉ cho các bác cách làm cho thứ đó mới trở lại (giống như lúc chưa được xem),rất dễ các bác chọn Remark Unread
ở trong Inbox của các bác ,rồi Ok thế là xong .Quá dễ nhưng rất hiệu quả do .
Các bác sẽ tha hồ xem thu mới của Victim, sau đó đánh dấu lá thư do lại ,như thế thì Victim sẽ không biết lá thư do đã bị xem,sướng nhẹ!!!!.
9.Có Pass của kẻ đáng ghét rồi , làm sao để cướp luôn hộp thư do của nó ????
Các bác nói để quá ai mà cha làm được ,vào Account Information ,chẳng password là xong chữ gì
====>làm to rồi nhẹ!!!!!!
Khi bị đôi Pass ,Victim không vào hộp thư của họ được nữa,biết là đã mất pass họ sẽ vào Password
lookup ,lấy lại pass mới ,thế là các bác tiêu rồi nhẹ ,bỏ công lấy pass của họ bây giờ hộ đói pass

sthe là công sức của ta đổ xuống sống ,xuống biển.
Tôi có méo này để cướp luôn hộp thư của người ta ,cũng để thôi
Đầu tiên vào Edit.yahoo.cơm các bác xóa account do đi mình biết pass rồi thì xóa rất dễ đúng không
===>bước tiếp theo vào yahoo đăng kí lại account do ===>thế là xong .
Đơn giản thôi nhưng cũng rất effect do
10)Con lo như bạn bị đình một con trojan rồi thì làm sao mà loại bỏ nó đây?????
Điều đầu tiên là bạn phải biết là bạn chạy chương trình gì mỗi khi khởi động máy
Sau đó bạn nhập Start==>Run gõ regedit rồi bạn tìm đến các khóa sau ,thông thường thì
các con trojan ghi vào 7 khóa sau :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServiceOnce
Đây là 7 khóa mà chương trình nếu mà đặt ở cho này thì sẽ tự động chạy mỗi khi vào Windows,nhờ vậy mà các con trojan mới có thể từ hoạt động mỗi khi mở máy
Các bác tìm thấy tập tin nào là mà nghi ngờ là trojan thì hay xóa nó đi,sau đó khởi động lại máy
tìm đến tập tín đồ rồi xóa nó đi ,thế là xong rồi.
Cách này của tôi không được hay chổ làm vì bạn cần phải nhỏ tất cả các tập tin thực thi ở 7 khóa trên ,nên khi có tập tin là, mới có thể biết là có Trojan ,thế nhưng đã có lần tôi đã xóa nhầm một file====>vì vậy bác bảo có cách nào hay hơn thì chỉ giun cho tôi đi (cảm ơn nhiều ha)

Thế là tôi đã trình bày cho các bạn về các cách sủ dụng và diệt trojan và các ****o xem thủ ,hy vọng các bạn mối vào nghề sẽ thích bài này

Quên mất, tôi chưa nói cho các bạn biết chỗ tôi thường download các con trojan tôi vừa nói ở trên

Mà trước khi giới thiệu dịa chỉ tôi xin mách (chỉ là mách bảo thôi chứ không dám lớn tiếng ,vì mình cũng là Newbie mà) với các bạn Newbie là nêu muốn học Hack nhanh thì
nên tự mình tìm Trojan hay tài liệu (có thể mới tiến bộ nhanh được , chứ cái gì có sẵn rồi đem ra dùng thì biết bao giờ mới tiến bộ được) và một điều quan trọng là phải học tiếng Anh thật tốt.mới mong làm dc .chúc
Còn nếu muốn tìm file down load thì hình như trong box này có ai đã từng đăng rùi đấy,hay pà kon len google mà tìm.Thân ái!
Ngoc*Anh(VNISS)

Thủ thuật cắt BAD ổ cứng

Thông thường khi ổ cứng (HDD) của bạn bị hư hỏng (xuất hiện Bad Sector) thì để bảo đảm an toàn dữ liệu, cách tốt nhất là thay đĩa cứng mới. Tuy nhiên, giá một ổ cứng không phải rẻ, bạn đừng vội vất nó vào sọt rác mà hãy cố gắng cứu chữa nó bằng các tiện ích chuyên dùng.

Nhận biết đĩa cứng bị bad:

1. Trong lúc đang cài đặt Windows hệ thống bị treo mà không hề xuất hiện một thông báo lỗi nào (đĩa cài đặt Windows vẫn còn tốt), mặc dù vẫn có thể dùng Partition Magic phân vùng cho HDD một cách bình thường.

2. không Fdisk được: khi Fdisk báo lỗi no fixed disk present (đĩa cứng hiện tại không thể phân chia) hoặc Fdisk được nhưng rất có thể máy sẽ bị treo trong quá trình Fdisk.

3. không Format được HDD: khi tiến hành format đĩa cứng máy báo lỗi Bad Track 0 – Disk Unsable.

4. khi đang format thì máy báo Trying to recover allocation unit xxxx. Lúc này máy báo cho ta biết cluster xxxx bị hư và nó đang cố gắng phục hồi lại cluster đó nhưng thông thường cái ta nhận được là một bad sector!

5. đang chạy bất kì ứng dụng nào, nhận được một câu thông báo như Error reading data on dirver C:, Retry, Abort, Ignore, fail? Hoặc A serious error occur when

reading driver C:, Retry or Abort?

6. khi chạy Scandisk hay NDD (Norton Disk Doctor) hay bất kỳ phần mềm kiểm tra bề mặt đĩa (surface scan) nào, ta sẽ gặp rất nhiều bad sector.

Cách khắc phục:

(tất cả các chương trình giới thiệu dưới đây nằm gọn trong đĩa Hiren's Boot có bán ở các cửa hàng phần mềm tin học phiên bản 7.7 hoặc 7.8).

o Cách 1: Dùng partition Magic cắt bỏ chỗ bad.

Thực hiện như sau:

Đầu tiên dùng chương trình NDD, khởi động từ đĩa Hiren's Boot, ở menu của chương trình chọn mục 6. Hard Disk Tools, chọn tiếp 6. Norton Utilities, chọn 1.Norton Disk Doctor.
Sau khi dùng NDD xác định được vị trí bị bad trên HDD, tiến hành chạy chương trình Partition Magic cắt bỏ phần bị bad bằng cách đặt partition chứa đoạn hỏng đó thành Hide Partition.

Ví dụ: khoảng bị bad từ 6.3GB đến 6.6GB, bạn chia lại partition, chọn partition C đến 6GB, partition D bắt đầu từ 7GB, cứ như thế bạn tiến hành loại bỏ hết hẳn phần bị bad.
Cách này sử dụng rất hiệu quả tuy nhiên nó chỉ khắc phục khi đĩa cứng của bạn có số lượng bad thấp.

Cách 2: dùng chương trình HDD Regenerator:

o Thông thường nhà sản xuất luôn để dự phòng một số sector trên mỗi track hoặc cylinder, và thực chất kích thước thực của sector vẫn lớn hơn 512bytes rất nhiều (tùy loại hãng đĩa). Như thế nếu như số sector bị bad ít hơn số dự phòng còn tốt thì lúc này có thể HDD Regenerator sẽ lấy những sector dự phòng còn tốt đắp qua thay cho sector bị hư, như vậy bề mặt đĩa trở nên "sạch" hơn và tốt trở lại. Dĩ nhiên nếu lượng sector dự phòng ổ cứng ít hơn thì ổ cứng sẽ còn bị bad một ít. Bạn có thể quay lại cách 1.

Cách thực hiện:

Khởi động hệ thống từ đĩa Hiren's Boot. Cửa sổ đầu tiên xuất hiện, chọn 6.Hard Disk Tools, chọn tiếp 2. HDD Regenerator, bấm phím bất kì để xác nhận. Kế đến ở dòng Starting sector (leave 0 to scan from the beginning) gõ vào dung lượng lớn nhất hiện có của HDD, gõ xong bấm Enter để chương trình thực hiện. Thời gian chờ, tùy thuộc vào dung lượng đĩa và số lượng bad.

Chẩn đoán bệnh qua tiếng bíp của BIOS

Nguồn: PCWorld.com.vn

Đã bao giờ bạn chú ý tới tiếng bíp mỗi khi khởi động máy tính? Nó chính là thông báo mã hoá chứa đựng thông tin kết quả của quá trình kiểm tra cơ sở các thiết bị phần cứng trong máy.Quá trình kiểm tra này được gọi là POST (Power-On-Self-Test). Nếu POST cho ra kết quả tốt, máy tính sẽ phát một tiếng bíp và mọi thứ diễn ra suôn sẻ. Nếu các thiết bị phần cứng máy có vấn đề thì loa sẽ phát ra vài tiếng bíp.Nếu giải mã được những tiếng bíp này thì bạn có thể tiết kiệm được nhiều thời gian trong việc chẩn đoán bệnh của máy tính.

Trên các máy tính đời mới hiện nay, mainboard được tích hợp các chip xử lý đảm nhiệm nhiều chức năng, giảm bớt card bổ sung cắm trên bo mạch. Tuy nhiên, điều này sẽ làm giảm tính cụ thể của việc chẩn đoán. Ví dụ, nếu chip điều khiển bàn phím bị lỗi thì giải pháp duy nhất là phải thay cả mainboard.

Bài này, chỉ đề cập tới 2 loại BIOS tương đối phổ dụng là Phoenix và AMI. Rất tiếc, Award BIOS hiện nay có rất nhiều phiên bản và do nhà sản xuất bo mạch chủ hỗ trợ, do đó chúng bị thay đổi nhiều trước khi được tung ra thị trường. Vì vậy, Award BIOS không được đề cập tới trong bài này.

(POST là quá trình kiểm tra nội bộ máy được tiến hành khi khởi động hoặc khởi động lại máy tính. Là một bộ phận của BIOS, chương trình POST kiểm tra bộ vi xử lý đầu tiên, bằng cách cho nó chạy thử một vài thao tác đơn giản. Sau đó POST đọc bộ nhớ CMOS RAM, trong đó lưu trữ thông tin về dung lượng bộ nhớ và kiểu loại các ổ đĩa dùng trong máy của bạn. Tiếp theo, POST ghi vào rồi đọc ra một số mẫu dữ liệu khác nhau đối với từng byte bộ nhớ (bạn có thể nhìn thấy các byte được đếm trên màn hình). Cuối cùng, POST tiến hành thông tin với từng thiết bị; bạn sẽ nhìn thấy các đèn báo ở bàn phím và ổ đĩa nhấp nháy và máy in được reset chẳng hạn. BIOS sẽ tiếp tục kiểm thử các phần cứng rồi xét qua ổ đĩa A đối với DOS; nếu ổ đĩa A không tìm thấy, nó chuyển qua xem xét ổ đĩa C).

Mô tả mã lỗi chẩn đoán POST của BIOS AMI

1 tiếng bíp ngắn: Một tiếng bíp ngắn là test hệ thống đạt yêu cầu, do là khi bạn thấy mọi dòng test hiển thị trên màn hình. Nếu bạn không thấy gì trên màn hình thì phải kiểm tra lại monitor và card video trước tiên, xem đã cắm đúng chưa. Nếu không thì một số chip trên bo mạch chủ của bạn có vấn đề. Xem lại RAM và khởi động lại. Nếu vẫn gặp vấn đề thì có khả năng bo mạch chủ đã bị lỗi. Bạn nên thay

bo mạch.

2 tiếng bíp ngắn: Lỗi RAM. Tuy nhiên, trước tiên hãy kiểm tra card màn hình. Nếu nó hoạt động tốt thì bạn hãy xem có thông báo lỗi trên màn hình không. Nếu không có thì bộ nhớ của bạn có lỗi chẵn lẻ (parity error). Cắm lại RAM và khởi động lại. Nếu vẫn có lỗi thì đảo khe cắm RAM.

3 tiếng bíp ngắn: Về cơ bản thì tương tự như phần 2 tiếng bíp ngắn.

4 tiếng: Về cơ bản thì tương tự như phần 2 tiếng bíp ngắn. Tuy nhiên cũng có thể là do bộ đặt giờ của bo mạch bị hong

5 tiếng bíp ngắn: Cắm lại RAM. Nếu không thì có thể phải thay bo mạch chủ.

6 tiếng bíp ngắn: Chip trên bo mạch chủ điều khiển bàn phím không hoạt động. Tuy nhiên trước tiên vẫn phải cắm lại keyboard hoặc thử dùng keyboard khác. Nếu tình trạng không cải thiện thì tới lúc phải thay bo mạch chủ khác.

7 tiếng bíp ngắn: CPU bị hỏng. Thay CPU khác.

8 tiếng bíp ngắn: Card màn hình không hoạt động. Cắm lại card. Nếu vẫn kêu bíp thì nguyên nhân là do card hỏng hoặc chip nhớ trên card bị lỗi. Thay card màn hình.

9 tiếng bíp ngắn: BIOS của bạn bị lỗi. Thay BIOS khác.

10 tiếng bíp ngắn: Vấn đề của bạn chính là ở CMOS. Tốt nhất là thay bo mạch chủ khác.

11 tiếng bíp ngắn: Chip bộ nhớ đệm trên bo mạch chủ bị hỏng. Thay bo mạch khác.

1 bíp dài, 3 bíp ngắn: Lỗi RAM. Bạn hãy thử cắm lại RAM, nếu không thì phải thay RAM khác

1 bíp dài, 8 bíp ngắn: Không test được video. Cắm lại card màn hình.

BIOS PHOENIX

Tiếng bíp của BIOS Phoenix chi tiết hơn BIOS AMI một chút. BIOS này phát ra 3

loạt tiếng bíp một. Chẳng hạn, 1 bíp dừng-3 bíp dừng. Mỗi loại được tách ra nhờ một khoảng dừng ngắn. Hãy lắng nghe tiếng bíp, đếm số lần bíp.

Mô tả mã lỗi chẩn đoán POST của BIOS PHOENIX

1-1-3: Máy tính của bạn không thể đọc được thông tin cấu hình lưu trong CMOS.

1-1-4: BIOS cần phải thay.

1-2-1: Chip đồng hồ trên mainboard bị hỏng.

1-2-2: Bo mạch chủ có vấn đề.

1-2-3: Bo mạch chủ có vấn đề.

1-3-1: Bạn cần phải thay bo mạch chủ.

1-3-3: Bạn cần phải thay bo mạch chủ.

1-3-4: Bo mạch chủ có vấn đề.

1-4-1: Bo mạch chủ có vấn đề.

1-4-2: Xem lại RAM.

2-_-_: Tiếng bíp kéo dài sau 2 lần bíp có nghĩa rằng RAM của bạn có vần đề.

3-1-_: Một trong những chip gắn trên mainboard bị hỏng. Có khả năng phải thay mainboard.

3-2-4: Chip kiểm tra bàn phím bị hỏng.

3-3-4: Máy tính của bạn không tìm thấy card màn hình. Thử cắm lại card màn hình hoặc thử với card khác.

3-4-_: Card màn hình của bạn không hoạt động.

4-2-1: Một chip trên mainboard bị hỏng.

4-2-2: Trước tiên kiểm tra xem bàn phím có vấn đề gì không. Nếu không thì

mainboard có vấn đề.

4-2-3: Tương tự như 4-2-2.

4-2-4: Một trong những card bổ sung cắm trên bo mạch chủ bị hỏng. Bạn thử rút từng cái ra để xác định thủ phạm. Nếu không tìm thấy được card bị hỏng thì giải pháp cuối cùng là phải thay mainboard mới.

4-3-1: Lỗi bo mạch chủ.

4-3-2: Xem 4-3-1.

4-3-3: Xem 4-3-1.

4-3-4: Đồng hồ trên bo mạch bị hỏng. Thử vào Setup CMOS và kiểm tra ngày giờ. Nếu đồng hồ không làm việc thì phải thay pin CMOS.

4-4-1: Có vấn đề với cổng nối tiếp. Bạn thử cắm lại cổng này vào bo mạch chủ xem có được không. Nếu không, bạn phải tìm jumper để vô hiệu hoá cổng nối tiếp này.

4-4-2: Xem 4-4-1 nhưng lần này là cổng song song.

4-4-3: Bộ đồng xử lý số có vấn đề. Nếu vấn đề nghiêm trọng thì tốt nhất nên thay.

1-1-2: Mainboard có vấn đề.

1-1-3: Có vấn đề với RAM CMOS, kiểm tra lại pin CMOS và mainboard.

Đảm bảo hoạt động cho máy in Laser

Thực hiện: Minh Xuân

Máy in laser cá nhân thường không có được sự hỗ trợ kỹ thuật, vì vậy bạn cần biết cách giải quyết một số sự cố.

Tham vấn wizard: Wizard Windows Printing Troubleshooter chỉ tập trung giải quyết các trục trặc cơ bản, nhưng rất đáng tham khảo. Trong WinXP, bạn chọn

Start.Help and Suport, gõ list of troubleshooter vào trong hộp Search, và nhấn <Enter>. Nhấn List of troubleshooters trong khung bên trái, chọn Printing trong cột troubleshooter ở bên phải, và làm theo từng bước. Trong Win2000, bạn nhấn Start.Help, và chọn Troubleshooting and Maintenance trên nhãn Contents. Chọn Win2000 troubleshooter, nhấn Print trong danh sách các wizard troubleshouter ở khung bên phải, và làm theo các bước hướng dẫn. Để mở wizard này trong WinMe, bạn nhấn Start.Help, gõ troubleshooter vào hộp Search, và nhấn OK. Trong Win98, bạn chọn Start.Help.Contents.Troubleshooting.Windows 98 Troubleshooter.Print, và làm theo wizard hướng dẫn.

Kiểm tra cơ bản: Kiểm tra điện vào máy in. Cắm chặt các đầu nối cáp. Nhiều máy in có nút điều khiển online/offline ở mặt trước và có thể bị vô tình chạm vào.
In trang thử: Hầu hết các máy in đều có thể chạy quá trình tự kiểm tra nếu bạn nhấn và giữ một hay nhiều nút trên panel điều khiển. Nếu như trang kiểm tra tốt thì trục trặc nằm ở cáp dữ liệu, PC, hoặc phần mềm. Nếu trang in thử không tốt, bạn tham khảo bảng "Những trục trặc phổ biến" để tìm cách giải quyết.

Dùng thứ mới nhất: Cài đặt driver và phần mềm mới nhất cho máy in. Cả hai thứ này đều có ở trang web của hãng sản xuất. Để cài đặt driver mới trong WinXP, bạn chọn Start.Printers and Faxes và chọn Add a Printer bên dưới Printer Tasks trên thanh Explorer trong cửa sổ Printer and Faxes. Trong Win 2000/Me/98, bạn loại bỏ driver của máy in và cài đặt lại. Chọn Start.Settings.Printers để mở cửa sổ Printers. Nhấn phải máy in này, chọn Delete (chọn Yes nếu được hỏi xác nhận), mở lại cửa sổ Printers nếu nó bị đóng, nhấn đúp Add Printer, và hoàn tất việc cài đặt lại.

Chấm dứt kẹt giấy: Tháo bỏ các tờ giấy bị kẹt bằng cách kéo chúng ra theo chiều thuận như khi in. Nếu máy in bị kẹt thường xuyên, bạn ngắt điện khỏi máy, để cho máy nguội, tháo cartridge mực ra ngoài, và kiểm tra xem có vật gì gây cản trở bên trong không.

Kiểm tra đầu nối: Nếu máy in dùng đầu nối USB, bạn mở Device Manager và tìm dấu X màu đỏ, hoặc dấu chấm than trong vòng tròn màu vàng nằm kề bên những liệt kê thiết bị USB. (Trong Win XP/2000/Me, bạn nhấn Start, nhấn phải My Computer, và chọn Properties.Hardware.Device Manager. Trong Win98, bạn nhấn phải My Computer và chọn Properties.Devices Manager). Những biểu tượng này

có thể là dấu hiệu của trục trặc trong kết nối máy in với PC. Nếu máy in ngưng hoạt động khi hệ thống ra khỏi chế độ hibernate hay chế độ chờ (suspend), bạn nhấn đúp lên từng Root Hub bên dưới mục USB, chọn Power Management, và bỏ chọn đối với Allow the computer to turn off this device to save power. Trường hợp đang dùng hub USB, bạn thử nối trực tiếp máy in với cổng USB trên PC xem có giải quyết được trục trặc không.

Minh Xuân
PC World Mỹ 3/2005

Làm thế nào phát hiện lỗi bộ nhớ

Bạn gặp phải trục trặc hệ thống với nhiều lỗi hệ thống kì lạ và nghi ngờ liệu có phải do những thanh nhớ RAM chất lượng kém ? Bài viết này sẽ giúp bạn lần theo dấu vết và xác định nguồn gốc những lỗi đó.

Chiếc máy tính chạy hệ điều hành Windows của bạn gặp lỗi mà không có lý do nào cả ? Chuyện này cũng bình thường thôi, với hàng triệu dòng lệnh cho Windows và các phần mềm, sai sót là điều khó tránh khỏi. Thế nhưng nếu nó có lặp lại nhiều lần vào những thời điểm lộn xộn lại là một vấn đề khác. Trong trường hợp này, có nhiều khả năng bộ nhớ của máy tính bạn đang sử dụng có vấn đề bất ổn. Bộ nhớ lỗi sẽ khiến cho máy tính không ổn định và gặp nhiều lỗi khó xác định. Những lỗi này đôi khi khiến cho bạn trở nên kẻ ngớ ngẩn trước những kĩ thuật viên ở các cửa hàng vì chúng cực khó để tái hiện lại. Trong bài viết này, chúng ta sẽ cùng đề cập tới các triệu chứng thường gặp của bộ nhớ bị lỗi cũng như tìm hiểu một số phần mềm kiểm tra RAM sẽ giúp bạn rà soát các trục trặc có thể phát sinh.

I – Khi bộ nhớ tốt gặp trục trặc:
Một thanh RAM máy tính bao gồm nhiều chip nhớ Silicon hàn vào một bản mạch. Cấu trúc này khiến cho bộ nhớ có tỉ lệ an toàn cao hơn nhiều so với các linh kiện khác trong PC. Tuy nhiên nó lại là một trong những thành phần được sản xuất với số lượng nhiều và nhanh nhất. Các chip DRAM được kiểm tra trước khi vận chuyển đi. Quy trình này sẽ loại bỏ phần lớn các chip lỗi. Mặc dù vậy, một thanh nhớ tốt có thể chuyển thành lỗi với vô vàn khả năng khác nhau.
Trước tiên cần đề cập tới vấn đề tĩnh điện từ những thao tác lắp ráp hoặc vận hành thiết bị sai quy cách. Bạn nên tránh vuốt ve chó mèo khi đang lắp cặp RAM 1GB đắt tiền mới mua. Tương tư như vậy, xung điện hoặc những bộ nguồn kém chất lượng sẽ "luộc" cặp RAM của bạn nhanh hơn trước khi bạn kịp nhận ra. Ngoài ra, nếu bạn là dân chơi ép xung, thao tác ép điện RAM lên quá cao cũng sẽ làm hỏng

những chủng loại RAM với chip nhớ kém sức chịu đựng.
Lý do thứ hai chính là vấn đề bụi bặm trong máy tính hoặc hơi ẩm trong không khí sẽ gây ra chạm mạch giữa các đoạn mạch gần nhau khiến cho RAM bị hỏng. Những tác động vật lý như rơi, dính nước, nhiệt độ cao cũng có tác động xấu.
Một lý do nữa hiếm xảy ra nhưng bạn cũng nên để ý đó là việc bo mạch chủ của bạn có các khe RAM lỗi. Bất cứ thanh RAM nào tốt khi gắn vào các khe cắm lỗi cũng trở nên bất ổn mặc dù chúng không phải như vậy.
Thật may mắn khi bộ nhớ máy tính hiện đại được sản xuất công nghiệp với số lượng lớn đồng loạt nên có rất ít lỗi từ phía nhà sản xuất so với các sản phẩm linh kiện còn lại. Đại đa số nơi bán đều cung cấp chế độ bảo hành lên tới vài năm. Thậm chí những nhà sản xuất như Corsair, Crucial hay Kingston còn bảo hành trọn đời cho các thanh RAM của họ. Tất nhiên người dùng phải trực tiếp gửi về tận hãng sau thời hạn bảo hành do đại lý đặt ra.
II – Dấu hiệu nhận biết bộ nhớ bị lỗi:
Có hàng trăm, thậm chí hàng ngàn dấu hiệu để người dùng xác định bộ nhớ gặp trục trặc, tuy nhiên chúng ta hãy bắt đầu với nhưng thứ thông dụng nhất:
1. MÀn hình xanh BSOD (Blue Screen of Death) trong khi bạn đang cài hệ điều hành Windows 2000/XP. Đây là dấu hiệu rõ ràng nhất của việc bộ nhớ hoạt động bất bình thường.
2. Trong khi chạy Windows 2000/XP, hệ thống thỉnh thoảng phát sinh lỗi gây sụp ngẫu nhiên hoặc tự nhảy ra BSOD. Chi tiết này đôi khi còn là do quá tải nhiệt nên bạn cần kiểm tra kĩ lưỡng thêm trước khi kết luận.
3. Lỗi trong khi bạn đang sử dụng những ứng dụng đòi hỏi nhiều RAM ví dụ như game 3D, các phép thử nghiệm, dịch mã, photoshop…
4. Hình ảnh trên màn hình bị vỡ, xé… lỗi này đôi khi còn do card đồ họa, bạn nên kiểm tra thêm.
5. Máy tính không khởi động được. Dấu hiệu này đôi khi còn đi kèm thông báo của BIOS về lỗi bộ nhớ với những tiếp bíp dài lặp lại liên tục. Đối với trường hợp này, bạn không thể sử dụng các ứng dụng kiểm tra mà nên yêu cầu có thiết bị chuyên dụng hoặc gửi trả RAM về nơi mua để nhận được chế độ bảo hành thích hợp.
III – Thủ thuật kiểm tra lỗi bộ nhớ:
Trước khi tiến hành chạy bất cứ chương trình kiểm tra nào được nêu ra dưới đây, bạn nên xác định có bao nhiêu thanh nhớ RAM đang được sử dụng trong hệ thống. Nếu bạn đã biết con số này, bạn có thể chuyển thẳng sang bước tiếp theo. Nếu không, bạn mở nắp máy tính rồi xác định vị trí RAM trên bo mạch chủ tương tự như trong hình bên (thường nằm ngay sát CPU). Chú ý không đụng tới những thành phần có dán tem bảo hành. Thật chẳng thích thú chút nào khi vừa phát hiện ra lỗi hệ thống vừa làm mất giá trị bảo hành của máy.
Các chương trình chẩn đoán bao gồm:
- Memtest86+ (www.memtest.org):

Cũng tương tự như Windows Memory Diagnostic được nêu lên ở phía dưới bài viết, Memtest86+ có hai phiên bản một trên đĩa mềm khởi động và một trên CD. Phiên bản mới nhất của chương trình này còn nhận diện được một số thông tin về máy tính ví dụ như số hiệu chipset, chủng loại CPU và tốc độ bộ nhớ. Khả năng cơ bản của Memtest86+ là thực hiện nhiều phép thử ở mức thường lẫn nâng cao với những khoảng thời gian và độ nặng biến đổi liên tục. Điều này giúp cho bộ nhớ trải qua mọi điều kiện làm việc đa dạng tạo khả năng cho lỗi xuất hiện dễ dàng hơn nếu chúng đang tiềm ẩn. Để sử dụng chương trình, bạn tải về một trong hai phiên bản ảnh đĩa mềm hoặc file ISO ảnh đĩa CDROM. Đối với file ảnh đĩa mềm, bạn chỉ việc chạy nó và cho một đĩa mềm trống vào ổ, chương trình sẽ tự động tạo đĩa khởi động. Vời CDROM, các bước phức tạp hơn vì sau khi tải được file ảnh CD về máy, bạn phải sử dụng một trong các chương trình ghi đĩa chuyên dụng ví dụ như Nero Burning ROM hay Easy CD Creator để ghi ra CD trắng dưới dạng đĩa khởi động Boot-CD.
Sau khi xong, bạn khởi động lại máy tính ở chế độ boot từ CD hay đĩa mềm (xác lập trong BIOS bằng cách nhấn phím Del khi có thông báo hiện ra trên màn hình). Memtest sẽ tự động được kích hoạt và kiểm tra bộ nhớ. Các thông tin chi tiết về hệ thống sẽ hiển thị ở góc trái màn hình. Bạn có thể mở menu chức năng thông qua phím C và chọn giữa các menu bằng các con số để thiết lập chế độ kiểm tra phù hợp với nhu cầu của mình. Thông thường phép thử số 5 và số 8 là nặng nề nhất.
- Docmem:
Docmem là một tiện ích của Simmtester và nó đã có mặt trên thị trường từ rất lâu, tuy nhiên đa số được sử dụng trong các cửa hàng máy tính hoặc trung tâm bảo hành. Mặc dù được phân phối miễn phí nhưng để tải Docmem về máy tính của mình, bạn phải thực hiện việc đăng kí tài khoản trên website của hãng tại (www.simmtester.com/PAGE /products/doc/docinfo.asp)
Tương tự như với Memtest, bạn phải cài đặt Docmem lên một đĩa mềm rồi dùng nó để khởi động hệ thống. Chương trình sẽ tiến hành kiểm tra bộ nhớ ở hai chế độ nhanh (Quick Test) hoặc kéo dài thử độ bền (Burn-In), chế độ này chỉ ngừng lại khi có lệnh của bạn. Bất cứ lỗi nhớ nào được phát hiện sẽ hiện lên phía dưới màn hình.
- Windows Memory Diagnostic:
Đây là một công cụ miễn phí của Microsoft với chức năng hoạt động tương tự như Memtest. Nó có hai phiên bản đĩa mềm và đĩa CD ROM, cách cài đặt hoàn toàn giống như Memtest. Tính năng của Windows Memory Diagnostic có phần đơn giản hơn so với hai công cụ trên nhưng vẫn đầy đủ những phép thử cơ bản và nâng cao. Thậm chí đôi khi nó còn có thể báo với bạn chính xác thanh RAM nào bị lỗi (Rất tuyệt phải không nào). Sau khi kích hoạt thành công chương trình, các phép thử sẽ lần lượt được tiến hành. Mỗi khi muốn dừng lại, bạn nhấn phím X. Những lỗi phát sinh sẽ xuất hiện phía dưới màn hình.

IV – Những bước cơ bản khắc phục lỗi:
Một khi bạn đã xác định được rằng hệ thống của mình đang phát sinh lỗi khi kiểm tra bằng những chương trình thử nghiệm ở trên, bước tiếp theo chính là vấn đề phải định vị được nguồn gốc lỗi. Trong trường hợp lỗi nằm ở bộ nhớ, bạn chắc chắn sẽ phải cần tới dịch vụ bảo hành và thay thế nên việc phải xác định đúng thanh nhớ lỗi rất quan trọng.
Nếu chỉ có một thanh RAM trong máy, mọi việc sẽ đơn giản hơn rất nhiều, bạn chỉ cần chạy thêm một hoặc đủ ba ứng dụng đã nêu trên, nếu tất cả chúng đều báo lỗi, bạn hãy tháo RAM và cắm sang khe khác rồi thử lại vì có thể khe cắm RAM trên bo mạch chủ bị lỗi.
Chú ý khi thay khe RAM, bạn phải tắt điện toàn hệ thống (rút dây nguồn là tốt nhất), rồi nhấn công tắc máy vài lần để xả hết điện tích trong bộ nguồn. Sau đó nhấn hai đầu chốt giữ RAM để bật nó ra khỏi khe cắm rồi đặt sang khe khác và nhấn nhẹ nhàng vào vị trí. Nếu làm đúng thì hai chốt giữ sẽ tự động di chuyển vào vị trí khóa. Nếu không, bạn kiểm tra lại xem có đặt thanh RAM vào khe ngược chiều hay không.
Khi đã hoàn thành công việc, bạn hãy bật lại máy và tiếp tục chạy các chương trình thử, nếu lỗi vẫn xảy ra thì có vẻ như thanh RAM của bạn cần phải gửi đi bảo hành rồi đó.
Trong trường hợp hệ thống của bạn có nhiều thanh RAM khác nhau (thường thấy trên các máy tính hiện đại do công nghệ bộ nhớ kênh đôi Dual-Channel yêu cầu tối thiểu hai thanh RAM giống nhau). Việc thử lỗi mất nhiều thời gian hơn do bạn phải tháo toàn bộ RAM rồi thử chi tiết trên từng thành để nhận diện linh kiện có vấn đề. Chú ý nếu tất cả các thanh RAM đều báo lỗi, bạn sẽ cần phải kiểm tra lại cả bo mạch chủ hoặc CPU vì điều này cực kì hiếm khi xảy ra.
Ngoài ra, nếu khi kiểm tra từng thanh bạn không gặp lỗi mà chỉ gặp lỗi khi chạy ở nhiều thanh RAM, bạn nên xem lại các khe cắm RAM hoặc kiểm tra thông số bộ nhớ trong phần Advance Chipset Configurations trong BIOS của máy tính nhằm đảm bảo chúng được thiết lập đúng với chỉ số nhà sản xuất RAM yêu cầu (chi tiết thông số thiết lập nâng cao có thể tham khảo thêm tại www.xtremevn.com).
Dĩ nhiên, bạn có thể tìm được nhiều thiết bị kiểm tra RAM chuyên nghiệp ví dụ như một số sản phẩm của Innoventions. Những thiết bị như vậy ngoài việc báo lỗi còn có thể chỉ rõ chi tiết từng đoạn mạch bị in lỗi trên mỗi thanh nhớ. Tuy vậy, với mức giá hàng ngàn USD, nó phù hợp hơn cho môi trường kinh doanh chuyên nghiệp hơn là người dùng đơn lẻ. Trong điều kiện tài chính tương đối hạn hẹp,

những bước như đã nêu có lẽ vấn là sự lựa chọn hàng đầu để phát hiện lỗi bộ nhớ trên máy tính PC.

Nguyễn Thúc Hoàng Linh
www.xtremevn.com

Giảm tiếng ồn cho máy tính

Thực hiện: Xuân Cường

Bạn có nghĩ những hệ thống máy tính hiện nay tạo ra quá nhiều tiếng ồn không? Dù chúng ta đã bỏ không ít tiền để trang bị những bộ loa chất lượng cao nhằm thưởng thức âm nhạc hay hơn, nhưng âm thanh từ loa cộng với tiếng ồn phát ra từ máy tính làm cho gian phòng trở nên ầm ĩ và hỗn loạn.

Nói chung, máy tính làm việc càng êm ái thì chúng ta càng dễ chịu. Làm cho tiếng ồn của máy tính giảm đến mức chấp nhận được là chuyện dễ dàng và không mấy tốn kém. Bạn không nhất thiết phải làm cho máy tính trở nên hoàn toàn "câm lặng" (thực tế là không có bất kỳ biện pháp nào để thực hiện điều đó), mà chỉ cần làm cho hệ thống vận hành trong im lặng ở mức gọi là "tạm đủ". Bài viết sẽ giúp bạn xác định và di dời các bộ phận là thủ phạm chính gây ra những tiếng ồn khó chịu trong máy tính.

Tiếng ồn và nhiệt độ

Bộ phận phát ra nhiều tiếng ồn nhất trong hệ thống là quạt làm mát và hầu hết mọi máy tính đều được trang bị cùng lúc nhiều thiết bị này. Ví dụ, máy tính Pentium 4 được PC World Mỹ thử nghiệm khi thực hiện bài viết này được trang bị đến bốn quạt làm mát: bộ nguồn cấp điện, CPU, card đồ họa và ở mặt sau thùng máy.

Dĩ nhiên, những chiếc quạt này có chức năng làm mát cho các mạch điện mỏng manh bên trong thùng máy và đó là một nhiệm vụ hết sức quan trọng. Tuy nhiên với những thiết bị phù hợp, bạn có thể vừa bảo vệ máy tính để nhiệt độ không quá nóng vừa vận hành êm ái hơn.

Trước hết bạn cần mua quạt làm mát mới. Loại quạt làm mát với tốc độ quay chậm tuy phát ra ít tiếng ồn nhưng không thể cung cấp nhiều khí mát cho CPU và các bộ phận trong thùng máy. Những loại quạt có kích thước lớn hơn có thể quay chậm hơn nữa nhưng chúng thổi được nhiều không khí mát vào bên trong hơn. Tuy nhiên vì cánh quạt quá to nên có thể không vừa với thùng máy. Một số loại quạt

làm mát đắt tiền (khoảng 20 USD trở lên thay vì chỉ 2 USD như thông thường) có cùng kích thước và tốc độ được thiết kế đặc biệt nhằm giảm thiểu tiếng ồn. Cuối cùng, bạn có thể giảm bớt phụ thuộc vào quạt làm mát bằng cách lắp những phiến tỏa nhiệt hiệu quả cao trên CPU và những nơi khác trong hệ thống.

Để đánh giá nhiệt độ của hệ thống, bạn có thể dùng một chương trình theo dõi nhiệt độ. Thông thường, các máy tính hoặc bo mạch chủ đều đi kèm một chương trình như vậy, hãng sản xuất máy tính cũng có thể cung cấp cho bạn dưới dạng một phần mềm tải về miễn phí từ Internet. Nếu máy tính của bạn không có công cụ này, hãy dùng thử tiện ích Motherboard Monitor miễn phí của Alex Van Kaam (tải về tại www.pcworld.com.vn, ID: 47642; xem hình 1). Chương trình này cho biết nhiệt độ của máy tính và thậm chí đưa ra thông tin cảnh báo khi nhiệt độ trong thùng máy xấp xỉ mức nguy hiểm được bạn thiết lập sẵn. Một phương án khác là dùng tiện ích CPUCool giá 15USD của Podien (tải về bản dùng thử tại find.pcworld.com/48561).

Trước khi mở thùng máy và động đến các bộ phận bên trong, bạn phải nhớ kỹ một số biện pháp an toàn: Rút cáp điện ra khỏi ổ cắm (ở cả hai đầu). Đối với mọi bộ phận không phải là ổ đĩa, bạn để nằm máy tính với bo mạch chủ ở dưới đáy, khi tháo một bộ phận, bạn mở tất cả các vít rồi mới nhấc nó ra. Và khi lắp một bộ phận vào, bạn cắm tất cả các vít, vặn nửa vòng rồi mới vặn chặt. Sau khi xong mọi việc, cắm cáp nguồn và bật điện máy tính, nếu máy hoạt động tốt, bạn hãy tắt điện một lần nữa, tháo cáp điện, đóng thùng máy lại và sau đó mới cắm lại cáp nguồn.

Xác định nguyên nhân gây ồn

Việc thay tất cả các bộ phận gây ồn trong máy tính sẽ lãng phí nhiều thời gian và tiền bạc, cho nên bạn hãy bắt đầu với thiết bị phát ra tiếng ồn lớn nhất. Nếu máy vẫn còn quá ồn, hãy tiếp tục thay bộ phận phát ra tiếng ồn ở mức thứ hai.

Để xác định nguồn gốc tiếng ồn, bạn dùng ống thử Cardboard Tube Test thông dụng. Bằng cách đặt một đầu của ống có gắn loa giấy vào tai, đầu kia đặt gần ổ đĩa, quạt làm mát và các thiết bị khác trong thùng máy, bạn có thể xác dịnh đâu là bộ phận ồn nhất.

Nếu ống thử này không đủ tin cậy, bạn có thể dùng biện pháp Elimination Test: tắt và mở lần lượt các quạt làm mát và ổ đĩa cứng để xem thử thiết bị nào gây ồn nhất (không có gì nguy hiểm khi máy tính với thùng máy được mở hoạt động không có quạt trong vài giây). Để làm "câm" một chiếc quạt làm mát hay một đĩa cứng (bộ

phận gây ồn chủ yếu ngoài quạt), bạn hãy tháo điện cung cấp cho thiết bị đó (phải bảo đảm máy tính đã được ngắt điện trước đó). Quạt làm mát thường được nối điện qua một chân cắm nhỏ (ba lỗ) trên bo mạch chủ; ổ cứng thì dùng đầu nối lớn có bốn chân từ bộ nguồn máy tính. Cắm lại cáp điện của máy tính vào ổ cắm, bật máy lên và chú ý lắng nghe mà không dùng đến ống Cardboard.

Đương nhiên, phương pháp này không thể thực hiện được đối với quạt trên bộ nguồn vì bạn không thể ngắt điện cung cấp cho thiết bị này. Nếu máy tính đã tắt điện nhưng vẫn cắm cáp điện vào ổ cắm, bạn hãy cài một que tăm nhỏ vào giữa các cánh quạt và giữ nó ở đó trong khi bật điện máy tính; nếu máy tính trở nên yên tĩnh thì bạn đã tìm ra thủ phạm.

Bộ nguồn cấp điện thường là thiết bị đầu tiên mà bạn muốn thay, vì quạt làm mát bên trong thiết bị này thường gây ồn nhất trong thùng máy. Hãy tìm một bộ nguồn thay thế mới có công suất ít nhất cũng phải bằng công suất của bộ nguồn đang sử dụng. Tuy nhiên, bạn cần nhớ bộ nguồn công suất lớn có khả năng dự phòng cho việc nâng cấp thiết bị trong tương lai thường có giá cao hơn và phát ra nhiều tiếng ồn hơn so với những bộ nguồn công suất nhỏ.

Bạn có thể dùng bộ nguồn S12-330 của Saesonic có công suất 330 watt (find. pcworld.com/48562; xem hình 2) được bán trên mạng với giá khoảng 60 USD. Với cỡ cánh 120 mm, quạt làm mát này quay chậm hơn và phát ra tiếng ồn nhỏ hơn so với loại quạt có cỡ cánh 80mm phổ biến trong hầu hết các bộ nguồn hiện nay. Thậm chí, sản phẩm này còn cho phép làm chậm tốc độ của quạt làm mát CPU và quạt ở mặt sau thùng máy.

Nếu bộ nguồn Seasonic chưa làm bạn hài lòng, thì thử dùng bộ nguồn Phantom 500 của Antec có công suất 500 Wat (find.pcworld.com /48564). Bộ nguồn này hoạt động tuyệt đối yên tĩnh trong hầu hết thời gian. Tuy nhiên, Phantom 500 có kích thước to, nặng và rất đắt (giá trên mạng khoảng 175 USD). Thân bộ nguồn Phantom đồng thời là bộ phận tản nhiệt và quạt làm mát chỉ hoạt động khi nhiệt độ vượt qua ngưỡng được người dùng định sẵn. Dù vậy, đối với nhiều người, sự im lặng tuyệt đối không tốt bằng khi làm việc với một chút tiếng ồn. Người dùng có thể dễ dàng chấp nhận tiếng ồn nhỏ thường xuyên hơn là lúc ồn lúc không.

Việc lắp đặt bộ nguồn mới cũng không có gì khó khăn. Bạn chỉ cần tháo điện cung cấp cho bo mạch chủ và các ổ đĩa, tháo vít và nhấc bộ nguồn cũ ra. Sau đó, đặt bộ nguồn mới vào, vặn chặt các vít và cắm mọi thứ như cũ. Bộ nguồn Seasonic và Antec có kèm theo hướng dẫn lắp đặt nhưng không phải mọi nhà sản xuất đều có.

Nếu máy tính sử dụng quạt làm mát gắn vào thùng máy (chứ không phải gắn vào CPU, bộ nguồn hay các thiết bị khác) thì bạn có thể thay bằng loại khác ít ồn hơn. Quạt làm mát kích thước 92mm trong máy tính thử nghiệm là bộ phận phát ra nhiều tiếng ồn nhất. Giải pháp tốt nhất là thay thế bằng một quạt lớn hơn, nhưng rất khó vì thùng máy của bạn có nhiều khả năng không có chỗ trống cho quạt kích thước 120 mm. Ngoài ra, việc dùng quạt tốt hơn (và có lẽ quay chậm hơn) sẽ làm giảm tiếng ồn của hệ thống.

Hãng News sản xuất các loại quạt làm mát gắn vào thùng máy không gây ồn với nhiều kích cỡ khác nhau, có giá dưới 20 USD. Các quạt này không có bản hướng dẫn lắp đặt, nhưng việc thay thế chúng khá đơn giản: chỉ cần tháo dây cấp điện cho quạt cũ, tháo quạt, lắp quạt mới vào và cắm lại dây cấp điện. Quạt làm mát Real Silent 92mm của Nexus (find.pcworld.com/58566; xem hình 3) đã làm việc tốt trong hệ thống thử nghiệm của PC World Mỹ. Chỉ còn một bận tâm nhỏ: chương trình theo dõi các thông số trên bo mạch chủ cho thấy quạt này chỉ quay bằng nửa tốc độ của quạt cũ. Tuy nhiên, tốc độ này không làm cho nhiệt độ của máy tính tăng lên.

Hầu hết các ổ đĩa cứng đều không có quạt làm mát nhưng chúng vẫn gây ra nhiều tiếng ồn trong quá trình hoạt động. Tuy nhiên, có nhiều model mới ít gây tiếng ồn vì chúng dùng trục dạng lưu chất thay cho trục bi. Cho nên, nếu bạn cần máy tính hoạt động "êm ái" hơn thì đây là cơ hội tốt để nâng cấp đĩa cứng.

Bọc kín đĩa cứng

Một biện pháp khác, bạn có thể đặt đĩa cứng đang dùng vào trong hộp cách âm lắp vừa vào khoang 5,25 inch (dùng cho ổ CD hoặc DVD) như loại Nexus Drive-A-Way có giá khoảng 60 USD (find.pcworld.com/48568). Nhóm thử nghiệm đã tiến hành lắp đặt thiết bị này với vài trục trặc nhỏ trước khi đọc được hướng dẫn được ghi dưới đáy hộp. Drive-Way đã hoàn toàn triệt tiêu tiếng ồn của đĩa cứng trên máy tính thử nghiệm.

Bộ phận làm mát CPU hiệu quả nhất là phiến tản nhiệt nhỏ cùng với một quạt rẻ tiền nhưng nhiều tiếng ồn. Thêm một ít tiền, bạn có thể mua được loại tốt hơn. Tuy nhiên, việc thay bộ phận làm mát cho CPU không thể thực hiện dễ dàng. Một phần của khó khăn này là kích thước phải tuyệt đối chính xác. Bộ phận làm mát CPU không gây ồn có thể khá kềnh càng, với phiến tản nhiệt giống như các ngôi nhà cao tầng thu nhỏ, được gắn với quạt có kích thước bằng máy nghe đĩa xách tay. Bạn

phải bảo đảm bộ làm mát mới này lắp vừa trên bo mạch chủ và đế cắm CPU (socket). Có thể bạn biết rõ mình có loại bộ vi xử lý nào, nhưng một số CPU có khả năng phù hợp với nhiều loại đế cắm. Hãy tham khảo tài liệu kỹ thuật đi kèm của máy hoặc bo mạch chủ (hay website của hãng sản xuất).

Khi đã tìm được bộ làm mát cần thiết, bạn phải tiến hành lắp đặt. Trước hết phải tháo bỏ bộ làm mát cũ. Nhiều khả năng bộ làm mát cũ được kẹp vào đế cắm bằng những cách mà bạn không thể nhìn thấy bằng mắt và ở những nơi không thể thao tác được bằng tay. Tiếp theo, bạn hãy lau sạch lớp kem dẫn nhiệt cũ trên mặt CPU, rồi bôi một lớp mỏng kem mới (bộ làm mát mới có thể kèm theo ống kem này). Cuối cùng, bạn cài bộ làm mát vào trong các kẹp giữ.

Đối với các bo mạch chủ hỗ trợ socket 478, bạn nên dùng bộ phận làm mát Freezer 4 tương đối gọn của Arctic Cooling (find.pcworld.com/48570; xem hình 4). Mặc dù thiết bị này hoạt động không "êm" bằng một loại kích thước lớn khác, nhưng Freezer 4 có nhiều khả năng lắp vừa trong máy tính thông thường và có giá bán trên mạng vào khoảng 30 USD (Arctic Cooling cũng cung cấp các bộ làm mát dùng cho những dạng đế cắm khác).

Nếu việc thay bộ làm mát CPU trong máy tính làm bạn quá nản lòng, hãy đừng xem xét đến việc thay đổi các quạt làm mát nhỏ được gắn trên card đồ họa. Loại quạt này thường không gây ồn đáng kể, và việc thao tác trên card đồ họa là một việc làm hết sức nguy hiểm.

Chúng tôi cũng khuyên các bạn không nên thực hiện ngăn cách thùng máy. Việc dùng vật liệu cao su xốp gắn bên trong thùng máy để cách âm thường mất nhiều công sức nhưng hiệu quả đạt được lại không đáng kể.

Xuân Cường
PC World Mỹ 10/2005

Tổng hợp về những vấn đề liên quan đến ổ cứng!

Tổng hợp từ Echip.com.vn và PCWorld

Những bí ẩn của ổ đĩa cứng

Giới hạn 32GB của FAT32 trong Windows 2000

Theo lý thuyết, kích thước của phân vùng (partition) đĩa đối với FAT32 trong Windows 2000 là 2 TB (Terrabytes) (xấp xĩ 2000GB). Tuy nhiên, trên thực tế kích thước lớn nhất của một phân vùng (cũng là kích thước của một ổ đĩa logic) khi sử dụng FAT32 là 32GB.

Lưu ý: Khi cố gắng định dạng một phân vùng đĩa FAT32 lớn hơn 32GB, việc định dạng sẽ kết thúc thất bại ở gần cuối quá trình với thông báo lỗi sau đây: Logical Disk Manager: Volume size too big.

Như vậy nếu bạn có một đĩa cứng từ 40GB trở lên bạn nên chia thành nhiều phân vùng, mỗi phân vùng có kích thước tối đa là 32GB, nếu bạn quyết định sử dụng hệ thống tập tin FAT32.

Thiếu sót vùng đĩa trống (Free Space Flaw) của FAT32

Hiện tượng Free Space Flaw (Thiếu sót vùng đĩa trống) là một sơ sót nhỏ đối với hệ thống FAT32, nó làm cho Windows thỉnh thoảng không báo đúng dung lượng đĩa còn trống (ví dụ nó báo chỉ còn vài chục MB đĩa trống, trong khi thực tế là hơn 500 MB), đặc biệt là khi máy tính của bạn bị "treo" hay tắt máy "không đúng thủ tục" (do cúp điện chẳng hạn).

Tình trạng này không có gì nguy hiểm và tất cả những gì bạn cần làm để sửa chữa là chạy tiện ích Scandisk (scandskw.exe trong Windows, scandisk.exe trong DOS). Nên nhớ rằng Scandisk chỉ giải quyết nhất thời, vấn đề này vẫn có thể xảy ra sau đó mỗi khi máy của bạn bị "treo" hay bạn tắt máy không đúng cách.

Lưu ý:

* Windows 95 OSR 2.x và các Windows 9x sau này được cài đặt chế độ tự động chạy Scandisk mỗi khi hệ thống của Bạn bị tắt không đúng "thủ tục".
* Thiếu sót này chỉ ảnh hưởng đến vùng đĩa trống do Windows tính toán chứ không phải là nguồn gốc của việc mất dữ liệu.

DMA

Tương tự như ổ CD (xem bài DMA và những vấn đề liên quan đến ổ CD và CD R/W ở báo e-Chip số 4), khi thiết lập đặc tính hỗ trợ DMA cho ổ đĩa cứng bạn có thể làm cho hệ thống của bạn chạy nhanh hơn nếu hệ thống của bạn đáp ứng được đầy đủ các yêu cầu kỹ thuật (loại chipset trên bo mạch chủ hỗ trợ Bus Mastering DMA, trình điều khiển thiết bị thích hợp, ổ cứng hổ trợ DMA). Ngược lại, bạn

cũng có thể gặp nhiều rắc rối với nó. Có một điều lạc quan là hiện nay hết các bo mạch chủ và ổ cứng có mặt trên thị trường trong thời gian gần đây đều hỗ trợ UDMA.
Ổ đĩa cứng quá nóng

Nói chung khi nhiệt độ trong máy tăng lên quá cao (do quạt thoát nhiệt bị hư hay hệ thống thoát nhiệt không hiệu quả) có thể gây ra nhiều sự cố đau đầu nếu bạn chưa có kinh nghiệm về chuyện này. Riêng về đĩa cứng, nếu nhiệt độ trong môi trường gần nó tăng cao có thể gây ra lỗi khi ghi đĩa (disk write errors). Nếu bạn để ý thấy khi máy mới chạy thì không có gì xảy ra, nhưng khi chạy được một thời gian (khoảng 30 phút) máy bắt đầu báo lỗi thì bạn có thể nghi ngờ hệ thống thoát nhiệt của bạn có vấn đề.

Quạt làm mát

Có một số đĩa cứng được tăng cường làm mát bằng cách gắn thêm quạt ở mặt dưới của đĩa (phần gắn bo mạch). Tuy nhiên, nếu quạt có chất lượng "dỏm" thì sau một thời gian quạt bị trục trặc (chạy chậm, "giật cục" hay không khởi động nổi) và điều này có thể làm ảnh hưởng đến đĩa cứng, thậm chí có thể làm hư đĩa cứng. Nếu bạn cảm thấy máy của bạn đặt ở nơi thoáng mát, hoặc trong phòng lạnh thì bạn có thể không cần sử dụng quạt làm mát này bằng cách ngắt nguồn cấp điện cho quạt hoặc thay bằng một quạt đảm bảo chất lượng cao để bảo vệ ổ đĩa cứng.

Những thông số "biết nói"

Khi m.u.a đĩa cứng thường bạn chỉ quan tâm đến dung lượng đĩa cứng, tốc độ ATA, tốc độ quay (5400, 7200 RPM...) chứ bạn ít khi quan tâm đến những thông số khác. Thực ra, đĩa cứng còn nhiều thông số "biết nói" khác giúp bạn dễ dàng nhận định chất lượng của đĩa cứng hoặc khi nghe quảng cáo về một đĩa cứng mới bạn cũng không cảm thấy "ù ù, cạc cạc".
ĐẶC TRƯNG KỶ THUẬT

TÁC DỤNG

9, 11MS AVERAGE SEEK TIME Truy xuất nhanh (càng nhỏ càng tốt)

AT/IDE INTERFACE Giao diện thông dụng nhất – Tiết kiệm hơn

300,000 / 500,000 HOURS MTBF Tuổi thọ cao, bền

8.33MB/SEC DIRECT MEMORY ACCESS Hiệu suất đĩa và hệ thống được cải thiện

POWER MANAGEMENT FOR GREEN PC Tiêu thụ ít năng lượng

SELF DIAGNOSTICS Xác nhận chất lượng và độ tin cậy của ổ đĩa

SHOCK & VIBRATION Đã kiểm tra hoạt động dưới những điều kiện bất thường (như va đập hay rung động)

HIGHER RPM MOTOR Tăng hiệu suất chung của ổ đĩa

DATA TRANSFER RATE Luồng lưu thông dữ liệu nhanh hơn

AUTO PARKING & LOAD Giảm thiểu nguy cơ làm hỏng đĩa cứng

AUTO REASSIGN DEFECTIVE SECTOR Tính toàn vẹn dữ liệu được nâng cao

BUFFER Tốc độ truyền dẫn dữ liệu được nâng cao

VARIETY OF HIGH CAPACITY DRIVES Cần thiết cho nhiều đối tượng sử dụng cũng như nhiều ứng dụng khác nhau

FORMATTED CAPACITY Ổ đĩa cung cấp thêm nhiều vùng lưu trữ

ENHANCED IDE COMPLIANT/FAST ATA Có khả năng tương thích hoàn toàn

Tối ưu hóa hoạt động của đĩa cứng

Khi các máy vi tính trở nên mạnh mẽ hơn, với các bộ vi xử lý lên đến hàng gigahertz (GHz) và giá RAM giảm nhanh, bạn sẽ nhận thấy rằng hệ thống của bạn vẫn còn bị "ùn tắc" (tức hiệu ứng "nghẹt cổ chai") ngay ở việc truy xuất đĩa cứng. Mặc dù bạn không đủ giàu như... Bill Gate để sắm một dãy đĩa SCSI cao tốc (high-speed SCSI disk arrays) cho máy của bạn, nhưng bạn vẫn có cách tối ưu hóa hoạt động của đĩa cứng, nhờ đó làm tăng khả năng hoạt động của toàn bộ hệ thống. Trong bài này, chúng ta sẽ cùng khảo sát một số cách có thể làm cho ổ cứng đạt được hiệu suất tối đa mà nó có thể cung cấp được.

Các hệ thống tập tin và tính hiệu quả

Windows 2000 hỗ trợ các hệ thống tập tin FAT16 (FAT), FAT32 và NTFS. Có nhiều lý do thuyết phục để sử dụng NTFS trên tất cả các phân vùng đĩa cứng của bạn. Việc mã hoá tập tin (File encryption), nén tập tin, cấp hạn ngạch đĩa (disk quotas), tính bảo mật ở mức độ từng tập tin, và những đặc trưng khác của Windows 2000 đòi hỏi NTFS; Bạn không thể sử dụng các đặc tính này trên các phân vùng được định dạng trong các hệ thống tập tin FAT. Vì NTFS là một hệ thống tập tin mạnh hơn, nó cũng đòi hỏi sự phục vụ nhiều hơn của hệ thống (tức là làm cho hiệu suất của hệ thống giảm đi chút xíu). Tuy nhiên, trong hầu hết các trường hợp, sự khác biệt nhỏ về hiệu suất không đáng kể so với những ưu điểm nó mang lại.

Định dạng so với chuyển đổi

Có một điều mà nhiều người không để ý là bạn có thể tăng hiệu suất hoạt động của đĩa cứng bằng cách tiến hành định dạng sạch trong NTFS. Windows 2000 cho phép bạn chuyển đổi từ một phân vùng FAT hay FAT32 thành NTFS, nhưng một đĩa được chuyển đổi sẽ không "ngon lành" như một đĩa được định dạng ở NTFS ngay từ đầu. Như vậy, nếu bạn phải chọn lựa giữa chuyển đổi và định dạng, bạn có thể cần lưu lại dữ liệu và định dạng phân vùng ở NTFS.

Lời khuyên
Nhớ lưu lại bất kỳ dữ liệu nào trên đĩa FAT/FAT32 trước khi bạn định dạng nó ở NTFS, vì việc định dạng làm cho bạn bị mất tất cả dữ liệu trên phân vùng.

Tinh chỉnh hiệu suất của NTFS

Bằng cách vô hiệu hóa các chức năng và những đặc tính không cần thiết, bạn có thể cải thiện đáng kể hiệu suất của NTFS. Do khả năng tương thích "lùi" (backward compatibility), NTFS tạo ra một tập tin "tám-chấm-ba" (tên tập tin kiểu MS-DOS) song hành với tên tập tin dài mà bạn gán cho một tập tin. Nếu bạn không chia xẽ các tập tin với các hệ điều hành 16-bit (MS-DOS, Windows 3.x) hay các ứng dụng chạy dưới dấu nhắc DOS (như Foxpro for DOS chẳng hạn), bạn không cần đến đặc tính này. Khi vô hiệu hóa việc tạo tự động các tên ngắn sẽ loại trừ "phí tổn" cần để thực hiện nhiệm vụ này và nâng cao hiệu suất. Một đặc tính khác của NTFS có thể cho vô hiệu hóa để cải thiện hiệu suất là tự động cập nhật dấu ngày/giờ (cho biết thời gian truy cập gần đây nhất) khi bạn lướt qua một thư mục. Cả hai sự điều chỉnh nhằm tinh chỉnh hiệu suất đĩa cứng này đòi hỏi bạn phải điều chỉnh Registry. Nhớ luôn luôn thận trọng khi thay đổi trực tiếp đối với Registry.

Lời khuyên

Trên các phân vùng NTFS nhỏ thì ảnh hưởng về hiệu suất do việc tự động cập nhật ngày/giờ truy cập gần đây nhất có thể không đáng kể nhưng trên các phân vùng lớn thì khá đáng kể.

Từ lệnh Run trên trình đơn Start, đánh Regedit hay Regedt32 và truy xuất khóa dưới đây (xem Hình A):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

Hình A

Bạn có thể nâng cao hiệu suất hoạt động của đĩa cứng bằng cách điều chỉnh Registry để vô hiệu hóa các đặc tính NTFS không cần thiết.

Để vô hiệu hóa các tên tập tin ngắn, thay đổi trị của NtfsDisable8dot3NameCreation thành 1. Để vô hiệu hóa việc cập nhật nhãn thời gian truy cập gần đây nhất, thay đổi trị của NtfsDisableLastAccessUpdate thành 1. Nếu mục kiện chưa có sẵn, bạn sẽ phải tạo nó.

Các đĩa động (Dynamic disks)

Windows 2000 hổ trợ việc tạo một kiểu đĩa mới (cách thức truyền thống để tổ chức các đĩa là chia chúng thành các phân vùng, được gọi là một đĩa cơ bản – basic disk), kiểu đĩa mới này, có tên gọi là các đĩa động (dynamic disks), hổ trợ các cấp RAID phần mềm 0, 1, và 5. Các cấp RAID này cung cấp khả năng chịu đựng sai sót (fault tolerance) và cũng có thể làm tăng hiệu suất. Các cấp RAID chịu đựng sai sót (1 và 5) chỉ có sẵn trên Windows 2000 Server, nhưng Windows 2000 Professional cho phép bạn tạo striped volumes trên các đĩa động.

Lời khuyên

Mặc nhiên, các đia được cấu hình như là các đĩa cơ bản. Để chuyển đổi một đĩa cơ bản thành đĩa động, mở Disk Manager (bấm nút phải con chuột trên My Computer,

chọn Manage, và chọn Storage | Disk Management trong khung cửa sổ bên trái). Bấm nút phải chuột trên ổ đĩa trong ô cửa sổ bên phải và chọn Upgrade To Dynamic Disk (trong Windows 2000 Server). Lưu ý là bạn không thể đảo ngược quá trình và "giáng cấp" về đĩa cơ bản mà không làm mất tất cả các dữ liệu trên

đĩa.

Hiệu quả hoạt động của các striped volumes

Các Striped volumes (RAID 0) không có tác dụng gì về mặt chịu đựng sai sót. Mục đích của việc tạo một volum RAID 0 là để nâng cao hiệu suất của đĩa. Một Striped volume rãi dữ liệu xuyên suốt qua hai hay nhiều đĩa cứng vật lý, các đĩa cứng này tạo thành một đĩa trên phương diện logic, theo "sọc" (tức ghi luân phiên các kh?i dữ liệu trên đĩa thứ nhất, đến thứ hai,... rồi lại quay trở lại đĩa thứ nhất và cứ như thế). Thông lượng (hay năng suất chuyển tải dữ liệu) được tăng lên, vì hệ điều hành có thể truy xuất đồng thời cả hai đĩa. Striped volumes cung cấp hiệu suất tốt nhất trong tất cả các loại volums của Windows 2000.

"Đoàn tụ" đĩa cứng

Phân mãnh đĩa là một trong những nguyên nhân phổ biến nhất đối với việc làm suy giảm hiệu suất đĩa cứng. Một đĩa cứng bị phân mãnh khi các tập tin bị xóa và các tập tin mới được ghi lên đĩa, vì các tập tin mới không được lưu trữ trong các liên cung kề cận nhau. Điều này làm tăng thời gian tìm kiếm vì hệ thống phải tìm tất cả các "mãnh" của tập tin đã bị phân chia tứ tán trong các vị trí vật lý khác nhau trên đĩa.

Một công cụ "đoàn tụ" đĩa cứng tái sắp xếp lại dữ liệu trên đĩa sao cho các tập tin được lưu trữ trên các liên cung liền kề nhau. Windows 2000 Professional chứa một công cụ gọi là Disk Defragmenter, truy xuất bằng Computer Management hay thông qua Start | Programs | Accessories | System Tools. Bạn nên sử dụng công cụ Disk Defragmenter để phân tích các đĩa cứng của bạn thường xuyên (như mô tả trong Hình B) và "đoàn tụ" khi cần thiết. Điều này có thể làm tăng tốc độ truy cập đĩa đáng kể.

Hình B

Bạn nên phân tích đĩa thường xuyên và "đoàn tụ" khi cần.

Kết luận

Hiện tượng thắt cổ chai ở đĩa cứng là "kẻ tội đồ" đáng nghi nhất khi máy chạy Windows 2000 Professional (kể cả bất kỳ hệ điều hành nào) bị chậm lại. Ta cần phải thực hiện một số thao tác để tối ưu hóa hiệu suất đĩa cứng và tăng tốc độ chung cho cả hệ thống trước khi móc "hầu bao" cho việc nâng cấp phần cứng.

"Bắt mạch đĩa cứng" dùm bạn

Hỏi: Máy của tôi gần đây chạy chậm và hay bị treo máy. Tôi cho chạy ScanDisk với kiểu kiểm tra (Type of test) là Thorough và chọn Automatically fix errors (tự động sửa lỗi) nhưng chỉ chạy được khoảng 10% thì máy bị đứng. Có cách nào để khắc phục không?

Đáp: Khi chạy ScanDisk, chọn kiểu kiểm tra là Throrough và bấm chọn nút Options... Khi xuất hiện khung thoại "Surface Scan Options", chọn "Data area only" và "Do not perform write-testing" (xem hình), rồi bấm OK, bấm Start để bắt đầu kiểm tra đĩa. Nếu đĩa cứng không gặp vấn đề gì quá nghiêm trọng thì hy vọng bạn vượt qua được "cửa ải" này. Nếu kiểm tra thành công, Bạn có thể chạy lại ScanDisk nhưng lần này chọn "System area only" (tất nhiên vẫn chọn "Do not perform write-testing"). Nếu việc kiểm tra lần thứ hai diễn ra suôn sẽ thì bạn thử cho chạy lại ScanDisk lần thứ ba nhưng lần này chọn "System and data areas" và không chọn "Do not perform write-testing".

- Nếu lần kiểm tra thứ ba máy bị treo thì đĩa cứng của bạn có thể gặp vấn đề khi ghi lên đĩa. Có nhiều nguyên nhân như: đĩa cứng có "lỗi" về phần cứng, máy bị virus, trình điều khiển thiết bị đĩa cứng bị hư, có tranh chấp giữa các phần mềm không tương thích, đĩa cứng quá nóng... Trước khi "cầu cứu" chuyên gia, bạn thử thực hiện các bước dưới đây:

- Tắt máy, chờ cho máy nguội khoảng 30 phút.

- Kiểm tra các cáp nguồn và cáp dữ liệu nối với đĩa cứng xem có bị lỏng không. Nếu có thì gắn lại cho chặc.

- Bật máy lại. Nếu máy khởi động vào Windows bình thường, lưu lại tất cả những dữ liệu cần thiết (phòng khi đĩa sắp bị hư thật sự). Đây là bước quan trọng mà bạn nên làm ngay.

- Quét virus.

- Gỡ bỏ bớt những phần mềm mới cài đặt trong thời gian gần đây hay phần mềm mà bạn thấy không cần thiết.

- Nạp lại (từ đĩa kèm theo bo mạch chủ) hay nâng cấp trình điều khiển thiết bị đĩa cứng (download từ web site của hãng sản xuất bo mạch chủ trên internet).

- Nếu tất cả các bước trên cũng không giải quyết được vấn đề, có lẽ bạn phải thực hiện bước sau cùng (dù bạn không hề muốn) là cài lại hệ điều hành Windows (nếu đĩa vẫn còn đọc/ghi bình thường).

Hỏi: Khi chạy bất kỳ ứng dụng nào, tôi để ý thấy khi nó bắt đầu thực hiện tác vụ ghi lên đĩa cứng là xuất hiện thông báo lỗi "Serious Disk Error Writing" (lỗi ghi đĩa nghiêm trọng). Có phải đĩa cứng của tôi sắp bị hư không? Tôi phải xử lý như thế nào đây?

Đáp: Chờ một "xị" (xí), đóng tất cả các chương trình đang chạy khác, thử cho thực hiện lại tác vụ ghi đĩa (bằng cách nhấn nút Retry chẳng hạn). Nếu vẫn không có tác dụng, bạn thử cho chạy chương trình ScanDisk: chọn Windows Start/Programs/Accessories/System Tools/Scandisk. Chọn ổ đĩa cứng, bấm chọn Thorough, và sau đó bấm chọn Start. Nếu Scandisk bị đứng, thử đóng lại và khởi động lại ScanDisk. Nếu Scandisk báo lỗi mà nó có thể khắc phục được, bấm Finish và kiểm tra xem lỗi có được khắc phục không. Nếu Scandisk báo là không thể khắc phục được (có thể do sự cố phần cứng hay hư hỏng vật lý), bạn tắt máy và tháo nắp máy để kiểm tra bên trong. Kiểm tra lại các đầu cáp nốii (gắn chặt nếu cần) đồng thời kiểm tra xem nhiệt độ môi trường. Nếu máy quá nóng, bạn cần chờ khoảng 30 phút đến một tiếng cho máy nguội hẳn sau đó bật máy trở lại. Nếu máy vào được Windows bình thường và không báo lỗi ghi đĩa thì cáp lỏng hay máy quá nóng là nguyên nhân của vấn đề, lúc này bạn nên tranh thủ sao lưu tất cả các dữ liệu cần thiết lên ổ đĩa khác. Nếu lỗi ghi đĩa vẫn tiếp tục xuất hiện và máy cũng không quá nóng thì đĩa cứng của bạn có trục trặc về vật lý, bạn cần liên hệ với nhà cung cấp nếu còn thời gian bảo hành.

Hỏi: Tại sao hệ thống của tôi (chạy Windows 2000) bị treo và hiển thị lỗi 0x00000054 trên một màn hình xanh?

Đáp: Bạn có thể nhận được thông báo lỗi này khi bạn gán một ký tự ổ đĩa cho một phân vùng (partition) đĩa chưa được định dạng. Tuy nhiên, tuỳ thuộc vào cấu hình, máy có thể tự động khởi động lại trước khi bạn có thể phát hiện được vấn đề. Cho dù máy của bạn có khởi động lại hay không, bạn có thể thấy trong bản ghi nhật ký sự cố (event log), phần thông tin về lỗi như sau:

Event Type: Information

Event Source: Save Dump

Event Category: None

Event ID: 1001

Description: The computer has rebooted from a bugcheck.

The bugcheck was: 0x00000054 (0x003612ca, 0xf2688d00, 0x00000000,

0x00000000).

Để giải quyết lỗi này, Bạn thực hiện một trong các động tác sau:

* Sử dụng thành phần Disk Management của Computer Management Microsoft Management Console (MMC) của Windows 2000 để xóa phân vùng chưa được định dạng.
* Sử dụng thành phần Disk Management của Computer Management MMC của Win2K để định dạng phân vùng.
* Sử dụng thành phần Disk Management của Computer Management MMC của Win2K để gỡ bỏ ký tự ổ đĩa.

Để chạy thành phần Disk management của MMC trong Win2K Professional, Bạn dùng chuột bấm chọn các mục theo trình tự như sau (tất nhiên với điều kiện là Bạn

phải đăng ký vào máy bằng tài khoản người dùng có quyền hạn của một local Administrator)

Start \Settings \Control Panel \Administrative Tools \Computer Management \Disk management.

Hỏi: Tại sao tôi nhận được các lỗi về bộ nhớ hay vùng đĩa trống (storage space) sau khi cài đặt phần mềm mới?

Đáp: Windows XP, Windows 2000, và Windows NT đều có một trị IRPStackSize kiểm soát việc có bao nhiêu dung lượng RAM và dung lượng đĩa cứng vật lý còn trống đối với các ứng dụng mới, nhưng một số phần mềm mới cài đặt lại thiết lập trị này không đúng. Trị này trong phạm vi từ 11 đến 20 đối với XP và từ 11 đến 15 đối với Win2K và NT. Nếu Bạn thiết lập trị này nhỏ hơn 11, Bạn sẽ nhận được một thông báo lỗi cho biết rằng hệ thống không có đủ vùng lưu trữ trống trên máy chủ (hoặc máy đóng vai trò máy chủ trong một tác vụ chủ/khách nào đó). Kết quả là các máy trạm (clients) sẽ không thể truy cập các tài nguyên dùng chung trên mạng và mã biến cố (Event ID) 2011 sẽ xuất hiện trong bản nhật ký hệ thống (System log).

Để thiết lập IRPStackSize trở lại trị mặc nhiên (15 đối với XP, 11 đối với NT), Bạn thực hiện các bước sau:

1. Khơi động registry editor (tức là regedit.exe).
2. Duyệt đến mục khóa HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters.
3. Bấm kép IRPStackSize (hoặc nếu mục này chưa có, tạo mới mục dữ liệu IRPStackSize (nhớ đúng chử in và chử thường) có kiểu là DWORD.
4. Thay đổi base về decimal, thiết lập trị 11 đối với Win2K hay NT hay 15 đối với XP, và bấm OK.

Khởi động lại máy tính.

Hỏi: Tại sao khi cài đặt Windows 2000 hệ thống bị treo với một lỗi “0x0000001E

exception error”?

Đáp: Nếu máy tính của bạn sử dụng một bo mạch chủ với chipset VIA MVP3 và một ổ cứng Ultra ATA/100, Win2K có thể treo với lỗi mà bạn đề cập. Nói chung, những bo mạch chủ này không hỗ trợ UDMA 100 mà các đĩa cứng có đặc trưng kỹ thuật ATA/100 yêu cầu (những bo mạch chủ này thường chỉ hỗ trợ UDMA 33 hay UDMA 33/66). Rõ ràng là ổ đĩa không báo cho hệ thống biết về khả năng tương thích lùi (backward compatibility), và vì quá trình cài đặt Win2K lại chú ý rất kỹ về phần cứng, hệ thống bị treo ở điểm này

Có thể thực hiện 1 trong hai giải pháp sau để khắc phục:

* Nâng cấp BIOS của bạn, nếu việc làm đó sẽ cho phép hệ thống của bạn hỗ trợ ATA/100 (UDMA 100).
* Thực hiện những thay đổi sau đây đối với BIOS của bạn:
1. Vào BIOS và vô hiệu hóa (tắt) UDMA trên kênh IDE nối với đĩa cứng của Bạn (chẳng hạn kênh Primary IDE).

2. Vẫn ở trong BIOS, thiết lập chế độ programmed input/output (PIO) ở Mode 4 thay vì để auto.
3. Cài đặt Win2K. Việc cài đặt sẽ tiếp tục mà không gặp rắc rối gì.
4. Khôi phục lại hai thay đổi đối với BIOS mà bạn đã thực hiện ở bước 1 và 2 trở lại các trị đã có trước đó và xem thử Win2K có còn chạy ổn định không.
5. Nếu Win2K không ổn định, có lẽ cần sẽ cần phải giữ lại 2 thay đổi mà bạn đã thực hiện đối với BIOS nếu như Bạn vẫn sử dụng ổ đĩa đó.

Bạn nên sử dụng ổ đĩa cứng ATA/100 với một bo mạch chủ cũng hỗ trợ ATA/100.

Hỏi: Khi cài đặt Windows 2000 tôi gặp phải lỗi "Windows 2000 could not locate your hard disk". Tại sao xảy ra chuyện này?

Đáp: Có nhiều khả năng Bạn cần phải cài đặt các trình điều khiển thiết bị lưu trữ đệ tam nhân (third party mass storage device drivers) vào lúc bắt đầu quá trình cài đặt bằng cách nhấn phím F6. Bước này sẽ cho phép Bạn mô tả và cài đặt các trình điều khiển SCSI hay UDMA 100/66 do hãng sản xuất cung cấp.

Hỏi: Tôi có một hệ thống dual-boot gồm Windows 98SE và Windows 2000 trên các phân vùng (partitions) riêng biệt. Mọi thứ đều làm việc tốt ngoại trừ một điều là tôi không thể đọc được phân vùng Windows 2000 khi khởi động Windows 98SE. Tại sao vậy?

Đáp: Khi Bạn cài Windows 2000 Bạn đã chọn định dạng phân vùng NTFS. Windows 98SE chỉ đọc được FAT 16 và FAT 32.

"Disk Manager"

DISK MANAGER (DM) là một chương trình chạy ngoài MS-DOS để xử lý ổ cứng, như định dạng, phân vùng,... DM chia ổ đĩa cực kỳ nhanh. Đặc biệt là nó định dạng HDD với dung lượng chính xác nhất và được coi là tối ưu trong chuyện "xử" các gã HDD có dung lượng khổng lồ. Bạn phải dùng DM để tạo đĩa mềm khởi động và cài đặt DM lên đĩa mềm này. Bạn chỉ được sử dụng DM của đúng nhãn hiệu ổ cứng.
Định dạng và phân vùng HDD:

Giai đoạn ban đầu của mỗi DM tuy có thể khác nhau, nhưng phần cơ bản cũng tương tự nhau. Hiện nay, hầu hết các đĩa mềm DM đều tự boot và tự chạy.

Sau những thủ tục ban đầu, bạn chọn chức năng Install HDD. Ở DM của IBM, bạn

phải chọn ngay tác vụ cần thực hiện. Nếu muốn định dạng HDD, bạn nhấn phím số 2 để chọn tác vụ DM.

_ Menu Disk Manager Main Menu có bốn mục:

- (E)asy Disk Installation: Định dạng đơn giản.

- (A)dvanced Options: Các tùy chọn nâng cao.

- (V)iew/Print Online Manual:

Xem và in hướng dẫn sử dụng on-line.

- Exit Disk Manager: Thoát khỏi DM.

Bạn chọn mục 2 (A)dvanced Options để định dạng ổ HDD.

_ Menu Advanced Options gồm bốn mục:

- (A)dvanced Disk Installation: Cài đặt đĩa nâng cao.

- (M)aintenance Options: Các tùy chọn bảo dưỡng.

- (U)pgrade Disk Manager: Nâng cấp DM.

Bạn chọn mục 1 (A)dvanced Disk Installation để cài đặt HDD nâng cao.

_ DM nhận diện HDD đang có trong hệ thống của bạn. Chọn Yes để xác nhận. Khi trong máy có tới hai HDD, bạn phải cẩn thận chọn đúng HDD mình muốn "xử".

_ Trên màn hình chọn loại hệ điều hành, bạn chọn loại dự định sử dụng.

Có các tùy chọn:

- Windows 95, 95A, 95 OSR1 (FAT 16)

- Windows 95 OSR2, 98, 98SE, Me, 2000 (FAT 16 or 32)

- Windows NT 3.51 (or earlier)

- Windows NT 4.0 (or later) or OS/2

- DOS/Windows 3.1x (FAT 16)

- Other Operating System

Bạn nên chọn mục 2 Windows 95 OSR2, 98, 98SE, Me, 2000 (FAT 16 or 32) cho nó rộng đường "binh" sau này.

_ DM hỏi bạn có đồng ý cho nó format HDD bằng hệ thống file FAT 32 hay không? Nên chọn Yes.

_ Trên menu Select a Partition Option, bạn chọn một tùy chọn phân vùng (hay gọi là chia partition) mà mình muốn.

_ Nếu muốn để nguyên HDD làm một partition, bạn chọn OPTION (A).

Nếu để DM chia thành bốn partition bằng nhau, bạn chọn OPTION (B).

Còn trong trường hợp muốn phân các vùng có dung lượng khác nhau theo ý mình, bạn chọn OPTION (C).

Xin lưu ý: Khi chia HDD ra càng nhiều vùng, bạn sẽ càng mất nhiều tài nguyên cho chuyện quản lý từng vùng và tốc độ HDD sẽ bị chậm lại. Với các HDD có dung lượng lớn, dứt khoát bạn phải chia vùng để những phần mềm hệ thống cũ chẳng bị "sốc", có thể nhận diện được; đồng thời khi cần xóa phân mảnh (defragment), công cụ này chạy nhẹ hơn và nhanh hơn.

Bạn lần lượt gõ dung lượng từng vùng vào hộp Size of Partition.

Với BestCrypt bạn có thể tạo nhiều ổ đĩa "ảo" trên một ổ đĩa "thực" và chỉ có bạn hay những người được bạn cho phép mới sử dụng được những ổ đĩa ảo này. Thực chất, mỗi ổ đĩa ảo là một file có tên đuôi .jbc (gọi là file container) và nội dung cũa file chính là nội dung đã được mã hoá của ổ đĩa ảo. Bestcrypt hoạt động như một bộ phận của hệ điều hành (tự động mã hoá và giải mã khi đọc/ghi đĩa), bạn chỉ cần nhập đúng mật khẩu để mở file container là bạn có thể làm việc với file này như với một ổ đĩa "thực thụ", thậm chí bạn còn có thể chia sẽ (share) ổ đĩa ảo trên mạng cho mọi người "xài".

Đặc điểm của BestCrypt

- Tương thích hoàn toàn với Windows 95/98/ME/NT/2000/XP

- Có thể di chuyển file container qua một vật trữ tin khác như: ổ rời, ổ quang, ổ mạng (kể cả khi máy tínhtrên mạng không cùng hệ điều hành) mà vẫn truy xuất được bình thường.

- Tự động đóng ổ đĩa ảo nếu không sử dụng sau một thời gian quy định.

- Cho phép người dùng chọn lựa thuật toán mã hoá trong số các thuật toán chuẩn: Blowfish, Twofish, GOST, Rijndael. Ngoài ra BestCrypt còn cho phép "nhúng" thêm các thành phần mã hoá của hãng thứ ba.

- Tự động lưu các thông tin về việc chia sẽ ổ đĩa ảo trong mạng để người dùng khỏi "mắc công" tái lập mỗi khi khởi động lại máy.

1/ Tạo ổ đĩa ảo:

Cho phép tạo ổ đĩa ảo có dung lượng tối thiểu 20Kb và tối đa là 512Gb (NTFS), 4Gb (FAT32), 2Gb (FAT).

- Chạy BestCrypt, mở menu Container/New container. Trong hộp thoại New container, đặt tên cho file container (FileName), chỉ định ổ đĩa chứa file container (Location), chỉ định dung lượng cho ổ đĩa ảo (Size), chọn thuật toán mã hoá (Algorithm), chỉ định ký tự cho ổ đĩa ảo (Mount drive). Bấm nút Creat.

- Trong hộp thoại Enter Password, nhập mật khẩu truy cập ổ đĩa ảo 2 lần (ít nhất là 8 ký tự).

- Bấm phím bất kỳ liên tục cho đến khi nút OK trong hộp thoại Seed value generation có hiệu lực, bấm OK.

- Format ổ đĩa ảo theo FAT, FAT32 hay NTFS.

2/ "Cài/Gỡ" ổ đĩa ảo

- Để sử dụng, bạn cần phải "cài" (mount) ổ đĩa ảo vào hệ thống bằng cách chọn file

container rồi chọn menu Container/Mount (hay bấm phím phải chuột lên file để mở menu rút gọn). Trong hộp thoại Enter Password, chỉ định ký tự ổ đĩa, nhập mật khẩu, chọn Auto Mount để tự động cài ổ đĩa ảo mỗi khi khởi động Windows, chọn Read only (chỉ đọc) nếu không cho phép ghi. Chú ý: Các ổ đĩa ảo mới tạo sẽ tự động được cài vào hệ thống ngay lập tức.

- Để gỡ ổ đĩa ảo, chọn ổ đĩa đang cài rồi chọn menu Container/Dismount.

3/ Thay đổi xác lập

Đối với những ổ đĩa ảo chưa "cài", bạn bấm phím phải chuột vào file container rồi chọn Properties. Trong hộp thoại Change container properties, bạn có thể thay đổi tên và di chuyển file container, thay đổi các mã hoá và mật khẩu, thêm hay bỏ bớt mật khẩu (khi có nhiều người cùng sử dụng file container).

Bạn có thể tải phần mềm và đăng ký key bản quyền tại website http://www.jetico.com hay tìm key trên đĩa CDROM ở các cửa hàng dịch vụ Tin học.

Giải quyết sự cố đĩa cứng

Như thường lệ, khi bật máy tính, thay vì logo Windows quen thuộc, thì hôm nay bạn chẳng nhìn thấy gì cả. Bạn nghĩ, thế là đĩa cứng của mình đi đứt rồi!, và bắt đầu lo lắng, phải làm gì đây?

Cũng giống như viên phi công khi đối mặt với một sự cố nghiêm trọng: dùng cuốn cẩm nang cứu hộ và cố gắng chỉnh từng thứ một.

1. Đừng quá lo lắng: Màn hình trống rỗng hoặc trục trặc trong quá trình khởi động không phải lúc nào cũng do hỏng đĩa cứng. Đĩa cứng hiện nay thường thọ hơn các bộ phận khác của PC, cũng như việc chạy các tiện ích hệ thống không cần thiết hoặc thay và cài đặt lại phần cứng thường.

2. Khởi động lại: Tắt máy tính, chờ 10 giây, và bật máy lại. Động tác này sẽ điều chỉnh lại máy tính - và thông thường thì vậy là đủ để giải quyết trục trặc này.

3. Kiểm tra bên ngoài: Nếu màn hình vẫn trống rỗng, kiểm tra lại tất cả các dây tiếp điện, cáp nối, và các đầu nối để bảo đảm là chúng không bị lỏng. Kiểm tra

thiết bị chống đột biến điện, bảo đảm cầu chì của nó chưa bị đứt hoặc chưa bị hư hỏng. Đồng thời phải kiểm tra lại các núm vặn tương phản và xem độ sáng màn

hình có bị vặn xuống mức thấp nhất không.

4. Lắng nghe tiếng động: Khi PC khởi động bạn phải lắng nghe tiếng quạt chạy ở bộ nguồn cấp điện. Bạn cũng phải nghe thấy tiếng quay của đĩa cứng. Nếu tất cả đều im lặng, có thể nguồn cấp điện bị hỏng hay một chỗ nối điện bị lỏng. Hãy mở nắp hộp máy và kiểm tra để bảo đảm tất cả các dây cáp đều được gắn chắc. Nên nhớ là phải luôn đeo vòng chống tĩnh điện hay có các biện pháp khử tĩnh điện thân thể trước khi chạm vào bất kỳ một bộ phận nào bên trong PC.

Nếu nghe thấy một loạt tiếng bip trước khi hệ thống bị treo, bạn phải ghi nhớ số tiếng bip và các tiếng đó dài hay ngắn. Thông báo lỗi bằng âm thanh này được tạo ra từ BIOS hệ thống và cho bạn biết những thông tin về một trục trặc đã được phát hiện. Tìm nhà sản xuất máy tính để xác định thông báo lỗi đó có nghĩa cụ thể là gì.

5. Tìm các đầu mối: Khi khởi động PC chạy chương trình Power-On Self Test (Kiểm tra khi mở máy) để xác nhận sự hiện diện của các bộ phận phần cứng chủ yếu như chip nhớ, card video và ổ đĩa.

Quan sát kỹ các thông báo lỗi xuất hiện trên màn hình.

Bạn cũng có thể đọc thấy câu xác nhận hoặc thông báo lỗi khi hệ thống khởi động các thiết bị cao cấp hơn như ổ CD-ROM. Tuy vậy, không phải lúc nào cũng cần thông báo lỗi. Nếu hệ thống bị treo trong khi đang thiết lập cấu hình cho một thiết bị ngoại vi thì có khả năng đó chính là thủ phạm.

Nếu hệ thống của bạn khởi động Windows thì ít nhất một phần đĩa của bạn vẫn hoạt động. Windows 95 và 98 vẫn dùng các tập tin DOS autoexec.bat và config.sys để nạp các driver đối với một số bộ phận phần cứng cũ. Nếu PC của bạn bị treo trong lúc nạp driver này, hãy nhấn sau khi thấy Starting Windows 9x. Động tác này cho phép bạn chạy các tập tin đó mỗi lần một dòng để thấy rõ trục trặc xảy ra khi đang nạp thiết bị nào.

- Nếu nhìn thấy thông báo lỗi Boot disk failure hoặc Operating system not found thay vì thông báo Starting windows 9x, thì có nghĩa là PC không nạp được Windows từ đĩa cứng. Có thể đĩa cứng đã bị hỏng nặng.

6. Khởi động từ đĩa mềm. Quá trình này sẽ bỏ qua ổ đĩa cứng và dùng để xác nhận máy tính của bạn vẫn bình thường. Dùng đĩa khởi động Windows kèm theo máy của bạn (nếu không có đĩa khởi động này thì tốt nhất là tạo ra một đĩa như vậy). Cách làm như sau: Đưa đĩa vào ổ đĩa mềm, nhấn Add/Remove Programs trong

Control Panel, chọn Startup Disk và nhấn Create Disk.

Khởi động lại hệ thống bằng đĩa khởi động trong ổ đĩa mềm. Nếu hệ thống khởi động thành công và hiển thị dấu nhắc A:\> có nghĩa là PC của bạn đang hoạt động tốt. Thử truy cập đĩa cứng bằng cách gõ C: và nhấn . Nếu thấy xuất hiện dấu nhắc C:\>, thì chuyển đổi các thư mục và thử chép một tập tin nhỏ vào đĩa mềm.

Nếu thành công, bạn có thể ghi vào đĩa cứng, và đĩa cứng có thể vẫn còn một sức sống nào đó (đôi khi các đĩa cứng chết từ từ). Tận dùng thời cơ để sao lưu các tập tin quan trọng, sau đó chạy một tiện ích chẩn đoán đĩa cứng như ScanDisk hoặc Norton Disk Doctor.

7. Kiểm tra thông số CMOS. Nếu gặp thông báo lỗi Dirve C: not found (hoặc đại khái như vậy), có thể PC của bạn không nhận ra đĩa cứng vì bị mất các thông số thiết lập CMOS. Điều này xảy ra khi pin nuôi CMOS yếu hoặc hỏng. Để khắc phục, vào chương trình setup CMOS: Trong khi PC đang khởi động, nhấn phím hoặc hoặc hoặc bất kỳ phím nào do nhà sản xuất PC quy định (xem tài liệu kỹ thuật kèm theo máy). Nếu không có đĩa cứng nào được liệt kê, bạn phải nhập lại thông số cài đặt đĩa cứng này. Bạn có thể khai báo các thông số một cách thủ công (các thông số này thường được in trên vỏ ổ đĩa cứng), nhưng hầu hết các PC sẽ nhập lại chúng dùm bạn bằng tiện ích tự động lập cấu hình ổ cứng của chương trình cài đặt CMOS.

Nếu đã thực hiện tất cả các bước kể trên mà ổ đĩa cứng của bạn vẫn bị trục trặc thì đã đến lúc phải hỏi các chuyên gia.

Theo PCWorld

ĐỪNG ĐỂ LAPTOP HỎNG DO VÔ TÌNH

Mua được một chiếc laptop ưng ý đã khó mà sử dụng nó thế nào cho đúng cách càng khó hơn. Theo các thông tin từ phòng bảo hành của chính hãng và các trung tâm sửa chữa máy tính xách tay, phần lớn những hư hỏng của laptop là do người dùng vô tình gây nên.
Hư hỏng thường gặp nhất là vấn đề màn hình tinh thể lỏng. Việc hỏng hóc màn hình thường là do người sử dụng dùng các dung dịch lau kính, cồn... đề lau màn hình LCD giống như với màn hình CRT. Màn hình LCD rất khó sửa chữa, còn thay mới lại rất tốt kém.

Khi màn hình bị bẩn, bạn sử dụng các loại giấy mềm và nước sạch để lau. Thấm

vừa đủ ướt, bạn chỉ được lau nhẹ từ trên xuống dưới mà không lau theo hình xoáy tròn, trái qua phải hay phải qua trái. Sau đó, dùng giấy mềm sạch lau nhẹ lại. Chú ý đến động tác phải hết sức nhẹ nhàng, tránh không để nước bắn vào khe màn hình. Khi lau cần tắt nguồn. Đặc biệt, tuyệt đối không được dùng ngón tay ấn vào màn hình, bởi sẽ gây tổn thương cấu trúc màn hình, dẫn tới hư hỏng màn hình.

Pin

Hiện tượng chai pin rất hay gặp ở máy tính xách tay, đúng ra là ở loại pin nạp lại. Đặc biệt hiện tượng này sẽ đến sớm ở những người chủ không biết dùng đúng cách. Nếu hỏng pin trong thời gian bảo hành, bạn nên yêu cầu thay mới vì việc sửa chữa để pin hoạt động tốt như ban đầu gần như là không thể. Không nên bật tắt nhiều lần trong một khoảng thời gian ngắn. Ngoài ra, nên hạn chế việc cắm pin trực tiếp vào lúc máy đang sử dụng tức là bắt pin vừa nạp vừa xả. Bạn cũng nên chú ý thiết bị adapter phải phù hợp với từng dòng máy và loại máy.

Túi xách chuyên dụng

Một phụ kiện nhỏ nhưng không thể thiếu là các túi xách chuyên dụng dành cho laptop. Bạn không cần quan tâm nhiều đến mẫu mã, kiểu dáng mà lưu ý khả năng chịu lực, chống ma sát, tính cơ động và chống thấm nước khi gặp mưa. Trong đó, khả năng giữ cố định máy trong khi di chuyển là điều kiện bạn cần đặc biệt quan tâm. Khi để máy vào túi cũng nên để đúng chiều. Các túi xách cho laptop thường còn có chứa các gói chống ẩm.

Miếng kê máy

Không nên sử dụng các loại khăn trải bàn dạng bông để lót dưới máy vì có thể dẫn đến nóng máy. Nên để máy trên những mặt phẳng cố định, thoáng rộng và cách xa các vật dễ vỡ. Một điểm nữa, sau khi sử dụng bạn nên tắt máy và chờ một lát cho máy nguội rồi mới cho vào túi xách.

Việc để máy lên đùi khi làm việc lâu nhiệt toả ra từ CPU có thể gây bỏng. Nếu cần thiết bạn có thể trang bị thêm cho máy giá đỡ laptop chuyên dụng, tấm cách nhiệt để khỏi bị bỏng.

Không nên mở đĩa bị trầy xước

Với ổ đọc đĩa quang CD/DVD, bạn không nên cho thiết bị đọc các đĩa bị trầy xước quá nhiều lần trong thời gian dài. Đặc biệt không thường xuyên để ổ đọc các loại

đĩa có dán lớp giấy trên bề mặt chứa thông tin vì có thể gây hiện tượng kén đĩa hoặc mắt đọc kém đi.

Mở màn hình một góc 90 hoặc 120 độ

Khi sử dụng laptop, bạn nên đóng mở nhẹ nhàng, tránh gây ra hiện tượng đứt cáp nối giữa mainboard và màn hình. Khuyến cáo của hãng sản xuất là nên mở màn hình ở một góc thích hợp nhất là từ 90 đến 120 độ và không nên đóng mở liên tục nhiều lần trong một thời gian ngắn.

Chuột và bàn phím

Ngoài những vấn đề chính nêu trên bạn cần quan tâm, một số vấn đề tưởng nhỏ như bàn phím và chuột mà không nhỏ chút nào. Mỗi dòng máy đều có thiết kế bàn phím riêng. Vì các phím đều khá mềm nên rất dễ bị hỏng hóc khi có va đập mạnh nên cần cẩn thận khi thao tác với bàn phím. Khi dùng chuột nối ngoài, bạn nên chú ý khoá chức năng di chuột cảm biến touchpad.

Lưu ý: Nếu không thông thạo về phần cứng, khi gặp bất cứ sự cố nào về phần cứng của laptop, tốt nhất bạn nên đem đến các trung tâm sửa chữa, không nên tự ý tháo máy để sửa dẫn đến hư hỏng nặng hơn.

Laptop rơi xuống nước

Sau khi chiếc máy tính xách tay đã bị "vô nước" và không còn hoạt động được, bạn phải tiến hành một số thao tác sau để hy vọng hồi phục lại máy và lấy lại dữ liệu.

1. Tháo pin ra để không “đốt” các thiết bị còn lại bên trong máy.

2. Dốc máy lên để cho nước chảy ra.

3. Tháo máy: lấy ổ quang và bàn phím ra. Điều này có thể hơi khó khăn, bạn nên tham khảo thêm tài liệu hướng dẫn đi kèm máy. Sau khi tháo ra, dùng khăn thấm lau sạch những chỗ còn nước. Theo một chuyên gia kỹ thuật của HP, bạn cũng có thể dùng máy sấy tóc để làm khô nước.

Nước là hiểm hoạ tiềm ẩn đối với máy tính

4. Hãy để khô máy từ 12 đến 24 giờ. Theo chuyên gia của IBM, bạn không nên bật máy lên khi máy chưa hoàn toàn khô.

5. Bật lại máy, nếu máy hoạt động lại được, sao chép mọi dữ liệu quan trọng và gọi điện cho nhà sản xuất, các đại lý hay kênh phân phối chính thức của hãng, vì ngay cả khi máy đã hoạt động lại, rất cần sự kiểm tra của các chuyên gia.

6. Nếu mọi việc vẫn chưa ổn, bạn còn một tùy chọn nữa là nhờ các cơ sở dịch vụ phục hồi dữ liệu từ ổ cứng.

"Luộc" Laptop

Một bạn đồng nghiệp của tôi kể rằng, anh vừa mua một máy tính xách tay (MTXT) dòng Centrino tốc độ xử lý 1.5 Ghz, giá 950 USD. Khi mang đồ nghề cao cấp này khoe với nhiều người, điều ngạc nhiên nhất đối với anh là nhận được quá nhiều khen chê.

Người thì cho là quá đắt, người khác lại nhận xét quá rẻ. Người thì cho rằng pin MTXT mà sử dụng được khoảng 2 giờ là tốt rồi. Nhưng cũng có ý kiến cho rằng với dòng Centrino, pin phải sử dụng được trên 3 giờ... Tôi quyết định đột nhập vào thị trường MTXT và khám phá được nhiều bí ẩn.

"Luộc" phần cứng

Bạn hàng xóm của tôi đang là kỹ thuật viên của một công ty bán máy tính ở khu Tôn Thất Tùng, quận 1- TPHCM khẳng định kinh doanh MTXT hiện nay là siêu lợi nhuận. Bán được một máy tính giá 1.200-1.300 USD, lời khoảng 500 USD - 600 USD là bình thường. Thấy tôi ngạc nhiên, anh bạn giải thích chi tiết: Mỗi MTXT mới mà các công ty VN nhập về hầu hết đều có hai cục pin và hai đồ sạc pin đi kèm. Nhưng khi mua, phần lớn khách hàng chỉ nhận được 1 pin và 1 bộ sạc. Giá thị trường hiện nay pin MTXT mới là 80 USD, bộ sạc là 70 USD. Chỉ đơn giản vậy thôi, nhiều cửa hàng đã kiếm được 150 USD.

Kiếm bộn như vậy vẫn chưa đủ, một số cửa hàng còn "luộc" luôn phần cứng thuộc cấu hình của máy. Thí dụ ổ cứng 80 GB thì thay bằng ổ cứng 40 GB; ổ cứng 40 GB thì giảm còn 20 GB. Tương tự, bộ nhớ 512 MB thì giảm còn 256 MB... Trong khi giá ổ cứng 80 GB hiện nay trên 120 USD, còn ổ cứng 40 GB chỉ có khoảng 75 USD. Ram 512 MB giá bán khoảng 85 USD, còn ram 256 MB chỉ 45 USD. Với cách làm này, nhiều cửa hàng đã kiếm thêm được khoảng 100 USD mỗi máy. Theo nhận xét của một số nhân viên bán máy vi tính, tỉ lệ máy bị "luộc" ổ cứng và ram

không dưới 30%.

“Phù thủy” của pin MTXT

Trong MTXT, pin là bộ phận được khách hàng rất quan tâm vì giá của pin khá cao lại hay bị trục trặc. Vì vậy, nhiều cửa hàng bán MTXT thường chỉ bảo hành pin và màn hình khoảng 6 tháng trong khi các linh kiện khác thì bảo hành đến 1 năm.

Một nhân viên kỹ thuật chuyên về bảo hành tiết lộ pin là lĩnh vực còn quá nhiều bí ẩn. Các cửa hàng hiện phải lệ thuộc vào một người tên T. đang có hai cửa hàng ở TPHCM. T. được mệnh danh là "phù thủy của pin MTXT". Thí dụ, thời hạn bảo hành của pin là 6 tháng nhưng khách hàng sử dụng được 5 tháng 25 ngày thì pin bị trục trặc. Nếu không khắc phục được, nơi bán máy phải đổi cục pin mới cho khách hàng. T. là người chuyên trị các trường hợp này. Chỉ cần mang cục pin đến và cho biết thời gian bảo hành còn bao lâu là T. sẽ làm cho pin "sống lại" qua thời gian bảo hành rồi mới chết, nơi bán máy hoàn thành trách nhiệm bảo hành. Giá mỗi lần phục hồi như vậy chỉ khoảng 100.000 đồng. Nếu kéo dài trên 1 tháng thì cao hơn, khoảng 350.000 đồng.

Cứu pin là mục tiêu mà các nhân viên kỹ thuật máy tính và thợ điện tử chợ Nhật Tảo - TPHCM luôn nhắm đến. Tuy vậy, đến giờ vẫn chưa ai có thể thay T. Các chuyên viên trong lĩnh vực này đều biết, trong pin MTXT có 8 cục pin tương tự pin tiểu nhưng lớn hơn một tí. Loại pin này cũng có bày bán trong chợ Nhật Tảo. Nhưng vấn đề quan trọng là vỏ pin MTXT có chip, bo mạch, phần mềm. Làm sao để khi thay các cục pin nhỏ vào, phần mềm của vỏ pin chấp nhận "sống chung" là điều chưa thấy ai làm được, và đó là bí quyết của T.

Hiện nay không chỉ "cứu" pin, vị "phù thủy" này còn sản xuất cả pin để bán, giá chỉ bằng một nửa so với pin nhập. T. khẳng định pin do anh sản xuất có thể xem hết 1,5 đĩa phim DVD, tương đương khoảng 4 giờ!

Kiểm tra máy bằng cách nào?

Làm sao biết máy mình mua có bị "luộc" hay không? Theo giới chuyên môn trên lĩnh vực này, thông thường nếu là máy mới, hàng hiệu, bao giờ cũng kèm theo máy là phần mềm có bản quyền. Vì vậy, máy mới của các hãng lớn sản xuất mà không có phần mềm hợp pháp thì rất dễ đã bị "luộc" ổ cứng. Giá của một bộ phần mềm hợp pháp lên cả trăm USD. Riêng dòng máy IBM có chức năng kiểm tra phần cứng bằng cách nhấn Thinkpad + F11 thì máy tính sẽ tự kiểm tra. Nếu có phần cứng lạ, máy sẽ báo lỗi. Đối với hàng hiệu, tất cả phần cứng trong máy có cùng số xê ri. Phần cứng nào không cùng số xê ri thì đó là phần cứng đã bị "luộc"...

Tuy nhiên, gần đây, không ít cửa hàng bán MTXT đã đối phó với cách kiểm tra trên bằng việc dán tem bảo hành của cửa hàng mình lên ốc thân máy. Nếu khách

hàng tháo ốc để mở thân máy kiểm tra số xê ri linh kiện bên trong thì tem bảo hành bị rách, nơi bán viện cớ này để từ chối trách nhiệm bảo hành.

MÀN HÌNH BỊ HƯ ?

Theo một số nhà "ngâm kíu" thì máy tính thuộc giống cái vì nó nói không là có, nói có là ...chưa chắc. Màn hình tối thui chưa chắc tại màn hình hư. Theo tôi bịnh của nó có thể do một số nguyên nhân sau:

* Bạn (hay ai đó) đặt độ phân giải màn hình (hoặc tần số refresh) quá cao ngoài tầm của cái monitor. Thí dụ monitor của bạn có độ phân giải lớn nhất là 1024x768. Trong Windows bạn lại đặt là 1280x1024. Triệu chứng: khi màn hình chuyển từ text mode (có độ phân giải thấp) sang graphic mode (có độ phân giải cao) thì màn hình bị chớp, sọc, trôi, hình ảnh chồng lên nhau... Để lâu có thể làm "đứt bóng". Nguyên nhân này ít có khả năng xảy ra vì nếu bạn đặt sai thông số thì màn hình sẽ tịt ngay sau khi bạn set. 15 giây sau Windows sẽ tự động trở về như cũ trừ phi bạn vô tình click trúng nút OK. Cách xử lý: mượn một cái monitor có độ phân giải cao gắn vào, chỉnh độ phân giải xuống mức thấp nhất. Thay trả lại monitor cũ và tăng dần độ phân giải lên đến khi vừa ý.

* Monitor của bạn bị "tai biến mạch máu não, liệt nửa người". Hôm qua còn chạy được độ phân giải cao. Hôm nay chỉ chạy được độ phân giải thấp. Bạn có thể dùng tạm bằng cách đặt độ phân giải thấp xuống trong khi chờ đem ra tiệm sửa. Cách làm giống như trên.

* Bạn không nói rõ "đèn hình tắt" là sao? Là cái màn hình đen thui hay cái đèn nhỏ xíu ở cạnh cái công tắc không sáng? Nếu cái đèn nhỏ không sáng -> không có tín hiệu từ Card màn hình qua monitor, monitor chuyển sang chế độ standby để tiết kiệm điện. -> kiểm tra lại Card màn hình.

* Màn hình tối thui do máy bị treo: Lại phải xét ba trường hợp: (1) Mỗi lần khởi động máy đều bị treo sau một khoảng thời gian cố định: (1a)Windows bị lỗi -> recover hoặc reinstall. (1b) RAM bị "thủng", khi truy cập đến ô nhớ hỏng đó thì bị treo: Vào CMOS chọn Quickboot=Disable để kiểm tra RAM. Nếu máy bạn có nhiều thanh RAM thì gắn từng thanh một để tìm xem thanh nào hư. (2) Lần đầu chạy được 60 giây thì treo, lần sau 30 giây, lần kế 10 giây... -> Máy bị treo do nóng. Kiểm tra lại xem có cái quạt nào không quay không? Gắn thêm quạt thử xem sao. (3) Có khi chạy 1 phút, có khi chạy 2 phút mới treo: có một chỗ nào đó bị lỏng, tiếp xúc không tốt: vệ sinh máy, tháo rời từng bộ phận và lắp lại.

* Đôi khi nguồn điện không đủ cũng gây ra những hiện tượng "kỳ kỳ quái quái". Nếu bạn đang xài qua UPS hoặc ổn áp thì hãy thử bỏ chúng ra xem sao. Có thể UPS/ổn áp của bạn cho ra điện áp chỉ có 200V hoặc thấp hơn. Hoặc thay luôn cái bộ nguồn mới có công suất lớn hơn. Tôi đã từng gặp trường hợp cái máy tính mới ráp chạy hoàn toàn bình thường chỉ trừ một việc là không in được. Mới đầu tôi nghĩ là do cổng USB bị hỏng nên đem ra bảo hành đổi cái mainboard mới. Sau khi test tại chỗ cẩn thận đem về nhà thì vẫn bị y như cũ. Đến khi thay bộ nguồn khác thì mới hết bịnh.

Nói tóm lại mọi hư hỏng của máy tính đều không có nguyên nhân rõ ràng. Không thể chẩn đoán từ xa mà cho ra kết quả chính xác được. Phải nhìn tận mắt, sờ tận tay, nghe tận tai, ngửi tận mũi, thay cái này, thử cái kia... mới biết hư cái gì. Chúc bạn thành công.

Máy tính không nhận được ổ cứng SCSI

Máy tính có ổ cứng SCSI và chưa cài đặt hệ điều hành, tuy nhiên khi thử cài đặt Windows 2000/XP thì hệ thống báo không nhận được ổ cứng. Để giải quyết sai sót này bạn làm như sau:.

Ổ ứng SCSI cần cài driver trước khi sử dụng được nó. Để cài driver cho các thiết bị đặc biệt, bước đầu tiên trong quá trình cài đặt hệ điều hành Windows 2000/XP là trình cài đặt sẽ quét qua máy để kiểm tra thiết bị và cài đặt các driver cơ bản. Lúc đó tại màn hình cài đặt sẽ có dòng: “Press F6 if you need to install a 3rd party SCSI driver”. Bạn nhấn F6 và chờ một lúc cho đến khi nhận được hộp thoại: “Press S to specify” thì nhấn nút S theo yêu cầu.

Tiếp đó bỏ đĩa mềm chứa driver vào ổ đĩa rồi nhấn Enter, tiếp tới lựa chọn driver thích hợp từ danh sách. Nếu bạn chọn đúng driver thì trình cài đặt sẽ đưa ra một thông báo xác nhận rồi quá trình cài đặt sẽ diễn ra bình thường.

(Theo eChip)

Bảo vệ ổ đĩa cứng

Tác giả: **Tạ Xuân Quan**

Nguồn: Thanh Niên Online

Có nhiều loại thiết bị lưu trữ khác nhau như đĩa mềm, CD, DVD, thẻ nhớ hay USB flash driver... Tuy nhiên, đối với máy tính quan trọng hàng đầu vẫn là ổ đĩa

cứng HDD. Càng ngày ổ đĩa cứng có dung lượng càng lớn và giá cả thì có xu hướng rẻ đi.

Cách đây chừng 5 năm phổ biến là các loại ổ đĩa có dung lượng từ 1,2 GB đến tối đa là 10 GB. Bây giờ ổ đĩa cứng có dung lượng 40 GB, 80 GB, thậm chí hàng trăm GB.

Tuy nhiên, cái vô giá chính là dữ liệu chứa trong đĩa cứng. Một ngày không đẹp trời nào đó ổ đĩa bất thình lình "đột tử" trong khi chưa kịp sao lưu dữ liệu thì thật là tai họa. Chính vì vậy, hãy quan tâm đến sức khỏe của thiết bị lưu trữ hết sức quan trọng này để kịp thời ứng phó.

Một chuẩn mực rất quan trọng bắt buộc các nhà sản xuất phải tích hợp trong đĩa cứng để đem lại niềm tin cho người tiêu dùng là S.M.A.R.T (Self-Monitoring Analysis and Reporting Technology - Kỹ thuật tự kiểm tra, phân tích và báo cáo các trục trặc). Khi phát hiện ra các dấu hiệu hư hỏng gần ngưỡng quy định có thể làm ổ đĩa cứng ngừng hoạt động, tính năng này sẽ đưa ra các cảnh báo cho người dùng. S.M.A.R.T được phát triển dựa trên kỹ thuật Predictive Failure Analysis - PFA (phân tích sự cố dự báo trước) của hãng IBM ứng dụng cho các Mainframe Computer (máy tính cỡ lớn dùng trong quân sự và công nghiệp). Còn công ty đầu tiên nghiên cứu kỹ thuật này cho máy tính để bàn là Compaq với tên gọi Drive Failure Prediction (dự báo trước các sự cố cho ổ đĩa). Bạn nên biết hãng IBM đã thử nghiệm trên 3 triệu ổ đĩa cứng khác nhau để có thể đưa ra các chuẩn cho S.M.A.R.T.

Nếu đã kích hoạt tính năng S.M.A.R.T trong mainboard từ BIOS setup, nếu ổ đĩa cứng chuẩn bị hỏng, chúng ta có thể nhận được thông báo có nội dung "HDD Bad, Backup and Replace".

Kỹ thuật S.M.A.R.T

Gồm khoảng 35 đặc tính khác nhau, giúp dò tìm khoảng 70% lỗi trong ổ đĩa cứng. Báo cáo cho người dùng biết thông qua màn hình BIOS hoặc thông qua một phần mềm chẩn đoán. Mỗi hãng sản xuất đĩa tích hợp vào sản phẩm của mình những đặc tính có thể khác nhau. Nhưng mục tiêu cuối cùng là phải dự báo trước được những sự cố nguy hiểm có thể xảy ra, dự đoán gần chính xác thời gian xảy ra để người dùng kịp thời sao lưu dữ liệu dự phòng. Một số đặc tính các hãng sản xuất đĩa cứng thường tích hợp trong kỹ thuật S.M.A.R.T là: ghi nhận nhiệt độ của đĩa cứng, khả năng quay của đĩa cứng, tỷ lệ lỗi thô đã xảy ra, đếm số lần khởi động và tắt máy...

Các phần mềm chẩn đoán

- HDD Health V 2.1: Của tác giả Aleksey S Cherkasskiy, dung lượng 879KB, tham khảo thêm và tải về từ địa chỉ www.panterasoft.com. Phần mềm này phân tích được 15 đặc tính kỹ thuật. Quan trọng nhất là khi bạn bấm vào thẻ Health, nếu khung Known Problems ghi: "There are no problems with this hard drive" là tương đối yên tâm. Nếu thêm khung Overall health status cũng như khung Nearest T.E.C đều ký hiệu N/A thì chắc chắn ổ đĩa cứng của bạn còn rất tốt, không phải lo lắng gì.

- D-Temp: Dung lượng khá bé 144KB, miễn phí, không cần cài đặt chỉ kích chuột là nó chạy với một biểu tượng trên khay hệ thống có ghi nhiệt độ hiện thời của đĩa cứng. Tải về từ địa chỉ http://private.peterlink.ru/tochinov/download.html .

- HDD Thermometer: Giám sát nhiệt độ ổ đĩa cứng, dung lượng 213 KB là một Free Software nhưng không hoàn toàn miễn phí, nó bắt chúng ta phải đăng ký để sử dụng nhưng không phải trả tiền. Nếu chưa đăng ký, mỗi lần chạy chương trình là một lần gặp Nag screen nhắc nhở phải đăng ký (Nag: mè nheo, càu nhàu). Độ tin cậy khi giám sát nhiệt độ khá cao. Chương trình này cũng hiển thị nhiệt độ ổ đĩa cứng trên khay hệ thống. Tác giả Georgy Koychev, tải về từ địa chỉ www.rsdsoft.com .

Bảo vệ và khôi phục dữ liệu trên bộ nhớ Flash

Bạn gặp rắc rối vì mất dữ liệu trên thẻ nhớ USB hoặc trên card Flash và không biết phải làm gì? Khôi phục dữ liệu từ thiết bị nhớ là có thể và không quá phức tạp. Vậy còn chần chừ gì mà không kiếm một phần mềm có thể giúp bạn giải quyết những rắc rối trên.

Thẻ nhớ đã trở nên nhanh hơn nhiều so với những thiết bị nhớ ngoại vi của máy tính trong thời gian gần đây. Những thẻ nhớ 32 hay 64MB của 4 năm trước là món hàng thú vị và khá hiếm thấy một phần vì giá của chúng không hề rẻ. Tuy nhiên cho đến nay việc mỗi người sử dụng máy tính có thể sở hữu nó không còn là chuyện quá xa xỉ. Chúng đã trở nên bình thường và rất đáng tin cậy giống như đĩa mềm và đĩa CD. Thiết bị sử dụng bộ nhớ Flash có một vài ưu điểm chính tốt hơn những chuẩn lưu trữ lưu động khác đó là tính thông dụng lớn. Chúng còn có khả năng chứa đựng và tốc độ truy xuất lớn hơn rất nhiều so với những đĩa mềm lỗi thời, và còn bền hơn đĩa mềm và đĩa CD. Hiện nay trình điều khiển USB được tích hợp trực tiếp vào hệ điều hành Windows và một số khác như Linux, MacOSX, nên đại đa số các thiết bị Flash đều có thể sử dụng như một đĩa cứng nhỏ lưu động, mà

không vướng phải những nhược điểm của ổ cứng lưu động truyền thống như có kích thước lớn hay mỏng mảnh dễ bị trục trặc do hệ thống cơ học. Tuy nhiên,

không có thiết bị nào là hoàn hảo, dù có tất cả những ưu điểm kể trên tuy nhiên ổ USB và những thiết bị ghi nhớ khác như compact flash và card SD cũng có một vài trục trặc và những khó khăn không ngờ tới mà bạn – người dùng cần phải biết cách đề phòng và khắc phục khi vấn đề phát sinh.

1. Bộ nhớ Flash - Có gì đặc biệt ?

Đặc điểm đặc trưng của bộ nhớ Flash chính là tính chất "tĩnh" của nó. Các loại bộ nhớ động truyền thống cần một nguồn cấp điện ổn định về điện thế để lưu trữ được dữ liệu, nhưng các loại bộ nhớ flash không cần điều này. Cũng giống như loại chip nhớ EEPROM thường được sử dụng để lưu thông số BIOS trên bo mạch chủ, bộ nhớ flash cần điện để có thể ghi và đọc dữ liệu nhưng vẫn tiếp tục lưu trữ dữ liệu sau khi nguồn điện bị ngắt. Điều này làm nó trở nên vô giá đối với việc sử dụng những thiết bị lưu động với những ràng buộc nhất định về nguồn điện. Nét đặc trưng này có được nhờ sử dụng các transistor như là một thiết bị lưu trữ dữ liệu. Những transistor ở bên trong bộ nhớ flash có thể được dùng để thay đổi trạng thái (từ giá trị "1" đến giá trị "0" và ngược lại) với nguồn điện chính, nhưng sẽ vẫn tiếp tục trạng thái đó trong khi nguồn điện bị ngắt. Hầu hết những thiết bị bộ nhớ flash hiện nay sử dụng công nghệ NAND – được đặt tên dựa trên trật tự sắp xếp logic của các chip nhớ. Chip Flash NAND nhỏ gọn, bền và có khả năng thực hiện tác vụ đọc/ghi rất nhanh. Một thiết bị nhớ sử dụng công nghệ NAND thường sẽ chứa nhiều chip nhớ, tương tự với hình thức của các module nhớ như RAM hay trên card đồ họa, và mạch điều khiển kết nối giữa bộ nhớ và giao diện điều khiển của nó với những thiết bị khác. Hầu hếu các loại bộ nhớ Flash đều dùng hệ thống tập tin FAT-32 hay FAT-16 tuỳ thuộc vào dung lượng. Card dựa vào thiết bị flash thường sử dụng FAT-16, trong khi thẻ nhớ USB nói chung sử dụng FAT-32. Phần lớn những máy quay kĩ thuật số và các thiết bị khác không thể đọc được thẻ nhớ flash định dạng FAT-32. Bạn có thể sẽ ngạc nhiên khi biết rằng FAT-16 thực chất giống với hệ thống tập tin được sử dụng trên đĩa mềm từ ngày xưa. Do vậy chẳng có gì lạ khi các máy tính thông thường dễ dàng đọc và ghi lên thiết bị flash. Mỗi khi ổ USB làm việc, về cơ bản giống như một đĩa mềm với dung lượng lớn. Giống như tất cả các thiết bị sử dụng định dạng FAT (FAT 32 là hệ thống tập tin thường được sử dụng trên các ổ đĩa cứng), thiết bị flash nhất thiết phải bao gồm Master Boot Record (MBR), rãnh ghi khởi động (Boot Sector - BS) và bảng phân bố tập tin (File Allocation Table - FAT).

Bảng phân bố tập tin chứa một danh sách những file trên thiết bị bộ nhớ flash, kích thước và vị trí của chúng trong bộ nhớ. Mỗi lần thực hiện quy trình đọc ghi từ thiết bị đều phải lấy thông tin và cập nhật cho bảng FAT. Tất cả những gì gây thiệt hại cho FAT sẽ làm hư hỏng trật tự dữ liệu và đây là lý do tại sao hai bản copy lúc nào cũng hiện hữu ở những phần khác nhau của thiết bị nhớ.

2. Mối hiểm họa của thiết bị Flash:
Hãy nhìn một cách tổng quan một vài điều khác nhau có thể đi tới sai lầm trầm trọng khi sử dụng thiết bị nhớ flash và với những dữ liệu được lưu trên đó.
a. Người dùng:
Chẳng có gì ngạc nhiên khi yếu tố thường gặp nhất gây ra việc mất dữ liệu trên thiết bị nhớ Flash chính là con người. Bất kể em bé 3 tuổi của bạn đang nghịch ngợm với bàn phím máy tính hay bạn đang mơ màng lúc 3h sáng đều có thể dọn sạch nội dung của một thẻ nhớ Flash trong chớp mắt. Tuy nhiên vấn đề này dễ khắc phục nếu phát hiện kịp thời vì nếu phần đĩa chứa các file mới xóa chưa bị ghi đè lên thì cơ hội phục hồi bằng một vài phần mềm chuyên dụng rất lớn.

b. Safely Remove Hardware:
Lý do thứ hai xuất phát từ hệ điều hành tương thích USB trước đây như Windows 2000. Hệ điều hành bắt ổ lưu động phải dừng hoàn toàn thông qua tác vụ "Safely Remove Hardware" để sau đó không có bất kỳ dữ liệu nào được ghi lên đó nữa thì người dùng mới được phép rút ra. Điều này nảy sinh do thực tế khi dữ liệu được truyền tải lên một thiết bị lưu trữ di động, Windows thường hiển thị một thanh trạng thái mức dữ liệu đã copy, tuy nhiên không phải khi thanh này biến mất thì dữ liệu của bạn đã copy xong. Rắc rối sẽ nảy sinh khi người sử dụng giật thiết bị lưu trữ ra khỏi máy tính mà không sử dụng tuỳ chọn "Safely Remove Hardware". Những file chưa kịp đưa lên sẽ không xuất hiện trong đó hoặc bị lỗi do chưa copy hoàn thiện.

c. Đánh rơi thiết bị:
Thứ đến sau vấn đề vô tình, có nhiều trường hợp mất dữ liệu còn nảy sinh do chính việc người dùng làm mất thiết bị di động. Ngay cả những công cụ tối tân và đắt tiền nhất cũng không thể giúp gì nếu bạn đánh rơi bút lưu trữ USB của mình trên đường đi làm. Trong trường hợp này, việc cứu dữ liệu là không thể, bạn chỉ có thể đảm bảo rằng dữ liệu quan trọng hoặc nhạy cảm trong đó không bị lộ ra ngoài đề phòng trường hợp bị kẻ xấu lợi dụng. Có nhiều thiết bị lưu trữ được cài đặt sẵn chương trình mã hóa dữ liệu cho phép người dùng tự thiết lập hệ thống bảo vệ cho riêng mình. Những tên tuổi lớn như Corsair, Kingston, Crucial, Sandisk đều tặng kèm miễn phí tiện ích bảo mật khi khách hàng mua sản phẩm của họ trong khi nhưng nhà sản xuất nhỏ hơn thường bỏ qua chi tiết này.

d. Dữ liệu bị hư hại:
Hầu hết những thiết bị lữu trữ thông tin đều sử dụng một vài chuẩn giao diện hot-plug để kết nối với những thiêt bị điện khác nhau mà chúng hỗ trợ. Hot-plug cho phép cắm vào hoặc rút ra trong khi đang hoạt động mà không sợ bị hỏng hóc hay lỗi phần cứng. USB là thí dụ điển hình nhất của công nghệ này, và cũng quen

thuộc với tất cả mọi người. Vấn đề nằm ở chỗ người dùng thường quen với việc lắp hay tháo bỏ thiết bị nhớ mà không để ý rằng thao tác chuyển dời dữ liệu đã kết thúc hay chưa. Trên thực tế, chẳng có cách nào để làm dữ liệu trong thiết bị lưu trữ lộn tùng phèo lên tốt hơn việc rút nó ra khe cắm khi tác vụ đang được thực hiện. Không giống như hầu hết các chuẩn đĩa cứng, bộ nhớ Flash được sử dụng phổ biến trong nhiều thiết bị khác nhau. Máy quay kĩ thuật số, máy nghe nhạc, đầu DA , đầu DVD và hàng loạt những thiết bị điện tử khác đều có thể sử dụng những công cụ lưu trữ này. Tuy nhiên tính linh động cũng đi kèm với một vài rắc rối:
- Mặc dù toàn bộ các loại bộ nhớ Flash và thiết bị tương thích đều có nhiều đặc tính chung ví dụ như sử dụng bảng FAT để ghi thông tin nhưng cách thực hiện và quy trình thao tác đôi khi lại có điểm khác biệt. Nếu bạn thường xuyên di chuyển thiết bị nhớ của mình trên nhiều loại máy đọc khác nhau, trục trặc có nhiều khả năng sẽ phát sinh.
- Hệ thống tập tin trên Window XP của bạn rất mạnh, được trang bị tốt để xử lý những rắc rối trong việc đọc, ghi và xoá dữ liệu trên những thẻ nhớ nhỏ. Còn đối với chiếc máy ảnh số 3 năm tuổi thì sao ? Câu trả lời là chưa chắc. Mặc dù nó cho phép thực hiện những thao tác đơn giản ví dụ như ghi ảnh lên thiết bị lưu trữ, xem ảnh hiển thị và cũng có thể xoá chúng khi cần thiết nhưng chúng có thể sẽ không giải quyết tốt với những định dạng file không hỗ trợ hay dữ liệu được thêm vào bằng những thiết bị khác.

e. Tuổi thọ và ăn mòn:
Như đã đề cập ở trên, bộ nhớ flash cũng có mặt hạn chế trong việc xoá và ghi quay vòng. Một khối bộ nhớ NAND chỉ có thể ghi và xoá một số lần hữu hạn trước khi hoàn toàn mất khả năng cất giữ thêm dữ liệu. Đối với những thiết bị hiện đại, con số này có thể lên tới hàng triệu lần thao tác và tuổi thọ dài hơn được đảm bảo bằng thuật toán tích hợp sẽ buộc ổ đĩa ghi dữ liệu đều lên các chip với số lần trung bình ngang nhau để tránh một khoảng nhớ nào phải chịu tải quá nhiều. Đây là phương thức khá gần gũi với công nghệ tránh Bad Sector trên đĩa cứng. Ngoài ra, mặc dù các loại ổ đĩa USB và thẻ nhớ thông dụng có thể sử dụng liên tục vài năm, tuy nhiên nếu bạn thường xuyên truy xuất chúng ví dụ như chạy ứng dụng hoặc thậm chí là hệ điều hành thì tuổi thọ sẽ bị rút ngắn lại đáng kể hoặc thậm chí là hư hỏng.
3.Phục hồi dữ liệu đã bị xoá từ Thẻ nhớ Flash:
Một trong những lợi ích từ việc sử dụng FAT cho thiết bị nhớ Flash là làm cho chúng có khả năng tương thích với nhiều chương trình khôi phục dữ liệu được thiết kế để truy tìm những file tình cờ bị xoá nhầm. Phần nhiều những chương trình này hỗ trợ FAT 32 và 16 bởi FAT 32 vẫn được chấp nhận như một chuẩn định dạng phân vùng Windows thông thường. Nếu bạn vô ý xoá mất một file quan trọng trong thiết bị nhớ flash thì cũng không phải quá lo lắng. Cách tốt nhất để tìm lại dữ liệu bị mất là sử dụng một tiện ích cho thao tác không xoá khỏi ổ cứng. Đây là một

tiện ích đơn giản có thể tìm thấy và truy lục dễ dàng những file đã bị xoá từ bất kỳ thiết bị nào hỗ trợ định dạng FAT. Một trong những công cụ tốt nhất là REST2514 (http://www.snapfiles.com/download/dlrestoration.html). Công cụ đơn giản đến kinh ngạc này sẽ rà quét bất kỳ ổ NTFS hay FAT32 nào và tìm lại được danh sách những những file đã bị xoá để từ đó khôi phục lại được chúng. Chúng ta hãy cùng xem qua cách sử dụng:
- Khởi động Restoration:
- Chọn ổ bạn muốn quét trong "Drives" và ấn vào "'search by deleted files":
Danh sách những file bị xoá sẽ hiện ra. Để khôi phục 1 hoặc nhiều file, highlight chúng và ấn ''restore by copying'' sau đó chọn thư mục đến. Lưu ý rằng tên file mà bạn đang tìm có thể sẽ bắt đầu bằng biểu tượng $, vì đây là biểu tượng được hệ điều hành nối thêm vào dữ liệu khi nó bị xoá.Cũng xin lưu ý rằng không như PC inspector, quá trình khôi phục không phân loại những file bị xoá bằng folder, nó đơn giản chỉ để tất cả vào trong một danh sách đơn, điều này sẽ làm việc tìm kiếm của bạn trở nên khó khăn hơn.
Nếu file bạn cần không có trong danh sách, thử search lại với tuỳ chọn ''include used clusters by other files''. Việc này sẽ bao gồm cả những file đã hiện lên trên danh sách trước đó. Chú ý là điều này có thể giúp ích, có thể không vì điều này đồng nghĩa với chuyện file của bạn có thể sẽ bị sửa đổi sai lệch đi hoặc không thể đọc được.
4. Khôi phục dữ liệu từ thiết bị đã bị định dạng lại (Formatted):
Nếu bạn đã format ổ lưu trữ flash của mình và muốn tìm lại nội dung trước đó, bạn sẽ phải cần tới những công cụ mạnh hơn nhiều điển hình như Test Disk miễn phí của CG-Security. Mặc dù việc sử dụng không đơn giản nhưng hiệu quả mang lại rất lớn. Bản thân TestDisk không làm việc tốt trên thiết bị bộ nhớ flash, nhưng điểm tốt là những phiên bản chương trình gần đây đi kèm với một công cụ phần mềm khôi phục có tên gọi PhotoRec.PhotoRec được thiết kế đặc biệt để phục hồi ảnh và những file định dạng khác từ thiết bị nhớ flash.
- Sử dụng CGSecurity PhotoREC
+ Bạn cắm ổ vào máy và đảm bảo nó được nhận diện chính xác. Cài thêm phần mềm hỗ trợ đi kèm nếu cần thiết.
+ Download phiên bản mới nhất của TestDisk từ website của CGSecurity rồi giải nén ra một thư mục trên đĩa cứng. Sau đó bạn mở thư mục con "win" rồi click đúp vào biểu tượng PhotoREC để chạy chương trình.
- Tuy chương trình không có giao diện đồ họa cho người dùng như bạn không cần phải hoang mang vì trên thực tế PhotoREC được xem như là một công cụ dễ sử dụng hơn người anh TestDisk của nó, một phần vì có những tuỳ chọn hữu hiệu hơn.
Màn hình chính sẽ hiển thị danh sách những ổ gắn với hệ thống, bao gồm cả thiết bị nhớ của bạn. Phương pháp dễ dàng nhất để xác định ổ di động là nhìn vào kích

thước của mỗi ổ (dựa theo Megabyte) vì dung lượng ổ di động Flash thường khá nhỏ bé so với đĩa cứng. Thông thường chương trình sẽ hiển thị danh sách những ổ cứng lên đầu tiên.
Tuỳ thuộc vào kiểu dữ liệu bạn muốn khôi phục, bạn có thể sẽ muốn truy cập vào thực đơn "File Options" trước khi tiếp tục. PhotoREC sử dụng tùy chọn mặt định để tìm kiếm rất nhiều định dạng file nhưng các file BMP, MP3, EXE và TXT không thuộc số đó. Nếu bạn muốn phục hồi những file này, mở menu và cuộn xuống phía dưới tới mỗi mục nhập, nhấn spacebar để kích hoạt chúng.
Sau đó, bạn phải chọn ổ cần thiết để bắt đầu quá trình khôi phục bằng cách quay trở lại menu chính và lựa chọn từ danh sách các ổ. Chuyển tới tuỳ chọn "Search" và ấn ENTER để bắt đầu quy trình tìm kiếm các file thất lạc.
Chương trình sẽ bắt đầu tìm toàn bộ các dữ liệu thông tin có trên ổ để xác định sự có mặt của một số dấu hiệu nhận dạng chuẩn file. Tất cả những tập tin thỏa mãn yêu cầu sẽ được chuyển vào một thư mục con trong thư mục chính của PhotoREC. Thư mục con này được đặt là ''recup_dir.1''. Mỗi lần bạn khởi động một quá trình khôi phục mới, chương trình sẽ tạo một thư mục con mới là "'recup_dir.#" với # là số thứ tự tăng dần. Khi quá trình kết thúc, Bạn tìm tới thư mục 'recup_dir.#' bằng Explorer và kiểm tra bất cứ file khôi phục nào. PhotoREC sẽ lên danh sách chúng chỉ đơn giản như là F1, F2, F3.....nhưng định dạng file sẽ hiển thị rõ ràng. Click đúp để mở mỗi file, sau đó Rename và di chuyển những cái nào bạn muốn giữ lại.
5. Cố gắng phục hồi dữ liệu từ một ổ hỏng (Corrupted Drive)
Trong phần này, tỉ lệ thành công của bạn sẽ tùy thuộc vào tình huống hỏng hóc của thiết bị. Nếu hệ thống file bị hỏng do máy ảnh số hoặc một số thiết bị khác thực thi những thao tác sai hoặc đọc không chính xác thẻ nhớ, PhotoRec sẽ rất hữu ích để phục hồi lại dữ liệu của bạn bằng cách lặp lại những bước đã nói trên. Tuy nhiên, nếu khả năng hoạt động của thiết bị trở nên yếu do những hư hại tự nhiên hay hao mòn do sử dụng bình thường gây ra, khả năng khôi phục lại dữ liệu còn phải phụ thuộc hoàn toàn vào phần nào trên bộ nhớ flash bị hỏng. Có một ưu điểm của bộ nhớ Flash là nó không chứa các thành phần cơ học chuyển động nên sẽ không gây thêm thiệt hại khi người dùng cố gắng tìm cách cứu chữa thông tin.
PhotoRec của SGSecurity là thích hợp nhất cho việc khởi đầu mọi cố gắng phục hồi dữ liệu, nhưng nếu thất bại có một vài chương trình khác bạn có thể thử.
Chương trình Smart Recover của PC Inspector (http://www.pcinspector.de/smart_medi...uk/welcome.htm) là một tiện ích miễn phí với giao diện thân thiệp nhưng nó kém linh động so với PhotoRec trong việc khôi phục dữ liệu.

6. Sử dụng mã hoá để bảo vệ dữ liệu:
Như đã đề cập, lý do thường gặp nhất của việc mất dữ liệu trong thiết bị di động Flash chính là do người dùng làm thất lạc chính thiết bị. Những món đồ chơi càng

nhỏ bé, tỉ lệ khả năng mất càng cao. Khi vấn đề xảy ra, sự tiếc nuối dữ liệu và tài sản phần cứng chỉ là một phần nhỏ nếu như số dữ liệu quan trọng đó rơi vào tay kẻ xấu đang muốn gây ảnh hưởng không tốt tới công việc của bạn. Như vậy điều cần quan tâm ở đây là một phương pháp có thể đảm bảo rằng kể cả khi bạn bị mất thiết bị ghi nhớ thì những dữ liệu lưu trên đó sẽ trở nên vô dụng đối với người khác ngoài chủ sở hữu thực sự. Mã hoá file là câu trả lời bạn mong đợi. Hiện nay có nhiều phần mềm miễn phí hoặc mã nguồn mở cho phép mã hóa file sẵn có, tuy nhiên một trong những chương trình thông dụng được yêu thích nhất là AxCrypt của Axantum (http://axcrypt.sourceforge.net/). Chương trình này tự thêm chỉ mục của nó vào menu phím phải chuột, cho phép bạn mã hoá file bằng một cái click đúp. Mật khẩu được sử dụng cho việc mã hoá cũng như giải mã file được tích hợp thẳng vào gói dữ liệu mã hóa nên khi cần giải mã, bạn cũng không cần thiết phải cài đặt AxCrypt mà chỉ cần thực thi file mã hóa là được. Nếu bạn đang phải lo lắng về những hư hại xảy ra với dữ liệu do vô tình, AxCrypt là một biện pháp cứu chữa nhanh và dễ dàng. Đơn giản chỉ là copy những file vào thiết bị lưu trữ của bạn như bình thường, sau đó highlight tất cả, click chuột phải và mã hoá chúng với password mà bạn lựa chọn mà thôi.
Nhìn chung, bất kể thế nào thì phương châm "phòng hơn tránh" vẫn là giải pháp tối ưu. Thay vì mất mát và cuống cuồng tìm cách khắc phục, hãy tìm nhưng phương án an toàn từ trước như sử dụng các loại túi hay dây đeo chuyên dụng, đảm bảo tỉnh táo trước khi thao tác. Nghiên cứu kĩ tài liệu của các thiết bị đọc thẻ trước khi tiến hành một tác vụ… Đối với những thiết bị chịu nhiều tác động của môi trường ví dụ như USB Flash, bạn nên chọn những loại có khả năng chịu nước, chịu lửa và chịu va đập. Một số sản phẩm như Flash Voyager của Corsair thậm chí còn chịu được vài chục nhát búa mà không hề gặp bất cứ trục trặc nào. Tất cả chúng sẽ làm giảm bớt cho bạn nhiều trục trặc không đáng có. Chúc bạn may mắn.

Nguyễn Thúc Hoàng Linh
TG@ - www.xtremevn.com

Mười sự cố in ấn thường gặp và cách xử lý

Để giúp bạn tránh những sự cố trong khi in ấn, bài viết này sẽ điểm qua một số trường hợp trục trặc thường gặp nhất và hướng khắc phục chúng. Hy vọng qua bài viết này, bạn sẽ sử dụng chiếc máy in, một trong những công cụ không thể thiếu trong công việc thường ngày ở văn phòng, một cách hiệu quả hơn.

1/**Không có gì xuất hiện khi bạn cố in**

Không thể in bất cứ nội dung gì là sự cố in thông thường nhất nhưng cách khắc phục thường cũng đơn giản nhất: Bạn phải kiểm tra để xem dây nguồn của máy in đã được cắm vào ổ điện, máy in đã được bật và nối với máy tính hay chưa (!).

2/**Các lề và các ngắt dòng trên các trang của bạn đều không thích hợp**

Các lề của bạn quá rộng hoặc bạn in trên giấy có kích cỡ không chính xác (rất hay gặp nếu bạn nhận tài liệu từ một người khác). Trong trường hợp này hãy chọn File/Page Setup, nhấn tab Paper trong hộp thoại Page Setup và sau đó xem trong mục Paper Size để biết loại giấy Word sẽ dùng để in tài liệu. Nếu bạn thấy mục Paper Size là "A4 210x297mm" thì đây là một tiêu chuẩn kích cỡ giấy ngoại. Nhấp Cancel trong hộp thoại Page Setup và thực hiện các bước sau đây để giải quyết vấn đề này :

+. Chọn Tools/Options để mở hộp thoại Options.
+. Chọn tab Print.
+. Chọn hộp kiểm Allow A4/Letter Paper Resizing nếu nó chưa được chọn và nhấp OK.
+. In tài liệu của bạn

3. **Bạn gặp sự cố trong việc in một tài liệu dài mà bạn đã chia thành các phần**

Việc in các tài liệu đã được tổ chức thành các phần riêng biệt là điều rắc rối, đặc biệt nếu mỗi phần có sơ đồ đánh số riêng của nó (ví dụ, các trang trong phần thứ nhất của tài liệu – phần mục lục chẳng hạn - không được đánh số). Việc biết trang nào mà bạn đang xem và các trang nào để in có thể là điều khó khăn. Thanh Status cho bạn biết rằng bạn đang ở trang 8 nhưng tiêu đề trên trang 8 lại cho thấy rằng bạn đang ở trang 5 (trang thứ 5 trong phần hai). Vì thế, nếu một tài liệu được tổ chức thành các phần có cách đánh số trang khác nhau, hãy in lần lượt từng phần một.

4. **Các Fonts có diện mạo không thích hợp**

Trước tiên, bạn hãy xem tài liệu từ cửa sổ Print Layout để bạn có thể thấy các font hiển thị như thế nào. Nếu chúng không hiển thị đúng thì có thể tài liệu của bạn chứa các font mà máy in của bạn không hỗ trợ. Hãy thay thế các font này bằng các font TrueType. Những font này có các mẫu tự "TT" kế bên tên của chúng trên menu Font, có đặc điểm là hiển thị giống nhau khi được xem trên màn hình và khi được in ra giấy.

5. **Hình ảnh không được in ra**

Máy tính của bạn có thể thiếu bộ nhớ. Thử tắt máy, khởi động lại máy tính và in lại. Nếu như vậy vẫn không được gì, hãy kiểm tra những khả năng dưới đây :

+ Chọn File/Print và nhấp nút Options trong hộp thoại Print. Trong hộp thoại Print thứ hai, hãy đảm bảo hộp kiểm Drawing Object đã được chọn.
+ Cũng trong hộp thoại Print thứ hai, hãy đánh dấu vào hộp kiểm Draft Output để yêu cầu Word in các tài liệu với ít định dạng hơn. Tùy chọn này dùng để làm việc với các tài liệu trong giai đoạn sửa bản in.

6. **Một trang trống được in tại cuối tài liệu**

Trang trống được in ra bởi vì bạn để lại một vài đoạn trống ở cuối tài liệu. Nhấn CTRL+ END để đi đến cuối tài liệu, nhấp nút Show/Hide để xem các ký hiệu định dạng đoạn ở cuối văn bản và xoá các ký hiệu này.

7. **Header và Footer xuất hiện không chính xác**

Nếu header và footer của bạn không nằm vừa trên trang, không có đủ chỗ trống trong lề dành cho header hay footer hoặc chúng nằm trong phần không in ra của trang. Để tạo nhiều chỗ trống hơn cho các header và footer, hãy chọn File/Page Setup, chọn tab Margin trong hộp thoại Page Setup và phóng to lề trên và lề dưới. Đi đến tab Layout và tăng khoảng cách From Edge để header và foooter không bị đẩy vào phần không in của trang.

8. **Word không cho bạn chọn lệnh File -> Print**

Nếu lệnh File/Print mờ đi trên máy tính của bạn và bạn không thể chọn lệnh này là do máy tính của bạn không biết rằng nó được liên kết với một máy in. Hãy cài đặt lại máy in.

9. **Bạn không thể in các đường viền trang**

Hầu hết các máy in không thể in text hay hình ảnh nằm quá gần mép của trang. Theo mặc định, các đường viền nằm gần mép của trang, đây là lý do tại sao máy in của bạn không thể xử lý chúng. Hãy thực hiện các bước sau đây để giải quyết sự cố này :

+. Chọn Format/Borders and Shading. Hộp thoại Borders and Shading xuất hiện

+. Chọn tab Page Boder
+. Nhấp nút Options để mở hộp thoại Borders and Shading Options.
+. Bên dưới Margin, nhập các kích cỡ (tính theo điểm ảnh) lớn hơn vào các hộp Top, Bottom, Left và Right để di chuyển các đường viền hơi ra xa khỏi mép của trang.
+. Nhấp OK hai lần.

10. **Máy in của bạn in quá chậm**

Tốc độ in phụ thuộc vào tốc độ xử lý các yêu cầu in tài liệu. "In ở chế độ nền " nghĩa là Word có thể in các tệp trong khi bạn thực hiện những tác vụ khác - định dạng một tài liệu hay nhập văn bản chẳng hạn. Bằng cách tắt chế độ in nền, bạn yêu cầu Word dành tất cả nguồn tài nguyên của nó vào tác vụ in và kết quả các tài liệu sẽ được in nhanh hơn. Tuy nhiên, điểm bất lợi là bạn không thể thực hiện công việc nào cả trên tài liệu khi nó đang được in ra.

Thực hiện các bước sau nếu bạn muốn tắt cơ chế in trong nền
- Chọn Tools/Options.
- Chọn tab Print trong hộp thoại Options.
- Hủy chọn hộp kiểm Background Printing và nhấp OK.

Một số lời khuyên khi sử dụng máy in để phục vụ cho việc in ấn

- Bạn nên chọn mua chủng loại giấy in theo đúng yêu cầu của sách hướng dẫn đi kèm, không nên mua những giấy in kém chất lượng (như quá mỏng chẳng hạn) vì giấy chất lượng kém dễ bị kẹt trong khi in. Không nên để giấy in trong môi trường ẩm ướt vì như vậy khi in có thể sẽ có các đốm mực trên giấy.
- Luôn cập nhật trình điều khiển (driver) cho máy in từ website của nhà sản xuất để cải thiện hoạt động của máy in như sửa lỗi các sự cố in ấn trong máy và có thêm nhiều tính năng mới.
- Luôn dành thời gian vệ sinh máy in hàng tuần, không để bụi bẩn bám vào máy in hay giấy vụn sót lại trong máy vì nó sẽ dẫn đến hiện tượng kẹt giấy và nhất là bạn phải giữ cho đầu in (printhead) luôn được sạch.

Hy vọng qua bài viết này công việc in ấn của bạn được suôn sẻ và trôi chảy hơn.

Nguyễn Minh Luân – Nguyễn Thị Bích Nhung
(CLB Tin Học NiT – Trường ĐH Công nghiệp TP. Hồ Chí Minh)
Email: luan_nguyenvn@yahoo.com

Tối ưu hình ảnh cho màn hình LCD

Tác giả: Minh Phúc
Theo PCWorld, VietNamNet

Phải dành phần lớn thời gian của mình làm việc trên máy tính, bạn cảm thấy quá mệt mỏi, và không thoải mái khi làm việc với màn hình CRT cũ kĩ. Sở hữu màn hình LCD cho công việc của mình không phải là yêu cầu quá cao bởi giá cả và chủng loại màn hình LCD rất đa dạng, phong phú, phù hợp với mọi yêu cầu của người sử dụng.

Tuy nhiên, để hiệu chỉnh màn hình LCD sao cho thích hợp, tối ưu nhất thì lại hoàn toàn khác biệt so với màn hình CRT, mặc dù những thiết lập cấu hình cũng không có nhiều khác biệt lắm so với CRT. Bài viết này sẽ giúp bạn đọc tối ưu hình ảnh, đạt chất lượng tốt nhất với màn hình LCD.

Cài đặt driver cho card đồ hoạ mới nhất

Trước hết, để đạt chất lượng hình ảnh tốt nhất như mong muốn, một phần rất lớn còn phụ thuộc vào card đồ hoạ và chipset của máy tính. Hãy đảm bảo chắc chắn bạn đã cập nhật trình điều khiển (driver) cho card màn hình mới nhất, đó là cách đơn giản và nhanh nhất để tối ưu chất lượng hình ảnh. Để nâng cấp, hãy tải driver mới nhất về từ trang chủ của nhà sản xuất và thực thi file cài đặt (.exe).

Trong một số trường hợp, bạn cần phải thực hiện cài đặt bằng tay. Trong Windows XP, nhấn chuột phải vào *My Computer*, chọn *Properties*, và chọn *Hardware*, *Device Manager*, và nhấn đúp vào mục "*Display adapters*". Tiếp theo, lựa chọn *Update Driver* trong thẻ *Driver*.

Lưu ý: Một số trình điều khiển yêu cầu khởi động lại PC. Bạn cũng không nên tải các bản beta của những trình điều khiển này. Chúng đang được thử nghiệm và rất có thể gây ra những lỗi không mong muốn.

Đọc văn bản rõ nét hơn với ClearType

Windows XP hỗ trợ công nghệ ClearType cho phép làm phông chữ hiển thị trơn tru và rõ nét hơn đối với các văn bản trên màn hình LCD. Để sử dụng công nghệ này, hãy nhấn *Appearance -> Display Properties -> chọn Effects*, và đánh dấu vào lựa chọn *Use the following method to smooth screen fonts,* nhấn vào *ClearType* từ menu đổ xuống. Nhấn *OK* để hoàn thành.

Cập nhật DirectX mới nhất

DirectX là một công nghệ của Windows nhằm nâng cao khả năng đồ hoạ và âm thanh. Hãy cập nhật phiên bản DirectX mới nhất (DirectX 9.0c). Bạn có thể download dễ dàng phiên bản DirectX mới nhất tại trang chủ của Microsoft. Để biết mình đang sử dụng phiên bản DirectX nào, hãy nhấn *Start->Run,* và gõ **dxdiag** và nhấn *Enter*. Tiếp theo nhấn vào tab *System* để xem phiên bản bạn đang dùng.

Độ phân giải màn hình

Trong màn hình CRT, độ phân giải màn hình là những con số dots, pixel, để biểu thị hình ảnh trên màn hình. Bạn có thể tăng độ phân giải lên cao hơn, hoặc chỉnh xuống thấp tuỳ theo ý mình mà không làm ảnh hưởng tới chất lượng hình ảnh. Tuy nhiên, điều này lại hoàn toàn không đúng với LCD. Màn hình LCD sẽ hiển thị đẹp nhất và đem lại chất lượng cao nhất chỉ với một độ phân giải chuẩn.

Hầu hết các màn hình LCD 15" đều có độ phân giải chuẩn 1024x768, trong khi đó, những màn hình 17" hoặc 19" cho độ phân giải tối ưu là 1280x1024. Khi điều chỉnh độ phân giải chuẩn này sẽ làm giảm chất lượng hình ảnh, kích thước ảnh thay đổi, hoặc dẫn tới méo ảnh, mất pixel... Tuy nhiên, có một ngoại lệ là khi tăng hay giảm độ phân giải chỉ bằng một nửa độ phân giải chuẩn thì chất lượng hình ảnh vẫn khá tốt. Chẳng hạn, độ phân giải nguyên thuỷ là 1600x1200 là khi giảm xuống 800x600 thì chất lượng hình ảnh đạt chất lượng tốt và không bị méo.

Chất lượng màu

Màn hình càng hiển thị được nhiều màu thì độ trung thực của hình ảnh càng cao. Hầu hết PC đều yêu cầu hỗ trợ thiết lập màu cao nhất, thường là chế độ 32 bit màu. Nhưng nếu đang sử dụng đồ hoạ tích hợp thì điều này có thể làm giảm hiệu năng máy tính, hãy giảm lượng màu xuống còn 24 bit hoặc 16 bit để tăng tốc cho hệ thống.

Tần số làm tươi (*Refresh rate*) và thời gian đáp ứng (*response time*)

Màn hình CRT thường bị nhấp nháy, gây mỏi mắt và khó chịu cho người sử dụng, nguyên nhân có thể là do đặt tần số làm tươi quá thấp. Lời khuyên hữu ích cho người sử dụng là nên đặt độ phân giải mà màn hình hỗ trợ tần số làm tươi tối thiểu ở mức 72 Hz để tránh mỏi mắt.

Tuy nhiên, với màn hình LCD, màn hình bị nhấp nháy không phải là vấn đề bởi thiết bị này không làm tươi toàn bộ màn hình mà chỉ thay đổi điểm ảnh. Tần số làm tươi chỉ ở 40 Hz cho tới 60 Hz đối với màn hình LCD cũng đủ tốt. Một vấn đề cần khác cần phải chú ý đối với người sử dụng màn hình LCD mà đặc biệt là các game thủ lại là thời gian đáp ứng của màn hình. Tần số đáp ứng là khoảng thời gian cần thiết để một điểm ảnh cần phải được chuyển từ đen sang trắng và lại chuyển sang đen. Những màn hình LCD cũ thường có thời gian đáp ứng chậm hơn 20 ms nhưng gần đây những màn hình LCD mới có thời gian đáp ứng nhanh hơn rất nhiều, màn hình cao cấp có thời gian đáp ứng là 12 ms hoặc thấp hơn.

Tinh chỉnh bằng các nút điều khiển

Khi sử dụng màn hình LCD hoặc CRT, đừng ngại mò mẫm các nút điều chỉnh của nó. Những thiết lập thích hợp có thể đem lại hình ảnh sắc nét và tuyệt vời hơn rất nhiều so với thiết lập sẵn từ nhà sản xuất.

Màn hình LCD thường dễ dàng điều chỉnh hơn nhiều so với CRT. Rất hiếm khi bạn phải điều chỉnh màn ảnh sang bên trái, bên phải, đi lên hay xuống dưới... giống như CRT. Mặc dù vậy, màn hình LCD cũng hỗ trợ nút bấm hoặc thiết lập tự điều chỉnh vị trí của màn ảnh. Cuối cùng, màn hình LCD thường yêu cầu ít tinh chỉnh màu sắc hay độ tương phản khi lựa chọn ở độ phân giải chuẩn.

Độ sáng và độ tương phản

Thiết lập độ sáng quản lý cường độ sáng của màn hình. Màn hình LCD thường sáng hơn màn hình CRT, vì vậy tăng độ sáng có thể là không cần thiết và đem lại kết quả không mong muốn. Điều chỉnh độ tương phản sử dụng biểu đồ màu xám như các chương trình như DisplayMate để đem lại khả năng thể hiện màu xám tốt nhất. Màn hình LCD thường gây mất những chi tiết tối ở cuối dải màu này.

Sắc thái và độ ấm của màu

Có hai loại nguồn sáng khác nhau là loại nguồn sáng trắng-xanh lạnh và nguồn sáng trắng-đỏ nóng. Hầu hết các màn hình đều đưa ra ít nhất 3 lựa chọn và sắc thái hoặc độ ấm của màu dựa theo nguồn sáng vị trí đặt màn hình. Những thiết lập này

được đặt nhãn là Mode1 , Mode 2, Mode 3 tương ứng với Cao, Trung bình và Thấp. Ngoài ra, các nhà sản xuất thường đặt độ ấm của màu sắc dựa theo độ Kelvin(K). Thông thường thiết lập chuẩn là 9300K hoặc trung tính với 6500K và sắc thái hơi đỏ với 5000K. Rất nhiều loại LCD cho phép người sử dụng tinh chỉnh màu sắc bằng cách cân bằng 3 màu cơ bản đỏ, xanh da trời, và xanh lá cây.

Chuẩn đoán bệnh cho LCD

Màn hình LCD thường dễ duy trì và bảo dưỡng hơn màn hình CRT. Tuy vậy, trước khi mua sắm và sử dụng bạn cần chú ý tới những 2 "căn bệnh" khá phổ biến của LCD:

Màn hình trống

Nếu đèn nguồn vẫn sáng mà lại không hiển thị hình ảnh, hãy kiểm tra kết nối giữa màn hình LCD và PC để kiểm tra chắc chắn rằng màn hình vẫn nhận được tín hiệu video. Nếu cáp tín hiệu video vẫn được cắm cả hai đầu, hãy thử kết nối màn hình khác vào PC để đảm bảo rằng cáp hoặc card đồ hoạ vẫn hoạt động tốt. Nếu màn hình thứ hai hiển thị tốt, rất có thể màn ảnh của LCD đã bị hỏng. Nếu màn hình LCD vẫn còn thời gian đang bảo hành hãy đem ra trung tâm bảo hành.

Điểm chết trên màn hình LCD

Hầu hết các nhà sản xuất màn hình LCD đều không thể cam đoan rằng không có những điểm chết trong các sản phẩm của họ. Những điểm chết này thường gây khó chịu cho người sử dụng nhưng số điểm ảnh chết cho phép của mỗi màn hình là từ 3 cho đến 10 điểm chết. Chính vì vậy, khả năng đổi màn hình mới khi có điểm chết là rất khó khăn. Do đó, trước khi mua màn hình LCD, bạn hãy bật màn hình lên và quan sát thật kĩ xem có điểm chết nào không trước khi mua hàng.

Tự bảo trì máy vi tính

Trong quá trình sử dụng máy vi tính, bạn nên bỏ ra một chút thời gian để chăm sóc nó. Một số thao tác đơn giản có thể giúp máy chạy nhanh và êm hơn, cũng như có thể phòng tránh những hư hỏng

Những việc nên làm thường xuyên là:

- Lau chùi và tra dầu cho quạt: Trong các thiết bị của máy vi tính thì quạt dễ bị đóng bụi và gây tiếng ồn nhất. Để lau chùi, trước tiên bạn phải tháo quạt ra, sau đó

dùng một chổi lông mềm quét sạch bụi xung quanh và trên cánh quạt. Chú ý, bạn không nên dùng khí nén để thổi bụi trên các cánh quạt, vì tốc độ thổi của khí nén có thể làm cánh quạt quay quá tốc độ giới hạn và làm hỏng quạt. Để tra dầu cho quạt thì trước tiên bạn dùng vít hay vật nhọn nào đó tháo nắp nhựa đậy trên quạt (có một số quạt không có nắp này), tiếp theo gỡ miếng bảo vệ ra, sau đó nhỏ duy nhất một giọt dầu vào lỗ chính giữa của quạt, rồi đậy kín lại là xong.

- Làm sạch các bộ phận bên trong: Công việc này nên làm ít nhất hai lần mỗi năm. Đầu tiên, bạn mở thùng máy ra và dùng khí nén để thổi vào các góc khuất của máy trước, sau đó bạn mới thổi tới các phần còn lại, nếu không có dụng cụ thổi khí nén thì bạn có thể dùng chổi lông mềm để lau chùi cũng được, sau đó lấy quạt gió thường để thổi sạch bụi còn bám vào máy. Bạn cũng cần làm sạch bộ phận tản nhiệt của CPU và các bộ tản nhiệt khác. Tháo quạt CPU ra, sau đó lấy khí nén hay chổi lông làm sạch các cánh tản nhiệt, giúp CPU giải nhiệt tốt hơn.

- Đặt máy ở vị trí thoáng mát: Đặt máy vi tính cao hơn mặt đất ít nhất 30 cm và xa tường ở khoảng cách tương tự. Chú ý không nên đặt máy ở góc tường và trong phòng kín vì nó có thể làm không khí trong phòng nóng lên và gây nóng máy! Bạn cũng nên tránh để chó, mèo đến gần máy vì lông của nó có thể bay vào máy tính, quạt, bàn phím...

- Thường xuyên kiểm tra hệ điều hành: Tốt nhất là nên nâng cấp nó lên phiên bản mới nhất, cũng như tải các bản update để vá các lỗ hổng.

- Chạy Defragment cho ổ cứng: Thực hiện thao tác này ít nhất một lần mỗi tháng nhằm sắp xếp lại các dữ liệu trên ổ cứng, giúp máy chạy nhanh hơn. Để chạy Defragment thì bạn vào phần: Start\programs\accessories\system tools\disk defragmenter.

- Loại bỏ các chương trình chạy ở chế độ Startup: Quá nhiều chương trình ở chế độ Startup sẽ làm máy vi tính của bạn chạy chậm trong quá trình khởi động. Để bỏ bớt có hai cách: 1- Bỏ dấu chọn chạy ở chế độ Startup ngay trên chính chương trình đó (nếu có); 2- Vào Start/Run, gõ lệnh là msconfig, tiếp theo nhấn OK. Trong phần này bạn nhấp vào Tab Startup, tiếp theo bỏ dấu chọn các chương trình cần bỏ và nhấn OK là xong.

- Chạy Disk Cleanup: Nên thực hiện thường xuyên nhằm loại bỏ bớt các file không cần thiết để tăng dung lượng trống của ổ cứng, giúp máy tính chạy nhanh hơn. Để chạy nó bạn vào: Start\programs\accessories\system tools\disk cleanup.

- Tìm và loại bỏ Spyware: Có thể dùng chương trình như Spybot Search & Destroy để loại bỏ.

- Quét virus: Nên làm thường xuyên với một số chương trình như Norton Antivirus, Mc Afee, Bkav, D32... đồng thời luôn luôn cập nhật các phiên bản diệt virus mới nhất.

Bạn làm gì khi không vào XP được nữa?

Đây là một tình huống thường gặp nhất cho mọi bạn thích vọc máy, hay cài phần mềm mới, cài game chép từ bạn bè từ đĩa mềm có virus.
Bao gi, ờ bạn cũng nên chuẩn bị sẵn mọi thứ cho thật tốt cho tình huống xấu nhất này. Không biết làm gì hay chưa chuẩn bị sẵn cho chuyện ấy ư ?
Chỉ còn một cách duy nhất nhờ bạn bè rành vi tính hay mang đến tiệm cục CPU tổ chảng giúp mình ư? Nhưng rồi lỡ họ lại quá bận thì sao, làm thế nào bạn làm việc bình thường ngay đây ?
Bạn khao khát tự mình giải quyết sự cố ấy ư? Chỉ cần 1 tí kinh nghiệm và một ít tinh thần chuẩn bị thật tốt là bao cho bạn chỉ cần từ 1-3 phút sau là máy tính của bạn chở vào lại windows dễ dàng như trước thôi. Phải chuẩn bị những thứ gì cho tình huống tệ hại này đây?
I) Chuẩn bị vài công cụ cứu hộ sẵn dành có ngay khi trục trặc dùng được ngay:
1) Đĩa mềm auto bootable (tự khởi động) : Tải file boot98.rar từ Mega là http://www.megaupload.com/?d=UO45ZFK0 . Trích xuất bằngWinRAR 351, ra file boot98.IMA.
Dùng Winimage 80 open, đọc file boot98.IMA sau đó chọn Write to A. Chép vào đĩa mềm các file, giúp nó có tính auto boot.

2) 2) Đĩa Hiren boot CD 7.x (mới là 79) tích hợp ngay cùng với các phần mềm, bán nhiều ở Tôn thấtTùng, Bùi Thị Xuân TP HCM.
3) Cây viết Flash Drive có tính autoboot to DOS bằng HP tools, có chứa sẵn file sysXPfat.com và bootpart.exe .

(Xem lại bài làm cho cây viết USB khởi động được vào DOS)
4) XP của bạn có sẵn DOS thực(xem lại bài Cài Hiren 79 vào ổ cứng để biết cách tạo thêm DOS thực cho XP).
Nhớ trong ổ C cũng lưu sẵn 2 files dành cứu hộ là SysXPfat.com và bootpart.exe

II) Có sẵn đồ nghề, không vào được XP bạn vẫn phục hồi

bạn đã có sẵn dụng cụ cứu hộ loại nào, phải cho nó là phần boot đầu tiên tiên trước ổ cứng
Máy vừa mới khởi động vài giây, ấn ngay nút delete(hay nút khác tuỳ máy) để vào BIOS(CMOS) chọn lại boot 1st device(dụng cụ boot đầu tiên). Tuỳ ý mình là đĩa mềm(Flopy disk), hoặc CD_ROM, hoặc USB-HDD;save lại cấu hình mới chọn. Exit và reboot máy lại .
1) Cứu hộ bằng đĩa mềm: đút đĩa mềm vào ổ làm bằng boot 98IMA, cho boot đi đến dấu nhắc A:\>
a) Đánh lệnh từ đây sysXPfat C: Khi thấy dòng chữ thành công Successful và Congratulations là tốt rồi; cần reboot máy lại là xong, bạn sẽ vào WinXP lại tốt thôi.
b) Có thể thất bại trong 30o/o , bạn lại để đĩa mềm vào, đánh bootpart winnt boot: C:
Reboot máy, cũng vào được XP lại như cũ.
2) Bằng đĩa CD XP cài đặt: hản hữu lắm, bạn mới cần đến đĩa XP cài đặt này, chọn vào repair thay vì install và đánh lệnh F:\I386\winn32.exe /cmdcoms để vào phần Recovery console . (F là tên ổ CDROM có đĩa CD XP).
Đánh lệnh Fixboot C: để chỉnh lại phần boot của C ; vào XP được trở lại như cũ.
3) Nếu C bạn đã có DOS thực, cũng thử cứu hộ bằng 1 trong 2 lệnh sau SysXPfat C: hoặc
bootpart winnt boot: C:
4) Dùng cây viết USB cho boot vào C , USB FD(FD Flash Drive) giờ có tên ổ C ; C có XP cũ đã chuyển qua tên mới D .
Dùng 2 file lưu trữ đã nòi trên cứu hộ, nhằm trở vào lại XP .
II) Đôi lúc làm như thế, bạn vẫn không vào WinXP được là khi ổ C của bạn có nhiều lost links, bad sector nào đó khiến một số file nào đó trong Windows bị corrupted (huỷ hoại, hư). Lúc ấy, bạn muốn vào WinXP lại chỉ còn cách dùng những bản sao lưu ổ C của bạn đã có trước đây như Ghost 80, Drive image 2002 hay True Image 80, chọn vào restore thành công. Reboot máy lại thì bạn mới có WinXP hoạt động bình thường lại thôi.
Nếu không chuẩn bị sẵn các bản sao lưu cho ổ này , bạn chỉ có cách cài lại WinXP từ đầu và các phần mềm khác mất cả ngày, chưa chắc có đủ như trước kia nhất là driver cũ không còn hay sao lưu để dành thì rất mệt đa..

1)
1) Nếu có sẵn Hiren bootCD 79 , bạn để đĩa cứu hộ ấy vào cho boot . Chọn vào Ghost trong Disk clone tools hay True image 80 tuỳ theo bạn có lưu sẵn bản nào tốt dành cho C như gho hay TIB của True image .
Cứ chọn vào ghost hay True Image restore(phục hồi) cho về đúng nơi cũ là C .
Reboot máy lại, là vào XP như cũ.

Trong Hiren mới cũng có True Image 80, chọn vào đấy nếu bạn có sẵn file tib của TI 80 lưu sẵn trong ổ cứng. Phục hồi lại file TIB này lưu sẵn của ổ C , trở lại đúng vào C là xong .
2) Cây viết FD autoboot cũng cứu hộ được khi bạn có lưu sẵn file ghost.exe trong ổ E(giờ thành ra F do USB chiếm tên ổ C)
3) Trường hợp bạn biết làm ra BartPE, XPE, thì cứu hộ còn dễ dàng hơn với chạy Ghost 32 bit, cần với bản lưu qua cổng USB đều quá dễ dàng nhanh sau 2 phút

III) Bạn nên chuẩn bị sẵn các bản sao lưu ổ C như thế nào tốt nhất? Không bao giờ bạn nên sao lưu có 1 bản duy nhất của ổ C trong đĩa CD? Vì sao lại như vậy? CD của VN làm rất dễ hư và trầy đột xuất, nhất là khi bạn để chung trong túi ni lông cả chục đĩa hay để chúng chồng lên nhau.
Một khi đĩa đã trầy, hư như vậy khi đang phục hồi bằng Ghost hay Drive Image 2002 (Image center 56), dù gần xong đến 98o/o hay 99o/o chăng nữa: ổ C của bạn chắc chắn sẽ hư.
Máy bạn cũng hết boot được nữa và bạn cũng hết xài WinXP luôn. Nguy nhất đĩa CD trầy có lưu file pqi của Drive Image hay Image center: Lúc ấy ổ C sẽ mất tên, bạn khoan phục hồi lại vì chắc chắn sẽ nhầm chỗ . Phải vào ngay Partition Magic 805 trong Hiren tạo lại ổ C primary, active.
Phục hồi file pqi khác còn tốt, lúc ấy ổ C mới bình thường lại được
a) Nên chuẩn bị ít nhất là 2 bản Ghost hoặc Drive image(Image center 56) lưu trong 2 đĩa CD và cả trong ổ cứng , tốt nhất là luôn 1 bản nữa trong hộp ổ cứng USB. Lỡ hư đĩa CD này còn cái khác vẫn còn bản CD khác hay trong ổ USB mà restore ngay lại, không gì phải lo lắng.
b) Cần nhớ 1 điểm nữa: bao giờ bạn cũng nên chuyển My Documents(bài v,ở tư liệu, hình ảnh quí của bạn) và các mail(thư từ trong Outlok Express hay Microsoft Outlook) sang ổ E, F trước khi sao lưu để dành bằng các bản Ghost hay Drive image.
Nếu vài tháng hay cả năm bạn mới sao lưu 1 lần thì bản ấy quá cũ, khi phục hồi lại có các thư hoặc tài liệu mới có lưu trong ấy kể như tiêu.
c) Có nên Dùng Ghost 80 , Drive Image 2002 hoặc True Image 80?
Với các bạn chưa rành vi tính nhiều lắm, nên dùng Drive image 2002(hay Image center 56 ở Hiren 79) là an toàn nhất vì có sẵn nút kiểm để chọn thật đúng ổ C phục hồi lại, không bao giờ có chuyện nhầm.
Đối với các bạn quá rành không dùng đến chuột lúc phục hồi, dùng Ghost 82 phục hồi lại không có chuyện gì khó và nhầm.
Trái lại với newbie, Ghost có hình trong DOS tối tăm như ma quỉ, nếu người thích

dùng chuột chọn lại: rất hay chạy lên xuống, dễ chọn nhầm nơi phục hồi nhất là các bạn chưa quen.
Bạn chỉ được phép dùng 4 nút: 1 tabs, 1 enter và 2 nút mũi tên lên xuống thay cho chuột lúc phục hồi bằng Ghost. Chọn sai chỗ phục hồi với ghost là tiêu tùng , máy tính của bạn hết khởi động đấy.
III) Có` nên dùng các phiên bản mới nhất Ghost 90,10 , Drive Image 703 , True Image 80 không?
Lời khuyên với các bạn là không nên dùng 2 anh đầu ? Vì sao? Norton Ghost 90 và Drive image 703 khi cài, phải có thêm Microsoft Frame .NET 2. 0, tốn thêm 70 MB và nó khi sao lưu ngay trong ổ C không biết lọc ra file hoán chuyển của XP là pagefile.sys khá lớn để giảm bớt kích thước file sao lưu ổ C: lên đến lớn vài GB không thể nào để trong một đĩa CD rồi.
Lưu Bản ghost nếu trong nhiều đĩa CD , nguy cơ hư đột xuất ở 1 đĩa nào đó càng lớn hơn. Khi cần phục hồi , bạn phải mua đĩa CD dành riêng phục hồi cho chính Norton Ghost 90 hay Drive image 703, không có đành chịu thua thôi với các file có đuôi v2i, thật đặc biệt của chúng. Symantec không có chuyện chỉ bạn tự mình làm ra đĩa cứu hộ miễn phí, nhằm phục hồi như True Image 80 đâu nhé. Bạn nên dùng True Image 80 là tốt nhất, ngoài chuyện sao lưu thẳng trong ổ C, nó còn thông minh hơn biết loại file

Đang

pagefile.sys của XP .lúc làm việc , nên kích thước file sao lưu dạng tib nhỏ hơn nhiều. Khi cần phục hồi lại(cứu hộ) trong môi trường PE(Preinstallation Environment), mà không phải là DOS trước khi vào lại Windows.
Bao giờ True Image cũng tử tế, sẵn sàng chỉ bạn cách làm 2 đĩa mềm hay đĩa CD miễn phí quá dễ dàng ở giao diện đầu tiên, ngay phần Tools\Create bootable Rescue media.
V) Kết luận: Cứu hộ máy tính của khi không khởi động vào WinXP là chuyện rất dễ xảy ra bất cứ lúc nào bạn không ngờ đến được.
Do vậy, để dành 2 files SysXpfat.com, Bootpart.exe, hay các bản sao lưu ở C bằng ghost, drive image (image center) là chuyện tối cần giúp bạn khỏi cần đến giúp đở của bất cứ ai một khi máy tính bạn trở chứng.
Bao giờ cũng nên nhớ phải có nhiều bản sao lưu bằng gho trong đĩa CD, ổ cứng và cả ổ cứng USB, nếu bạn có được.
Và không bao giờ bạn chỉ có 1 bản duy nhất trong CD, đó là điều tối nguy hiểm, rất dễ phải cài lại từ đầu mọi thứ từ XP tốn rất nhiều thời gian, mất vài ngày vẫn chưa xong..
Dr Hoàng

Chế ngự các phiền toái trong Windows

Thực hiện: Bùi Xuân Toại

Microsoft càng "cải tiến" Windows thì hệ điều hành này ngày càng có nhiều vấn đề. Bài viết giới thiệu 8 thủ thuật có khả năng nhanh chóng khắc phục các sự cố thường xảy ra trong Windows XP và 2000.

HÃY GIỮ TẬP TRUNG

Triệu chứng: Đang mải mê ngồi trước máy tính để làm việc như soạn thảo văn bản, gửi email hay tán gẫu (chat)... và rồi bạn rời bàn làm việc trong ít phút. Khi quay trở lại, bạn nhận ra mình chưa nhập xong các dòng chữ cuối cùng. Hoàn toàn bất ngờ, một cửa sổ hoặc hộp thoại "lạ hoắc" xuất hiện và vài dòng văn bản của bạn được đẩy vào đó hoặc biến mất hoàn toàn.

Các ứng dụng "cướp quyền" điều khiển máy tính có thể đem đến nhiều phiền toái hơn bạn nghĩ, vì sẽ rất mạo hiểm nếu hộp thoại này yêu cầu thực hiện một tác vụ nguy hiểm và người dùng vô tình ấn phím hoặc gõ y ("yes": đồng ý) trước khi nhìn thấy câu hỏi. Bạn cũng có thể bỏ qua nhắc nhở về một lịch công việc quan trọng mà không hề nhận ra.

Cách khắc phục: Hiện tại, không có biện pháp nào có khả năng ngăn ngừa sự cố này, nhưng cách sau có thể giúp bạn duy trì quyền ưu tiên cho các ứng dụng của mình trong Windows XP/2000.

Nếu tình huống trên chưa lần nào xảy ra trong hệ thống của bạn, hãy tải về và cài đặt tiện ích Tweak UI miễn phí của Microsoft (find.pcworld.com/54026). Trong Windows XP, bạn mở Tweak UI (bằng cách nhấn chuột lên biểu tượng của tiện ích này trong trình đơn Start hoặc bằng cách chọn Start.Run, gõ vào lệnh tweakui, và ấn). Sau đó, trong khung cây bên trái, tìm và di chuyển đến mục General.Focus. Trong Windows 2000, bạn nhấn đúp lên biểu tượng Tweak UI trong Control Panel, chọn nhãn General. Với cả hai phiên bản Windows, bạn phải kiểm tra để bảo đảm mục "Prevent applications from stealing focus" đã được đánh dấu chọn (Hình 1). Bạn cũng có thể chỉ định nút ấn trên thanh tác vụ có chớp sáng hay không (và số lần chớp) khi có tiện ích khác chiếm quyền ưu tiên để báo cho bạn biết. Để kết thúc, nhấn OK.

Hình 1: Sử dụng tiện ích Tweak UI để ngăn cản các ứng dụng không được phép xuất hiện.

Ngoài ra, vài thiết lập của Tweak UI sẽ trở lại như cũ khi một chương trình sau đó có thực hiện thay đổi Registry. Để bảo đảm việc cố định quyền ưu tiên cho ứng dụng luôn hiệu quả mỗi khi khởi động Windows, bạn chạy Notepad hoặc một tiện ích soạn thảo văn bản nào đó, sau đó nhập vào nội dung sau:

```
Windows Registry Edition Version 5.00
(dòng trống)

[HKEY_CURRENT_USER\Control Panel\Desktop]

"Foreground LockTimeout"=dword:00030d40
```

Nhập xong, chọn File.Save As và lưu tập tin với tên có phần mở rộng là .reg (ví dụ như focus.reg). Tiếp theo, bạn chọn Start.Programs (hoặc All Programs), nhấn phải chuột vào trình đơn Startup và chọn Open. Trong một vùng trống bất kỳ của thư mục Startup, bạn nhấn phải chuột và chọn New.Shortcut. Trong wizard hướng dẫn Create Shorcut, bạn chọn tập tin .reg được tạo ra ở bước trên rồi nhấn OK. Hãy nhớ đặt dấu ngoặc kép (") vào trước và sau đường dẫn đến tập tin vừa chọn, sau đó ấn phím . Tiếp tục, bổ sung nội dung regedit.exe /s và theo sau đó là một khoảng

cách vào trước dấu ngoặc kép đầu tiên. Khi thực hiện xong, lệnh cuối cùng sẽ là regedit.exe /s "c:\Registry files\focus.reg" (đường dẫn riêng của bạn có thể khác).

Nhấn Next, đặt tên cho biểu tượng shortcut này rồi nhấn Finish. Từ đây trở đi, bất cứ lúc nào máy khởi động, shortcut này sẽ đưa cài đặt chống mất quyền ưu tiên vào hệ thống.

Đáng tiếc, giải pháp này không thể khắc phục mọi trường hợp xảy ra hiện tượng mất quyền điều khiển hệ thống. Nếu phát hiện một tiện ích nào đó thường xuyên chiếm quyền thì bạn hãy cân nhắc đến việc thay thế một tiện ích khác có tính năng tương đương.

CHẶN POP-UP

Triệu chứng: Bạn cảm thấy "bực mình" vì một quả bóng tròn kèm chữ thường xuyên bật ra từ khay hệ thống trên thanh tác vụ Windows XP để nhắc nhở một bản vá (hay cập nhật) mới đã sẵn sàng để tải về từ trang web của Microsoft hoặc cung cấp những thông tin không mấy quan trọng khác.

Cách khắc phục: Tweak UI có thể giải quyết phiền toái này. Trước hết, chạy tiện ích Tweak UI và chọn mục Taskbar and Start menu trong khung cửa sổ bên trái. Tiếp đến, bỏ đánh dấu chọn mục Enable ballon tips ở cửa sổ bên phải và sau cùng là nhấn OK.

TĂNG LỰC ỨNG DỤNG

Triệu chứng: Sẽ có lúc tiện ích mà bạn đang sử dụng trở nên hoạt động "ì ạch" do các ứng dụng không quan trọng khác hay các chương trình hoạt động ở chế độ nền đã chiếm dụng gần hết tài nguyên của Windows.

Hình 2: Tăng mức ưu tiên để giúp ứng dụng quan trọng chạy nhanh hơn.

Cách khắc phục: Trong Windows XP, bạn có thể cung cấp nhiều tài nguyên hơn cho một chương trình cụ thể bằng cách thay đổi độ ưu tiên của ứng dụng đó thông qua công cụ Task Manager. Bạn nhấn phải lên thanh tác vụ rồi chọn Task Manager. Chọn nhãn Processes và nhấn phải chuột lên tập tin thực thi tương ứng với ứng dụng đang "khát" tài nguyên. Nhấn Set Priority, rồi chọn mức ưu tiên cao hơn – như AboveNormal hay High chẳng hạn (Hình 2). Khi thông tin cảnh báo xuất hiện, nhấn Yes.

Cũng xin lưu ý, việc thay đổi mức ưu tiên của một quá trình (mà cụ thể hơn là ứng dụng) sẽ gây ảnh hưởng đến tốc độ xử lý của các quá trình khác. Ví dụ, chọn mức độ ưu tiên Realtime sẽ thiết lập quyền ưu tiên cao nhất và điều này có thể làm cho những ứng dụng còn lại trong hệ thống trở nên "chết đứng", tốt nhất không nên chọn mức độ này. Trừ trường hợp, nếu đang gặp trục trặc trong việc ghi dữ liệu lên đĩa CD thì bạn cần tăng độ ưu tiên cho phần mềm ghi CD của mình. Và nếu có một ứng dụng dạng chạy nền nào đang xử lý một số công việc không mấy quan trọng, bạn có thể cân nhắc để thiết lập cho ứng dụng này một mức ưu tiên thấp hơn. Bạn cũng nên nhớ rằng những thay đổi này sẽ chỉ được áp dụng cho phiên làm việc hiện tại và mọi thứ sẽ trở về trạng thái cũ vào lần khởi động Windows kế tiếp.

Để xem cùng lúc mức độ ưu tiên của tất cả quá trình đang chạy trong hệ thống, bạn chọn trình đơnView.Select Colums trong cửa sổ Task Manager. Đánh dấu chọn Base Priority và nhấn OK.

XEM CHI TIẾT THEO Ý RIÊNG

Triệu chứng: Tùy chọn Details trong tính năng hiển thị của tiện ích Windows Explorer (chọn trình đơn View.Details) sẽ liệt kê nhiều thông tin về các tập tin của bạn, nhưng đôi khi bạn phải kéo thanh cuộn ngang qua lại hoặc xem những thông tin mà bạn không hề muốn biết.

Hình 3: Yêu cầu Windows không tạo tập tin lưu hình thu nhỏ của thư mục.

Cách khắc phục: Để Windows Explorer hiển thị đúng những thông tin cần thiết, bạn nhấn phải chuột lên bất kỳ cột thông tin nào và bỏ chọn khoản mục không cần thiết (cũng như đánh dấu chọn những khoản mục cần hiển thị). Ngoài ra, bạn có thể chọn More để xem các tùy chọn bổ sung. Để sắp xếp thứ tự các cột, bạn hãy kéo (drag) tiêu đề một cột (ví dụ Date Modified) về phía phải hoặc trái rồi thả cột này lên đường biên giữa các cột. Muốn thu giảm kích thước (resize) cho một cột đơn lẻ, bạn nhấn đúp chuột lên đường biên phải của cột đó. Còn muốn cùng lúc resize cho tất cả các cột để phù hợp với cửa sổ thư mục hay cửa sổ tiện ích Explorer, bạn ấn tổ hợp phím -+ trên bàn phím số.

LOẠI BỎ RÁC TRONG THƯ MỤC

Triệu chứng: Khi mở một thư mục ở chế độ hiển thị hình thu nhỏ (thumbnails), Windows XP sẽ tạo một tập tin có tên là Thumbs.db trong thư mục đó để cất giữ các hình thu nhỏ này, giúp người dùng xem lại chúng nhanh hơn ở những lần sau. Bạn sẽ không thấy được tập tin này trừ khi máy tính của bạn được thiết lập để hiển thị các tập tin ẩn (trong Windows Explorer hay cửa sổ thư mục bất kỳ, chọn Tools.Folder Options, ở thẻ View, đánh dấu tùy chọn Show hidden files and folders).

Cách khắc phục: Khi đã kích hoạt khả năng hiển thị tập tin và thư mục ẩn, bạn hãy tìm và xóa các tập tin Thumbs.db không cần đến. Nếu muốn các tập tin này không xuất hiện trở lại, bạn mở cửa sổ thư mục hoặc tiện ích Explorer bất kỳ rồi chọn Tools.Folder Options. Trong nhãn View, đánh dấu tùy chọn Do not cache thumbnails (Hình 3). Cuối cùng, nhấn OK để hoàn tất.

TRÁNH HỖN LOẠN TRÌNH ĐƠN

Triệu chứng: Khi thao tác với trình đơn Start trong mọi phiên bản Windows, nhiều khả năng bạn sẽ vô tình kéo các mục (biểu tượng) ra khỏi vị trí mặc định của chúng.

Cách khắc phục: Bạn có thể tắt tính năng kéo và thả các mục trên trình đơn Start. Đầu tiên, bạn cần kiểm tra để bảo đảm các mục trong tất cả trình đơn đã được xếp theo đúng thứ tự mà bạn muốn. Sau đó, bạn nhấn phải chuột lên nút Start (trong Windows XP) hoặc thanh tác vụ (đối với các phiên bản Windows khác) và chọn Properties. Trong Windows XP, bạn nhấn vào nút Customize bên cạnh tùy chọn Start menu hoặc Classic Start menu. Tiếp đến, bỏ đánh dấu mục Enable dragging and dropping (có thể bạn phải nhấn Advanced để thấy tùy chọn này). Nhấn OK hai lần để kết thúc.

LIÊT KÊ NHIỀU TÀI LIÊU

Triệu chúng: Trong phiên bản Windows XP Pro, bạn dễ dàng truy cập các tài liệu vừa mở bằng cách mở chọn Start.My Recent Documents (hoặc Start.Documents) nhưng danh sách này chỉ liệt kê được 15 tập tin gần nhất.

Hình 4: Thiết lập để Windows XP Pro hiển thị nhiều tập tin được sử dụng gần đây hơn trong mục Documents bằng công cụ Group Policy.

Cách khắc phục: Nhấn Start.Run, gõ vào lệnh gpedit.msc và ấn . Trong khung cây bên trái, bạn di chuyển và chọn User Configuration\Administrative Templates\Windows Components\Windows Explorer. Nhấn đúp vào mục Maximum number documents trong khung cửa sổ bên phải. Tiếp đến, chọn Enable và sau đó đặt cho khóa Maximum number of recent documents một giá trị cao hơn con số 15 mặc định (Hình 4).

Trong các phiên bản Windows khác (không phải XP Pro hoặc 2000), bạn phải trông cậy vào giải pháp "chắp vá" là tạo một biểu tượng shortcut trỏ đến thư mục "C:\Documents and Settings\username\Recent", với username là tên tài khoản đăng nhập hệ thống.

XÓA BIỂU TƯỢNG THỪA

Triệu chứng: Mỗi hai tháng, Windows XP đưa ra thông báo cho biết bạn đã không sử dụng một số biểu tượng trên màn hình desktop trong một thời gian dài. Thậm chí hệ điều hành còn tỏ ý giúp cất các biểu tượng này vào một thư mục khác trên desktop.

Cách khắc phục: Bạn cần biết rằng việc chuyển các biểu tượng trực quan trên màn hình Windows sang một thư mục khác chắn chắn sẽ làm người dùng mất "hứng thú" nhấn chuột vào chúng, nếu không nói là khá bất tiện để tìm một biểu tượng ở đâu đó. Nếu thực sự không còn nhu cầu sử dụng các biểu tượng này, hãy xóa chúng.

Để tắt tính năng nhắc nhở dọn dẹp các biểu tượng không còn dùng đến, bạn nhấn chuột vào màn hình desktop và chọn Properties. Ở nhãn Desktop, nhấn Customize Desktop, và ở dưới cùng hộp thoại đó, bạn bỏ đánh dấu chọn mục Run Desktop

Cleanup Wizard every 60 days rồi nhấn OK hai lần để kết thúc.

Bùi Xuân Toại
PC World Mỹ 11/2006

Chống "đóng băng" máy tính

Thực hiện: Bùi Xuân Toại

Làm thế nào để máy tính hoạt động lại sau khi bị "đóng băng" và không đáp ứng với bàn phím?
Máy tính của bạn thật sự bị "đóng băng" hay chỉ là hoạt động rất chậm? Hãy suy nghĩ kỹ một tí và nếu mọi thứ vẫn hoạt động tốt sau khi bạn khởi động lại máy thì bạn nên kiểm tra tình trạng rối rắm này bằng cách nhấn chuột chọn Start.Turn Off Computer.Restart (nếu máy tính thực sự có "bệnh", tình trạng lờ đờ sẽ tiếp diễn).

Nếu máy tính vẫn "mắc kẹt" nhưng bàn phím còn hoạt động, bạn ấn tổ hợp phím Ctrl, Alt, và Del để cửa sổ Task Manager (trong Windows Vista, nút phải nhấn là Start Task Manager). Ở thẻ Application, đánh dấu chọn cột Status đối với bất kỳ trình ứng dụng nào được ghi chú Not Responding. Nếu tìm thấy một ứng dụng nào như vậy, bạn chọn nó và nhấn End Task. Tiếp theo, bạn chọn thẻ Processes và tìm bất kỳ quá trình nào sử dụng 100% khả năng CPU (hoặc 50% nếu bạn sử dụng hệ thống lõi kép – dualcore). Nếu không có, bạn chọn Shut Down. Restart để khởi động lại máy tính.

Nếu bàn phím và chuột cùng không đáp ứng, bạn ấn đồng thời quan sát nhìn xuống bàn phím. Nếu đèn chỉ thị Caps Lock không thay đổi thì bàn phím và máy tính đã mất liên lạc với nhau. Tương tự, di chuyển chuột và quan sát trên màn hình, nếu con trỏ không nhúc nhích – ngay cả sau vài giây chờ đợi – thì chuột cũng mất liên lạc với máy tính. Trong trường hợp này, máy tính của bạn cần phải khởi động lại bằng phần cứng (tắt/mở máy), hoặc bàn phím và chuột của bạn bị hỏng.

Nếu sử dụng chuột và bàn phím có dây, rút dây nối ra và sau đó gắn chúng trở lại. Nếu là loại không dây, bạn ấn nút reset của chúng, hoặc thay pin hoặc thực hiện cả

hai.

Nếu mọi thứ vẫn “bình chân như vại” thì kế sách cuối cùng là thực hiện một khởi động lại phần cứng. Bạn có thể mất đi những công việc chưa kịp lưu lại trước khi

sự cố bắt đầu, nhưng nếu không có chọn lựa nào khác, bạn ấn và giữ nút bật/tắt nguồn của máy tính trong khoảng 5 giây. Còn nếu thao tác này không làm tắt máy, bạn hãy rút dây cắm điện ra khỏi ổ (với máy tính xách tay, có thể bạn phải tháo pin).

Lần trình khởi động tiếp theo này có thể kéo dài hơn bình thường vì Windows sẽ chạy các công cụ chẩn đoán mỗi khi người dùng tắt máy không đúng cách. Tuy nhiên, nếu Windows hoàn toàn không khởi động lại, bạn hãy tìm cách khắc phục trong bài viết "Khi Windows XP hoặc 2000 không khởi động" (ID: A0311_134). Để chuẩn bị sẵn sàng cho những sự cố Windows sau này, bạn nên chuẩn bị một đĩa CD khởi động khẩn cấp (ID: A0512_146). Để có nhiều thủ thuật hơn, bạn đến địa chỉ find.pcworld.com/56023.

Đồng bộ Outlook

Cách đồng bộ dữ liệu Outlook trên hai máy tính?

Đồng bộ Inbox của Outlook và dữ liệu trên 1-2 máy tính bằng SynchPST

Các dịch vụ miễn phí của Yahoo có thể đồng bộ danh bạ liên lạc (adress boook), lịch làm việc (calendar), chú thích (notepad) và danh sách việc cần làm (to-do list) của Outlook nhưng không thể đồng bộ các e-mail. Các dịch vụ này yêu cầu bạn phải có một tài khoản Yahoo miễn phí (đăng ký tại www.yahoo.com). Bạn đăng nhập vào tài khoản này, nhấn Mail và sau đó chọn nhãn Calendar. Nhấn Sync để tải xuống và cài đặt tiện ích Intellisync for Yahoo, có khả năng đồng bộ dữ liệu Outlook của bạn với các dịch vụ của Yahoo. Nếu muốn chia sẻ e-mail, bạn phải sử dụng dịch vụ Webmail của ISP và sau đó bổ sung tài khoản này vào hộp thư đến của tiện ích Outlook. Để đồng bộ một tài khoản, bạn thử dùng Synch PST (tải về bản demo miễn phí tại địa chỉ find.pcworld.com/56024; Hình 1). Phiên bản Basic (40USD) của tiện ích này đáp ứng tất cả yêu cầu thông thường nhưng phiên bản Professional (70USD) còn bổ sung thêm tính năng tự động đồng bộ email và bảo vệ mật khẩu.

Bùi Xuân Toại
PC World My 3/2007

Tìm lại Password Win XP NTFS

Chuẩn bị

- Đầu tiên các bạn hãy vào trang Offline NT Password & Registry Editor, Bootdisk / CD để lấy chương trình bootdisk.zip

- Chuẩn bị một đĩa mềm sạch

- Các bạn về và chạy file install.bat trong đấy, chương trình sẽ thực hiện việc ghi thông tin ra đĩa mềm.

Thao tác

- Vào CMOS thiết lập cho máy khởi động từ đĩa mềm

- Khởi động máy bằng đĩa mềm vừa tạo

Sau một lúc đọc các thông số + và các lời giới thiệu về chương trình:

Nó sẽ đưa ra các thông tin để Bạn chọn lựa:

[1] Select disk where the Windows installation is (Bạn sẽ chọn đĩa bạn cài Win ở đây)

[2] Select PATH and registry files (Đường dẫn đến các file thông tin)

Bạn không cần phải quá lo lắng, ở những bước này hầu như bạn chỉ cần phải nhấn Enter

[3] Password or registry edit:

Ở đây bạn sẽ được hỏi là bạn muốn chọn thao tác reset lại password hay là muốn sữa chữa registry. Thông thường là bạn chỉ muốn dùng để reset lại password cho nên đơn giản hãy nhấn Enter.

Sau đấy chương trình sẽ hiện lên hàng loạt các username để bạn chọn lựa

RID: 01f4, Username: <Administrator>

RID: 01f5, Username: <Guest>, *disabled or locked*

RID: 03e8, Username: <HelpAssistant>, *disabled or locked*

RID: 03eb, Username: <pnh>, *disabled or locked*

RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)

or simply enter the username to change: [Administrator]

Hãy chọn account mà bạn muốn đặt lại password. Lúc này chương trình sẽ yêu cầu bạn gõ lại password cho account đấy. bạn nên gõ dấu * tương đương với việc bạn chọn password là rỗng, bạn nên chọn password rỗng sẽ tốt hơn là bạn gõ một password mới vào (Lý do vì sao thì chốc nữa tôi sẽ trình bày).

[4] Kết thúc: Tất cả những gì bạn làm đã xong, hãy rút đĩa mềm ra và khởi động lại máy, nhập vào account bạn vừa reset lại pass để đăng nhập.

Rút ra một số kết luận về các điều kiện cần phải có của một chương trình dùng để reset lại password trong Win2000/XP/2003:

Như chúng ta đã biết, các thông tin về username và password đều được ghi lại trong file SAM. Vấn đề là định ra được file SAM nằm ở đâu trên hệ thống và đọc và sửa chữa lại được các thông số trong file SAM đấy. NTFS cũng như là cơ chế FAT nếu đứng về mặt lưu trữ nhưng NTFS bảo mật vì cơ chế lưu trữ thông tin của nó không được tiết lộ chi tiết. Cho nên vấn đề khi tìm lại password của một hệ thống không quan trong đấy là FAT hay NTFS mà điều quan trong là tìm ra được file SAM được lưu trữ ở đâu

Khi có được file SAM thì phải hiểu được cấu trúc của file SAM: nghĩ là trường tên user ở đâu, trường password ở đâu. Tất nhiên là chúng đều đã được mã hóa.

Dù chúng ta có được trường thông tin password nhưng vấn đề ở đấy là chúng ta không thể decode các thông tin đấy để nó trở thành lại password cũ được, bởi vì như vậy thì đâu có là bảo mật nữa, thằng MS chết từ lâu rồi.... , nhưng vấn đề là chúng ta có thể ghi đè lên các thông tin đấy. Vậy để reset lại password thì ta có thể ghi đè password mới lên trên đấy (tất nhiên phải sau khi mã hóa password mới). Chúng ta có thể thấy rằng, trên khắp thế giới, thì password rỗng được mã hóa giống nhau trên mọi hệ Win các thứ tiếng. (Korea, Japan...) cho nên nếu ghi đè lên bằng một password rỗng thì luôn an toàn hơn, phù hợp cho mọi loại Win hơn. Nếu bạn ghi đè một password khác rỗng, nhưng Win đấy có thể là Win tiếng nhật, tiếng Hàn thì bạn có thể gặp vấn đề.

Chương trình boot disk trên kia đã làm được những yêu cầu đấy:

- Xác định được file SAM trên ổ đĩa.

- Xác định được vị trí của các trường user và pass được lưu trữ trong file SAM

- Có cơ chế mã hóa và ghi đè lại password.

Nhược điểm của phương pháp reset lại password kể trên: (Hay kể cả phương pháp xóa file SAM cổ lổ sĩ)

- Dữ liệu của account đấy mà đã encrypt trước đấy thì sẽ không khôi phục lại được, vì một lý do là khi encrypt dữ liệu, hệ thống sẽ sử dụng cả password của account đấy để encrypt. ---> dẫn đến không thể khôi phục lại những dữ liệu đấy khi mình đã set lại password mới.

Phương pháp này đã được thử nghiệm thành công trên các Win2000/XP/2003.

Tuy nhiên, hi vọng đấy chỉ là bài viết để mọi người cứu mình và cứu người khác trong trường hợp "hiểm nghèo" chứ không nên lạm dụng để đi phá hoại người khác.

sưu tầm

Giải quyết trục trặc sau khi cài phần mềm mới

Thực hiện: Minh Xuân

Sau khi cài một phần mềm mới, máy tính của tôi trở nên chậm và không ổn định. Không những vậy, việc gỡ cài đặt chương trình này cũng không thể khắc phục được hiện tượng này. Liệu có biện pháp nào an toàn hơn để cài đặt phần mềm không?

Thực tế cho thấy, nhiều tiện ích cài đặt phần mềm có khả năng làm thay đổi đáng kể các cấu hình quan trọng của Windows, và làm tăng nguy cơ gây ra "gục ngã" của hệ thống. Đồng thời, các tiện ích gỡ bỏ cài đặt (uninstall) cũng gần như không thể sửa được lỗi này. Hãy tham khảo các bước được trình bày bên dưới, chúng sẽ giúp bạn tạo an toàn cho quá trình cài đặt phần mềm.

Lựa chọn cẩn thận: Trước khi cài đặt bất kỳ ứng dụng nào, bạn cần đọc thật kỹ các bài viết đánh giá, trao đổi với những ai đã từng dùng qua hay biết rõ về ứng dụng

này, và tìm kiếm những ý kiến phản hồi (comment) tại các diễn đàn mạng (như groups.google.com chẳng hạn). Sau đó, hãy tự hỏi chính mình rằng liệu những lợi ích mà ứng dụng này đem lại có đáng giá hơn mối nguy hiểm đang rình rập bạn hay không.

Gỡ cài đặt phần mềm bằng Add or Remove Programs của Windows.

Bạn nên nhớ đừng bao giờ cài đặt một ứng dụng mới hay cập nhật bản nâng cấp cho đến khi chúng đã xuất hiện được vài tháng. Quãng thời gian này thường được các hãng sản xuất nhận thông tin phản hồi từ người dùng, sau đó tiến hành "vá" các lỗi hay thậm chí là lỗ hổng bảo mật vừa được phát hiện.

Và bạn cũng đừng vội khẳng định một chương trình nào đó thực sự an toàn vì được tạo ra bởi một hãng phần mềm nổi tiếng. Điều này có thể dễ dàng nhận ra với các phần mềm của Microsoft và Symantec.

Đề phòng bất trắc: Công việc quan trọng đầu tiên mà bạn cần thực hiện trước khi cài đặt một phần mềm mới vào máy tính là tiến hành sao lưu lại cấu hình hiện tại của Windows. Tính năng System Restore trong Windows XP sẽ tự động tạo ra một cột mốc hồi phục (restore point) trước khi khởi động mỗi quá trình cài đặt ứng dụng mới, nhưng để an toàn hơn, bạn hãy thực hiện việc này một cách thủ công: nhấn Start.All Programs.Accessories.System Tools.System Restore.Create a restore point.Next, và thực hiện các bước còn lại theo hướng dẫn.

Việc cài đặt một ứng dụng mới cũng có thể dẫn đến việc "phá hoại" các thông số Registry và trong vài trường hợp sẽ gây nên sự mất ổn định của hệ thống hoặc thậm chí gây treo máy. Do vậy, hãy tiến hành sao lưu lại toàn bộ Registry của Windows trước khi tiến hành công việc, bạn có thể sử dụng công cụ sẵn có trong tiện ích Registry Editor (chọn Start.Run, gõ vào lệnh regedit và ấn <Enter>) hay tiện ích của hãng thứ 3 như Emergency Recovery Utility NT (hay còn gọi là ERUNT, www.pcworld.com.vn, ID: 51392). Đề biết thêm nhiều thủ thuật tinh chỉnh các thông số phức tạp này, bạn có thể tham khảo mục Phương thuốc Registry

trong bài biết "Giải mã Windows XP" (ID: A0604_98).

Đánh giá sự cố: Sau khi cài đặt xong chương trình, bạn hãy kiểm tra các biểu tượng mới xuất hiện trên khay hệ thống. Nhiều khả năng, chương trình mới này đã

bổ sung vài tiện ích không cần thiết – và thường rất nguy hiểm – vào danh sách ứng dụng được khởi chạy cùng lúc với quá trình khởi động của Windows. Để biết cách tinh giản danh sách các ứng dụng tự khởi động và làm gọn khay hệ thống, bạn có thể tham khảo mục Chặn ứng dụng tự khởi chạy trong bài viết "Bôi trơn cỗ máy tính" (ID: A0601_86) và mục Làm gọn khay hệ thống trong bài viết "Sao lưu dữ liệu nhanh chóng và dễ dàng bằng CD-RW" (ID: A0202_82).

Ngoài ra, bạn đừng cài đặt thêm bất kỳ chương trình nào khác vào máy tính trong khoảng vài ngày (hoặc lâu hơn càng tốt) để nếu chẳng may xảy ra trục trặc, việc xác định nguyên nhân cũng sẽ dễ dàng hơn.

Rút lui nếu cần: Nếu chương trình vừa được cài đặt không làm hài lòng bạn, hãy xóa chương trình này khỏi hệ thống bằng cách sử dụng tiện ích gỡ bỏ cài đặt đi kèm (thường tìm thấy trong trình đơn Start.All Programs). Nếu không tìm thấy tiện ích gỡ bỏ cài đặt, bạn chọn Start.Control Panel.Add or Remove Programs (hay Start.Settings.Control Panel.Add/Remove Programs ở các phiên bản Windows khác), chọn ứng dụng cần xóa trong danh sách vừa xuất hiện, và nhấn Remove để chạy tiện ích gỡ bỏ cài đặt (Hình 1). Tính năng Add/Remove Programs và biểu tượng từ trình đơn Start dù khác nhau nhưng cùng khởi chạy tiện ích gỡ bỏ cài đặt.

Nếu cách trên không thể loại bỏ chương trình vừa chọn, bạn hãy chạy tiện ích System Restore để đưa Windows quay lại hiện trạng trước khi tiến hành cài đặt chương trình đó. Nếu tiếp tục không thành công, bạn cần sử dụng tuỳ chọn gỡ bỏ cài đặt trong tiện ích ERUNT được giới thiệu ở phần trên.

Cũng xin lưu ý, việc phục hồi Registry từ một bản sao lưu cũ có thể gây mất vài thông số cài đặt, hoặc làm vô hiệu hóa những chương trình được cài đặt sau khi thực hiện sao lưu đó. Đây là một lý do khác để bạn cần

AN TOÀN HƠN VỚI TRUECRYPT

Trong bài viết "Tạo đĩa CD khởi động khẩn cấp" (ID: A0511_146) có giới thiệu hai tiện ích là Cryptainer LE (www.pcworld.com.vn, ID: 47758) và Cryptainer PE (45 USD, find.pcworld.com/49372), giúp tạo ra các vùng dữ liệu riêng biệt được mã hóa với thuật toán Blowfish trên đĩa cứng hay bút nhớ USB. Gần đây, một bạn đọc đã khám phá ra một tiện ích khác hiệu quả hơn và dĩ nhiên cũng hoàn toàn miễn phí: TrueCrypt (www.pcworld.com.vn, ID: 52242). Chương trình mã nguồn mở này có thể tạo các vùng dữ liệu với kích thước lớn trong phạm vi mà Windows và đĩa cứng cho phép (Cryptainer LE chỉ hỗ trợ 25MB), hỗ trợ nhiều thuật toán mật mã hóa như AES, Blowfish, và Triple DES. Thậm chí, bạn có thể mã hóa một phần hoặc toàn bộ ổ đĩa.

chờ đợi một khoảng thời gian giữa các lần cài đặt chương trình.

Ngoài ra, để tìm hiểu về cách dọn sạch những "tàn dư" còn sót lại sau khi tiến hành gỡ bỏ cài đặt các ứng dụng, bạn có thể tham khảo lại bài viết "Dọn sạch những gì Uninstall bỏ sót" (ID: A0411_142).

Minh Xuân
PC World Mỹ 6/2006

Giúp WinXP nhận dạng những driver đặc biệt

GIÚP WINXP NHẬN DẠNG DRIVER NGAY TRONG QUÁ TRÌNH SETUP

Nếu bạn đã đọc wa bài viết hướng dẫn cách TÍCH HỢP DRIVER VÀO PHẦN SOURCE WIN98, thì hẳn bạn đã công việc này có ý nghĩa như thế nào. Trước nhất, nó giúp bạn tiết kiệm rất nhiều thời gian, sau hết, giúp bạn sở hữu 1 bản Win mang tính cá nhân hóa cao (mang phong cách Personal / Unattended / Unofficial).

Đó là với Win98, còn WXP ? Dĩ nhiên là được rồi bạn ạ ! WinXP có thể nhận biết hầu hết các thiết bị trong máy bạn. Những file driver này nằm trong file DRIVER.CAB trong folder I386. Tuy nhiên, số lượng thiết bị mà WinXP có thể nhận biết chỉ là "hầu hết" chứ không phải là "tất cả" => phải tự cài 1 số driver cho máy là điều rất có thể xảy ra. Bạn biết đấy, bản thân WXP (2K/2K3) là 1 OS khó chịu, tính bảo mật của nó rất cao (đó là lý do tại sao, khi thấy có sự mất cân bằng, thiếu ổn định trong hệ thống, thì trình Windows File Protection (WFP) sẽ tự động được kích hoạt & liên tục réo inh ỏi, đòi bạn phải insert CD WXP vào để copy những file nằm trong folder I386 sang hệ thống của bạn).

Nói tóm lại, việc thay đổi / bổ sung vào hệ thống WXP là điều rất khó. Hơn thế nữa, công việc bạn phải làm ko đơn giản là can thiệp vào hệ thống của WXP (sau khi setup), mà là can thiệp vào phần source của nó (trước khi setup).
Khó chứ ko phải ko làm được. Bởi thực tế, WXP đã cung cấp cho bạn sẵn 1 công cụ để làm công việc này.

Xin bạn lưu ý, sau khi công việc hoàn tất, CD WXP của bạn sẽ được gọi bằng 1 cái tên là WXP Unattended (có thể tạm hiểu là WXP theo kiểu "KO GIỐNG AI"). Điều này có lẽ ko cần thiết & ko đáng để bạn wan tâm nhiều lắm, nhưng

thiết nghĩ, nếu bạn muốn tìm hiểu thêm về vấn đề này (bằng cách search với các công cụ như Google), thì từ khóa (keyword) (trong trường hợp này là Windows Unattended) là điều rất cần thiết.
1/ Quy ước: folder mà bạn sẽ làm việc được đặt ở D:\XPPE
+ Bạn tiến hành copy nguyên phần source của WXP vào đây.
+ Tạo 1 folder tên OEM, đặt cùng cấp với folder I386
+ Tạo tiếp D:\XPPE\$OEM$\$1\PhanCung

2/ Tạo file kịch bản:
+ Trên mỗi CD WXP (thông thường, chưa edit) đều có 1 folder tên SUPPORT. Giả sử, "X" là ký tự đại diện cho ổ CD, thì file chứa công cụ mà bạn đang cần là: X:\SUPPORT\TOOLS\DEPLOY.CAB
+ Giải nén file này ra, bạn sẽ được 1 số file như sau:

+ Trong đó, SETUPMGR.EXE là công cụ bạn đang cần ! Chạy file này để kích hoạt trình SETUP MANAGER (SM).
Code:
- Công dụng chính (& cũng là duy nhất) của SM là tạo ra 1 file kịch bản có tên là WINNT.SIF. Nghĩa là, trong suốt wá trình setup, WXP sẽ dựa theo những gì được đưa ra trong "kịch bản" này & cứ thế làm theo.
+ Sau khi đã vào giao diện chính của chương trình, bạn tiến hành làm theo tuần tự như sau:

+ Phần License Agreement: chọn Accept
+ Tiến hành khai báo các thông số cần thiết
+ Sau khi hoàn tất, chương trình sẽ lưu lại toàn bộ những thông số mà bạn đã đưa ra, vào 1 file, được đặt tên mặc định là UNATTEND.TXT (chính là file kịch bản) (đường dẫn để lưu thì bạn tự chọn, nhưng ... phải nhớ giùm !). Giả sử, mình save file này vào: + Đổi tên file UNATTEND.TXT thành WINNT.SIF
+ Đặt WINNT.SIF vào folder I386 (bắt buộc).

+ Đến đây thì coi như bạn đã hoàn thành xong việc tạo 1 kịch bản cơ bản (tôi nói là cơ bản mà thôi). Bởi do, toàn bộ nội dung của kịch bản này là do trình SM tạo ra, nên chưa thật sự POWERFUL lắm (bạn có thể tham khảo thêm phần help trong REF.CHM để biết thêm về cách sử dụng 1 số thẻ (tag - những module con, đóng vai trò cực kỳ wan trọng trong nội dung của WINNT.SIF).

Sẽ có 1 bài viết khác hướng dẫn bạn cách wản lý toàn diện về WINNT.SIF.
+ File WINNT.SIF được tạo ra, có thể sửa đổi nội dung dễ dàng bằng cách dùng trình Notepad (có sẵn trong Win) / bất cứ chương trình nào có chức năng tương tự.
3/ Tổng hợp dirver:
- Có nhiều cách để làm việc này, nhưng tối ưu hơn hết là dùng các chương trình backup driver (trình nào cũng được). Cái cốt lõi trong mỗi bộ driver chính là file .INF (mình đã đề cập trong bài Tích hợp driver vào source Win98).
- Bạn cần xác định xem, máy bạn thật sự cần những driver nào ? Nếu trong những lần setup Win trước đây, sau khi hoàn tất, còn có những thiết bị nào mà Win chưa nhận biết (hoặc đã nhận biết rồi, nhưng driver wá cũ) thì mới tiến hành backup driver cho những thiết bị đó mà thôi.

+ Những driver đã được bạn tổng hợp, phải được phân loại rõ ràng & đặt vào những folder có tên dạng:
Code:
xxx-<tên folder>, với xxx là 1 con số, nhỏ nhất là 000
VD: 000-chipset, 001-vga, 002-sound

- **Giả sử: mình đã backup những driver cần thiết & đặt chúng vào D:\XPPE\$OEM$\$1\PhanCung**
  - Bây giờ, bạn đã có 1 cây folder có cấu trúc (đại loại) như sau:

4/ Biên tập lại nội dung file kịch bản (WINNT.SIF)
+ Dùng Notepad để mở file WINNT.SIF
+ Tìm đến thẻ [Unattended] & bổ sung những dòng sau:
Code:
[Unattended]
OemPnPDriversPath=”PhanCung\000-chipset;PhanCung\001-Vga;PhanCung\002-sound“
DriverSigningPolicy=Ignore
+ Save lại.

5/ Hoàn tất
+ Việc còn lại duy nhất bây giờ mà bạn phải làm là đóng gói trở lại toàn bộ phần source này thành 1 file ISO (để cất giữ / test thử trên máy ảo), hoặc ghi ra CD (nên dùng CDRW) & tiến hành cài đặt như bình thường.
+ Chắc hẳn, bạn sẽ phải ko khỏi ngạc nhiên khi thấy rằng, sau khi wá trình setup WXP hoàn tất, thì tất cả những những dirver cũng đều đã được setup / update. Đỡ tốn thời gian biết chừng nào !.

- Xin bạn lưu ý:
+ Đây ko phải là wá trình tích hợp driver vào phần source WXP, mà chỉ đơn thuần là giúp cho WXP nhận diện được driver, thông wa những folder đã được chỉ ra sẵn (trong thẻ [Unattended]). Nói cách khác, cách làm này ko giống với cách làm bên Win98, tuy nhiên, cũng mang lại cùng 1 hiệu wả).
+ Tích hợp ? Công việc này đòi hỏi độ khó cao, rất phức tạp bạn ạ !. Trước mắt, nếu muốn tích hợp, bạn chỉ có thể dùng bộ DriverPack (DP) (1 module nhỏ trong dự án phát triển cho XP Personal Edition) mà thôi. Nhưng ngặc nổi, khi dùng gói này, phần source của WXP sẽ phình ra khá lớn. Bởi đơn giản vì, gói DP này ....cũng tổng hợp rất nhiều dirver bên trong (hoá ra nó chính là .... DRIVER.CAB thứ hai !). Mà cái bạn cần ở đây là gì ??? Chỉ cần XP nhận diện những driver trong máy bạn là đủ rồi !.

Hy vọng bài viết sẽ giúp ít cho các bạn nhiều !
Thân chào !!!.

Cách phá đóng băng ổ cứng

Hiện nay hầu hết các quán net đều sử dụng chương trình đóng băng DeepFreeze(các bạn hãy nhìn vào góc phải dưới cùng của màn hình sẽ có jinhf 1 chiếc máy tính trăng trắng) vì vậy nên chúng ta cài keylog sẽ không hiệu quả , sau đây mình sẽ chia sẻ chút kinh nghiệm phá băng và cài keylog các quán net cho các bạn .
---Đầu tiên chúng ta muốn phá băng thì phải sử dụng chương trình phá băng UnDeepFreeze , đay là link down mình đã sưu tầm được trong diễn đàn mà mình thấy vẫn còn sử dụng tốt :
http://65.254.55.106/download/phahoa...reezerU1.6.exe

trang chủ:

http://usuarios.arnet.com.ar/fliamarconato/pages/edeepunfreezer.html

---Sau khi down về các bạn chạy chương trình UnDeepFreeze , sẽ hiện ra một cái bảng như sau

Có 3 mục lựa chọn , các bạn hãy nhấp chọn vào mục thứ 2 vì theo mình đây là phương pháp lựa chọn an toàn nhất (Phá băng sau 1 lần khởi động lại máy và trả

lại chương trình đóng băng sau khi tắt máy).
--- Sau đó cá bạn restart lại máy , khi vào lại các bạn hãy chú ý hình chiếc máy tính

góc phải dưới cùng màn hình đã bị gạch chéo đỏ ,tức là chương trình DeepFreeze đã bị gỡ bỏ , giờ thì các bạn có thể tha hồ cài các chương trình Keylog hay làm bất kì điều gì mình muốn.

Nếu link die thì bạn có thể lên google để search hoặc download ở đây:

Code:

```
http://usuarios.arnet.com.ar/fliamarconato/pages/DeepUnfreezerU1.6.exe
http://usuarios.arnet.com.ar/fliamarconato/pages/DeepUnfreezer1.6.exe
http://music.geocities.jp/www_netvn_tk2006/DeepUnfreezer1.6.zip
```

Sưu tầm
Posted by YemEmDaiKho(HCE)

Đơn giản hóa việc phục hồi driver cho card đồ họa

Đối với máy tính có gắn thêm card tăng tốc đồ họa rời (nhất là khi phục vụ cho việc chơi game), công việc thường xuyên của người dùng là update (cập nhật) các driver mới nhất. Cách làm tiện lợi nhất là bạn tải file update trên trang chủ của nhà sản xuất rồi chạy file đó trên máy để cài đặt.

Vấn đề xuất hiện ở chỗ không phải cứ cài driver mới nhất là tốt nhất, đôi khi bạn sẽ gặp tình trạng driver mới không tương thích với hệ thống (vì driver mới ngoài việc bổ sung các chức năng cho các card cũ thì còn có tác dụng chủ yếu là hỗ trợ cho các card đời mới). Lời khuyên mà bạn hay nhận được là gỡ bỏ driver mới và dùng lại driver cũ, quá trình này sẽ được thực hiện nhanh hơn nếu bạn biết rằng Windows XP hỗ trợ phục hồi lại driver cũ cho card đồ họa cực nhanh (dù đã tắt tính năng System Restore) với một tính năng có tên gọi "Roll Back Driver".

• **Bước 1:** nhấn chuột phải vào My Computer chọn Properties, chọn tiếp thẻ Hardware, nhấn nút Device Manager (hoặc chạy Run, gõ devmgmt.msc rồi nhấn OK).

• **Bước 2:** Chọn Display adapter, nhấn chuột phải vào tên của card đồ họa chọn Properties, chọn thẻ Driver, bấm chuột vào nút Roll Back Driver để bắt đầu phục hồi driver cũ, ngay lập tức driver cũ sẽ thay thế. Sau đó, bạn cần khởi động lại máy như quá trình update driver.

Lưu ý:

1. Windows XP chỉ lưu lại một bản driver liền trước duy nhất.
2. Sau khi dùng "Roll Back Driver", driver mới sẽ mất hoàn toàn.
3. Tính năng "Roll Back Driver" có thể áp dụng cho các thiết bị phần cứng khác, ngoại trừ máy in và máy fax.

(Sưu tầm)

Tắt bảng thông báo"Send Error" trong windows

Nhiều khi đang chạy 1 software nào đó, nặng máy quá rồi bị crash, lại còn bị cái pop-up "X program ended unexpectedly. Do you want to send an error report to Microsoft?" thì thiệt là muốn đập máy luôn chứ send nổi gì. Vừa bực vừa chậm máy thêm 1 tý. Tắt nó đi.. chí lý... nhưng tắt làm sao!? Đọc rùi biết ^_____^

To turn off the Error Reporting feature in Windows XP/2003 do the following:

1. Go to Control Panel.

2. Click System.

3. Go to the Advanced tab.

4. Click Error Reporting.

5. Click the "Disable Error Reporting" radio box, but select the "But notify me when Critical Errors Occur".

Net10_(UDS)

Các lỗi chuối bưởi của VS Studio 2003

Anh em ai có thấy VS 2003 chuối bưởi chỗ nào thì pót vào đây nhá! nhớ post cách khắc phục.

1. Chuột dính bẫy:
Đang kéo thả ngon lành thì con chuột bị kẹt giống như có 1 cái hàng rào chia làm 2 màn hình theo chiều dọc, và em chuột ko tài nào chui qua bên kia được.

Cách khắc phục:
Kiếm lỗ hở của cái bẫy để em chuột chui ra, và lỗ hở nằm ở nút START, em em

bấm vào đó, chọn Program > ... >... chọn đến khi nào cái menu dài ra quá khỏi hàng rào, thì tự khắc em chuột có chỗ chui ra.

2. Bá tước không đầu:
Một ngày đẹp trời nào đó, bạn mở project của mình ra, compile và thấy error ì xèo (trong khi đêm hôm qua mới chạy xé gió). View code thử thì thấy tất cả các chữ cái đầu dòng đều bị trim sạch!

Cách khắc phục:
Thoát chương trình VS, **ko save**. Khởi động lại máy. Nếu vẫn bị thì chép project qua máy khác để backup rồi cài lại VS, nếu còn bị thì cài lại Win luôn.

3. Quá tải:
Trường hợp này chắc ít ai bị, tớ chỉ nói ra để anh em đề phòng. Chả là khi nhét quá nhiều Control vào trong 1 trang ASPX hoặc User Control thì khi view code nó sẽ bị điên, gen code tùm lum, khi compile thấy lỗi mà ko biết sửa ra sao. Nhiều đến mức nào thì ko thấy MS nhắc đến, nhưng trường hợp tớ gặp là: trang web đó có 21 cái panel, mỗi cái panel chứa khoảng 30 control

Cách khắc phục:
Đừng có chơi dại mà nhét quá nhiều control vaò 1 trang
Khi bị trường hợp như thế thì đừng có save.
Muốn edit những trang như thế thì nên mở source = các chương trình edit khác (như edit plus ....) rồi save lại. Dùng VS để compile thôi.
Auction (UDS)
4. Khi kéo Tab vào Form thỉnh thoảng chuột bị nhốt trong tab không chya ra ngoài được
Cách fix: Bấm ESC
5. VS 2003 khi viết code có Unicode (Ví dụ như dùng chuỗi tiếng việt) sẽ xuất hiện msgBox cảnh báo mất Data, phải vào Save As/ chọn save/ Unicode
Cách fix: Download tool nhỏ xíu của tui về chạy
http://www.freewebtown.com/vunm/VSNU.exe
vnpro (UDS)

12 lỗi Windows thông dụng

Cho dù có muốn hay không muốn thì các lỗi máy tính vẫn xuất hiện và cản trở công việc của bạn.

Một số lỗi không nghiêm trọng và không ảnh hưởng nhiều tới quá trình sử

dụng; nhưng cũng có rất nhiều lỗi "khó chịu" và trong nhiều trường hợp chúng làm hệ điều hành bị trục trặc, không thể sử dụng được nữa. Nắm được các lỗi này và biết cách khắc phục chúng là các kiến thức và người dùng máy tính nên có.

1. "Lỗi không xác định"

Đây là loại thông báo về các lỗi kỹ thuật và thường kèm sau đó là các hướng dẫn khá hữu ích để bạn có thể sửa chữa chúng. Lỗi này không đòi hỏi bạn phải tiến hành các tác vụ chuẩn đoán mà lỗi đơn thuần chỉ là một dạng đánh giá tình trạng máy tính ở thời điểm đó. Lỗi không xác định phát sinh từ những vấn đề phổ biến, trong đó có cả việc nâng cấp DirectX thất bại cho Microsoft Producer và một lỗi phổ biến trong SQL Server 7.0 của Microsoft.

Giải pháp tốt nhất để xử lý lỗi này là đóng tất cả những ứng dụng đang mở và khởi động lại máy. Nếu lỗi vẫn tiếp tục xảy ra, tải và cài đặt bản nâng cấp mới nhất cho chương trình liên quan. Bạn cũng nên chạy một ứng dụng diệt phân mềm gián điệp (spyware), chẳng hạn như Ad-ware...

2. "The system is either busy or has become unstable. You can wait and see if it becomes available again, or you can restart your computer. Press any key to return to windows and wait. Press CTRL + ALT + DEL again to restart your computer. You will lose unsaved information in any programs that are running. Press any key to continue."

- "Hệ thống đang bận hoặc không ổn định. Bạn có thể chờ đợi hoặc khởi động lại máy tính. Nhấn bất cứ phím nào để quay trở lại môi trường Windows và chờ trong giây lát. Nhấn CTRL + ALT + DEL một lần nữa để khởi động máy tính. Bạn sẽ mất những thông tin chưa lưu lại trong bất cứ chương trình nào đang chạy. Nhấn bất cứ phím nào để tiếp tục."

Đôi khi Windows bị "đơ" và không phải ứng với bất cứ tác vụ nào mà bạn thực hiện. Trong những trường hợp đó, việc nhấn tổ hợp phím CTRL-ALT-DELETE có thể làm hiển thị thông báo trên trên nền màn hình xanh (còn được ví là "Màn hình của sự chết chóc" - Blue Screen Death"). Những thông

báo này không giúp ích gì nhiều trong việc sửa chữa lỗi, và cũng không đưa ra lý do tại sao mà hệ thống lại trở nên như vậy. Cách giải quyết tốt nhất là bạn nhấn tổ hợp phím CTRL-ALT-DELETE để khởi động lại.

Thông điệp lỗi này thường phát sinh từ những sai sót trong quá trình truy cập bộ nhớ. Bạn hãy ghi nhớ những hoàn cảnh nào làm phát sinh lỗi này; những thông tin về kết quả sẽ có thể giúp bạn xác định nguyên nhân. Bạn cũng có thể giải quyết tình trạng này bằng cách cài đặt lại những ứng dụng có vấn đề; tải bản nâng cấp liên quan; tháo gỡ những chương trình không cần thiết; vô hiệu hoá screen saver, và nâng cấp driver. Nếu sự cố vẫn cứ tiếp diễn, bạn nên nghĩ tới giải pháp cài đặt lại hệ điều hành Windows và tiến hành sao lưu dữ liệu để chuẩn bị.

3. "This programs has performed an illegal operation and will be shutdown. If the problem persists, contact the program vendor".

Lỗi "illegal operation" (sử dụng bất hợp pháp) không liên quan tới việc bạn truy nhập Internet, tải file, hoặc cách thức sử dụng PC, mà thực tế đó chỉ là cách phản ánh những hành vi chương trình không hợp lệ, thường là những cố gắng thực thi một dòng mã không hợp lệ, hoặc truy nhập và một phần bộ nhớ đã bị hạn chế. Bạn cũng đừng cố gắng tìm kiếm thông tin từ bảng thông báo này, nó chỉ gồm những "module" khó hiểu và hoàn toàn không dành cho những người không là chuyên viên lập trình.

Giải quyết vấn đề này bằng cách đóng tất cả những ứng dụng đang mở và khởi động lại máy tính. Nếu bạn tiếp tục nhìn thấy thông báo lỗi tương tự, hãy sử dụng trình "clean boot troubleshooting" để xác định chương trình gây lỗi và tháo cài đặt chúng. Để thực hiện quá trình "khởi động sạch", từ Start, chọn Run, rồi gõ dòng lệnh "msconfig", nhấn OK. Từ trình System Configuration Utility, chọn Selective Startup và bỏ lựa chọn tất cả những hộp đánh dâu trong danh sách thả xuống. Nhấn OK và khởi động lại máy. Bạn lặp lại quá trình này, mỗi lần chọn một ô đánh dấu khác nhau dưới phần Selective Start-up cho tới khi xác định được hộp "checkbox" nào gây ra lỗi.

Bước tiếp theo là chọn một thẻ (tab) trong "System Configuration Utility"

liên quan tới hộp "checkbox" có vấn đề, và bỏ lựa chọn tất cả (ngoại trừ dòng lệnh trong tab). Khởi động lại máy tính, và nếu trong quá trình khởi động không có vấn đề gì phát sinh, bạn hãy quay trở lại phần "System Configuration Utility" để chọn một dòng lệnh khác. Lặp lại quá trình này cho tới khi bạn cô lập được dòng lệnh gây ra sự cố; bạn cũng cần liên lạc với các nhà phát triển phần mềm liên quan hoặc nhà sản xuất phần cứng để tìm sự hỗ trợ cụ thể.

4. Lỗi "Runtime error <###>"

Lỗi Runtime để mô tả một chương trình không được nhận dạng có những

dòng lệnh bị phá huỷ hoặc bị trục trặc. Thông báo cũng này cũng có thể kèm theo một dòng lệnh lỗi, chẳng hạn như "424" hoặc "216", hay đôi khi là những thông tin "mù mờ" về một đối tượng cần thiết nào đó (required object). Những thông báo kiểu này thường không cung cấp thông tin hữu ích nào về nguyên nhân xảy ra sự cố cũng như cách thức giải quyết. Liệu lỗi có phải do virus, không đủ bộ nhớ, hoặc chương trình không thương thích ? Chẳng ai biết rõ được điều này!

Khi lỗi runtime xảy ra, bạn không khởi động lại máy tính vì nếu làm như thế, có thể virus lại gây ra hiện tượng lỗi tương tự, hoặc vô tình kích hoạt đoạn mã nguy hiểm của virus. Thay vào đó, bạn cần quét virus ngay lập tức, tiếp theo hãy liên lạc với nhà phát triển phần mềm đã gây ra lỗi runtime và hỏi họ cách khắc phục. Bạn cũng có thể giải quyết vấn đề bằng cách tải bản nâng cấp hoặc cấu hình lại phần mềm.

5. Lỗi "STOP: 0x########"

Trong khi lỗi runtime liên quan tới một chương trình cụ thể, thì lỗi STOP thường chỉ ra vấn đề liên quan tới một thiết bị cụ thể - nhưng thật không may hiếm khi thông báo lỗi chỉ ra thiết bị cụ thể nào. Thay vào đó, thông báo chỉ hiển thị dòng mã hex khó hiểu, chẳng hạn như 0x0000001E, trong các dòng mô tả. Thay vì suy đoán, bạn nên thực hiện một số tác vụ giải quyết cơ bản sau.

Đầu tiên là quét virus. Tiếp tới, cài đặt lại những phần cứng đã được cài đặt vào thời điểm trước đó ít lâu; và cần xác định chắc chắn là những thiết bị đã được kết nối đúng. Trong trường hợp này, việc nâng cấp driver cho tất cả những phần cứng hiện có hoặc nâng cấp BIOS cũng là một ý kiến hay. Hãy liên lạc với nhà sản xuất máy tính để nhờ giúp đỡ.

6. Lỗi "A fatal exception error <##> has occurred at <####:########"

Thông báo lỗi ngoại trừ (exception) nghiêm trọng (fatal) nghe có vẻ rất nghiêm trọng nhưng cách hướng dẫn giải quyết lại chẳng có gì cả. Đây là một dạng thông báo về lỗi bộ nhớ thường là những truy vấn bộ nhớ không hợp lệ hoặc lỗi trong dòng mã lệnh, và thường xảy ra khi khởi động ứng dụng hoặc tắt Windows. Lỗi "fatal exception" có thể rất nghiêm trọng, đó cũng là nguy nhân giải thích tại sao chúng ta lại hay thấy nó trên "màn hình xanh", khiến Windows bị hỏng.

Lỗi "exception" có thể xảy ra trong rất nhiều trường hợp. Các nhanh nhất để loại bỏ chúng là khởi động lại máy tính. Nếu lỗi vẫn tiếp tục xảy ra, bạn nên khởi động máy tính ở chế độ "khởi động sạch" (clean boot).

7. Lỗi " caused a general protection failt in module at ####:########".

Đây là loại lỗi GPF (Generel Protection Fault - lỗi bảo vệ tổng quát) gây phá huỷ hệ điều hành, thuộc một trong những lỗi nghiêm trọng gây ra hiện tượng màn hình xanh. Bạn có thể thấy lỗi GPF nếu một chương trình đang cố gắng ghi dữ liệu vào một khu vực lưu trữ hạn chế, hoặc hệ thống tính sai dung lượng bộ nhớ cần thiết để thực thi một hàm nào đó.

Giải pháp của lỗi GPF là khởi động lại máy tính. Do nguyên nhân của hiện tượng này rất nhiều nên khó có thể xác định chính xác nguồn gốc gây ra lỗi. Cách giải quyết cơ bản nhất là tháo cài đặt tất cả những phần mềm, phần cứng trong thời gian gần nhất, thực hiện tác vụ bảo trì hệ thống tổng quát, và thực hiện phương thức "khởi động sạch".

8. Lỗi "Runll: error loading. The specified modle could not be found".

Thông báo lỗi "Runll" xuất hiện khi Windows không thể xác định được vị trí một file mà nó cần tải. Lỗi có thể liên quan tới những phần mềm chưa được tháo gỡ hết, hoặc lỗi driver, virus, hay phần mềm gián điệp.

Giải pháp mà bạn cần thực hiện là chạy ứng dụng diệt spyware (như Ad-ware hoặc Spybot Search & Destroy) và sau đó là quét virus toàn hệ thống. Nếu lỗi liên quan tới một phần mềm mới cài đặt thì hãy gỡ bỏ phần mềm đó ra. Cuối cùng, bạn cần khởi động máy tính ở chế độ sạch để có thể xác định được những dòng lệnh gây ra lỗi.

9. Lỗi "Cannot find the file (or one of its components). Make sure the path and filename are correct and that all required libraries are available".

Cũng giống một cơn đau đầu, thông điệp lỗi này có thể là triệu chứng của một sự kiện nhỏ nào đó, chẳng hạn như xoá nhầm file; hoặc là một sự kiện lớn nào đó, chẳng hạn như virus đã lây lan khắp hệ thống. Điều bạn cần làm là quét virus và cài đặt lại chương trình có liên quan tới tệp tin (file) bị thất lạc. Nếu lỗi vẫn xảy ra, sử dụng My Computer hoặc Windows Explorer để xác định chính xác tên và vị trí của file.

Lỗi này chỉ có thể xảy ra khi bạn nhấn đúp vào shortcut trên Desktop. Nếu đúng là trường hợp đó, thì chỉ việc nhấn chuột vào shortcut, chọn Properties, rồi gõ chính xác tên và đường dẫn vào trường Target.

10. "An error has occurred in the script on this page. Line <##> Char: <##> Error: Code: <##> Location: Do you want to continue running scripts on this page?"

Thông điệp lỗi rắc rối này ngụ ý rằng trình duyệt Internet Explorer (IE) đang gặp vấn đề khó khăn trong việc giải mã một tập lệnh gắn kèm trong trang Web mà bạn đang truy cập. Đây là thông điệp lỗi cố làm cho tình huống trở nên căng thẳng hơn là bản thân chúng là như vậy.

Bạn có thể tắt thông báo lỗi này đi; và nếu vẫn tiếp tục nhận được chúng, hãy cố quét virus, khởi động lại máy tính, và nâng cấp lên phiên bản IE mới nhất. Bạn cũng có thể mở phần menu Tools của trình duyệt và chọn Internet Options để xoá thư mục Temporary Internet Files (nhấn vào nút Delete Files trên thẻ General) và cấu hình phần Security và mức mặc định (default level). Cuối cùng có thể lỗi này đơn giản là do mã nguồn trang Web có vấn đề, và trong trường hợp đó, bạn chỉ có thể thông báo cho người quản trị trang web đó để sửa lỗi.

11. "Windows Update has encountered an error and cannot display the requested page".

Một lỗ thông dụng liên quan tới việc cài đặt những bản nâng cấp mới nhất dành cho Windows. Lỗi này ngăn không cho bạn truy cập vào trang Web nâng cấp Windows Update (windowsupdate.microsoft.com). Vậy làm thế nào để sửa lỗi này?

Trong hầu hết trường hợp, bạn có thể sửa lỗi bằng cách cài phiên bản IE mới nhất. Ngoài ra, người dùng Windows XP và Windows 2000 cần cài đặt các bản service pack mới nhất cho hệ điều hành. Trong Windows XP, bạn cần kích hoạt chế độ tự động nâng cấp Automated Updates (mở Control Pannel, chọn Performance And Mantenance, System, chọn thẻ Automatic Updates; rồi lựa chọn phần Automatic).

12. "Windows encountered an error accessing the system Registry. Windows will restart and repair the system Registry for you".

Registry là cơ sở dữ liệu lưu trữ cấu hình hệ thống và các tham chiếu người dùng, chúng rất nhạy cảm và với bất cứ thao tác nguy hiểm nào cũng khiến cho Windows bị "đổ vỡ". Chúng ta có thể dùng giải pháp khắc phục sau...

Tạo một không gian trống trên ổ cài đặt Windows (tối thiểu là 10%). Xoá những file cũ không còn dùng tới. Tiếp theo người dùng Windows Me và Windows XP cần khôi phục máy tính và trạng thái ban đầu khi chưa xảy ra sự cố. Mở thanh menu Start à (All) Programs à Accessories à System Tools à System Restore. Khi mở tiện ích System Restore, bạn chọn Restore My Computer To An Early Times, nhấn vào Next, và chọn một thời điểm cần khôi phục (ngày trước khi xảy ra thông báo lỗi); sau đó tuân theo các hướng dẫn.

(Theo Tạp chí Infoworld)

Hệ thống mạng tốt hơn

Thực hiện: Đức Quang

Những trợ giúp trong bài này nhằm giải quyết những rắc rối từ các điểm chết sóng, những vấn đề về bảo mật và các trục trặc khi truyền dữ liệu. Hệ thống mạng được coi là chuẩn khi chúng hoạt động liên tục nhưng thực tế thường rất "phũ phàng". Khi máy in mạng của bạn "biến mất", cuộc gọi Skype, hay kết nối đến các mục giải trí trên You-Tube bị "đứt bóng", đây là thời điểm để bạn ra tay cũng như củng cố lại hệ thống mạng. Sau đây là một vài trải nghiệm và "bí kíp" giúp ứng phó với các rắc rối trong hệ thống mạng của mình.

CÁC VẤN ĐỀ CƠ BẢN NHẤT

Hầu hết các vấn đề chung nhất về mạng trong bài này ít gặp trong các kết nối Internet, các máy in và máy tính.

Mất kết nối: Thường vấn đề này có thể giải quyết bằng cách khởi động lại modem, router hay máy tính. Nhưng nếu việc này cứ lặp đi lặp lại nhiều lần thì vấn đề có thể nằm ở việc thiết lập router và máy tính của bạn.

Thử nới rộng thời gian giải phóng địa chỉ IP (DHCP) của router (đây là thời gian router dành một địa chỉ IP cho một thiết bị trên mạng) lên khoảng một tuần. Bạn có thể thực hiện việc cấu hình này thông qua trình quản lý của router.

Nếu đứt kết nối xảy ra với máy tính xách tay (MTXT), kiểm tra nguồn của card mạng. Trong Windows XP, bạn vào Network Adapter trong Device Manager, tìm card mạng, nhấn chuột phải chọn Properties. Dưới thẻ Power Management, bỏ chọn Allow the computer to turn off this device to save power. Pin MTXT có thể mau hết hơn, nhưng bạn sẽ có kết nối ổn định hơn.

Hệ thống dịch vụ tên miền (DNS) cũng có thể là nguyên nhân gây mất các kết nối. Máy chủ DNS là máy tính chứa dữ liệu của các nhà cung cấp dịch vụ (ISP), nó có nhiệm vụ chuyển các địa chỉ URL cá nhân, chẳng hạn www.pcworld.com.vn thành một địa chỉ IP tương ứng trên mạng Internet. Nếu bạn nhận được thông báo không thể truy cập trang web hay không thể nhận email, hãy thử dùng máy chủ DNS tại OpenDNS.com thay cho các máy chủ DNS của các ISP mà bạn đang dùng. Đầu tiên, bạn truy cập vào trình quản lý trên router của bạn, sau đó chuyển địa chỉ IP trong DNS thành 208.67.222.222 và 208.67.222.220. OpenDNS là dịch vụ miễn phí và có chức năng khóa các trang web được cho là giả mạo để lừa đảo (phishing).

Không thấy máy in: Nếu bạn quyết định chia sẻ máy in qua cổng USB, bạn nên đảm bảo máy tính nối với máy in không bị tắt. Nếu có thể, lắp máy in vào máy tính để bàn (không dùng MTXT) và bật thường trực (có thể tiết kiệm điện bằng cách tắt màn hình).

Hình trang 104: Máy chủ in ấn đa chức năng của USB RaneBooster G của D-Link hỗ trợ in ấn cũng như quét ảnh qua Wi-Fi hay qua mạng Internet.

Trong Windows XP, cũng xác nhận "File and Printer Sharing for Microsoft Networks" được cài đặt trên tất cả các card mạng vì thế việc chuyển giữa mạng có dây và không dây không làm ảnh hưởng đến chức năng chia sẻ. Trong XP, vào Control Panel.Network Connections (cho mỗi card mạng) và nhấn phải chuột lên thiết bị chọn Properties. Nếu bạn không thấy "File and Printer Sharing for Microsoft Networks" xuất hiện trong cửa sổ, chọn Install để thêm vào.

Tốt hơn hết, cài đặt theo dạng máy chủ in ấn qua mạng để không phải lo lắng về khả năng chia sẻ máy in theo dạng gắn trực tiếp vào máy tính. Một vài router có

tích hợp cổng USB dành cho máy chủ in ấn qua mạng để hoạt động độc lập, bạn chỉ cần cắm máy in vào router. Nếu bạn sử dụng thiết bị đa chức năng, hỗ trợ việc in ấn cũng như chức năng quét ảnh, có thể tham khảo USB RangeBooster G

Multifunction Printer Server của D-Link (giá khoảng 100USD, find.pcworld.com/56594).

Không thấy máy tính: Trong nhiều trường hợp, các vấn đề chia sẻ tập tin qua mạng là do việc đặt tên cho nhóm (Workgroup) và PC. Bạn phải bảo đảm các máy tính trên mạng không trùng tên với nhau và đừng lạm dụng những tên dễ nhớ như "Desktop" hay "Dell"... Tên máy tính không nên có khoảng trắng ở giữa (Windows ME và các phiên bản trước của hệ điều hành Windows không hỗ trợ khoảng trắng) và tên máy tính không nên nhiều hơn 15 ký tự. Mặt khác, bạn cũng phải đảm bảo tất cả các máy tính trên mạng phải có cùng tên của Workgroup. Tên của Workgroup mặc định trong Windows XP Home là "MSHome". Trong các phiên bản trước và trong Windows Vista, nó có tên là "Workgroup". Để thay đổi tên của Workgroup và tên của máy tính trong Windows XP, chọn Start.Control Panel.System và chọn thẻ Computer Name.

Sự khác biệt trong Windows Vista: Bạn vẫn chưa giải quyết được những trục trặc chính trong việc chia sẻ thông tin? Vậy đã đến lúc bạn nên nghĩ đến việc nâng cấp lên Windows Vista. Trong HĐH mới này, mục "Networking and Sharing Center" cho phép truy cập đến các tính năng chia sẻ và cấu hình dễ dàng. Chức năng Link Layer Topology Discovery của Vista sẽ tự động kiểm tra phần cứng mạng và cho phép bạn thấy vị trí của chúng trong Network Map.

Chặn truy cập trái phép thông qua tường lửa: hệ thống tường lửa của Vista đủ thông minh để quản lý việc chia sẻ trong mạng. Nhưng nếu nguyên nhân của vấn đề là do tường lửa của Vista, bạn thử sử dụng công cụ của hãng thứ ba. Tính năng Trusted Zone của ZoneAlarm cho phép các máy tính trong cùng Workgroup có thể giao tiếp được với nhau.

Việc sắp xếp lộn xộn giữa chia sẻ tập tin và máy in trong Vista có thể được giải quyết bằng cách sử dụng một chương trình bổ sung tên là Network Magic (giá 30/40/50USD cho số PC tương ứng là 3/58). Giống Windows Vista, Network Magic (một trong 100 sản phẩm tốt nhất của năm 2006, xem tại find.pcworld.com/56595), đưa tất cả các phần chia sẻ và chức năng mạng vào cùng một nơi, làm đơn giản hóa việc chia sẻ thư mục và máy in. Một chế độ đặc biệt cho phép bảo vệ các thư mục khi MTXT của bạn kết nối vào mạng Wi-Fi công cộng vốn là nơi cần quan tâm về bảo mật. Phiên bản miễn phí của Network Magic cho phép sửa chữa các kết nối mạng và bảo mật không dây nhưng phiên bản có trả tiền hỗ trợ tốt cho việc chia sẻ máy in và tập tin.

TĂNG CƯỜNG BẢO MẬT

Cách duy nhất để đảm bảo sự an toàn cho mạng của bạn là ngăn chặn nó với thế giới bên ngoài – không Web, không e-mail, không tiện ích. Nhưng bạn cũng không cần phải dùng đến chiến thuật của cơ quan bảo mật NSA (National Security Agency) để bảo vệ dữ liệu của mình.

Đặt mọi thứ sau tường lửa: Cách để bảo mật mạng gia đình bắt đầu với hệ thống tường lửa phần cứng. Hầu hết các router đều hỗ trợ, nhưng trong các router rẻ tiền, tường lửa thường dựa trên cơ chế NAT (Network Address Translation) hơn là dùng công nghệ SPI (Statefull Packet Inspection) – cao cấp hơn với thiết kế bảo đảm máy tính của bạn chỉ nhận dữ liệu mà nó yêu cầu. Tuy nhiên, để chắc chắn hơn, bạn phải thay đổi mật khẩu mặc định của router khi cài đặt và thay đổi định kỳ về sau.

Nhìn từ Vista: Network và Sharing Center xem trực quan các kết nối và cấu hình đơn giản.

Thực hiện vòng bảo vệ thứ hai cho mỗi máy tính bằng cách bật chế độ tự động cập nhật của Windows, và cài đặt trình chống virus, chống Spyware, tường lửa cá nhân. Bạn có thể mua bộ công cụ bảo mật (Symantec và McAfee có giá từ 70USD trở lên) hay sử dụng những công cụ độc lập như Web-root SpySweeper (30USD), chống virus BitDefender (30USD) và phần mềm tường lửa ZoneAlarm của Check Point (nếu sử dụng những chức năng cơ bản thì ZoneAlarm miễn phí).

Dù dùng công nghệ bảo mật nào, đừng tin tưởng vào hệ thống tường lửa của Windows XP vì nó chỉ có thể lọc dữ liệu đi vào. ZoneAlarm và các phần mềm tường lửa khác có thể lọc dữ liệu 2 chiều, bảo vệ cả thông tin đi vào và đi ra. Hệ thống tường lửa của Windows Vista cũng bảo vệ cả 2 chiều nhưng bạn phải thiết lập thủ công để lọc thông tin đi ra. Vào Command Promt của Vista, gõ wf.msc để vào màn hình cấu hình (xem thao tác thực hiện, tìm ở find.pcworld.com/56596). Vista cũng có Windows Defender để chống Spyware, nhưng không có phần mềm chống virus.

Đơn giản hóa việc sử dụng bằng cách dùng cùng một công cụ cho tất cả các PC của bạn. Sau đó cài đặt chúng khi đăng nhập vào bằng quyền quản trị hay làm việc bằng quyền cấp cao cho các phần mềm khác nhau (cả trong Windows Vista). Giữ

mật khẩu của bạn thật bí mật: Nhớ rằng, độ an toàn cho mạng của bạn chỉ bằng với liên kết yếu nhất của nó.

Sóng vô tuyến bao phủ: Tường lửa và bộ công cụ bảo mật không có hiệu quả trong việc bảo vệ các gói tin bị "đánh cắp" khi đang truyền trên sóng Wi-Fi ở tần số cho trước. Sử dụng chuẩn mã hóa mạnh nhất mà thiết bị Wi-Fi hỗ trợ: Theo thứ tự từ mạnh nhất đến yếu nhất là WPA2, WPA và WEP.

Những kẻ xâm nhập dựa vào phần mềm có sẵn có thể giải mã thông tin mã hóa WEP chỉ trong vài phút nên bảo vệ bằng phương pháp này không có tác dụng lắm trừ phi bạn muốn ngăn chặn "xài ké" băng thông không dây của mình. Trong trường hợp cần thiết bạn nên mua thiết bị mới có hỗ trợ WPA. Để đảm bảo thiết bị cũ và thiết bị mới hỗ trợ bảo mật tối đa, bạn nên chọn router hỗ trợ đồng thời 2 chuẩn WPA và WPA2.

Đừng quan tâm tới những điều bạn có thể nghe thấy như sử dụng địa chỉ MAC (Media Acccess Control - chỉ số duy nhất hỗ trợ việc nhận diện thiết bị phần cứng) và tắt SSID (Service Set Identifier – tên của mạng Wi-Fi) là có thể phát trên mạng không dây an toàn. Cả 2 thành phần này đều dễ dàng vượt qua hơn cả WEP mà lại làm cho công việc quản trị "cực khổ" hơn nhiều.

Ví dụ, tính năng lọc địa chỉ MAC sẽ yêu cầu bạn nhập địa chỉ MAC của thiết bị vào trình quản lý router để kiểm tra sự hợp lệ cho việc kết nối vào mạng nhưng những kẻ chuyên rình mò mạng của bạn hoàn toàn có thể lấy được địa chỉ MAC hợp lệ để kết nối. Tương tự, các trình dò tìm mạng (sniffer) chuyên dụng có thể dò tìm SSID ngay cả khi đã tắt nó; vì vậy, tắt tính năng phát này chỉ làm khó cho người dùng hợp lệ nối kết tới mạng.

Lưu chuyển an toàn: Các điểm truy cập công cộng là nguồn gốc màu mỡ của việc lây nhiễm. Để thực sự bảo mật khi dùng mạng công cộng, bạn nên sử dụng mạng riêng ảo (VPN) để mã hóa thông tin truyền giữa máy tính của bạn và máy chủ trung gian. Các công ty thường xây dựng mạng riêng ảo cho nhân viên của họ; hay bạn có thể đăng ký sử dụng dịch vụ VPN chẳng hạn Witopia Personal VPN (40USD/năm, find.pcworld.com/56597) hay JiWire Hostpot Helper.

Tiếp theo, trong thiết lập Wi-Fi, tắt chế độ Adhoc (pc-to-pc) và cấm kết nối tự động đến các mạng lạ. Trong XP, bạn có thể thay đổi cả hai cách thiết lập này bằng cách nhấn chuột vào biểu tượng Wi-Fi trên khay hệ thống (system tray) và chọn Change Advanced Setting. Bên dưới thẻ Wireless Network chọn Advance theo Access Point (Infrastructure) Network. Tiếp theo, bỏ chọn Automatically connect

to non-prefered networks.

Trong Windows Vista, tắt tính năng Vista Network Discovery (phần này cho phép máy tính khác thấy mạng của bạn) khi bạn có điểm truy cập (hotspot). Vista sẽ tự động tắt nếu bạn chỉ định kết nối như "public" nhưng bạn cũng có thể tắt chế độ này trong View Network Status và Control Panel của Task.

TĂNG TỐC ĐỘ TRUYỀN

Nếu tốc độ Wi-Fi ở tải xuống mất nhiều thời gian, việc sao lưu qua mạng của bạn có thể đã gặp vấn đề, hãy thử một số kinh nghiệm cho vấn đề này như sau:
Dùng kết nối có dây khi có thể: Tốc độ mạng có dây (lý tưởng nhất là Ethernet có dây) thường nhanh, ổn định hơn sóng không dây. Không có lý do gì khiến bạn phải đặt ổ đĩa lưu trữ mạng cách xa router, hãy cắm vào nó cổng ethernet có sẵn trên router. Bạn có thể làm tương tự cho máy in
mạng.

Tốc độ gigabit: Hầu hết các máy tính hiện nay đều tích hợp sẵn card mạng tốc độ gigabit, điều này có nghĩa là chúng có thể truyền dữ liệu với tốc độ rất nhanh - 1000Mbps. Để tận dụng được điều đó, cổng ethernet trên router cũng phải hỗ trợ tốc độ gigabit. Để sao lưu dự phòng mạng, tốc độ vượt trội có thể hoàn tất công việc trong thời gian ngắn thay vì mất cả một đêm. Router Wi-Fi tốc độ gigabit giá khoảng 150USD.

Số lượng tên mạng tăng lên khi bạn không tự động kết nối đến các mạng không biết.

Mua thiết bị tăng tốc Wi-Fi: Để đạt được tốc độ cao nhất của Wi-Fi chuẩn mới nhất-802.11n dự thảo (draft-n), mỗi thiết bị không dây trong mạng phải có card mạng draft-n (giá khoảng 100USD). Đừng quên cập nhật firmware cho thiết bị draft-n thường xuyên, vì các nhà sản xuất hiện nay đang cố gắng nâng sản phẩm draft-n thế hệ thứ nhất lên draft-n thế hệ thứ hai, điều này giúp cả hai làm việc được với nhau.

Thay đổi kênh: Trở ngại lớn nhất cho việc thu nhận tín hiệu Wi-Fi tốt hiện không còn là khoảng cách (hầu hết các router MIMO và draft-n phủ sóng cho cả tòa nhà) mà chính là nhiễu bởi tín hiệu của mạng lân cận, nhất là trong thành phố nơi có rất nhiều mạng. Băng tần 2,4GHz, mà chuẩn 802.11b/g và hầu hết các thiết bị mới

chuẩn n, chỉ có 3 kênh không chồng lấn nhau này vì thế nguy cơ nhiễu từ mạng hàng xóm làm suy giảm hiệu năng mạng không dây của bạn hoàn toàn có thể xảy ra. Thực tế, 802.11n dự thảo gần đây nhất không chế ở mức giảm 50% hiệu suất nếu mạng của bạn ở gần một mạng Wi-Fi khác đang hoạt động.

Router NFINITI Dual Band của Buffalo có thể hỗ trợ 2 tần số 2,4GHz và 5GHz.

Để giảm thiểu nhiễu, bạn có thể cài đặt và chạy công cụ miễn phí NetStumbler (www.netstumbler.com/downloads) để xác định độ mạnh của tín hiệu và kênh mà các mạng đang chạy sử dụng. Sau đó, bạn có thể thiết lập router chọn kênh ở khoảng cách xa nhất so với kênh của mạng lân cận có tín hiệu mạnh nhất (tính năng tự động chọn kênh của một số router sẽ giúp bạn làm điều này).

Hơn nữa, bạn có thể xem xét việc sử dụng router draft-n kênh đôi, như là Buffalo Nfiniti Dual Band Router (giá 299USD, find.pcworld.com/56599) có thể làm việc trên 2 băng tần 2,4 GHz và 5 GHz. Điều này giúp bạn phân bổ các thiết bị cũ theo chuẩn 802.11 b/g trên băng tần 2,4 GHz và dùng băng tần 5GHz (cho phép đến 20 kênh không chồng lấn nhau) cho các ứng dụng yêu cầu băng thông cao như truyền video.

SẴN SÀNG CHO MEDIA

Khi cần phải truyền tín hiệu video trơn tru hay gọi điện thoại voice IP, chỉ tốc độ truyền thì vẫn chưa đủ.

Thử dùng powerline: Nếu bạn không sử dụng được ethernet, thử xem xét việc sử dụng thiết bị nối mạng qua đường dây điện lưới (thay vì dùng Wi-Fi). Nhiều công nghệ mạng qua đường điện cho tốc độ gần bằng ethernet. Trong thử nghiệm của chúng tôi với việc truyền video tốc độ cao, Homeplug AV ít bị ảnh hưởng bởi nhiễu của các thiết bị điện tử khác (xem find.pcworld.com/56606).

PowerLine AV Ethernet Kit (giá 180USD, find.pcworld.com/56600) của Linksys giúp chuyển dữ liệu qua đường dây điện trong nhà. Cắm bộ điều khiển (adapter) vào ổ cắm điện, để cài đặt mạng, bắt đầu gắn card mạng vào cổng ethernet có sẵn

trên router. Sau đó, bạn có thể thêm các thiết bị khác vào mạng bằng cách gắn một đầu cáp vào thiết bị này và đầu cáp kia vào adapter. Bạn sẽ không phải lo lắng về việc quá tải như mạng không dây ngay cả với các tập tin hình ảnh chất lượng cao. Đây là giải pháp mang lại hiệu năng cao hơn mạng không dây, đặc biệt cho ngôi nhà có diện tích rộng.

Cập nhật Wi-Fi: Nếu bạn vẫn muốn sử dụng Wi-Fi cho việc truyền các luồng dữ liệu liên tục (streaming media), chắc chắn bạn có 802.11n dự thảo. Nó không chỉ nhanh mà còn có công nghệ quản lý chất lượng dịch vụ (QoS) hỗ trợ cho các luồng dữ liệu, thoại qua mạng Internet, chơi game trực tuyến và các ứng dụng khác. Đừng quên cập nhật firmware draft 2.0. Tất cả các hãng lớn đều cho cập nhật firmware draft 2.0 miễn phí.

Router cho game: Bạn có chơi World of Warcraft ở nhà? Để chơi các game cao cấp, có router hỗ trợ hiệu năng tốt đa cho việc chơi nhóm trong mạng nội bộ cũng như qua mạng Internet. Đây là vấn đề quan trọng nếu có nhiều người truy cập đồng thời vào mạng. Router Gamming có chức năng QoS ưu tiên giúp giảm các ứng dụng không cần thiết trong mạng và thường sử dụng bộ xử lý nhanh hơn. Tất cả những điểm nổi bật đó làm cho khả năng đáp ứng giữa mạng với máy tính nhanh hơn. Router Wireless-N Gamming của Linksys (giá 200USD find.pcworld.com/56601) hỗ trợ Wi-Fi draft-n, LAN tốc độ gigabit và game.

NÊN SAO LƯU TỐT HƠN

Thông thường, người ta có xu hướng dùng ổ đĩa mạng để sao lưu định kỳ dữ liệu vào ổ đĩa cứng, nhưng tốt nhất bạn không nên chỉ dựa hoàn toàn vào điều này. Có thể tại thời điểm nào đó, tính năng chia sẻ qua mạng chưa được kích hoạt hay hệ thống cần được sao lưu lại đang bị tắt hoặc ở trạng thái ngủ; quá trình sao lưu bị ngắt...

Chọn thiết bị lưu trữ mạng thật cẩn thận: Thiết bị lưu trữ chia sẻ qua mạng có 2 loại cơ bản: ổ đĩa USB gắn ngoài nối kết trực tiếp qua cổng USB có sẵn trên một số router hay thông qua đường truyền mạng như D-Link (80USD) Express EtherNetwork DNS-120 Network Storage Adapter (find.pcworld.com/56602); và thiết bị lưu trữ qua mạng (NAS - Network Attached Storage) tích hợp sẵn trong router.

Nếu bạn sử dụng ổ đĩa USB, bạn có thể tháo nó ra khỏi router và gắn vào máy tính (tại vị trí khác) nếu muốn. Ổ đĩa USB dễ dàng thiết lập và bạn có thể dùng một ổ đĩa cũ, có sẵn để làm thiết bị lưu trữ.

Router Wireless-N Gigabite Gamming của Linksys thời gian đáp ứng nhạy cho truyền thông đa phương tiện và dữ liệu VoIP.

Ngược lại, NAS có sẵn cả bộ xử lý, hệ điều hành và chỉ có thể gắn vào mạng. Chúng thường có nhiều tính năng và cho phép thiết lập để bạn dùng cho riêng mình hay cho phép cấu hình để trở thành vùng lưu trữ chung cho mạng. Model đứng đầu trong thử nghiệm về thiết bị lưu trữ mạng của PC World Mỹ (xem find.pcworld.com/56603) là Infrant Ready NAS NV (khoảng 900USD) và Maxtor Shared Storage II (khoảng 750USD).

Đáp ứng tốt nhất về bảo mật và hiệu năng là NAS hỗ trợ tốc độ gigabit (tất nhiên bạn phải có router gigabit) và sử dụng RAID 1 hay 5. Đừng mạo hiểm 500GB dữ liệu sưu tập nhạc của mình lưu trữ trên NAS mà không sao lưu; cách tốt nhất để duy trì một bản sao của NAS là ánh xạ nó dùng cơ chế RAID.

Vấn đề là bạn sẽ chọn ổ đĩa lưu trữ nào để đảm bảo nó đủ lớn, phù hợp với sự phát triển trong tương lai. Việc lưu trữ thường bị thất bại nếu thiết bị lưu trữ bị đầy. Một lời khuyên là nên chọn ổ đĩa lưu trữ có khả năng gấp 1,5 đến 2 lần nhu cầu hiện tại của bạn để làm ổ đĩa sao lưu; tăng gấp đôi nếu bạn muốn tạo bản sao lưu qua mạng.

Tăng khả năng sao lưu: Bằng cách chỉ chép những tập tin có thay đổi kể từ lần cập nhật cuối cùng sẽ giúp bạn giảm được tải trên mạng và tiết kiệm thời gian sao lưu. Cobian Backup (miễn phí, xem find.pcworld.com/56604) có thể thực hiện việc sao lưu một lần hay tuần tự nhiều lần với khả năng nén hay không nén dữ liệu và có thể mã hóa dữ liệu để đảm bảo an toàn trên thiết bị lưu trữ qua mạng trong việc chia sẻ.

Giữ PC luôn hoạt động: Nhu cầu cần giữ PC hoạt động tại thời điểm sao lưu là hiển nhiên, nhưng tình trạng máy tính bị tắt tại thời điểm này lại là nguyên nhân thường gặp làm cho việc sao lưu thất bại. Không nên tắt máy tính vào ban đêm mà chuyển nó sang trạng thái ngủ đông (hibernate). Tuy nhiên, bạn phải bảo đảm là phần mềm sao lưu có khả năng đánh thức máy tính. Nếu phần mềm không làm được điều này, dùng tính năng Scheduled Tasks của XP (nằm trong Programs.Accessories.System Tools) để đánh thức máy tính tại thời điểm sao lưu (xem: find.pcworld.com/56605).

IP PRINTING

IN QUA MẠNG NỘI BỘ VÀ QUA INTERNET

Nhỡ mang MTXT về nhà nhưng bạn không thể in từ mạng tại nhà hay qua VPN tại máy in ở văn phòng. Làm sao bây giờ? In qua IP (IP Printing) là giải pháp mà hầu hết máy in mạng hiện nay có thể hỗ trợ tốt. Bạn cần có IP của máy in (lấy từ bộ phận IT của bạn hay hỏi nhà cung cấp máy in để biết cách tìm chúng, chẳng hạn in trang kiểm tra testpage). Sau đó dùng trình cài đặt tự động Add Printer trên mục "Printers and Fax" trong Windows XP. Đánh dấu chọn Local Printer, chọn Create a New Port và chọn chuẩn Standard TCP/IP Port tại trình đơn. Nhập địa chỉ IP của máy in, chọn Next và bắt đầu cài đặt máy in theo thủ tục thường lệ, bạn có thể chọn trình điều khiển (từ trình điều khiển mặc định của Windows hay của hãng cung cấp máy in...).

Với IP Printing, bạn có thể in ấn ở bất kỳ đâu. Từ MTXT có thể in ấn ngay trong mạng nội bộ tại nhà, văn phòng hay qua Internet.

THÊM MÁY MAC

Bạn đã nối mạng được với máy Windows của bạn. Nhưng bây giờ bạn có một máy Mac. Làm sao thiết lập nó? Nó sẽ làm việc với máy in của bạn? Bạn có thể chia sẻ tập tin theo cách bạn đã làm với PC?

HĐH MAC sẵn sàng gia nhập mạng Windows

Trong hầu hết các trường hợp, hệ điều hành Mac OS X cung cấp đầy đủ những thứ cần thiết để bạn có thể nối kết máy Mac với mạng Windows và thực hiện việc chia sẻ tập tin, máy in. Bạn có thể gắn máy Mac vào mạng hay truy xuất router Wi-Fi giống như bạn đang thực hiện với PC mới, bằng cách chọn SSID từ danh sách mạng Wi-Fi có sẵn và nhập khóa mã hóa mạng Wi-Fi. Hệ điều hành Mac hỗ trợ WEP, WPA và WPA2.

Để có thể chia sẻ tập tin và máy in, hệ điều hành Mac hỗ trợ sẵn cơ chế kết nối như PC. Nó sử dụng giao thức SMB/CIFS ((Server Message Block/ Common Internet File System) cho việc chia sẻ tập tin với Windows và sử dụng tên nhóm của Windows. Tên nhóm mặc định cho bất kỳ máy Mac nào là Workgroup. Tuy nhiên, bạn có thể thay đổi tên, ví dụ, thành MSHOME bằng cách sử dụng công cụ Mac Directory Access. Đồng thời, nó cũng hỗ trợ Windows Active Directory (được dùng cho các máy chủ cộng tác).

Kế tiếp, bật Windows Sharing trong Sharing Preference Pane của hệ điều hành Mac và cấp phép cho mỗi tài khoản người dùng mà bạn muốn chia sẻ. Máy Mac sẽ xuất hiện như là thành viên của mạng khi bạn truy xuất vào mạng.

SAO LƯU

Sao lưu mạng nhiều hệ điều hành

Nếu bạn có nhiều máy tính chạy trên các HĐH khác nhau và muốn sao lưu tất cả chỉ trên một thiết bị lưu trữ mạng, bạn có thể gặp rắc rối với các tên tập tin – hợp lệ với HĐH này nhưng không hợp lệ với HĐH khác. Nếu bạn cắt xén hay thay đổi tên khi sao lưu các tập tin thì những bản sao lưu có thể không còn dùng được nữa. Vì thế, thay vì dùng các ổ lưu trữ USB vốn chỉ có thể định dạng

Sau khi chọn máy Mac và nhập tài khoản, mật khẩu, bạn có thể xem thông tin trên ổ đĩa của máy Mac và sao lưu hay tải tập tin lên bằng cách kéo thả. Tác vụ này cũng có thể thực hiện trên cả XP và Vista. Tương tự, bạn có thể in từ máy Mac qua máy in chia sẻ từ Windows dựa vào giao thức SMB, mặc dù quá trình thiết lập không đơn giản. Trong tiện ích thiết lập máy in của máy Mac, chọn Add. Nếu máy in trong Windows không hiển thị trong danh sách máy in có sẵn, chọn nút More Printer để kích hoạt hộp thoại Printer Browser.

với trình điều khiển của Windows, bạn nên mua đĩa cứng lưu trữ qua mạng (NAS) với khả năng hỗ trợ cho từng HĐH. Sau đó, bạn có thể chỉ định thư mục chia sẻ một cách thích hợp (Windows hay MAC).

Bây giờ, chọn Windows Printing và Network Neighborhood từ trình đơn. Các nhóm làm việc trên mạng cục bộ sẽ xuất hiện trong cửa sổ, khi chọn nó, bạn sẽ thấy danh sách các máy in được chia sẻ để chọn. Từ đó về sau, máy in trên Windows sẽ xuất hiện trong hộp thoại in của máy Mac.

Nếu tất cả các thao tác này có vẻ quá rắc rối, bạn có thể mua phần mềm Network Magic của Pure Networks cho máy Mac (30USD cho 3 máy, 40USD cho 5 máy và 50USD cho 8 máy Mac). Phiên bản thử cũng có sẵn cho tải về (xem: find.pcworld.com/56806), cho phép thực hiện các thao tác mạng trên máy Mac tương tự như các máy trên Windows.

BẢO MẬT

THÊM MẠNG THỨ 2 CHO AN TOÀN

Nếu các cô cậu nhóc ở nhà yêu cầu mở nhiều cổng trên router cho game, chat bằng hình ảnh hay muốn chạy máy chủ web tại nhà hay trên mạng Wi-Fi công cộng, bạn nên dùng router thứ 2 để tách biệt những nguy cơ bên ngoài với mạng của bạn. Trong lớp mạng này bạn có thể cắm thêm một router khác, và chỉ định địa chỉ IP bắt đầu khác (chẳng hạn 192.168.1.1 và 192.168.2.1). Sau đó bạn lắp các máy chủ hay máy tính vào router có modem băng rộng và tất cả các máy tính còn lại ở router thứ 2. Luồng dữ liệu truy cập từ trong ra ngoài và ngược lại nếu không an toàn cũng sẽ không ảnh hưởng đến mạng con của bạn.

Đức Quang
PC World Mỹ 05/2007

Trung tâm xử lý sự cố máy tính và an ninh mạng khu vực miền Bắc

www.911.com.vn

Đây là địa chỉ của Trung tâm xử lý sự cố máy tính và an ninh mạng 911 (thành viên trực thuộc Công ty cổ phần tư vấn và thương mại điện tử Năm Sao), và là trung tâm cứu hộ máy tính chuyên nghiệp đầu tiên tại Hà Nội và cả miền Bắc. Trang web sưu tầm nhiều thông tin, bài viết về bảo mật, sửa chữa, phòng chống virus, cài đặt hệ điều hành, sao lưu phục hồi hệ thống... khá hữu ích cho những ai thích "vọc" máy tính. Ngoài ra, trung tâm còn có đường dây nóng xử lý các sự cố khẩn cấp: (04) 5.188.199.

LÊ QUỐC CÔNG (Quảng Nam)

POP Before SMTP

POP Before SMTP

Local sender must have accessed mailbox within last [XX] minutes

Lựa chọn này xác định rằng người dùng mà server quản lý phải truy nhập vào hộp thư để kiểm tra thư trong vòng một số phút xác định thì mới được phép gửi thư

Messages collected via ATRN are exempt from this requirement

Lựa chọn cho phép những thư lấy qua *ARTN* sẽ không cần sử dụng *POP before SMTP*

Messages sent to local recipient are exempt from this requirement

Lựa chọn này cho phép những thư gửi từ một người dùng của hệ thống đến một người dùng khác cũng thuộc hệ thống thì không phải kiểm tra *POP before SMTP*

Messages sent from trusted IPs are exempt from this requirement

Lựa chọn cho phép thư trong danh sách *"Currently defined domain/IP pairs"* sẽ không phải kiểm tra hộp thư trước khi gửi thư

Site Policy

Creating an SMTP Session Policy Statement

Cửa sổ hiển thị *Text file policy.dat* trong thư mục *app*\ được sử dụng để gửi khi bắt đầu một phiên làm việc của SMTP. Ví dụ *"This server does not relay"* để thông báo

220-Alt-N Technologies ESMTP MDaemon v6.8

220-This site does relay unauthorized email.

220-If you are not an authorized user of our server

220-then you must not relay mail through this site.

220

HELO domain.com…

File POLICY.DAT phải ở dạng ASCII không chưa hơn 512 ký tự một dòng và dung lượng lớn nhất là 5000 bytes

Relay Settings

Vào *Setup→Security Setting→Relay Control...* để thiết lập các hành động của server thư với việc trung chuyển thư (relay mail). Khi một thư đến mail server mà thư đó không đến một người dùng nào của hệ thống, thì server sẽ được yêu cầu chuyển thư đó và gửi đi . Nếu không muốn làm trung gian để chuyển thư thì có thể thiết lập ở đây

Relay Settings

Mail Relay Control

This server does not relay mail for foreign domains

Lựa chọn cho phép MDaemon từ chối nhận chuyển các thư mà cả *FROM* và *TO* không có người dùng của hệ thống

Refuse to accept mail for unknown local users

Lựa chọn cho phép MDaemon sẽ từ chối chấp nhận thư gửi đến cho domain mà nó quản lý như địa chỉ người dùng không tồn tại

Sender's address must be valid if it claims to be from a local domain

Lựa chọn cho phép khi gửi thư từ một trong MDaemon domain thì account gửi đi sẽ được kiểm tra trong cơ sở dữ liệu về account và nó phải tồn tại. Nếu không MDaemon sẽ từ chối chấp nhận gửi thư đi

Mail addressed to know aliases can always be relayed

Lựa chọn cho phép MDaemon trung chuyển thư của các địa chỉ Aliases mà không cần biết các thiết lập trung chuyển

Mail sent via authenticated SMTP sesions can always be relayed

Khi lựa chọn MDaemon sẽ cho phép trung chuyển các thư điện tự được gửi thông qua xác thực SMTP

Mail can always be relayed through domain gateways

Lựa chọn nếu muốn MDaemon cho phép trung chuyển thư thông qua một domain gateway mà không cần biết các thiết lập cài đặt trung chuyển. Theo mặc định lựa chọn này không được chọn và khuyến cáo không sử dụng.

Trusted Hosts

Domain and IP Permissions

Trusted domains

Như domain trong danh sách sẽ không bị ảnh hưởng bởi các thiết lập trung chuyển. Như domain này được tin tưởng và người dùng của domain này thì được phép trung chuyển thư

New trusted domain

Điền domain muốn thêm vào danh sách *Trusted Domains*

Add

Bấm vào nút này để thêm domain được điền trong *new trusted domain* vào danh sách *Trusted Domains*

Remove

Xóa domain được lựa chọn trong danh sách *Trusted Domains*

Trusted IP addresses

Danh sách các địa chỉ IP mà không bị ảnh hưởng bởi các thiết lập trung chuyển (relay). Các địa chỉ IP này được tin tưởng và MDaemon sẽ không từ chối trung chuyển thư của người dùng từ các địa chỉ này

New trusted IP address

Điền địa chỉ IP mà muốn điền vào danh sách *Trusted IP Addresses*

Add

Bấm nút này cho phép điền các địa chỉ IP vào danh sach *Trusted IP Addresses*

Remove

Bấm nút này và xóa lựa chọn trong danh sách *Trusted IP Addresses*

Reverse Lookup

Sử dụng này của MDaemon có thể cấu hình sử dụng lookup ngược trong phần *HELO/EHLO* trong thư. Khi gửi thư MDaemon sẽ cố gắng phân giải các bản ghi MX và A ra địa chỉ IP của domain. Sau đó IP của nơi nhận sẽ được phân giải ngược ra domain và xác định có chính xác.

Reverse lookup

Perform reverse PTR record lookup on inbound SMTP connections

Lựa chọn cho phép MDaemon kiểm tra lookup ngược cho các phiên STMP gửi vào

...send 501 and shutdown connection if no PTR record match

Lựa chọn cho phép MDaemon sẽ gửi mã lỗi 501 và hủy bỏ kết nối nếu kiểm tra lookup ngược không đúng

Refuse to accept mail if a lookup return 'domain not found'

Lựa chọn cho phép khi kết quả của lookup là *"domain not found"* thì thư sẽ bị từ chối với mã lỗi là *451*

...send 501 error code (normally send 451 error code)

Lựa chọn này cho phép mã lỗi khi *"domain not found"* sẽ là *501*

...and then shut down the socket connection

Lựa chọn này cho phép kết nối được dừng ngay lập tức thay cho việc kết thúc bình thường khi lookup ngược cho kết quả *"domain not found"*

Insert 'X-Lookup-Warning' header into suspicious messages

Lựa chọn cho phép điền kết quả vào phần header của thư theo kết quả của lookup ngược

4.1.8.Thay đổi địa tại phần header của thư

Tính năng *Header Translation* cho phép thay đổi địa chỉ trong phần header của thư với một giá trị mới. Khi thư từ mail server gửi ra internet. Tính năng này thường được sử dụng để MDaemon thay đổi tên miền của thư gửi ra khỏi mail server. Trong trường hợp đó Header Translation sẽ thực hiện việc chuyển đổi Ví dụ "@localdomain.com" thành "@remotedomain.com"

Header Translation

Enter New Header Translation

Existing header text

Điền phần mà bạn muốn sẽ được thay thế tìm trong header của thư gửi ra.

New header text

Điền phần mà bạn muốn thay thế cho phần tìm được trên *"Existing Header Text"*

Translate headers in forwarded messages

Lựa chọn nếu nếu bạn muốn *header translation* thực hiện thay đổi phần domain name của thư được tự động chuyển sang địa chỉ khác.

Translate header in gateway messages forward to host or IP

Lựa chọn nếu bạn muốn phần header sẽ được chuyển đổi trong *"forwarded domain gateway mail"*

Currently Defined Header Translation

Danh sách các phần mà MDaemon sẽ tìm trong header của thư để thay thế

Remove

Chọn mục mà bạn muốn xóa trong *"Current Header Translation"* và bấm vào nút này để xóa

Exception

Bấm nút này để mở phần *"Header Translation Exception"* để chọn phần nào của header mà bạn không muốn *Header Translation* có tác động.

Header Translation Exceptions

Do Not Translate Values in These Headers

Header value

Điền phần nào của header mà bạn không muốn *Header Translation* tác động

Add

Bấn nút này để điềm thành phần header của thư mà không muốn *Header Translation* tác động

Except These Headers

MDaemon sẽ không tìm kiếm các phần của header có trong danh sách

Remove

Chọn phần có trong danh sách để xóa đi

4.1.9.Sử dụng IP Cache và thực hiện truy vấn DNS

Để cho tốc độ chuyển thư được nhanh và thời gian xử lý thư là ngắn MDaemon thực hiện lưu giữ địa chỉ IP của tất cả các server mà nó đã gửi thư đến để sử dụng cho quá trình gửi thư sau. Và những địa chỉ IP đó được tái sử dụng lại mỗi khi MDaemon muốn yêu cầu truy vấn DNS cho một domain name đã được sử dụng. Nếu domain name có trong IP cache thì việc truy vấn DNS sẽ được bỏ qua và sử dụng những thông tin đã được lưu giữ và nó sẽ tích kiệm thời gian. Việc thiết lập này sẽ được tự động như bạn cũng có thể thêm hoặc bớt bằng biện pháp thủ công, danh sách và thiết lập dung lượng của cache để lưu trữ. Vào *Setup→IP Cache ...* để thiết lập lưu giữ cache và truy vấn DNS

IP Cache

Caching Options

Clear cache at each processing interval

Lựa chọn sẽ cho phép cache được giải phóng và thiết lập lại theo các chu trình xử lý. Vì cache sẽ bị đầy sau một qúa trình xử lý gửi nhận thư.

Automatically cache uncached domains

Lựa chọn nếu bạn muốn MDaemon lưu giữ địa chỉ vào cache một cách tự động. Nếu bạn muốn tự xây dựng bảng IP cache của riêng mình thì không nên chọn.

Default time to live

Khoảng thời gian mặc định lưu giữ bảng IP cache (tính bằng phút). Nếu một bản ghi được ghi đạt đến khoảng thời gian này thì sẽ bị xóa. Giá trị 9999 cho phép các bản ghi trong IP cache sẽ không bị hết hiệu lực.

Max cache entries

Xác định dung lượng của cache dành cho lưu trữ IP cache

Currently Cached IPs

Remove

Chọn danh sách trong *"Currently Cached IPs"* và bấm vào nút này để hủy

No cache

Xóa hết IP Cache và MDaemon không muốn sử dụng *IP Cache*

Clear

Xóa cache

Add New IP Cache Entry

Domain

Điền domain name mà bạn muốn điền vào *IP cache*

IP

Điền địa chỉ IP mà bạn muốn điền vào *IP cache*

Add

Sau khi đã điền vào hộp domain và ip bấm vào nút này để điền vào *IP cache*

DNS Lookup

Vào *Setup→Perform a DNS Lookup* ... để sử dụng. Truy vấn DNS rất hữu dụng khi kết hợp với *IP Cache*. *DNS Lookup* cho phép bạn nhanh chóng và dễ dàng truy vấn một domain name. Và kết quả của nó có thể được tự động điền vào *IP Cache*

Host Information

Điền domain name mà bạn muốn truy vấn DNS để lấy thông tin

"A" Record Results

Add results to IP cache

Lựa chọn nếu bạn muốn kết quả truy vấn DNS được điền vào IP Cache

Domain name

Là domain name được truy vấn

Domain IP

Là địa chỉ IP của domain name được truy vấn

"MX" Record Results

Hiện bản ghi thư điện tử *"MX"* của domain đã được truy vấn

Lookup!

Bấm vào nút này để thực hiện việc truy vấn DNS để lấy thông tin

4.1.10.Sử dụng thiết lập biểu và sử dụng truy nhập thoại

Phần này cho phép lập kế hoạch các hoạt động của hệ thống thư điện tử một cách đơn giản và theo ý muốn. Bạn có thể lập kế hoạch theo thời gian để chuyển nhận thư hoặc tính toán để xử lý thư theo chu trình thời gian. Và cũng có thể thiết lập các điều khiển để xử lý thư không theo một kế hoạch thời gian như: đến khi có một số lượng thư nhất định hoặc thư đợi đến một khoảng thời gian xác định thì sẽ gửi đi. Nếu bạn có cài MDaemon AntiVirus với phần AntiVirus thì có thể lập lịch đến khoảng thời gian thì cập nhập dữ liệu về virus.

Để thực hiện vào menu *Setup→Event scheduling...*

Event Scheduler

Gửi và nhận thư (Send & Receive Mail)

Local/RAW/System Mail Processing Interval

Thanh trượt này cho phép trượt sang trái hoặc phải để chọn khoảng thời gian giữa các chu trình xử lý, nó có thể thiết lập từ 1 đến 60 phút. Hết khoảng thời gian đó

MDaemon sẽ gửi và nhận thư điện tử của hệ thống và sau đó thiết lập đếm ngược để chuẩn bị cho quá trình tiếp theo. Theo mặc định nó chỉ xử lý với local, RAW và các messages của hệ thống. Nếu chọn *"Deliver remote mail at this internal also"* thì nó cũng cho phép đặt đồng thời kế hoạch cho các thư mà địa chỉ không do hệ thống quản lý (*Remote mail).* Nếu lựa chọn *"Deliver remote mail at this internal also"* không được chọn thì chu trình xử lý Remote mail sẽ được quyết định trong phần "Event Scheduler"

Deliver/collect remote mail at the above interval

Lựa chọn nến muốn các thư gửi cho các địa chỉ mà MDaemon không quản lý cũng được xử lý theo chu trình thời gian xác định bởi thanh trượt.

Deliver local mail immediately upon reception

Lựa chọn khi muốn Local, RAW hoặc thư của hệ thống sẽ được xử lý và chuyển đi ngay khi nhận được (tiến trình đến SMTP kết thúc)

Deliver remote mail immediately upon reception

Lựa chọn khi muốn các thư cho địa chỉ mà nó không quản lý sẽ được xử lý và chuyển đi ngay lập tức (ngay khi một tiến trình SMTP kết thúc)

Simple Scheduling

Có một số cách để bắt đầu một tiến trình của remote mail. *Simple Scheduling* cho phép bắt đầu một tiến trình sử lý remote mail một cách mềm dẻo hơn không chỉ căn cứ vào khoảng thời gian.

Scheduling Options

Always send mail if there's xx or more messsages waiting in the outbound queue

MDaemon sẽ bắt đầu tiến trình khi số lượng thư đợi trong queue gửi ra bằng hoặc hơn số lượng mà bạn xác định ở đây.

Always send mail if a waiting message is more than xx minutes old

Lựa chọn này cho phép tiến trình sẽ bắt đầu khi một thư đợi trong outbound queue đến khoảng thời gian được xác định tại đây.

Scheduled Remote Mail Processing Events

What day?

Chọn ngày bạn muốn lập kế hoạch

What hour?

Chọn giờ mà bạn muốn lập kế hoạch

What minute?

Chọn phút mà bạn muốn lập kế hoạch

Add

Sau khi đã chọn ngày, giờ và phút thì bấm vào nút này để điền vào danh sách.

Remove

Bấm vào nút này nếu bạn muốn xóa một danh mục khỏi danh sách lập kế hoạch

Clear all

Xóa bỏ tất cả các danh mục khỏi danh sách lập kế hoạch

RAS setup

Bấm vào nút này sẽ vào phần thiết lập RAS (xem chi tiết tại phần RAS Setting Remote Access Sevices)

AntiVirus Updates

Simple Scheduling

Wait XX minutes after the last AntiVirus update before conducting another one

Chọn phần này và khoảng thời gian (theo phút) là khoản thời gian mà MDaemon AntiVirus đợi trước khi kiểm tra cập nhập dữ liệu về virus mới. Cập nhập có thể thực hiện tự động theo lịch hoặc thủ công.

Urgent Updates

Activete urgent updates

Chọn nếu bạn muốn cập nhập khẩn cấp dữ liệu về virus. Khi nó được chọn thì MDaemon AntiVirus sẽ ngay lập tức kết nối đến nơi chứa dữ liệu và cập nhập bản mới nhất khi nhận được message "Urgent Update".

Để nhận được bạn phải đăng ký là thành viên của mail list của "Urgent Update" tại "http://www.altn.com/Products/Urgent_Update.asp"

Scheduled AntiVirus Updates

What day?

Chọn ngày bạn muốn lập kế hoạch

What hour?

Chọn giờ mà bạn muốn lập kế hoạch

What minute?

Chọn phút mà bạn muốn lập kế hoạch

Add

Sau khi đã chọn ngày, giờ và phút thì bấm vào nút này để điền vào danh sách.

Remove

Bấm vào nút này nếu bạn muốn xóa một danh mục khỏi danh sách lập kế hoạch

Clear all

Xóa bỏ tất cả các danh mục khỏi danh sách lập kế hoạch

RAS Dialup Settings

Chọn *Setup→RAS Dialip/Dialdown...* menu để cấu hình thiết lập truy nhập thoại. Nó chỉ xuất hiện khi có cài đặt *Remote Access Services* cùng với hệ thống. Nó sử dụng với MDaemon khi cần truy nhập thoại tới nhà cung cấp dịch vụ ISP

Dialup Settings

Dialup Control

Enable RAS dialup/dialdown engine

Lựa chọn này cho phép MDaemon sử dụng các thiết lập kết nối đến một host ở xa để gửi và nhận thư.

Dialup only if remote mail is waiting in outbound queue

Lựa chọn cho phép MDaemon sẽ không truy nhập thoại tới ISP trừ khi có các remote mail gửi đi có trong Remote queue.

Notify [address] when dialup attempts fail

Lựa chọn khi muốn MDaemon gửi một cảnh báo tới một địa chỉ được xác định khi truy nhập thoại bị lỗi.

Dialup Attempts

Make this many attempts to establish a session

MDaemon sẽ cố gắng kế nối đến remote host một số lần thiết lập ở đây trước khi từ bỏ kết nối.

After dailing, wait this many seconds for a valid connection

Là giá trị xác định bao lâu MDaemon sẽ đợi cho remote computer trả lời và hoàn thành RAS kết nối.

Connection Persistence

Once establish, MDaemon will not close the RAS session

Theo mặc định MDaemon sẽ hủy bỏ kết nối ngay lập tức sau khi tất cả các giao dịch thư hoàn thành và kết nối không được sử dụng nữa. Lựa chọn này sẽ cho phép kết nối luôn luôn tồn tai ngay cả khi tất cả các giao dịch thư đã hoàn thành.

Keep session alive for at least xx minutes

Lựa chọn cho phép MDaemon tạo kết nối RAS tồn tại một số phút xác định sau khi các phiên trao đổi hoàn thành.

ISP Logon Settings

Dialup Profile

Use any current active dialup sessions

Lựa chọn này cho phép MDaemon có thể tận dụng thông số của kết nối thoại đang tồn tại. Khi cần kết nối thoại thì MDaemon sẽ kiểm tra liệu có kết nối nào đang có sẵn, nếu có thì nó sẽ sử dụng mà không cần phải truy nhập lại.

Logon name

Giá trị sử dụng để logon dùng xác thực kết nối

Logon password

Là password đi kèm với logon

Use this RAS dialup profile

Lựa chọn tập hợp thông số (profile) cho kết nối đã được thiết lập trước tại *Window Dialup Networking* hoặc *Remote Access Services*

New profile

Bấm vào đây để tạo mới thông số *Dialup Networking* hoặc *Remote Access Service*

Edit profile

Bấm vào đây để sửa thông số *Dialup Networking* hoặc *Remote Access Service* được chọn.

Maximized Use

Maximized use of this connection profile

Lựa chọn cho phép MDaemon giám sát kết nối và nếu có một chương trình khác đã thiết lập kết nối thì nó sẽ sử dụng. Và nếu kết nối vẫn tiếp tục tồn tại thì quá

trình sẽ xử lý các remote mail theo quy trình thời gian được thiết lập tai *"Use existing every XX minutes"*

Hang-up now

Bấm vào nút này cho phép đóng kết nối tới ISP. Nút này chỉ hiện khi MDaemon đang kết nối RAS

Post Connection

Post Connection Process

Once connected, run this process

Cho phép MDaemon chạy một chương trình ngay sau khi RAS kết nối. Nó rất có ích khi ISP yêu cầu chạy một chương trình FINGER hoặc các xử lý khác để lấy thư.

Pause server for xx seconds (-1=infinite,0=no waiting)

Nếu phần *"Once connected, run this process"* thực hiện một chương trình và server sẽ dừng hoạt động một số phút xác định để tiến trình thực hiện xong.

Force process to shutdown after pause interval has alapsed

Khi chương trình muốn chạy không tồn tại và một số chương trình yêu cầu một khoảng thời gian để kết thúc dẫn đến MDaemon sẽ chạy không phải làm gì trong khoảng thời gian đó. Nếu lựa chọn này được chọn thì nó sẽ kết thúc tiến trình mà không cần quan tâm đến khoảng thời gian thiết lập trong *"Pause server for xx seconds"*

Lan Domains

These domains are on my local LAN

Những domain ở trong danh sách sẽ được coi là một phần của mạng *local LAN*. Và do đó không cần thiết lập nhập thoại để chuyển thư đi

New local LAN domain

Điền domain name muốn điền vào danh sách *Local LAN* và bấm nút *Add* để thêm vào danh sách

Relay mail for these domain

Lựa chọn cho phép chung chuyển thư (relay) cho các domain trong danh sách. Nó cho phép cung cấp một số điều khiển lưu lượng gửi ra và vào các domain

Add

Bấm nút này để thêm vào danh sách của *LAN domains*

Remove

Bấm nút này để xóa một lựa chọn trong danh sách *LAN Domains*

LAN IPs

These IPs are on my local LAN

Như phần *LAN Domains*. Danh sách này là danh sách địa chỉ IP của mạng LAN và nó không yêu cầu quay thoại để chuyển thư đến các địa chỉ IP trong danh sách

Remove

Lựa chọn một địa chỉ IP và bấm nút này để xóa khỏi danh sách

New local LAN IP

Điền địa chỉ IP vào và bấm Add

Add

Sau khi đã điền địa chỉ IP vào *New local LAN IP* và bấm nút này để điền vào danh sách.

4.1.11.Sử dụng DomainPOP để lấy thư

Vào *Setup→DomainPOP Mail Collection...* để cấu hình MDaemon kết nối POP vào ISP để lấy thư về cho người dùng. Thư được lấy về và phân loại và dựa theo

các thông số để chuyển đến hộp thư của người sử dụng hoặc gửi vào trong remote queue để MDaemon chuyển đi.

DomainPOP cho phép MDaemon nhận thư một cách an toàn và nhanh chóng đồng thời cung cấp các phương thức xử lý khi thư được nhận về. Khi MDaemon nhận các thư đến qua POP nó sẽ ngay lập tức kiểm tra phần header và thiết lập danh sách người nhận, quá trình xử lý sẽ chia danh sách người nhận ra làm hai phần local (người nhận do nó quản lý) và remote (danh sách không do nó quản lý). Các thư do nó quản lý (local mail) sẽ được gửi đến người nhận. Còn với thư không do nó quản lý (remote mail) sẽ phụ thuộc vào thiết lập của MDaemon (có thể bỏ qua hoặc chuyển cho postmaster).

Đồng thời phần này cũng cho phép quan tâm đến các thư bị trùng nhau hoặc bị gửi vòng (endlessly looping)

DomainPOP Mail Collection

Account

DomainPOP Host Properties

Enable DomainPOP mail collection engine

Lựa chọn cho phép người dùng sử dụng chức năng lấy thư bằng DomainPOP

Host name or IP

Điền tên của DomainPOP hoặc địa chỉ IP của server chứa thư. Nếu server mà ta kết nối vào để lấy thư lại không sử dụng cổng POP chuẩn để cho phép lấy thư thì ở đây ta điền cổng để lấy thư. Ví dụ "mail.altn.com:523" với 523 là cổng lấy thư.

Logon name

Điền logon của account POP sử dụng bởi DomainPOP

Password or APOP shared secret

Điền password của POP account hoặc APOP shared secret vào đây

Use APOP

Lựa chọn cho phép sử dụng APOP và phương pháp xác thực CRAM-MD5 khi nhận thư (nó yêu cầu xác thực được mã hóa chứ không phải là dạng text).

Mail Download Control

Leave a copy of message on host server

Nếu lựa chọn. MDaemon sẽ lấy thư về mà không xóa thư trên Server bị lấy.

Delete messages once [xx] or more have accumulate (0=no limit)

Nếu bạn muốn để thư trên server mà không xóa khi lấy về, thì khi số lượng thư đến số lượng xác định ở đây thì toàn bộ thư sẽ bị xóa. Điền '0' cho phép thư ở trên Server mà không cần quan tâm đến số lượng.

Don't download messages larger than [xx] KB (0=no limit)

Thiết lập độ lớn cho các thư, mà các thư lớn hơn hoặc bằng với độ lớn này sẽ không lấy về. Điền "0" nếu muốn MDaemon lấy về mà không quan tâm đến độ lớn của thư.

Delete large messages from DomainPOP and MultiPOP hosts

Lựa chọn cho phép MDaemon xóa các thư lớn hơn độ lớn cho phép. Thư sẽ đơn giản là bị xóa khỏi DomainPOP và MultiPOP và sẽ không lấy về.

Warn postmaster about large DomainPOP messages

Lựa chọn cho phép MDaemon sẽ gửi cảnh báo cho *postmaster* khi nhận được một thư lớn hơn cho phép.

Download messages according to size (small mesages first)

Lựa chọn cho phép MDaemon sẽ lấy các thư về dựa trên độ lớn. Các thư có độ lớn nhỏ được lấy trước và các thư có độ lớn sẽ lấy sau.

Over Quata Accounts

Warn account holder and delete over quota message

Khi lựa chọn này được chọn thì khi một account nhận được thư, như hộp thư đã bị đầy thì MDaemon sẽ xóa thư và gửi một cảnh báo tới người chủ của hộp thư biết hộp thư đã bị đầy.

Warn account holer and forward over quota message to Postmaster

Khi lựa chọn này được chọn thì khi một account nhận được thư mà hộp thư đã bị đầy. MDaemon sẽ chuyển thư tới *Postmaster* và gửi một cảnh báo tới người dùng cho biết hộp thư đã bị đầy.

Parsing

Parsing Properties

De-dupe collected mail using the Message-ID field

Lựa chọn này cho phép MDaemon sử dụng một phần xác định tại header của thư để so sánh tránh xử lý các thư đã được xử lý (thường trường được sử dụng là Message-ID)

Parse "Received" headers for email address

Lựa chọn cho phép chứa thông tin của người nhận trong header và từ đó xử lý thư và lấy ra được người nhận thực sự

Skip over the first xx "Received" headers

Đôi khi bạn cần phải bỏ qua một số lần của *"Received header"*. Lựa chọn này cho phép bỏ qua một số *"Received header"* sau đó mới bắt đầu xử lý.

Stop parsing if "Received" field a vaild local address

Cho phép trong quá trình xử lý nhận được một địa chỉ mà Serrver quản lý thì nó sẽ dừng xử lý.

Parse "Subject:" header for address inside "(" and ")" charaters

Lựa chọn cho phép MDaemon sẽ tìm địa chỉ chứa trong dấu "(...)" trong phần "Subject" và địa chỉ này được sử dụng cùng với các địa chỉ gửi đi khác để chuyển thư.

Parse these headers for email address

Hộp danh sách các phần của header mà MDeamon sẽ kiểm tra để lấy địa chỉ

Remove

Bấm nút này cho phép xóa lựa chọn khỏi danh sách header.

Default

Bấm vào nút này sẽ xóa toàn bộ nội dung trong phần danh sách header và điền lại các giá trị mặc định của MDaemon.

New header

Điền phần header mà bạn muốn thêm vào danh sách header.

Add

Thêm phần header trong *"New Header"* vào danh sách.

Processing

Domain Name Replacement

Enable domain name replacement engine

Lựa chọn cho phép khi các thư được lấy về thì phần domain name sẽ được loại bỏ và thay thế bằng domain name được xác định ghi ở phần hộp text dưới.

Ignore unknown local addresses parsed from messages

Khi thay thế domain name tất cả các địa chỉ thư sẽ được chuyển thành domain name mà bạn muốn chuyển sang. Như nó có thể tạo ra một số địa chỉ sẽ không có hộp thư tương ứng và MDaemon sẽ coi đó là local email như không xác định được hộp thư do đó nó sẽ sinh ra một cảnh báo với *"No Such User"* gửi tới *postmaster*. Lựa chọn này cho loại bỏ các cảnh báo *"No Such User"* và không cho gửi tới *postmaster*.

Routing Rules

Existing Rules

Danh sách các quy tắc đã tạo và để điền cho thư

Remove

Bấm nút này để hủy lựa chọn trong *"Existing Rules"*

Default

Bấm nút này để xóa tất cả các quy tắc đang tồn tại và trở về chế độ mặc định

Clear all

Bấm nút này để xóa tất cả các quy định.

New Rule

If the parsed address...

Is equal to, is not equal to, does not contain

Lựa chọn so sánh sẽ được sử dụng trong các quy tắc. MDaemon sẽ tìm kiếm địa chỉ so sánh với tên điền trong *"This text"* và xử lý dựa trên các thiết lập điều khiển - như địa chỉ phải chính xác, không cần chính xác, xuất hiện trong chuỗi ký tự hoặc không chứa nó.

This text

Điền chuỗi ký tự mà bạn muốn MDaemon tìm kiếm trong địa chỉ thư

Then do this with the message

Hộp danh sách các điều khiển sẽ thực hiện khi kết quả của quy tắc cho kết quả đúng. Sau đây là các điều khiển

Don't deliver to this address - Lựa chọn nếu muốn ngăn thư không được chuyển tới một địa chỉ xác định

Send to user or group of users - Lựa chọn sẽ cho phép bạn tạo danh sách thư sẽ nhận thư.

Foreign Mail

What to do with non-local mail

Forward summary of non-local addresses to postmaster

Lựa chọn này cho phép MDaemon sẽ tạo một bản danh sách các địa chỉ của thư gửi đến không phải do nó quản lý và gửi tới *postmaster*.

Deliver non-local mail to all remote recipients

Lựa chọn này cho phép chuyển một bản gửi cho người nhận không phải do MDaemon quản lý được xác định trong phần header.

Do not deliver mail addressed to non-local addresses

Lựa chọn này cho phép MDaemon xóa danh sách người nhận mà nó không quản lý

Security

Safety Option

Place an extra copy of all downloaded mail into this directory

Lựa chọn này cho phép chắc chắn bạn không bị mất bức thư nào bởi những xử lý không dự kiến hoặc một lỗi bất kỳ nào đó trong khi lấy về một số lượng lớn thư.

Name Matching

Real Name Matching Engine

Activate real name matching engine

Đặc tính này cho phép MDaemon so sánh phần xác định tên thật của người nhận của thư lấy về bởi DomainPOP . Ví dụ: tại phần TO: của thư

TO: Joe User <common-mailbox@isp.com>

Thì MDaemon sẽ không so sánh phần common-mailbox@isp.com mà sử dụng phần điền tên Joe User. Chỉ các thư có phần này giống với yêu cầu thì mới được nhận về.

Only apply this feature if the address portion maches this value

Đặc tính này cho phép MDaemon xác định địa chỉ thư nhận về phải đúng với với giá trị điền trong hộp. Ví dụ : bạn điền địa chỉ "common-mailbox@isp.com" thì chỉ những địa chỉ chính xác là "common-mailbox@isp.com sẽ được lấy.

4.1.12.Lọc thư và kiểm tra virus

Với sự phát triển nhanh chóng của mạng Internet thì số lượng email ngày càng tăng dẫn đến việc cần thiết phải quản lý thư điện tử ra vào. Mục đích chính của việc quản lý này là để đảm bảo an toàn cho mạng cũng như người dùng, tránh cho việc lãng phí tài nguyên mạng và người dùng bị quá tải thông tin không cần thiết... Ngày này hầu hết các phần mềm thư điện tử đầu cuối (mail client) đều cho phép tạo các quy tắc để hạn chế việc gửi và nhận thư và cũng như vậy tại server hệ thống cũng có các tính năng lọc các thư được phép gửi và nhận và nhiều các tiện ích cung cấp tính năng cho người dùng. Trên Server cũng có cung cấp các chính sách ngăn chặn thư, chống lại virus đi kèm thư, hạn chế spam, dễ dàng định hướng một email cho nhiều người và từ chối các thư không mong muốn để tích kiệm tài nguyên mạng.

Email tốt và xấu

Lợi ích của email thật rõ dàng với người dùng. Nó đem lại liên lạc nhanh chóng và hiệu quả giữa người gửi và người nhận tại bất cứ đâu. Các doanh nghiệp và người dùng sử dụng email để cung cấp thông tin, thuyết phục, thúc đẩy công việc, giải trí, thăm hỏi... Email thường được gửi kèm với các chương trình ứng dụng cho email client, bao gồm các mẫu báo cáo, các bảng thống kê, hình ảnh và các file văn bản... Bởi vì email rất dễ sử dụng nên nó được sử dụng rất phổ biến cho việc liên lạc cá nhân cũng như trong thương mại và các lĩnh vực khác. Email còn có thể sẽ là giải pháp liên lạc toàn diện và kinh tế hơn sử dụng điện thoại.

Ưu điểm của email :

- Dễ dàng sử dụng cho việc gửi và nhận cho tất cả người dùng. Do đó thư điện tử sẽ đem đến nhiều lợi ích hơn nhiều việc gửi thư bằng phương pháp thông thường.
- Rất nhanh chóng gửi đến người nhận với chỉ một động tác là bấm vào nút *"send"*. Do đó tích kiệm rất nhiều thời gian.
- Rất kinh tế là chỉ sử dụng các tín hiệu điện hơn là sử dụng giấy và phong bì.
- Rất rẻ. Các phần mền sử dụng email thường là cho không. Dù có bán thì cũng rất rẻ và thường xuyên được nơng cấp thêm các tính năng.
- Email cung cấp ít định dạng các loại văn bản khác như microsoft world do đó mọi người đều có thể chuyển đổi được.
- Rất mềm dẻo. Emails có thể ở dạng text, rich text hoặc HTML.

Dù sao, bởi vì sự phổ biến, tính mềm dẻo và dễ dàng sử dụng nên email dễ bị lạm dụng.

Những mặt không tốt:

- Làm phân tán công việc chính của mọi người bởi hàng chục đến hàng trăm email được gửi đến mỗi ngày.
- Làm giảm hiệu quả của công việc bởi có quá nhiều thư cá nhân gửi đến và gửi đi khi làm việc.
- Cung cấp khả năng cho người dùng sử dụng để gửi email quảng cáo như nó cũng có thể gây phiền cho người dùng.
- Giúp những người xấu dải virus máy tính trên mạng.
- Các thư vô bổ gây lãng phí lưu lượng và tài nguyên mạng.
- Tạo ra sự hỗn độn trên mạng khi người gửi đến người nhận không tồn tại.
- Giúp kẻ trộm như: nhân viên xấu trong một doanh nghiệp gửi thông tin của doanh nghiệp cho đối thủ cạnh tranh một cách dễ dàng.

Tóm lại email đem lại lợi ích rất to lớn như đồng thời nó cũng đem đến rất nhiều phiền toái giống như cuộc sống.

Lọc thư (Filtering Email)

Lọc thư hoạt động như một hệ thống lọc và phân phát email. Nó cho phép điều chỉnh lại đường đi cho thư đi đến, qua và ra khỏi hộp thư. Về một mặt nào đó, filtering email tương tự như bộ lọc không khí hoặc nước. Bộ lọc cho phép chặn lại các chất thải và chỉ cho thành phần tinh kiết đi qua. Trong nhiều trường hợp độ bộ lọc đạt được từ 98 phần trăm hoặc tốt hơn. Với email thì không phải là không khí và cũng không phải là nước, do đó không cần phải lọc khí hay chất lỏng. Mà email là lọc ra cái xấu và để cái tốt đi qua. Sự thật là thỉnh thoảng email filter cũng gây ra lỗi bởi chặn không cho thư tốt qua mà lại cho thư xấu qua bởi vậy email filter thường yêu cầu cơ chế hiệu chỉnh để tránh gây lỗi.

Một ví dụ: Virus-infected HTMP là virus có mang mã HTML. Các email có dạng HTML hoặc là các file đính kèm có dạng HTML. Mà mã HTML có thể mang các đoạn mã có thể tự động chạy và phá hoại khi người dùng mở email. Một cách chắc chắn và hiệu quả nhất là loại bỏ tất cả các email có dạng HTML. Nhưng điều đó đồng thời cũng loại bỏ rất nhiều email có ích mà chứa HTML. Một giải pháp hữu ích hơn là chặn tất cả các email có đoạn mã HTML xác định hoặc bộ lọc từ chối đoạn mã HTML từ bên ngoài gửi vào. Mỗi lần hiệu chỉnh tinh chế bộ lọc thì lại để cho nhiều thư chứa mã HTML đi qua và đồng thời cũng tiềm tàng sự không an toàn.

Ngoài ra Filter cũng cho phép cấm các email quảng cáo không mong muốn và spam. Filter có thể chặn và cho email qua bằng cách sử dụng nhiều các tiêu chuẩn khác nhau. Dù sao nó cũng có nhiều tác dụng hơn là chỉ để chống virus và lọc thư mà nó còn có tác dụng:

- Chuyển hướng email từ một địa chỉ này sang một địa chỉ khác.
- Tự động trả lời với một số email xác định.
- Phân phối một email tới nhiều địa chỉ.
- Điền ghi chú vào phía dưới của một email.

- Thêm hoặc loại bỏ file đính kèm.
- Thông báo cho người quản trị email những địa chỉ email server mà spam mail tới.
- Kết hợp các công cụ trên và hơn nữa.

Phác hoạ về bộ lọc (Filters)

Rất nhiều email client có tích hợp khả năng lọc thư. Khả năng lọc thư của client rất đa dạng. Một số công cụ cho phép đơn giản là chuyển thư tới các thư mục mong muốn trên máy của người dùng dựa trên địa chỉ của người gửi, chủ đề hoặc nội dung của thư. Và còn nhiều tính năng khác như chuyển thư đến địa chỉ xác định, tự động trả lời khi người dùng đi vắng, bỏ các file đính kèm, chặn virus, điền thêm vào chủ đề hoặc thêm thông báo vào thư...

Như theo điều tra thấy rằng hầu hết người dùng ít khi sử dụng các tiện tích của bộ lọc ngoài tiện ích phân loại thư chuyển về thư mục theo yêu cầu. Bởi vì tiện ích này rất dễ hiểu, dễ sử dụng và lợi ích là rất rõ dàng. Nói một cách khác, các filter như chuyển hướng thư sang địa chỉ khác, tự động trả lời và các chức năng khác nhưng dường như là nó không được người dùng biết đến. Do đó các tiện ích đó thường không đem lại lợi ích gì cho người dùng.

Thiết lập bộ lọc tại đầu server sẽ giúp các tổ chức hoặc các nhà cung cấp dịch vụ đạt được hiệu quả và độ linh hoạt cao. Đầu server cho phép chuyển qua hoặc chặn lại một khối lượng thư trước khi chuyển đến hộp thư của người dùng hoặc ra internet. Nó giúp làm giảm bớt như thư không cần thiết và thư bị nhiễm virus đồng thời cũng làm tăng nguồn tài nguyên của mạng bị chiếm dụng bởi các thư không cần thiết.

Hình bên miêu tả cả việc sủ dụng lọc thư cả ở đầu server và client.

Vị trí hoạt động của bộ lọc tại server

Bộ lọc tại Server hoạt động phân lớp để xử lý internet email . Internet email sử dụng ba lớp phần mền cơ bản sau:

- Mail User Agent (MUA), hay còn gọi là email client. Phần mền này chạy trên máy của người dùng và cho phép tạo, gửi và nhận email.
- Mail Transport Agent (MTA), hay còn gọi là SMTP server bởi vì nó sử dụng thủ tục SMTP (Simple Mail Transfer Protocol). Phần mền này chạy trên server cung cấp dich vụ và trao đổi email với MUA. Một email thường phải đi qua hai MTA - một phía người gửi và một phía người nhận -- khi gửi email từ một MUA tới một MUA khác.
- Mail Delivery Agent (MDA), hay còn gọi là email server. Nó là phần mềm chạy trên server, cùng với MTA. Nó quản lý các email nhận được bởi MTA và chuyển email đó đến dúng hộp thư.

Bộ lọc hoạt động tại MDA dùng để kiểm tra trước khi email được chuyển ra ngoài và được chuyển về hộp thư của người dùng.

Hướng dẫn sử dụng MDaemon Filter

Vào phần cấu hình *Setup→Content Filter...* cho phép ta sử dụng với rất nhiều mục đích như: ngăn chặn spam thư, chặn các thư có chứa virus không cho gửi đi, nhân bản thư cho một hay nhiều người dùng, thêm hoặc bớt nội dung vào cuối thư, thêm hoặc bớt phần header của thư, loại bỏ file đính kèm, xoá thư... tuỳ theo yêu cầu của người quản trị thiết lập trong *Content Filter*. Với khả năng rất mền dẻo đó và với một chút suy luận và kinh nghiệm thì với tính năng này rất có ích cho người quản trị MDaemon.

MDaemon AntiVirus được phát triển cài đặt và tích hợp với MDaemon cho phép phòng chống virus email cho các thư gừi đi và gửi đến.

Content Filter Editor

Tất cả các thư được xử lý bởi MDaemon sẽ tạm thời chứa trong messages queues. MDaemon sử dụng Content Filtering xử lý các thư trước khi gửi ra khỏi queue kết quả của quá trình xử lý đó sẽ quyết định thư sẽ được chuyển đến đâu.

Content Filtering Rules

Enable rules processing engine

Lựa chọn cho phép sử dụng *content filtering*. Và tất cả các thư của MDaemon sẽ được lọc qua *content filter* trước khi chuyển đi.

Existing Content Filter Rules

Danh sách các quy tắc để xử lý thư khi qua content filter. Ví dụ: nếu bạn có một quy tắc là yêu cầu xoá tất cả các thư có chứa các từ *"This is Spam!"* và một quy định tương tự là đồng thời gửi thư đó cho Postmaster.

Trong danh sách các quy tắc sẽ được thực hiện từ trên xuống. Bạn có thể sử dụng nút *More UP/ More Down* để chuyển các quy tắc nào được thực hiện trước và quy tắc nào sẽ thực hiện sau.

New rule

Bấm nút này cho phép tạo một quy tắc mới, nó sẽ mở một hộp *Setup New Rule* cho phép bạn điền quy tắc mới.

Edit rule

Mở một quy tắc được chọn để sửa đổi.

Copy rule

Bấm vào nút này để nhân bản các quy tắc giống với quy tắc được chọn. Quy tắc mới sẽ có tên là *"Copy of [Tên của quy định được lựa chọn] "*. Nó rất hữu dụng khi bạn muốn tạo nhiều quy tắc tương tự như nhau, bạn chỉ cần tạo một quy tắc sau đó nhân bản làm nhiều bản và sau đó là sửa chữa theo ý.

Deleted rule

Xoá một quy tắc mà bạn đang chọn trong content filter. Bạn sẽ được yêu cầu khẳng định lại quyết định xoá trước khi thực hiện

Move up

Chuyển một quy tắc lên trên để được thực hiện trước

Move down

Chuyển một quy tắc xuống dưới để thực hiện sau

Rule Descriotion [Rule Name] (Enabled/Disabled)

Hộp hiển thị này cho phép hiển thị nội dung của quy tắc đang được lựa chọn trong *Existing content filter rule*.

Creating a New Content Filter Rule

Hộp này được dùng để tạo một Content Filter Rules. Nó xuất hiện khi ta bấm nút *New Rule* trong hộp *Content Filter*

Give This Rule a Name

Điền tên (nên là tên có khả năng gợi nhớ) cho một quy tắc mới. Theo mặc định tên là *"New Rule #n"*

Define New Content Filter Rule

Select conditions for this rule

Lựa chọn các điều kiện gán cho quy tắc mới. Chọn các hộp lựa chọn điều kiện mà bạn muốn gán

IF the [HEADER] contains - Lựa chọn tìm nội dung được chứa trong phần header của thư

IF the user defined [#HEADER] contains - Lựa chọn nếu nội dung muốn tìm kiếm được chứa trong một phần nào đó của thư header như : To: ; From: ; Subject: . . .

If the MESSAGE BODY contains - Phần tìm kiếm nằm trong phần thân của thư

If the MESSAGE has Attachement(s) – Tìm các thư có file đính kèm

If the MESSAGE SIZE is greater than - Thực hiện quy tắc dựa trên dung lượng của thư

If the MESSAGES HAS A FILE called – Tìm thư có file đính kèm có tên được xác định

If message is INFECTED - Nếu điều kiện là đúng (TRUE) khi MDaemon AntiVirus xác định là thư có chứa virus

If the EXIT CODE form a previous run process is equal to – Các quy tắc khi xử lý sẽ cho ra kết quả sẽ là một chuỗi mã. Ta sử dụng quy tắc này để xác định quá trình xử lý dựa trên kết quả của quá trình xử lý trước

If ALL MESSAGES : - Luật này sẽ có tác dụng với tất cả các thư

Select action for this rule

Các hành động sẽ thực hiện với thư khi phù hợp với các điều kiện đã nêu ra (một số hành động sẽ yêu cầu các thông tin thêm)

Delete Message – Xoá thư

Strip All Attachments From Message - Loại bỏ các file đính kèm khỏi thư

Move Message to Bad Message Directory – Thư sẽ được chuyển vào thư mục chứa các thư lỗi

Skip n Rules - Bỏ qua quy định thứ n. Ví dụ: muốn xoá tất cả thư có chứa từ "Spam" như không muốn xoá với thư có chứa từ "Good Spam". Thì dùng lệnh này để bỏ qua quy định xoá nếu thư chứa từ "Good Spam"

Stop Processing Rules - Sẽ bỏ qua tất cảc các quy tắc còn lại

Copy Message to Specified User(s) - Sẽ chuyển thư phù hợp đến một hoặc nhiều người dùng được xác định

Append Standard Disclaimer - Sẽ cho phép tạo một nội dung để điền vào phần footer của thư

Add Extra Header Item To Message - Sẽ thêm vào phần header cho thư. Bạn phải điền tên của header và giá trị.

Delete A Header Item From Message – Xoá header khỏi thư, bạn phải xác định phần nào của header cần được xoá

Send Note To ... - Sẽ gửi email tới một địa chỉ xác định. Ví dụ: khi bạn nhận được các thư chứa "This is Spam" bạn sẽ có một lệnh chuyển đến thư mục thư lỗi và dùng lệnh này để gửi cảnh báo đến một địa chỉ xác định

Remove Digital Signature – Cho phép xoá chữ ký điện tử khỏi thư

Run Process ... – Cho phép chạy một chương trình đặc biệt khi thư gửi tới phù hợp với điều kiện đưa ra.

Send Message Through SMS Gateway Server – cho phép gửi thư thống qua một SMS gateway server. Bạn phải cung cấp Host hoặc địa chỉ IP và số phone của SMS cần nhắn

Copy Message to Folder ... - Sử dụng để cho phép copy thư đến một thư mục xác định

Add Line To Text File – Cho phép điền thêm một dòng text vào một file text xác định. Bạn cũng có thể sử dụng MDaemon macro để cho phép điền thông tin của thư như người gửi, người nhận, messages ID...

Move Message to Public Folders...- Để chuyển thư tới một hoặc nhiều Public Folder

Search and Replace Words in a Header–Quét một phần xác định của header để tìm các từ xác định và xoá đi hoặc thay thế.

Search and Replace Words in the Message Body–Quét nội dung của thư và thay thế một đoạn text

Jump to Rule... - Nhảy qua một số câu lệnh để xuống lệnh ở dưới. Những quy định ở giữa hai quy định đó sẽ được bỏ qua.

Rule description

Đây là hộp hiển thị nội dung của quy tắc và các đoạn chương trình. Các đoạn chương trình cho phép bấm vào để điền thêm thông tin cần thiết

Modifying an Existing Content Filter Rule

Cho phép sửa chữa các luật đã có sẵn, vào *Edit→Rule*

Using Regular Expressions in Your Filter Rules

Các phiên bản cũ trước đây của MDaemon phần Content Filtering chỉ hỗ trợ để tìm kiếm các chuỗi ký tự. Với các phiên bản MDaemon mới có hỗ trợ các công cụ mạnh hơn cho Content Filtering như tìm kiếm với các ký tự đặc biệt và các ký tự tắt.

What are Regular Expressions ?

Là định dạng text bao gồm tập hợp ký tự và các ký tự đặc biệt \ | ( ) [ ] ^ $ * + ? . < >

Ký tự đặc biệt	Miêu tả
\	Dấu sược trái "\" cho phép xử lý các ký tự đặc biệt như các ký tự bình thường. VD : bạn muốn tìm ký tự đặc biệt "+" trong chuỗi ký tự bạn phải điền là "\+" để tìm ký tự
|	Ví dụ tìm "abc|xyz" nó sẽ tìm chuỗi có kết quả abc hoặc là xyz
[...]	Tìm chuỗi ký tự trong dấu ngoặc vuông
^	Ký thự biển thị bắt đầu của dòng. Ví dụ "^a" sẽ xác định với

	dòng bắt đầu bằng ký tự a. "^ab" thì dòng bắt đầu bằng "ab"
[^...]	Với trường hợp này thì lại có nghĩa ngược lại. Ví dụ :"[^0-9]" chuỗi kỹ tự bắt đầu không được phép là số
(...)	Sử dụng cho tìm kiếm và thay thế. VD: hai chuỗi thay thế sau (abc)(xyz). Tìm chuỗi "a-\2-b-\1" và sẽ được chuyển thành "a-xyz-b-abc" hoặc tìm chuỗi "a-\0-a" sẽ thành "a-abcxyz-b". Với \1, \2,\3 là thư tự các chuỗi thay thế và \0 là toàn bộ các chuỗi gộp lại
$	Biểu thị cuối dòng. VD: "13 321 123" với "3$" thì cho kết đúng và với "123$" cũng cho kết quả đúng.
*	Dấu sao biểu thị phía bên trái phải là zero hoặc nhiều lần ký tự trong ngoặc. Ví dụ "1*abc" sẽ đúng với "111abc" và "abc"
+	Tương tự như ký tự sao, ký tự dấu cộng biểu thị phía bên trái phải đúng với từ 1 trở lên với ký tự trong ngoặc. Ví dụ "1+abc" sẽ đúng với "111abc" như không đúng với "abc"
?	Dấu chấm hỏi hiện thị phía bến trái phải phù hộp với zero hoặc với một ký tự trong ngoặc. Do đó "1+abc" sẽ đúng với "abc" và "1abc"
.	Dấu chấm sẽ đúng với bất kỳ ký tự khác. Ví dụ ".+abc" sẽ đúng với "123456abc". Và "a.c" sẽ đúng với "aac", "abc","acc" ...

Các điều kiện và các hành động thường được đi kèm với các câu lệnh. Ví dụ như *"If the FROM HEADER contains"* và *"if the MESSAGE BODY contains"*

Admins/Attachments

Phần này quy định cho các file đính kèm cho phép hoặc hạn chế. Những file đính kèm không được phép sẽ bị xoá khỏi thư.

Administrators

Những địa chỉ thư ở đây được là các địa chỉ quản lý các thay đổi tại content filter (nó tương ứng với Administrators control ở phần Notification). Những địa chỉ này sẽ nhận được thông báo khi có những thay đổi trong Content filter.

Điền địa chỉ và bấm Add để thêm địa chỉ, chọn địa chỉ cần xoá và bấm Remove để xoá địa chỉ ra khỏi hộp Administrators

Restricted Attachments

Các filename có trong phần *"RESTRICT these files"* sẽ bị loại bỏ ra khỏi thư một cách tự động. Nếu điền bất cứ file nào trong phần *"ALLOW these files only"* thì chỉ có file đó được phép đính kèm với thư còn tất cả các file khác bị loại bỏ khỏi thư. Sau khi file đính kèm bị loại bỏ thì MDaemon sẽ tiếp tục chuyển thư một các bình thường mà không có file đính kèm. Cũng có thể dùng điều khiển này trong phần Notification để thông báo.

Configure Exclusions

Bấm vào *"configure exclusion"* để chọn các địa chỉ mà không bị hạn chế. Khi thư từ địa chỉ này thì MDaemon sẽ cho phép thư chuyển qua ngay cả khi có chứa file đính kèm là file bị hạn chế.

File Compression

Với điều kiển này cho phép file đính kèm sẽ được tự động nén hoặc giải nén trước khi chuyển đi. Tính năng này cho phép giảm dung lượng chiếm đường truyền khi chuyển các thư ra ngoài.

Outbound Compression

Enable compression of attachments for outbound messages

Lựa chọn cho phép tự động nén file đính kèm khi chuyển thư. Lựa chọn này không có nghĩa là tất cả file đính kèm đều được nén mà nó chỉ bật chức năng này lên còn file có được nén hay không còn căn cứ vào các thông số thiết lập.

Compress outbound local domain attachments

Lựa chọn cho phép các thiết lập nén sẽ được thực hiện với thư gửi ra

Compression Options

Create self-extracting zips

Lựa chọn nến muốn nén file sử dụng tự động giải nén zip với phần mở rộng là EXE file. Nó rất hữu ích cho người nhận sẽ giải nén mà không cần có chương trình giải nén.

Compress only if compression % is greater than XX%

MDaemon sẽ nén những file đính kèm của thư có khả năng nén với phần trăm nén lớn hơn số xác định trong hộp điều kiển. Ví dụ : ta điền giá trị 20 và thì những file nào có khả năng nén được giảm hơn 20 % thì sẽ được nén.

Compress if total attachment size is greater than XX KB

Khi lựa chọn tự động nén file thì MDaemon sẽ chỉ cố gắng nén các file đính kèm khi độ lớn của nó lớn hơn giá trị được xác định ở đây. Còn những tổng số độ lớn file đính kèm nhỏ hơn giá trị đính ở đây sẽ gửi đi bình thường.

Compression level

Lựa chọn cấp độ nén file mà bạn muốn MDaemon sử dụng cho file đính kèm. Nó có ba cấp độ: minimum (nén nhanh), medium hoặc maximum (nén chậm, như dung lượng file nén sẽ được giá trị nhỏ nhất)

Use fixed archive name:[archive name]

Lựa chọn nếu bạn muốn xác định tên cho file đính kèm sau khi đã nén.

Compression exclusions

Exclude these attachments...

Bấm vào đây để điền tên những file sẽ không được phép nén. Khi một thư có đính file đúng với những file trong danh sách thì MDaemon sẽ không nén mà không cần quan tâm đến các thông số thiết lập khác.

Exclude these domains...

Bấm vào đây để điền các domain của nơi nhận thư gửi đến sẽ không được phép nén file đính kèm.

Inbound Decompression

Enable decompression of attachments for inbound messages

Lựa chọn cho phép tự động giải nén các file đính kèm khi các thư gửi đến. Khi một thư đến với file đính kèm được nén zip thì MDaemon sẽ giải nén trước khi chuyển đến người nhận

Decompress inbound local domain attachments

Lựa chọn nến muốn tự động giải nén với thư nội bộ

AntiVirus

Lựa chọn này chỉ có khi đã có cài đặt MDaemon AntiVirus

Scanner Configuration

Enable virus scanner

Lựa chọn này cho phép AntiVirus quét các thư. Khi MDaemon nhận một thư với file đính kèm MDaemon AntiVirus sẽ hoạt động và quét xem có virus trước khi chuyển thư tới nơi nhận

Enable background scanner

Nếu bạn có một chương trình diệt virus chạy ngầm trên hệ thống thì bạn sử dụng lựa chọn này để cho phép chương trình diệt virus đó quét virus thay cho MDaemon Antivirus

Exclude gateways from virus scanning

Lựa chọn nếu bạn muốn các thư đến từ một *MDaemon domain gateway* không bị quét virus.

Click to configure exclusion lists...Configure Exclusions

Bấm vào *"Configure Exclusions"* để điền các địa chỉ sẽ không bị quét virus bởi *MDaemon AntiVirus*.

Scanner Actions

Chọn các lựa chọn xác định phương pháp MDaemon sẽ xử lý khi phát hiện virus

Delete the infected attachment

Lựa chọn này cho phép xoá file đính kèm có virus. Thư sẽ tiếp tục được chuyển đi mà không có file đính kèm. Bấm vào *"Add a warning..."* để thêm phần cảnh báo vào thư đến người dùng rằng file đính kèm có virus và đã bị xoá.

Quarantine the infected attachment to...

Lựa chọn chỗ mà các file đính kèm sẽ được lưu lại khi xác định có virus. Và nó vẫn chuyển thư đến người nhận mà không có file đính kèm.

Delete the entire message

Lựa chọn cho phép xoá toàn bộ thư khi phát hiện ra virus chứ không chỉ xoá file đính kèm. Bởi vì khi xoá toàn bộ thư thì người nhận sẽ không được thông báo. Nhưng bạn vẫn có thể thiết lập gửi thông báo tới người nhận

Quaratine the entire message to ...

Giống như *"Delete the entire message"* lựa chọn này cho phép lưu lại toàn bộ thư vào một thư mục xác định

Add a warning message to the top of the message body if infected

Khi một lựa chọn *" ...attachment"* ở trên được chọn. Bấn vào đây nếu muốn có thêm thông báo vào phần trên nội dung của thư trước khi chuyển đến người nhận (để thông báo cho người nhận file đính kèm đã bị tách ra và tại sao)

Edit warning message...

Bấm vào nút này cho phép hiện đoạn thông báo sẽ đính thêm vào thư khi *"Add a warning message..."* được sử dụng. Và có thể thay đổi nội dung thông báo và bấm "OK" để ghi lại các thay đổi

AntiVirus Updater

Bảng điều khiển này cho phép tự động cập nhập hoặc cập nhập thủ công bảng MDaemon AntiVirus .

Scanner info

Phần này hiện version của MDaemon AntiVirus đã được cài đặt, ngày cập nhập Antivirus...

Updater Configuration

Activate urgent updates

Lựa chọn cho phép cập nhập khẩn cấp. Nếu được lựa chọn AntiVirus sẽ ngay lập tức kết nối vào nơi chứa các bản cập nhập mới và lấy về bản có độ ưu tiên lớn nhất khi MDaemon nhận được cảnh báo (để nhận được cảch báo thì MDaemon phải đăng ký là thành viên của mailing list)

Subscribe

Nút này cho phép mở trang web của Alt-N Technologies' Updates để đăng ký làm thành viên. Trong trang web này điền domain của bạn vào danh sách *"Urgent*

Updates mailing list". Khi có yêu cầu cập nhập khẩn cấp nó sẽ gửi một yêu cầu cập nhập bản virus mới nhất cho MDaemon AntiVirus

Update AV signature now

Bấm nút này cho phép cập nhập thủ công bản danh sách virus mới nhất

Configure updater

Bấm nút để mở bảng cập nhập. Bảng cập nhập bao gồm 3 phần : Update URLs, Connection, và Proxy

Update URLs là danh sách các nơi mà MDaemon sẽ nối tới để kiểm tra bảng cập nhập virus. Có thể thêm hoặc bớt danh sách. Chuyển URLs lên hoặc xuống trong danh sách . Vì việc kiểm tra sẽ tiến hành từ trên xuống dưới. Bấm nút điều khiển *"Use random staring point in the URL list"* cho phép việc kiểm tra là ngẫu nhiên.

Connection để thiết lập thông số kết nối của MDaemon AntiVirus khi kết nối tới nơi để cập nhập. Sử dụng *"Use internet Settings from Contronl Panel"* cho phép sử dụng các thông số của thiết lập kết nối internet.

Proxy chứa các thiết lập cấu hình cho HTTP và FTP proxy để kế nối lấy bản cập nhập virus về

View update report

MDaemon AntiVirus sử dụng công cụ này để kiểm tra thời gian cập nhập danh sách virus mới, các hành động sẩy ra (bấm vào nút View update report)

Scheduler

Bấm vào nút này để mở bản thiết lập kế hoạch của AntiVirus Update để thiết lập kế hoạch lấy các bản cập nhập virus mới về.

Test Scanner

Send EICAR

Bấm vào nút này để gửi kiểm tra tới postmaster với file EICAR virus đính kèm. File đính kèm này sẽ không có hại gì, nó chỉ có tác dụng kiểm tra MDaemon AntiVirus. Bằng cách theo dõi Content Filter log có thể thấy MDaemon sẽ làm gì với thư khi nó nhận được

Ví dụ

Mon 2002-02-25 18:14:49: Processing
C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2002-02-25 18:14:49: > eicar.com
(C:\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2002-02-25 18:14:49: > Message from: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message to: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2002-02-25 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@mycompany.com>
Mon 2002-02-25 18:14:49: Performing viral scan...
Mon 2002-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2002-02-25 18:14:50: > eicar.com was removed from message
Mon 2002-02-25 18:14:50: > eicar.com quarantined to
C:\MDAEMON\CFILTER\QUARANT
Mon 2002-02-25 18:14:50: > Total attachments scanned : 1 (including
multipart/alternatives)
Mon 2002-02-25 18:14:50: > Total attachments infected : 1
Mon 2002-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2002-02-25 18:14:50: > Total attachments removed : 1

Mon 2002-02-25 18:14:50: > Total errors while scanning : 0

Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com (sender)

Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com(recipient)

Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com (admin)

Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@example.com (admin)

Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active rules)

Notifications

Bảng thiết lập này cho phép thiết lập ai sẽ nhận được cảnh báo có virus hoặc các file đính kèm bị loại bỏ.

Notification Messages

Notification message from:

Sử dụng điều khiển này để xác định địa chỉ thư mà từ đó thông báo được gửi đi

Send virus notification message to...

Khi thư gửi đến với một file đính kèm có virus thì sẽ có một cảnh báo sẽ gửi tới theo các lựa chọn xác định ở dưới. Các thiết lập cho phép gửi đến người gửi, người nhận, người quản trị ...

Send restricted attachment notification message to...

Khi thư gửi đến với file đính kèm trong danh sách không cho phép thì thông báo sẽ gửi đến theo các lựa chọn như: người gửi, người nhận, người quản trị...

Subject

Hiển thị phần chủ đề của file cảnh báo sẽ được gửi

Message

Nội dung của cảnh báo sẽ gửi. Có thể sửa đổi lại nội dung trực tiếp tại đây.

Message Macros

Để cho tiện lợi thì một số macros sẽ được sử dụng trong cảnh báo

$ACTUALTO$ Trường "ActualTO" để xác định nơi đến của hộp thư

$CURRENTTIME$ Macro xác định thới gian thư xử lý

$ACTUALFROM$ Xác định hộp thư và địa host gửi đi

$FILTERRULENAME$ Tên của quy tắc mà thư phù hợp

$HEADER:XX$ Xác định các phần của header với xx là thành phần của header. Ví dụ: thư có "TO:joe@mdaemon.com" thì kết quả sẽ là "joe@mdaemon.com"

$HEADER:MESSAGE-ID$ Kết quả sẽ cho là Message-ID của header

$LIST_ATTACHMENTS_REMOVED$ Hiện danh sách các file đính kèm bị tách ra khỏi thư

$LIST_VIRUSES_FOUND$ Hiện danh sách tên các loại virus tìn thấy trong thư

$MESSAGEFILENAME$ Tên file đính kèm của thư

$MESSAGEID$ Như *$HEADER:MESSAGE-ID$* nhưng sẽ bỏ dầu "<>" khỏi kết quả

$PRIMARYDOMAIN$: cho kết quả là primary domain

$PRIMARYIP$: cho địa chỉ IP của primary domain

$RECIPIENT$: cho địa chỉ đầy đủ của người nhận

$RECIPIENTDOMAIN$ cho kết quả domain của người nhận

$RECIPIENTMAILBOX$ cho kết qua là hộp thư của người nhận

$REPLYTO$ cho kết quả điền tại "Reply-to" trong phần header của thư

$SENDER$ cho kết quả là địa chỉ đầy đủ của người gửi

$SENDERDOMAIN$ cho kết quả là domain của người nhận thư

$SENDERMAILBOX$ cho kết quả là hộp thư của người nhận thư

$SUBJECT$ hiện chủ đề của thư

4.1.13.Cấu hình thiết lập và sử dụng thư ưu tiên

Thư ưu tiên (Priority Mail) cho phép xác định các thư được quyền ưu tiên. Thư ưu tiên được quyền chuyển đi ngay lập tức bởi MDaemon mà không cần quan tâm đến thứ tự xử lý thư. Khi một thư đến MDaemon sẽ kiểm tra phần header và so sánh với các thiết lập trong hộp thiết lập ưu tiên. Nếu nó là thư ưu tiên thì MDaemon sẽ cố gắng gửi đi trước. Thiết lập vào *Setup→Priority Mail...*

Priority Mail

Priority Mail Engine

Enable priority mail checking engine

Lựa chọn này cho phép kích hoạt đặc tính thư ưu tiên của MDaemon. MDaemon sẽ kiểm tra mức độ ưu tiên của các thư đến.

Enter New Header/Value

Header

Điền phần nào header của thư sẽ được kiểm tra

Value

Giá trị của phần header xác định ở trên để thiết lập mức ưu tiên

Trigger even if value is a sub-string

Khi thiết lập ưu tiên cho thư thì nó sẽ kiểm tra điều kiện có phù hợp để là thư ưu tiên hay không. Phần này cho phép giá trị cần kiểm tra chỉ cần xuất hiện trong chuỗi ký tự là được. Ví dụ ta đặt ưu tiên cho giá trị *“BOSS”* trong phần *"To:"* của

header như nến lựa chọn phần này thì chỉ cần header chứa BOSS@anything cũng được xác định là thư ưu tiên. Nếu không lựa chọn phần này thì giá trị của header phải chính xác chuỗi cần tìm.

Add

Điền giá trị vào phần header/value và bấm nút này để ghi lại giá trị

Current Priority Mail Header/Value Pairs

Hiển thị tất cả các xác định của thư ưu tiên

Remove

Bấm nút này để xoá bỏ lựa chọn đã được chọn tại *"Current Priority Mail Settings"*

Exceptions

Cho phép bạn xác định địa chỉ thư dù phù hợp với các điều kiện là thư ưu tiên như sẽ không được coi là ưu tiên. Nó cho phép bạn khả năng mềm dẻo hơn trong việc điều khiển hoạt động của MDaemon.

4.1.14.Cấu hình thiết lập ghi log của hệ thống

Cấu hình vào *Setup→Logging options...* cho phép thiết lập các log của hệ thống. Log rất quan trọng sử dụng cho mục đích phân tích lỗi và những gì đã xẩy ra với server của bạn khi không được giám sát

Logging

Logging Mode

Create standard set of log files

Tạo ra một logfile tiêu chuẩn

Create a new set of log lifes each day

Cho phép chia logfile ra theo từng ngày. Tên của logfile sẽ tương ứng với từng ngày

Create logfile based on the day of the week

Cho phép chia logfile ra theo từng ngày. Tên của logfile sẽ được ghi ra theo tên của ngày

Log each service into a separate log file

Nó cho phép logfile ghi ra theo từng dịch vụ chứ không ghi riêng ta một file. Ví dụ : log của SMTP sẽ được ghi ra MDaemon-SMTP.log

5 cách khoá an toàn địa chỉ e-mail của bạn - 16/8/2006 8h:6

E-mail độc hại ngày càng nhiều. Chúng ta có thể thực hiện năm bước sau để bảo vệ an toàn cho e-mail của bạn chống lại những mối đe doạ an ninh nguy hiểm nhất.

Sau browser, e-mail client là con đường bị khai thác nhiều nhất của những kẻ phá hoại máy tính có tổ chức, các hacker và những người phát tán phần mềm gián điệp (spyware).

Thực tế, phá hoại e-mail là cách để xâm nhập vào hệ thống máy tính của bạn. Melissa, virus của năm 1999 đã được phát tán qua thư điện tử, rồi đến năm sau (năm 2000) malware I LOVE YOU dựa trên nền Visual Basic đã thay thế thời kì tấn công quy mô qua e-mail.

Mặc dù chúng ta nghĩ thời kỳ đó đã ngừng và những mối đe dọa có vẻ như không còn nhưng thực sự không phải vậy. Thực tế thì những kiểu tấn công máy tính đó chuyển sang một thời kỳ khác, thời kỳ của spam, trojan và những mạnh khóe dẫn người dùng đến những trang web độc hại.

Chúng ta có thể thực hiện 5 bước sau để khoá an toàn e-mail của bạn, không chỉ dùng riêng cho *Outlook* mà trong vài trường hợp có thể sử dụng cho cả *Thunderbird* cũng rất tốt. Trước hết, tất nhiên là Microsoft client cùng bộ Office;

sau đó là đối thủ cạnh tranh up-and-coming của Mozilla, hãng tạo ra Firefox. Lời khuyên ở đây là bạn nên áp dụng với cả cho dịch vụ e-mail khác, nhưng trước hết là với địa chỉ e-mail sẵn có của bạn.

Bước 1: Xem xét một cách cẩn thận.

Hầu hết kẻ tấn công đều cần sự giúp đỡ từ phía người dùng thì mới thực hiện hành động phá hoại. Chúng phải thuyết phục được người sử dụng viếng thăm một trang web hoặc mở một file đính kèm. Nhưng sử dụng một số tin nhắn độc hại thì nguy hiểm hơn: Các tin nhắn này chỉ cần được xem là đã có thể phá hoại.

Mặc dù ô xem trước email của bạn (nội dung hiển thị của một phần tin nhắn khi bạn chọn mail nào đó) có một khoảng thời gian an toàn (mail sẽ chỉ được mở nếu bạn xem qua mail đó vượt quá thời gian quy định). Bạn nên tắt chức năng đó đi nếu không khi bạn mở và xem nó, tin nhắn sẽ lây lan virus vào máy tính của bạn. Nó không phải là sự bảo vệ có hiệu quả nhưng ít nhất nó cho bạn có thể đọc dòng subject và người gửi mà không gặp rủi ro.

Để tắt chức năng đó bạn làm như sau:

- Trong Outlook 2003, chọn *View -> Reading pane -> OK*.

- Trong Thunderbird, chọn *View -> Layout*. Sau đó là "*Message Pane*", đánh dấu *unchecked*. (Bạn cũng có thể bật tắt hộp tin nhắn bằng cách ấn phím F8).

Bước 2: Vào Plain Vanilla

Một số mối đe doạ có thể đơn giản chỉ là khi bạn xem hoặc mở một tin nhắn trên ngôn ngữ HTML. Thông thường các cuộc tấn công khai thác điểm yếu trên e-mail client hay trên e-mail browser thông qua một tập lệnh HTML. (Mặt khác để đảm bảo an toàn, trong bước này bạn cũng nên loại trừ các quảng cáo hấp dẫn có thể

mang đến thư rác)

Một cách để ngăn cản các cuộc tấn công là bạn đọc mail dưới dạng Plain Text (dạng đơn giản) chứ không phải là dạng HTML.

Trong Outlook 2003 thì rất dễ dàng với client được gói cùng Office 2003.

- Chọn *Tool/Option*, sau đó click vào "*Preferences*"

- Click vào nút "*E-mail Option*" ở phần phía trên, bên phải

- Đánh dấu vào hộp "*Read all standard e-mail as Plain Text*". Kích *OK* trong hộp thoại này và tiếp theo.

Trong phiên bản Outlook 2002 (đi kèm với Office XP) bạn phải vào Windows Registry để thực hiện thay đổi này. Bạn có thể xem trong phần Microsoft support document. (*Chú ý: nhầm lẫn trong Registry có thể rất nguy hiểm vì vậy hãy cẩn thận khi tiến hành tiếp công việc mạo hiểm này của bạn*).

Thunderbird của Mozilla có thiết lập tương tự:

- Từ màn hình chính, chọn *View/Message Body As* và lấy ra "*Plain Text*".

Bạn cũng nên tăng cường bảo vệ bằng các chức năng mở rộng trong Thunderbird như:

- Chọn *Tool / Junk Mail Control*. Trong tab "*Settings*" đánh dấu vào hộp "*When displaying HTML messages marked as Junk, sanitize the HTML*" .

- Chọn *Tool / Option*, sau đó kích vào biểu tượng "*Privacy*". Đánh dấu vào các hộp "*Block loading of remote images in mail messages*" và "*Block JavaScript in mail messages*".

- Chọn *View / Display Attachments Inline*, bỏ dấu chọn tuỳ chọn này.

Bước 3: Bỏ qua các đường link

Các cuộc tấn công dựa trên việc dẫn người dùng click vào các đường link website đáng ngờ ngày càng tăng với mức độ nguy hiểm ngày càng cao. Cách tốt nhất bạn có thể làm là lờ chúng đi. *Nhưng chúng vẫn ở đó, đầy cám dỗ!*

Bạn có thể làm cho nó khó click hơn bằng cách vô hiệu hoá mọi đường link HTML đến. Đường link vẫn sẽ tồn tại, nhưng bạn không thể kích vào chúng để mở website. *Cám dỗ bị loại bỏ!*

Outlook 2003 làm việc này tự động đối với tất cả các mail bị phân loại là các spam. (Oulook gọi nó một cách khá thân thiệt là "Junk"). Bạn cần phải cập nhật Office 2003 với SP2 để có được tính năng này. (Có thể tải tại đây), Outlook cũng đóng các liên kết trong hộp tin nhắn mà nó cho là có virus. Bạn có thể mở lại các link bằng cách kích phải chuột lên phần đầu của hộp tin nhắn và chọn "*Turn on links (not recommended)*".

Đáng tiếc, những phiên bản trước của Outlook không có thành phần này.

Trong Thunderbird, hiện tại cả hai thành phần đều không được xây dựng. Mặc dù các message được xem như là spam có thể bị vô hiệu hoá (xem bước 2), nhưng vẫn còn các đường link thì vẫn có thể kích, tuy nhiên e-mail client của Mozilla cũng có một tính năng chống phishing cơ bản. Thunderbird đánh dấu một số message mà nó nghi ngờ bằng cách đặt cảnh báo mỗi khi người dùng sử dụng một đường link nhúng đặt trong e-mail (*một thủ đoạn phổ biến của những kẻ phá hoại*).

Bước 4: Block các file đính kèm (hay Unblock)

Ban biết rằng thật không thông minh khi click vào các file đính kèm, nhưng đôi khi bạn cũng không thể tự giúp được mình. Khi bạn nhận được một e-mail của người bạn thân với câu: "*Bạn nên xem cái này!*" và trêu chọc bằng một hình ảnh nào đó vô tội, tay bạn đã có thể click trước khi đầu bạn kịp nói là không.

Outlook có thể tự bảo vệ bạn trong một số trường hợp.

Từ Outlook 1998, cũng giống như các phiên bản Oulook 2000, 2002, và hiện tại là 2003, e-mail client của Microsoft có một thành phần ngăn chặn việc mở file đính kèm trong một danh sách dài các loại định dạng kiểu file. Bộ chặn file đính kèm cũng ngăn chặn việc bạn ghi lại các file bên trong Outlook có nguy cơ nguy hiểm vào ổ cứng.

Outlook 2002 và 2003 tích hợp tính năng này như là một sản phẩm tiêu chuẩn. Vì thế, nếu bạn dùng những phiên bản đó thì đã được thiết lập sắn có rồi. Outlook 2002 và 98 thực hiện bảo vệ mail của bạn thông qua một bản vá lỗi, còn Outlook 97 là trường hợp đặc biệt riêng trong tất cả.

Để kiểm tra xem liệu bản sao chép Outlook 98 hay 2000 của bạn được sửa chữa chưa, hãy vào mục Help/ About và chú ý tới phiên bản. Nếu nó là: Outlook 98: v. 8.5.7806 (hoặc cao hơn) và Outlook 2000: v. 9.0.0.4201 (hoặc cao hơn) thì được.

Bạn đã sẵn sàng để dùng? Nếu không thì download bản vá lỗi tại đây.

Outlook 97 là một trường hợp đặc biệt. Bạn có thể thêm chương trình bảo vệ cục bộ này vào khi thay đổi sơ lược Registry trong Microsoft support document. Khi đó sẽ có một cảnh báo đưa ra nếu bạn nhận được một file đính kèm đi cùng thư buộc bạn phải ghi vào ổ cứng trước khi đọc nó. (*Chú ý: nhầm lẫn trong Registry có thể rất nguy hiểm và hãy cẩn thận khi tiến hành tiếp công việc mạo hiểm này của bạn*).

Nếu bạn muốn chỉnh sửa danh sách các kiểu file bị chặn, Windows Registry tweak sẽ thực hiện thủ thuật trên Outlook 2000, Outlook 2002 và Outlook 2003. (Xem các hướng dẫn về phiên bản của Outlock tại đây).

Lo lắng về việc sửa đổi Registry như thế nào? Bạn có thể tránh điều phức tạp đó bằng cách tải phần mở rộng miễn phí "*Attachtment Options*" tại địa chỉ: http://www.slovaktech.com/attachmentoptions.htm. Nó sẽ đưa ra một giao diện để block hoặc unblock các file đính kèm đã mô tả.

Outlook block chỉ xem xét ba kí tự trong đuôi mở rộng của các file, vì vậy nếu một kẻ tấn công ngụy trang dưới một file "**.exe**" nguy hiểm là một file "**.gif**" vô hại, thì

malware có thể lẻn qua hàng rào bảo vệ.

Thunderbird không có chức năng xoá các file đính kèm. Nó cũng không tự động cấm các kiểu file nào đấy. Nhưng phần mở rộng "*Attactment Options*" cho phép bạn đặc tả các loại file mà bạn có thể phân tách ra từ thư của bạn. Tuy không nhiều, nhưng còn hơn không! Tải phần mở rộng tại đây.

Chú thích thêm: Một số chương trình diệt virút có các chức năng lọc hoặc chặn các file đính kèm cơ bản có thể thêm vào máy tính chạy e-mailer mà không cần các chương trình khác (như Thunderbird). Ví dụ như chương trình miễn phí AVG của Grisoft có thể được thiết lập để tự động loại bỏ tất cả các file đính kèm là file chạy hoặc tất cả các file có đuôi mở rộng nằm trong danh sách mà người dùng chỉ rõ.

Bước 5: Đúng lúc!

Chức năng bảo mật e-mail quan trọng nhất và cũng là vòng cuối trong hàng rào bảo vệ của bạn chính là các phần mềm diệt virút. Chúng có thể quét các file đính kèm trước khi nó được mở.

Việc này có thể diễn ra theo nhiều mức độ. Nhưng tất cả các phần mềm diệt virút đều quét file đính kèm đến trước khi chúng tới được e-mail client. Nếu có điều gì

đó đáng ngờ - có thể phụ thuộc vào phần mêm diệt virút hiện nay có phát hiện được hay không – chương trình có thể "làm sạch" file bằng cách lấy ra các phần bị nhiễm độc. Hoặc nó đơn giản chỉ là cách ly hay xoá tất cả các file đính kèm. Trong bất kì trường hợp nào bạn sẽ thấy một số cảnh bào nói rằng các thư đến của bạn đã bị nhiễm độc.

Để có được điều tốt nhất từ các phần mềm diệt virút:

- Cập nhật một cách đều đặn các chữ ký, tốt nhất là sử dụng bất kỳ một thành phần cập nhật tự động nào mà chương trình cung cấp.

- Hãy chắc chắn rằng tất cả các bộ phận của e-mail đều được mở. Không phải tất cả các phần mềm diệt virút đều được bật mặc định

- Quét vòng ngoài - nơi các phần mềm diệt virút dò các file đính kèm bạn đang gửi để chắc chắn bạn không giúp phát tán các malware cho người khác – có thể làm cho bạn là một công dân tốt. Nhưng trong thế giới khắc nghiệt sát phạt lẫn nhau thì không thể giảm được bộ nhớ của các phần mềm diệt virút cùng sự hoạt động ngon lành của bộ vi xử lý và tăng tốc độ truyền tải e-mail.

T.Thu - Quản Trị Mạng

TỰ LÀM 1 ĐĨA BOOT MẠNG

Chắc có lẽ chúng ta khi thiết lập một hệ thống mạng đều ngại nhất là công việc cài đặt hệ điều hành cho từng máy trong mạng.Nếu chúng ta không biết sắp xếp công việc thì việc cài đặt sẽ chiếm rất nhiều thời gian và công sức,có khi hiệu quả đạt được không cao.
Giả sử chúng ta phải thiết lập một hệ thống mạng gồm 1 máy Server và 30 máy Client.Yêu cầu cho việc cài đặt:
-Server sử dụng Windows 2000 Server(hay NT 4.0 Server).
-Các Client sử dụng Windows 2000 Pro hay 1 hệ điều hành nào khác.
Hướng giải quyết công việc:
-**Cách 1**:Chúng ta phải cài đặt cho từng máy:cài Server trước sau đó cài đặt cho từng Client trong mạng.Quá mất thời gian và chi phí cao do mỗi Client đều phải cần 1 ổ đĩa CD-Rom.
-**Cách 2**:Sử dụng công nghệ RIS(Remote Installation Service).Cách này thực sự hữu ích tuy nhiên có 1 nhược điểm là Server phải sử dụng hệ điều hành Windows 2000 Server,các Client chỉ có thể cài đặt hệ điều hành Windows 2000 Pro và card

mạng phải hỗ trợ Rom Boot theo chuẩn PXE.Tuy nhiên không phải card mạng nào cũng hỗ trợ Rom Boot.Trong trường hợp đó thì RIS không phải là cách hay.
-**Cách 3**:Chúng ta sẽ tiến hành làm 1 đĩa mềm có thể Boot mạng từ DOS.Sau đó chúng ta sẽ cho các máy Client cài đặt hệ điều hành từ source trên Server. Đây thực sự là 1 cách hữu ích.Bởi vì yêu cầu về phần cứng không cao và các máy Client có thể cài đặt bất kỳ hệ điều hành nào.
Ở đây chúng ta có 2 cách để tạo đĩa Boot mạng.Một là sử dụng Norton Ghost 2003,hai là sử dụng tiện ích NETSETUP trong bộ đĩa cài đặt Windows NT 4.0 Server (mở đĩa Windows NT 4.0 Server vào ..\CLIENTS\MSCLIENT\NETSETUP chạy file Setup.exe).Trong bài này tôi xin giới thiệu phương pháp làm đĩa Boot mạng sử dụng phần mềm Norton Ghost 2003.

Làm đĩa Boot mạng sử dụng Norton Ghost 2003:

Trước hết chúng ta phải cài đặt hệ điều hành cho Server. Ở đây Server sẽ sử dụng Windows 2000 Server.Kế tiếp chúng ta phải nâng cấp lên Active Directory(vào Start\Run\DCPROMO rồi enter).Sau khi nâng cấp lên Active Directory chúng ta phải cấu hình DNS Server và DHCP Server để Server cấp phát IP cho các Client.
Kế đó chúng ta sẽ tạo user để sử dụng cho việc Boot mạng từ DOS. Ở đây chúng ta phải tạo một thư mục để chép bộ Source cài đặt hệ điều hành (có thể sử dụng file Ghost của bất kỳ hệ điều hành nào).Thư mục này phải được share để cho các Client khi Boot vào mạng có thể truy cập được.
Cuối cùng là chúng ta tiến hành cài đặt Norton Ghost 2003 (lưu ý là chỉ có phiên bản 2003 mới hỗ trợ việc làm đĩa Boot mạng).Sau khi cài đặt xong chúng ta mở Norton Ghost 2003 lên,như hình bên dưới:
Chúng ta chọn mục Ghost Utilities.Bảng Norton Ghost Boot Wizard xuất hiện:

Kế tiếp chúng ta chọn tiếp "Drive Mapping Boot Disk",rồi Click Next.
Ở bảng này chúng ta sẽ thấy các Driver card mạng được hỗ trợ để làm đĩa Boot.Nếu chúng ta sử dụng 1 loại card mạng khác không có trong mục này,chúng ta có thể chọn nút Add để bổ sung thêm.Click Next để tiếp tục.

Click Next để tiếp tục.
Kế tiếp bảng Norton Ghost Boot Wizard-Network Client Configuration xuất hiện.Chúng ta cần điền đầy đủ cho các mục này.
-Client Computer Name:tên máy Client.
-User name:tên người sử dụng,có thể sử dụng tên Administrator hay chúng ta phải tạo 1 tài khoản riêng(sử dụng Server để tạo tài khoản người dùng).
-Domain:tên domain sau khi chúng ta đã nâng cấp lên Active Directory.
-Drive Letter:tên ổ đĩa mà Server đã chép Source cài đặt và share trên mạng.
-Map To: đường dẫn đến thư mục mà Server đã share.
Click Next tiếp tục.

Bảng kế tiếp xuất hiện,hỏi chúng ta cấp phát địa chỉ IP bằng dịch vụ DHCP hoặc cấp phát bằng tay. Ở đây do chúng ta đã cài đặt DHCP Server nên chúng ta chọn:"DHCP will assign the IP settings".Click Next để tiếp tục.
Bảng kế tiếp xuất hiện,chúng ta chọn các thông số cho phù hợp rồi Click Next.

Bảng trên sẽ cho chúng ta xem rõ chi tiết của các file như Autoxec.bat hay Config.sys.Click Next để cho công việc tạo đĩa bắt đầu.Cuối cùng là nhấn Finish để hoàn thành việc tạo đĩa.
Sau khi hoàn thành,chúng ta sẽ dễ dàng hơn trong việc cài đặt 1 hệ thống mạng mà không phải tốn nhiều thời gian và công sức cũng như tiền bạc.Chúc các bạn thành công.

Mạng máy tính (Computer Networks)

Về cơ bản, một mạng máy tính là một số các máy tính được nối kết với nhau theo một cách nào đó. Khác với các trạm truyền hình chỉ gửi thông tin đi, các mạng máy tính luôn hai chiều, sao cho khi máy tính A gửi thông tin tới máy tính B thì B có thể trả lời lại cho A.

Nói một cách khác, một số máy tính được kết nối với nhau và có thể trao đổi thông tin cho nhau gọi là mạng máy tính.

Từ nhiều máy tính riêng rẽ, độc lập với nhau, nếu ta kết nối chúng lại thành mạng máy tính thì chúng có thêm những ưu điểm sau:

- Nhiều người có thể dùng chung một phần mềm tiện ích.
- Một nhóm người cùng thực hiện một đề án nếu nối mạng họ sẽ dùng chung dữ liệu của đề án, dùng chung tệp tin chính (*master file*) của đề án, họ trao đổi thông tin với nhau dễ dàng.
- Dữ liệu được quản lý tập trung nên an toàn hơn, trao đổi giữa những người sử dụng thuận lợi hơn, nhanh chóng hơn.
- Có thể dùng chung thiết bị ngoại vi hiếm, đắt tiền (máy in, máy vẽ,...).
- Người sử dụng trao đổi với nhau thư tín dễ dàng (*E-Mail*) và có thể sử dụng hệ mạng như là một công cụ để phổ biến tin tức, thông báo về một chính sách mới, về nội dung buổi họp, về các thông tin kinh tế khác như giá cả thị trường, tin rao vặt (muốn bán hoặc muốn mua một cái gì đó), hoặc sắp xếp thời khoá biểu của mình chen lẫn với thời khoá biểu của những người khác,...

- Một số người sử dụng không cần phải trang bị máy tính đắt tiền (chi phí thấp mà chức năng lại mạnh).
- Mạng máy tính cho phép người lập trình ở một trung tâm máy tính này có thể sử dụng các chương trình tiện ích của một trung tâm máy tính khác đang rỗi, sẽ làm tăng hiệu quả kinh tế của hệ thống.
- Rất an toàn cho dữ liệu và phần mềm vì phần mềm mạng sẽ khoá các tệp tin (*files*) khi có những người không đủ quyền hạn truy xuất các tệp tin và thư mục đó.

Phân loại mạng máy tính theo phạm vi địa lý

Mạng máy tính có thể phân bổ trên một vùng lãnh thổ nhất định và có thể phân bổ trong phạm vi một quốc gia hay quốc tế.

Dựa vào phạm vi phân bổ của mạng người ta có thể phân ra các loại mạng như sau:

- GAN (Global Area Network) kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.
- WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.
- MAN (Metropolitan Area Network) kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).
- *LAN (Local Area Network)* - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trục thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức...Các LAN có thể được kết nối với nhau thành WAN.

Trong các khái niệm nói trên, WAN và LAN là hai khái niệm hay được sử dụng nhất.

Mạng cục bộ - LAN

Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một

khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà.... Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.

Các mạng LAN trở nên thông dụng vì nó cho phép những người sử dụng (*users*) dùng chung những tài nguyên quan trọng như máy in mầu, ổ đĩa CD-ROM, các phần mềm ứng dụng và những thông tin cần thiết khác. Trước khi phát triển công nghệ LAN các máy tính là độc lập với nhau, bị hạn chế bởi số lượng các chương trình tiện ích, sau khi kết nối mạng rõ ràng hiệu quả của chúng tăng lên gấp bội. Để tận dụng hết những ưu điểm của mạng LAN người ta đã kết nối các LAN riêng biệt vào mạng chính yếu diện rộng (WAN).

Các thiết bị gắn với mạng LAN đều dùng chung một phương tiện truyền tin đó là dây cáp, cáp thường dùng hiện nay là: Cáp đồng trục (*Coaxial cable*), Cáp dây xoắn (*shielded twisted pair*), cáp quang (*Fiber optic*),....

Mỗi loại dây cáp đều có tính năng khác nhau.

Dây cáp đồng trục được chế tạo gồm một dây đồng ở giữa chất cách điện, chung quanh chất cách điện được quán bằng dây bện kim loại dùng làm dây đất. Giữa dây đồng dẫn điện và dây đất có một lớp cách ly, ngoài cùng là một vỏ bọc bảo vệ. Dây đồng trục có hai loại, loại nhỏ (*Thin*) và loại to (*Thick*). Dây cáp đồng trục được thiết kế để truyền tin cho băng tần cơ bản (*Base Band*) hoặc băng tần rộng (*broadband*). Dây cáp loại to dùng cho đường xa, dây cáp nhỏ dùng cho đường gần, tốc độ truyền tin qua cáp đồng trục có thể đạt tới 35 Mbit/s.

Dây cáp xoắn được chế tạo bằng hai sợi dây đồng (có vỏ bọc) xoắn vào nhau, ngoài cùng có hoặc không có lớp vỏ bọc bảo vệ chống nhiễu.

Dây cáp quang làm bằng các sợi quang học, truyền dữ liệu xa, an toàn và không bị nhiễu và chống được han rỉ. Tốc độ truyền tin qua cáp quang có thể đạt 100 Mbit/s.

Nhìn chung, yếu tố quyết định sử dụng loại cáp nào là phụ thuộc vào yêu cầu tốc độ truyền tin, khoảng cách đặt các thiết bị, yêu cầu an toàn thông tin và cấu hình của mạng,....Ví dụ mạng Ethernet 10 Base-T là mạng dùng kênh truyền giải tần cơ bản với thông lượng 10 Mbit/s theo tiêu chuẩn quốc tế ISO/IEC 8802.3 nối bằng đôi dây cáp xoắn không bọc kim (UTP) trong *Topology* hình sao.

Việc kết nối các máy tính với một dây cáp được dùng như một phương tiện truyền tin chung cho tất cả các máy tính. Công việc kết nối vật lý vào mạng được thực hiện bằng cách cắm một card giao tiếp mạng NIC (*Network Interface Card*) vào trong máy tính và nối nó với cáp mạng. Sau khi kết nối vật lý đã hoàn tất, quản lý việc truyền tin giữa các trạm trên mạng tuỳ thuộc vào phần mềm mạng.

Đầu nối của NIC với dây cáp có nhiều loại (phụ thuộc vào cáp mạng), hiện nay có một số NIC có hai hoặc ba loại đầu nối. Chuẩn dùng cho NIC là NE2000 do hãng Novell và Eagle dùng để chế tạo các loại NIC của mình. Nếu một NIC tương thích với chuẩn NE2000 thì ta có thể dùng nó cho nhiều loại mạng. NIC cũng có các loại khác nhau để đảm bảo sự tương thích với máy tính 8-bit và 16-bit.

Mạng LAN thường bao gồm một hoặc một số máy chủ (*file server*, *host*), còn gọi là máy phục vụ) và một số máy tính khác gọi là trạm làm việc (*Workstations*) hoặc còn gọi là nút mạng (*Network node*) - một hoặc một số máy tính cùng nối vào một thiết bị nút.

Máy chủ thường là máy có bộ xử lý (CPU) tốc độ cao, bộ nhớ (RAM) và đĩa cứng (HD) lớn.

Trong một trạm mà các phương tiện đã được dùng chung, thì khi một trạm muốn gửi thông điệp cho trạm khác, nó dùng một phần mềm trong trạm làm việc đặt thông điệp vào "phong bì", phong bì này gọi là gói (*packet*), bao gồm dữ liệu thông điệp được bao bọc giữa tín hiệu đầu và tín hiệu cuối (đó là những thông tin đặc biệt) và sử dụng phần mềm mạng để chuyển gói đến trạm đích.

NIC sẽ chuyển gói tín hiệu vào mạng LAN, gói tín hiệu được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Khi nó chạy trong cáp dùng chung, mọi trạm gắn với cáp đều nhận được tín hiệu này, NIC ở mỗi trạm sẽ kiểm tra địa chỉ đích trong tín hiệu đầu của gói để xác định đúng địa chỉ đến, khi gói tín hiệu đi tới trạm có địa chỉ cần đến, đích ở trạm đó sẽ sao gói tín hiệu rồi lấy dữ liệu ra khỏi phong bì và đưa vào máy tính.

Các kiểu (Topology) của mạng LAN

Topology của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng như cách nối giữa chúng với nhau. Thông thường mạng có 3 dạng cấu trúc là: Mạng dạng hình sao (*Star Topology*), mạng dạng vòng (*Ring Topology*) và mạng dạng tuyến (*Linear Bus Topology*). Ngoài 3

dạng cấu hình kể trên còn có một số dạng khác biến tướng từ 3 dạng này như mạng dạng cây, mạng dạng hình sao - vòng, mạng hỗn hợp,v.v....

Mạng dạng hình sao (Star topology)

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với các chức năng cơ bản là:

- Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.
- Cho phép theo dõi và sử lý sai trong quá trình trao đổi thông tin.
- Thông báo các trạng thái của mạng...

Các ưu điểm của mạng hình sao:

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hoặc thu hẹp tuỳ theo yêu cầu của người sử dụng.

Nhược điểm của mạng hình sao:

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm . Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.
- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

Nhìn chung, mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần thông qua trục BUS, tránh được các yếu tố gây ngưng trệ mạng. Gần đây, cùng với sự phát triển *switching hub,* mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.

Mạng hình tuyến (Bus Topology)

Theo cách bố trí hành lang các đường như hình vẽ thì máy chủ (*host*) cũng như tất cả các máy tính khác (*workstation*) hoặc các nút (*node*) đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.

Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là *terminator*. Các tín hiệu và gói dữ liệu (*packet*) khi di chuyển lên hoặc xuống trong dây cáp đều mang theo địa chỉ của nơi đến.

Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi đó là sẽ có sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

Mạng dạng vòng (Ring Topology)

Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.

Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

Mạng dạng kết hợp

- Kết hợp hình sao và tuyến (*star/Bus Topology*)

Cấu hình mạng dạng này có bộ phận tách tín hiệu (*spitter*) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc *Ring Topology* hoặc *Linear Bus Topology*.

Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp *Star/Bus Topology*. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

- Kết hợp hình sao và vòng *(Star/Ring Topology)*

Cấu hình dạng kết hợp *Star/Ring Topology*, có một "thẻ bài" liên lạc (*Token*) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc (*workstation*) được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

Các giao thức (Protocol)

Một tập các tiêu chuẩn để trao đổi thông tin giữa hai hệ thống máy tính hoặc hai thiết bị máy tính với nhau được gọi là giao thức (Protocol).

Các giao thức (*Protocol*) còn được gọi là nghi thức hoặc định ước của mạng máy tính.

Để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (*medium access*) của giao thức, môi trường này ở dạng tuyến tính hoặc vòng.... Một trong các giao thức được sử dụng nhiều trong các LAN là:

1. Giao thức tranh chấp (*Contention Protocol*) CSMA/CD

   CSMA là viết tắt từ tiếng Anh: *Carrier Sense Multiple Access*, còn CD là viết tắt từ: *Conllision Detect.*

   Sử dụng giao thức này các trạm hoàn toàn có quyền truyền dữ liệu trên mạng với số lượng nhiều hay ít và một cách ngẫu nhiên hoặc bất kỳ khi nào có nhu cầu truyền dữ liệu ở mỗi trạm. Mối trạm sẽ kiểm tra tuyến và chỉ khi nào tuyến không bận mới bắt đầu truyền các gói dữ liệu.

   CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawai vào khoảng năm 1970, gọi là ALOHANET.

   Với phương pháp CSMA, thỉnh thoảng sẽ có hơn một trạm đồng thời truyền dữ liệu và tạo ra sự xung đột (*collision*) làm cho dữ liệu thu được ở các trạm bị sai lệch. Để tránh sự tranh chấp này mỗi trạm đều phải phát hiện được sự xung đột dữ liệu. Trạm phát phải kiểm tra *Bus* trong khi gửi dữ liệu để xác nhận rằng tín hiệu trên *Bus* thật sự đúng, như vậy mới có thể phát hiện được bất kỳ xung đột nào có thể xảy ra. Khi phát hiện có một sự xung đột, lập tức trạm phát sẽ gửi đi một mẫu làm nhiễu (*Jamming*) đã định trước để báo cho tất cả các trạm là có sự xung đột xảy ra và chúng sẽ bỏ qua gói dữ liệu này. Sau đó trạm phát sẽ trì hoãn một khoảng thời gian ngẫu nhiên trước khi phát lại dữ liệu. Ưu điểm của CSMA/CD là đơn giản, mềm dẻo, hiệu quả truyền thông tin cao khi lưu lượng thông tin của mạng thấp và có tính đột biến. Việc thêm vào hay dịch chuyển các trạm trên tuyến không ảnh hưởng đến các thủ tục của giao thức. Điểm bất lợi của CSMA/CD là hiệu suất của tuyến giảm xuống nhanh chóng khi phải tải quá nhiều thông tin.

2. Giao thức truyền token (*Token passing protocol*)

   Đây là giao thức thông dụng sau CSMA/CD được dùng trong các LAN có cấu trúc vòng (*Ring*). Trong phương pháp này, khối điều khiển mạng hoặc *token* được truyền lần lượt từ trạm này đến trạm khác. *Token* là một khối dữ liệu đặc biệt. Khi một trạm đang chiếm *token* thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó lại gửi *token* sang trạm kế tiếp.

   Trong *token* có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình mạng dạng xoay vòng thì trật tự của sự truyền *token* tương đương với trật tự vật lý của các trạm xung quanh vòng.

   Giao thức truyền *token* có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền *token* tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào sự xoay vòng tới các trạm. Việc truyền *token* sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra *token* để cho phép khôi phục lại *token* bị mất hoặc thay thế trạng thái của *token* và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).

Các chuẩn của mạng máy tính

Để mạng đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng không dự kiến trước trong tương lai tại lúc lắp đặt hệ thống và điều đó cũng cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.

Hội đồng tiêu chuẩn quốc tế là ISO (*International Standards Organization*), do các nước thành viên lập nên. Công việc ở Bắc Mỹ chịu sự điều hành của ANSI (*American National Standards Institude*) ở Hoa Kỳ. ANSI đã uỷ thác cho IEEE (*Institude of Electrical and Electronics Engineers*) phát triển và đề ra những tiêu chuẩn kỹ thuật cho LAN.

ISO đã đưa ra mô hình 7 mức (*layers*, còn gọi là lớp hay tầng) cho mạng, gọi là kiểu hệ thống kết nối mở hoặc **mô hình OSI (*Open System Interconnection*)**.

Chức năng của mức thấp bao gồm cả việc chuẩn bị cho mức cao hơn hoàn thành chức năng của mình. Một mạng hoàn chỉnh hoạt động với mọi chức năng của mình phải đảm bảo có 7 mức cấu trúc từ thấp đến cao.

- Mức 1: **Mức vật lý (*Physical layer*)**
  Thực chất của mức này là thực hiện nối liền các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý, ở mức này sẽ có các thủ tục đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các chuỗi bit thông tin.
- Mức 2: **Mức móc nối dữ liệu (*Data Link Layer*)**
  Nhiệm vụ của mức này là tiến hành chuyển đổi thông tin dưới dạng chuỗi các bit ở mức mạng thành từng đoạn thông tin gọi là *frame*. Sau đó đảm bảo truyền liên tiếp các frame tới mức vật lý, đồng thời xử lý các thông báo từ trạm thu gửi trả lại.
  Nói tóm lại, nhiệm vụ chính của mức 2 này là khởi tạo và tổ chức các *frame* cũng như xử lý các thông tin liên quan tới nó.
- Mức 3: **Mức mạng (*Network Layer*)**
  Mức mạng nhằm bảo đảm trao đổi thông tin giữa các mạng con trong một mạng lớn, mức này còn được gọi là mức thông tin giữa các mạng con với nhau. Trong mức mạng các gói dữ liệu có thể truyền đi theo từng đường khác nhau để tới đích. Do vậy, ở mức này phải chỉ ra được con đường nào dữ liệu có thể đi và con đường nào bị cấm tại thời điểm đó. Thường mức mạng được sử dụng trong trường hợp mạng có nhiều mạng con hoặc các mạng lớn và phân bổ trên một không gian rộng với nhiều nút thông tin khác nhau.
- Mức 4: **Mức truyền (*Transport Layer*)**
  Nhiệm vụ của mức này là xử lý các thông tin để chuyển tiếp các chức năng từ mức trên nó (mức tiếp xúc) đến mức dưới nó (mức mạng) và ngược lại. Thực chất mức truyền là để đảm bảo thông tin giữa các máy chủ với nhau. Mức này nhận các thông tin từ mức tiếp xúc, phân chia thành các đơn vị dữ liệu nhỏ hơn và chuyển chúng tới mức mạng.
- Mức 5: **Mức tiếp xúc (*Session Layer*)**
  Mức này cho phép người sử dụng tiếp xúc với nhau qua mạng. Nhờ mức tiếp xúc những người sử dụng lập được các đường nối với nhau, khi cuộc hội thoại được thành lập thì mức này có thể quản lý cuộc hội thoại đó theo yêu cầu của người sử dụng. Một đường nối giữa những người sử dụng được gọi là một cuộc tiếp xúc. Cuộc tiếp xúc cho phép người sử dụng được đăng ký vào một hệ thống phân chia thời gian từ xa hoặc chuyển một file giữa 2 máy.

- Mức 6: **Mức tiếp nhận (*Presentation Layer*)**
  Mức này giải quyết các thủ tục tiếp nhận dữ liệu một cách chính quy vào mạng, nhiệm vụ của mức này là lựa chọn cách tiếp nhận dữ liệu, biến đổi các ký tự, chữ số của mã ASCII hay các mã khác và các ký tự điều khiển thành một kiểu mã nhị phân thống nhất để các loại máy khác nhau đều có thể thâm nhập vào hệ thống mạng.
- Mức 7: **Mức ứng dụng (*Application Layer*)**
  Mức này có nhiệm vụ phục vụ trực tiếp cho người sử dụng, cung cấp tất cả các yêu cầu phối ghép cần thiết cho người sử dụng, yêu cầu phục vụ chung như chuyển các file, sử dụng các *terminal* của hệ thống,.... Mức sử dụng bảo đảm tự động hoá quá trình thông tin, giúp cho người sử dụng khai thác mạng tốt nhất.

Hệ thống kết nối mở OSI là hệ thống cho phép truyền thông tin với các hệ thống khác, trong đó các mạng khác nhau, sử dụng những giao thức khác nhau, có thể thông báo cho nhau thông qua chương trình *Pastren* để chuyển từ một giao thức này sang một giao thức khác.

Chuẩn IEEE

Tiêu chuẩn IEEE LAN được phát triển dựa vào uỷ ban IEEE 802. Tiêu chuẩn IEEE 802.3 liên quan tới mạng CSMA/CD bao gồm cả 2 *version* băng tần cơ bản và băng tần mở rộng. Tiêu chuẩn IEEE 802.4 liên quan tới sự sắp xếp tuyến *token* và IEEE 802.5 gồm các vòng truyền *token*.

Theo chuẩn 802 thì móc nối dữ liệu được chia thành 2 mức con: mức con điều khiển logic LLC (*Logical Link Control Sublayer)* và mức con điều khiển xâm nhập mạng MAC (*Media Access Control Sublayer*). Mức con LLC giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Mức con MAC chỉ làm nhiệm vụ điều khiển việc xâm nhập mạng. Thủ tục mức con LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp thâm nhập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn 802.4 thực chất là phương pháp thâm nhập mạng theo kiểu phát tín hiệu thăm dò *token* qua các trạm và đường truyền *bus*.

Chuẩn 802.5 dùng cho mạng dạng xoay vòng và trên cơ sở dùng tín hiệu thăm dò *token*. Mỗi trạm khi nhận được tín hiệu thăm dò *token* thì tiếp nhận *token* và bắt đầu quá trình truyền thông tin dưới dạng các *frame*. Các *frame* có cấu trúc tương tự như của chuẩn 802.4. Phương pháp xâm nhập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa cho người thiết kế vừa do người sử dụng tự quy định.

Mạng ETHERNET

Ethernet là mạng cục bộ do các công ty *Xerox, Intel* và *Digital equipment* xây dựng và phát triển. *Ethernet* là mạng thông dụng nhất đối với các mạng nhỏ hiện nay. *Ethernet* LAN được xây dựng theo chuẩn 7 lớp trong cấu trúc mạng của ISO, mạng truyền số liệu *Ethernet* cho phép đưa vào mạng các loại máy tính khác nhau kể cả máy tính mini. *Ethernet* có các đặc tính kỹ thuật chủ yếu sau đây:

- Có cấu trúc dạng tuyến phân đoạn, đường truyền dùng cáp đồng trục, tín hiệu truyền trên mạng được mã hoá theo kiểu đồng bộ (*Manchester*), tốc độ truyền dữ liệu là 10 Mb/s.
- Chiều dài tối đa của một đoạn cáp tuyến là 500m, các đoạn tuyến này có thể được kết nối lại bằng cách dùng các bộ chuyển tiếp và khoảng cách lớn nhất cho phép giữa 2 nút là 2,8 km.

Sử dụng tín hiệu băng tần cơ bản, truy xuất tuyến (*bus access*) hoặc tuyến *token* (*token bus*), giao thức là CSMA/CD, dữ liệu chuyển đi trong các gói. Gói (*packet*) thông tin dùng trong mạng có độ dài từ 64 đến 1518 byte.

Mạng TOKEN RING

Ngoài *Ethernet* LAN một công nghệ LAN chủ yếu khác đang được dùng hiện nay là *Token Ring*. Nguyên tắc của mạng *Token Ring* được định nghĩa trong tiêu chuẩn IEEE 802.5. Mạng *Token Ring* có thể chạy ở tốc độ 4Mbps hoặc 16Mbps. Phương pháp truy cập dùng trong mạng *Token Ring* gọi là *Token passing* . *Token passing* là phương pháp truy nhập xác định, trong đó các xung đột được ngăn ngừa bằng cách ở mỗi thời điểm chỉ một trạm có thể được truyền tín hiệu. Điều này được thực hiện bằng việc truyền một bó tín hiệu đặc biệt gọi là *Token* (mã thông báo) xoay vòng từ trạm này qua trạm khác. Một trạm chỉ có thể gửi đi bó dữ liệu khi nó nhận được mã không bận.

Các thiết bị kết nối chính của LAN

Hub

Hub là một trong những yếu tố quan trọng nhất của LAN, đây là điểm kết nối dây trung tâm của mạng, tất cả các trạm trên mạng LAN được kết nối thông qua HUB. Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi bó tín hiệu *Ethernet* được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của *hub*. Các *hub* thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý *hub.*

Có ba loại *hub:*

- Hub đơn (*stand alone hub)*
- Hub phân tầng (*stackable hub,* có tài liệu gọi là HUB sắp xếp)
- Hub modun (*modular hub)*

Modular hub rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, *modular* có từ 4 đến 14 khe cắm, có thể lắp thêm các modun *Ethernet* 10BASET.

Stackable hub là lý tưởng cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.

Chú ý: Uỷ ban kỹ thuật điện tử (IEEE) đề nghị dùng các tên sau đây để chỉ 3 loại dây cáp dùng với mạng *Ethernet* chuẩn 802.3.

- Dây cáp đồng trục sợi to (*thick coax)* thì gọi là 10BASE5 (Tốc độ 10 Mbps, tần số cơ sở, khoảng cách tối đa 500m).
- Dây cáp đồng trục sợi nhỏ *(thin coax)* gọi là 10BASE2 (Tốc độ 10 Mbps, tần số cơ sở, khoảng cách tối đa 200m).
- Dây cáp đôi xoắn không vỏ bọc (*twisted pair*) gọi là 10BASET (Tốc độ 10 Mbps, tần số cơ sở, sử dụng cáp sợi xoắn).
- Dây cáp quang (*Fiber Optic Inter-Repeater Link*) gọi là FOIRL

Liên mạng (internetworking)

Việc kết nối các LAN riêng lẻ thành một liên mạng chung được gọi là Internetworking. Internetworking sử dụng ba công cụ chính là: bridge, router và switch.

Cầu nối (bridge):

Là cầu nối hai hoặc nhiều đoạn (segment) của một mạng. Theo mô hình OSI thì *bridge* thuộc mức 2. *Bridge* sẽ lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối, hoặc gửi trả lại nơi xuất phát. Các *bridge* cũng thường được dùng để phân chia một mạng lớn thành hai mạng nhỏ nhằm làm tăng tốc độ. Mặc dầu ít chức năng hơn *router*, nhưng *bridge* cũng được dùng phổ biến.

Bộ dẫn đường (*router*)

Chức năng cơ bản của *router* là gửi đi các gói dữ liệu dựa trên địa chỉ phân lớp của mạng và cung cấp các dịch vụ như bảo mật, quản lý lưu thông...

Giống như *bridge*, *router* là một thiết bị siêu thông minh đối với các mạng thực sự lớn. router biết địa chỉ của tất cả các máy tính ở từng phía và có thể chuyển các thông điệp cho phù hợp. Chúng còn phân đường-định truyền để gửi từng thông điệp có hiệu quả.

Theo mô hình OSI thì chức năng của *router* thuộc mức 3, cung cấp thiết bị với thông tin chứa trong các *header* của giao thức, giúp cho việc xử lý các gói dữ liệu thông minh.

Dựa trên những giao thức, *router* cung cấp dịch vụ mà trong đó mỗi packet dữ liệu được đọc và chuyển đến đích một cách độc lập.

Khi số kết nối tăng thêm, mạng theo dạng *router* trở nên kém hiệu quả và cần suy nghĩ đến sự thay đổi.

Bộ chuyển mạch (*switch)*

Chức năng chính của *switch* là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (*backbone*) nội tại tốc độ cao. *Switch* có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ *Ethernet* LAN hoặc Token Ring.

Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Các *switch* là loại thiết bị mạng mới, nhiều người cho rằng, nó sẽ trở nên phổ biến nhất vì nó là bước đầu tiên trên con đường chuyển sang chế độ truyền không đồng bộ ATM.

Hệ điều hành mạng - NOS (*Network Operating System)*

Cùng với sự nghiên cứu và phát triển mạng máy tính, hệ điều hành mạng đã được nhiều công ty đầu tư nghiên cứu và đã công bố nhiều phần mềm quản lý và điều hành mạng có hiệu quả như: *NetWare* của công ty NOVELL, LAN *Manager* của *Microsoft* dùng cho các máy *server* chạy hệ điều hành OS/2, LAN server của IBM (gần như đồng nhất với LAN *Manager*), *Vines* của *Banyan Systems* là hệ điều hành mạng dùng cho *server* chạy hệ điều hành UNIX, *Promise* LAN của *Mises Computer* chạy trên *card* điều hợp mạng độc quyền, *Widows for Workgroups* của *Microsoft,* LANtastic của *Artisoft, NetWare Lite* của *Novell,....*

Một trong những sự lựa chọn cơ bản mà ta phải quyết định trước là hệ điều hành mạng nào sẽ làm nền tảng cho mạng của ta, việc lựa chọn tuỳ thuộc vào kích cỡ của mạng hiện tại và sự phát triển trong tương lai, còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều *Version* khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy *mini*, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).
- Hệ điều hành mạng *Windows* NT: Đây là hệ điều hành của hãng *Microsoft*, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS. Do hãng *Microsoft* là hãng phần mềm lớn nhất thế giới hiện nay, hệ điều hành này có khả năng sẽ được ngày càng phổ biến rộng rãi. Ngoài ra, *Windows* NT có thể liên kết tốt với máy chủ *Novell Netware*. Tuy nhiên, để chạy có hiệu quả, *Windows* NT cũng đòi hỏi cấu hình máy tương đối mạnh.
- Hệ điều hành mạng *Windows for Worrkgroup*: Đây là hệ điều hành mạng ngang hàng nhỏ, cho phép một nhóm người làm việc (khoảng 3-4 người)

dùng chung ổ đĩa trên máy của nhau, dùng chung máy in nhưng không cho phép chạy chung một ứng dụng. Hệ dễ dàng cài đặt và cũng khá phổ biến.

- Hệ điều hành mạng *NetWare của Novell*: Đây là hệ điều hành phổ biến nhất hiện nay ở nước ta và trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Trong những năm qua, *Novell* đã cho ra nhiều phiên bản của *Netware*: Netware 2.2, 3.11. 4.0 và hiện có 4.1. *Netware* là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính *Apple Macintosh*, chạy hệ điều hành MS-DOS hoặc OS/2.

  Hệ điều hành này tương đối gọn nhẹ, dễ cài đặt (máy chủ chỉ cần thậm chí AT386) do đó phù hợp với hoàn cảnh trang thiết bị hiện tại của nước ta. Ngoài ra, vì là một phần mềm phổ biến nên Novell Netware được các nhà sản xuất phần mềm khác hỗ trợ (theo nghĩa các phân mềm do các hãng phần mềm lớn trên thế giới làm đều có thể chạy tốt trên hệ điều hành mạng này).

Các Phương tiện Kết nối mạng liên khu vực (WAN)

Bên cạnh phương pháp sử dụng đường điện thoại thuê bao để kết nối các mạng cục bộ hoặc mạng khu vực với nhau hoặc kết nối vào Internet, có một số phương pháp khác:

- **Đường thuê bao (leased line)**. Đây là phương pháp cũ nhất, là phương pháp truyền thống nhất cho sự nối kết vĩnh cửu. Bạn thuê đường dây từ công ty điện thoại (trực tiếp hoặc qua nhà cung cấp dịch vụ). Bạn cần phải cài đặt một "*Chanel Service Unit*" (CSU) để nối đến mạng T, và một "*Digital Service Unit*" (DSU) để nối đến mạng chủ (primary) hoặc giao diện mạng.
- **ISDN (Integrated Service Digital Nework).** Sử dụng đường điện thoại số thay vì đường tương tự. Do ISDN là mạng dùng tín hiệu số, bạn không phải dùng một modem để nối với đường dây mà thay vào đó bạn phải dùng một thiết bị gọi là "*codec*" với modem có khả năng chạy ở 14.4 kbit/s. ISDN thích hợp cho cả hai trường hợp cá nhân và tổ chức. Các tổ chức có thể quan tâm hơn đến ISDN có khả năng cao hơn ("*primary*" ISDN) với tốc độ tổng cộng bằng tốc độ 1.544 Mbit/s của đường T1. Cước phí khi sử dụng ISDN được tính theo thời gian, một số trường hợp tính theo lượng dữ liệu được truyền đi và một số thì tính theo cả hai.
- **CATV link.** Công ty dẫn cáp trong khu vực của bạn có thể cho bạn thuê một "chỗ" trên đường cáp của họ với giá hấp dẫn hơn với đường điện thoại. Cần

phải biết những thiết bị gì cần cho hệ thống của mình và độ rộng của dải mà bạn sẽ được cung cấp là bao nhiêu. Cũng như việc đóng góp chi phí với những khách hàng khác cho kênh liên lạc đó là như thế nào. Một dạng kỳ lạ hơn được đưa ra với tên gọi là mạng "lai" ("*hybrid" Network*), với một kênh CATV được sử dụng để lưu thông theo một hướng và một đường ISDN hoặc gọi số sử dụng cho đường trở lại. Nếu muốn cung cấp thông tin trên Internet, bạn phải xác định chắc chắn rằng "kênh ngược" của bạn đủ khả năng phục vụ cho nhu cầu thông tin của khách hàng của bạn.

- **Frame relay.** Frame relay "uyển chuyển" hơn đường thuê bao. Khách hàng thuê đường Frame relay có thể mua một dịch vụ có mức độ xác định - một "tốc độ thông tin uỷ thác" ("*Committed Information Rale" - CIR*). Nếu như nhu cầu của bạn trên mạng là rất "bột phát" (*burty*), hay người sử dụng của bạn có nhu cầu cao trên đường liên lạc trong suốt một khoảng thời gian xác định trong ngày, và có ít hoặc không có nhu cầu vào ban đêm - Frame relay có thể sẽ kinh tế hơn là thuê hoàn toàn một đường T1 (hoặc T3). Nhà cung cấp dịch vụ của bạn có thể đưa ra một phương pháp tương tự như là phương pháp thay thế đó là *Switched Multimegabit Data Service*.
- **Chế độ truyền không đồng bộ (Asynchoronous Trangfer Mode - ATM).** ATM là một phương pháp tương đối mới đầu tiên báo hiệu cùng một kỹ thuật cho mạng cục bộ và liên khu vực. ATM thích hợp cho *real-time multimedia* song song với truyền dữ liệu truyền thống. ATM hứa hẹn sẽ trở thành một phần lớn của mạng tương lai.
- **Đường vi sóng (Microware links).** Nếu cần kết nối vĩnh viễn đến nhà cung cấp dịch vụ nhưng lại thấy rằng đường thuê bao hay những lựa chọn khác là quá đắt, bạn sẽ thấy *microware* như là một lựa chọn thích hợp. Bạn không cần trả quá đắt cho cách này của *microware*, tuy nhiên bạn cần phải đầu tư nhiều tiền hơn vào lúc đầu, và bạn sẽ gặp một số rủi ro như tốc độ truyền đến mạng của bạn quá nhanh.
- **Đường vệ tinh (satellite links).** Nếu bạn muốn được chuyển một lượng lớn dữ liệu đặc biệt là từ những địa điểm từ xa thì đường vệ tinh là câu trả lời. Tầm hoạt động của những vệ tinh cùng vị trí địa lý với trái đất cũng tạo ra một sự chậm trễ (hoặc "bị che dấu") mà những người sử dụng Telnet có thể cảm nhận được

Những hướng dẫn tăng cường an toàn, bảo mật cho hệ thống mạng

Giới thiệu

Bài viết này sẽ trình bày các vấn đề được xem là nền tảng của an toàn, bảo mật trong một tổ chức, doanh nghiệp. Các vấn đề được trình bày bao gồm cả bảo mật ở

mức hệ thống và ứng dụng sẽ là cơ sở cho các tổ chức khi muốn xây dựng cơ chế bảo mật. Tài liệu cũng giúp bạn rút ngắn được thời gian tiếp cận vấn đề đảm bảo an toàn cho hệ thống mạng nội bộ của mình. Bạn không cần mất nhiều thời gian để tìm hiểu mọi thứ. Khi xem xét mọi vấn đề, nơi tốt nhất để khởi đầu chính là các căn bản – ở đây, chúng tôi sẽ trình bày 6 bước cơ bản để hệ thống bảo mật tốt hơn.

Bước 1: Thành lập bộ phận chuyên trách về vấn đề bảo mật

Bất kỳ kế hoạch bảo mật nào cũng cần sự hỗ trợ trên nhiều phương diện khác nhau, nếu nó muốn thành công. Một trong những phương thức tốt nhất để có thể được sự hỗ trợ là nên thiết lập một bộ phận chuyên trách về vấn đề bảo mật. Bộ phận này sẽ chịu trách nhiệm trước công ty về các công việc bảo mật.

Mục đích trước tiên của bộ phận này là gây dựng uy tín với khách hàng. Hoạt động của bộ phận này sẽ khiến cho khách hàng cảm thấy yên tâm hơn khi làm việc hoặc sử dụng các dịch vụ của công ty. Bộ phận này có trách nhiệm thường xuyên cung cấp các lưu ý, cảnh báo liên quan đến an toàn bảo mật thông tin nhằm tránh các rủi ro đáng tiếc cho khách hàng và công ty.

Bộ phận này còn có trách nhiệm tìm hiểu, đưa ra giải pháp, cơ chế bảo mật cho toàn công ty. Sẽ là hiệu quả và xác thực hơn khi công việc này được thực hiện bởi chính đội ngũ trong công ty thay vì đi thuê một công ty bảo mật khác thực hiện.

Cuối cùng, một bộ phận chuyên trách về vấn đề bảo mật có thể thay đổi cách làm, cách thực hiện công việc kinh doanh của công ty để tăng tính bảo mật trong khi cũng cải tiến được sức sản xuất, chất lượng, hiệu quả và tạo ra sức cạnh tranh của công ty. Ví dụ, chúng ta hãy nói đến VPN (Virtual Private Network), đây là một công nghệ cho phép các nhân viên đảm bảo an toàn khi đọc email, làm việc với các tài liệu tại nhà, hay chia sẻ công việc giữa hai nhân viên hay hai phòng ban.

Bước 2: Thu thập thông tin

Trước khi đưa ra các thông báo mô tả thực hiện bảo mật, bạn phải lường được mọi tình huống sẽ xảy ra, không chỉ bao gồm toàn bộ các thiết bị và hệ thống đi kèm trong việc thực hiện bảo mật mà còn phải kể đến cả các tiền trình xử lý, các cảnh bảo bảo mật, sự thẩm định hay các thông tin cần được bảo vệ. Điều này rất quan trọng khi cung cấp một cái nhìn bao quát về hệ thống bảo mật của công ty. Sự

chuẩn bị này cũng nên tham chiếu tới các chính sách bảo mật cũng như các hướng dẫn thực hiện của công ty trong vấn đề an toàn bảo mật. Phải lường trước được những gì xảy ra trong từng bước tiến hành của các dự án.

Để kiểm tra mức độ yếu kém của hệ thống, hãy bắt đầu với những vấn đề có thể dẫn tới độ rủi ro cao nhất trong hệ thống mạng của bạn, như Internet. Hãy sử dụng cơ chế bảo mật bên ngoài từ sản phẩm của một hãng có danh tiếng, có thể cung cấp thông tin cần thiết để ước lượng mức bảo mật hiện tại của công ty bạn khi bị tấn công từ Internet. Sự thẩm định này không chỉ bao gồm việc kiểm tra các lỗ hổng, mà còn gồm cả các phân tích từ người sử dụng, hệ thống được kết nối bằng VPN, mạng và các phân tích về thông tin công cộng sẵn có.

Một trong những cân nhắc mang tính quan trọng là thẩm định từ bên ngoài vào. Đây chính là điểm mấu chốt trong việc đánh giá hệ thống mạng. Điển hình, một công ty sử dụng cơ chế bảo mật bên ngoài, cung cấp các dịch vụ email, Web theo cơ chế đó, thì họ nhận ra rằng, không phải toàn bộ các tấn công đều đến từ Internet. Việc cung cấp lớp bảo mật theo account, mạng bảo vệ bản thân họ từ chính những người sử dụng VPN và các đồng nghiệp, và tạo ra các mạng riêng rẽ từ các cổng truy cập đầu cuối là toàn bộ các ưu thế của cơ chế này.

Cơ chế bảo mật bên trong cũng giúp việc quản lý bảo mật công ty được tốt hơn. Bằng cách kiểm tra toàn bộ công việc kinh doanh, các cơ chế chính sách, các quá trình xử lý, xác thực dữ liệu tương phản với những gì được mô tả, hay sự tương thích với những chuẩn đã tồn tại được thẩm định. Cơ chế bảo mật bên trong cung cấp thông tin một cách chi tiết tương tự như việc khảo sát kỹ lưỡng phạm vi ở mức sâu hơn, thậm chí bao gồm cả việc phá mã mật khẩu và các công cụ phân tích hệ thống để kiểm tra tính tương thích về chính sách trong tương lai.
Bước 3: Thẩm định tính rủi ro của hệ thống

Khi thẩm định tính rủi ro của hệ thống, hãy sử dụng công thức sau:

Tính rủi ro = Giá trị thông tin * Mức độ của lỗ hổng * Khả năng mất thông tin

Tính rủi ro bằng với giá trị thông tin trong câu hỏi (bao gồm giá trị đồng tiền, giá trị thời gian máy bị lỗi do lỗi bảo mật, giá trị mất mát khách hàng – tương đối),

thời gian của quy mô lỗ hổng (tổng cộng/từng phần của tổn thất dữ liệu, thời gian hệ thống ngừng hoạt động, sự nguy hiểm khi dữ liệu hỏng), thời gian về khả năng xuất hiện mất thông tin.

Để lấy được các kết quả từ bước đầu (các giá trị, báo cáo về cơ chế bảo mật ngoài, và chính sách bảo mật), và tập trung vào 3 trong số các mặt thường được đề cập. Sau đó, bắt đầu với một số câu hỏi khung sau:

*Cơ chế bảo mật đã tồn tại của công ty có được đề ra rõ ràng và cung cấp đủ biện pháp bảo mật chưa?
*Kết quả từ cơ chế bảo mật bên ngoài có hợp lệ so với chính sách bảo mật của

công ty?
*Có mục nào cần sửa lại trong cơ chế bảo mật mà không được chỉ rõ trong chính sách?
*Hệ thống bảo mật sẽ mất tác dụng trong tính rủi ro cao nhất nào?
*Giá trị, thông tin gì mang tính rủi ro cao nhất?

Các câu trả lời cung cấp cái nhìn toàn diện cho việc phân tích về toàn bộ chính sách bảo mật của công ty. Có lẽ, thông tin quan trọng được lấy trong quá trình kết hợp các giá trị thẩm định và tính rủi ro tương ứng. Theo giá trị thông tin, bạn có thể tìm thấy các giải pháp mô tả được toàn bộ các yêu cầu, bạn có thể tạo ra một danh sách quan tâm về lỗ hổng bảo mật.

Bước 4: Xây dựng giải pháp

Trên thực tế không tồn tại giải pháp an toàn, bảo mật thông tin dang Plug and Play cho các tổ chức đặc biệt khi phải đảm bảo các luật thương mại đã tồn tại và phải tương thích với các ứng dụng, dữ liệu sẵn có. Không có một tài liệu nào có thể lượng hết được mọi lỗ hổng trong hệ thống và cũng không có nhà sản xuất nào có thể cung cấp đủ các công cụ cần thiết. Cách tốt nhất vẫn là sử dụng kết hợp các giải pháp, sản phẩm nhằm tạo ra cơ chế bảo mật đa năng.

Firewall

Xem xét và lựa chọn một sản phẩm firewall hợp lý và đưa và hoạt động phù hợp với chính sách của công ty là một trong những việc đầu tiên trong quá trình bảo mật hệ thống. Firewall có thể là giải pháp phần cứng hoặc phần mềm hoặc kết hợp cả hai. Nhiệm vụ của firewall là ngăn chặn các tấn công trực tiếp vào các thông tin quan trọng của hệ thống, kiểm soát các thông tin ra vào hệ thống. Việc lựa chọn firewall thích hợp cho một hệ thống không phải là dễ dàng. Các firewall đều phụ thuộc trên một môi trường, cấu hình mạng, ứng dụng cụ thể. Khi xem xét lựa chọn một firewall, cần tập trung tìm hiểu tập các chức năng của firewall, tính năng lọc địa chỉ, gói tin, ...

Hệ thống kiểm tra xâm nhập mạng (IDS)

Một firewall được gọi là tốt chỉ khi nó có thể lọc và tạo khả năng kiểm soát các gói tin khi đi qua nó. Và đây cũng chính là nơi mà hệ thống IDS nhập cuộc. Nếu bạn

xem firewall như một con đập ngăn nước, thì thì bạn có thể ví IDS như một hệ thống điều khiển luồng nước trên các hệ thống xả nước khác nhau. Một IDS, không liên quan tới các công việc điều khiển hướng đi của các gói tin, mà nó chỉ có nhiệm vụ phân tích các gói tin mà firewall cho phép đi qua, tìm kiếm các chữ kí tấn công đã biết (các chữ kí tấn công chính là các đoạn mã được biết mang tính nguy hiểm cho hệ thống) mà không thể kiểm tra hay ngăn chặn bởi firewall. IDS tương ứng với việc bảo vệ đằng sau của firewall, cung cấp việc chứng thực thông tin cần thiết để đảm bảo chắc chắn cho firewall hoạt động hiệu quả.
Hệ thống kiểm tra xâm phạm dựa theo vùng (H-IDS)

Sự lựa chọn, thực hiện và sử dụng một hệ thống kiểm tra sự xâm phạm trên máy chủ dựa trên nhiều hệ điều hành và môi trường ứng dụng chỉ định. Một hàm chức năng đầy đủ của H-IDS có thể cung cấp các thông báo đều đặn theo thời gian của bất kỳ sự thay đổi nào tới máy chủ từ tác động bên trong hay bên ngoài. Nó là một trong những cách tốt nhất để giảm thiểu sự tổn thương của hệ thống. Việc tìm kiếm hệ thống mà hỗ trợ hầu hết các hệ điều hành sử dụng trong tổ chức của bạn nên được xem như một trong những quyết định chính cho mỗi H-IDS.

Hệ thống kiểm tra xâm phạm dựa theo ứng dụng (App-IDS)

Số lượng App-IDS xuất hiện trên thị trường ngày càng nhiều. Các công cụ này thực hiện việc phân tích các thông điệp từ một ứng dụng cụ thể hay thông tin qua proxy tới ứng dụng đó. Trong lúc chúng có mục đích cụ thể, chúng có thể cung cấp mức bảo mật tăng lên theo từng mảng ứng dụng cụ thể. Khi được kết hợp với một H-IDS, chúng đảm bảo rằng sự xâm nhập tới một máy chủ sẽ giảm thiểu. Một App-IDS nên được xem như một chức năng hỗ trợ bảo mật trong suốt, mặc dù không đúng trong một số trường hợp.

Phần mềm Anti-Virus (AV)

Phần mềm AV nên được cài trên toàn bộ máy trạm (workstation), máy chủ (server), hệ thống hỗ trợ dịch vụ số, và hầu hết những nơi chứa dữ liệu quan trọng vào ra. Hai vấn đề quan trọng nhất để xem xét khi đặt yêu cầu một nhà sản xuất AV quản lý nhiều máy chủ và máy trạm trên toàn bộ phạm vi của công ty là khả năng nhà cung cấp đó có đối phó được các đe doạ từ virus mới hay không. (nguyên nhân: không bao giờ cho rằng phầm mềm đang chạy, luôn kiểm tả phiên bản của

virus và các file cập nhật cho virus mới).

Mạng riêng ảo (VPN)

Việc sử dụng VPN để cung cấp cho các nhân viên hay các cộng sự truy cập tới các tài nguyên của công ty từ nhà hay nơi làm việc khác với mức bảo mật cao, hiệu quả nhất trong quá trình truyền thông, và làm tăng hiệu quả sản xuất của nhân viên. Tuy nhiên, không có điều gì không đi kèm sự rủi ro. Bất kỳ tại thời điểm nào khi một VPN được thiết lập, bạn phải mở rộng phạm vi kiểm soát bảo mật của công ty tới toàn bộ các nút được kết nối với VPN.

Để đảm bảo mức bảo mật cho hệ thống này, người sử dụng phải thực hiện đầy đủ các chính sách bảo mật của công ty. Điều này có thể thực hiện được qua việc sử dụng các hướng dẫn của nhà sản xuất về dịch vụ VPN như hạn chế các ứng dụng có thể chạy ở nhà, cổng mạng có thể mở, loại bỏ khả năng chia kênh dữ liệu, thiết lập hệ thống bảo vệ virus khi chạy hệ thống từ xa, tất cả công việc này giúp giảm thiểu tính rủi ro. Điều này rất quan trọng đối với các công ty phải đối mặt với những đe doạ trong việc kiện cáo, mạng của họ hay hệ thống được sử dụng để tấn công các công ty khác.

Sinh trắc học trong bảo mật

Sinh trắc học đã được biết đến từ một số năm trước đây, nhưng cho đến nay vẫn có rất nhiều khó khăn cho việc nhân rộng để áp dụng cho các hệ thống bảo mật thương mại. Dấu tay, tròng mắt, giọng nói, ..., cung cấp bảo mật mức cao trên các mật khẩu thông thường hay chứng thực hai nhân tố, nhưng cho đến hiện tại, chúng cũng vẫn được coi như phương thức tốt nhất để truy cập vào hệ thống.

Các thế hệ thẻ thông minh

Các công ty gần đây sử dụng đã sử dụng thẻ thông minh như một phương thức bảo mật hữu hiệu. Windows 2000 cung cấp cơ chế hỗ trợ thẻ thông minh như một phương tiện chính trong việc chứng thực quyền đăng nhập hệ thống. Nói chung, sự kết hợp đa công nghệ (như tròng mắt, thẻ thông minh, dấu tay) đang dần hoàn thiện và mở ra một thời đại mới cho việc chứng thực quyền truy cập trong hệ thống bảo mật.

Kiểm tra máy chủ

Sự kiểm tra đều đặn mức bảo mật được cung cấp bởi các máy chủ phụ thuộc chủ yếu vào sự quản lý. Mọi máy chủ ở trong một công ty nên được kiểm tra từ Internet để phát hiện lỗ hổng bảo mật. Thêm nữa, việc kiểm tra từ bên trong và quá trình thẩm định máy chủ về căn bản là cần thiết để giảm thiểu tính rủi ro của hệ thống, như khi firewall bị lỗi hay một máy chủ, hệ thống nào đó bị trục trặc.

Hầu hết các hệ điều hành đều chạy trong tình trạng thấp hơn với mức bảo mật tối thiểu và có rất nhiều lỗ hổng bảo mật. Trước khi một máy chủ khi đưa vào sản xuất, sẽ có một quá trình kiểm tra theo một số bước nhất định. Toàn bộ các bản sửa lỗi phải được cài đặt trên máy chủ, và bất cứ dịch vụ không cần thiết nào phải được loại bỏ. Điều này làm tránh độ rủi ro xuống mức thấp nhất cho hệ thống.

Việc tiếp theo là kiểm tra các log file từ các máy chủ và các ứng dụng. Chúng sẽ cung cấp cho ta một số thông tin tốt nhất về hệ thống, các tấn công bảo mật. Trong rất nhiều trường hợp, đó chính là một trong những cách để xác nhận quy mô của một tấn công vào máy chủ.

Kiểm soát ứng dụng

Vấn đề an toàn bảo mật trong mã nguồn của các ứng dụng hầu hết không được quan tâm. Điều này không được thể hiện trên các sản phẩm như liệu nó có được mua, được download miễn phí hay được phát triển từ một mã nguồn nào đó. Để giúp đỡ giảm thiểu sự rủi ro bảo mật trong các ứng dụng, thẩm định lại giá trị của ứng dụng trong công ty, như công việc phát triển bên trong của các ứng dụng, Điều này cũng có thể bao gồm các đánh giá của các thực thể bên ngoài như đồng nghiệp hay các khách hàng.

Việc điều khiển cấu hình bảo mật các ứng dụng có thể làm tăng mức bảo mật. Hầu hết các ứng dụng được cấu hình tại mức tối thiểu của tính năng bảo mật, nhưng qua các công cụ cấu hình, mức bảo mật của hệ thống có thể được tăng lên. Lượng thông tin kiểm soát được cung cấp bởi ứng dụng cũng có thể được cấu hình. Nơi mà các ứng dụng cung cấp thông tin về quy mô bảo mật, thời gian kiểm soát và sự phân tích thông tin này sẽ là chìa khoá để kiểm tra các vấn đề bảo mật thông tin.

Các hệ điều hành

Sự lựa chọn hệ điều hành và ứng dụng là quá trình đòi hỏi phải có sự cân nhắc kỹ càng. Chọn cái gì giữa hệ điều hành Microsoft hay UNIX, trong rất nhiều trường hợp, điều thường do ấn tượng cá nhân è sản phẩm. Khi lựa chọn một hệ điều hành, thông tin về nhà sản xuất không quan trọng bằng những gì nhà sản xuất đó làm được trong thực tế, về khả năng bảo trì hay dễ dàng thực hiện với các tài liệu đi kèm. Bất kỳ một hệ điều hành nào từ 2 năm trước đây đều không thể đảm bảo theo những chuẩn ngày nay, và việc giữ các máy chủ, ứng dụng của bạn được cập nhật thường xuyên sẽ đảm bảo giảm thiểu khả năng rủi ro của hệ thống.

Khi lựa chọn một hệ điều hành, hãy tìm hiểu không chỉ các tiêu chuẩn thông thường như (quản trị, hiệu năng, tính chứng thực), mà còn phải xem xét khả năng áp dụng được của hệ điều hành với hệ thống hiện tại. Một hệ điều hành có thể cung cấp cơ chế bảo mật tốt hơn khi nó tương thích với các ứng dụng chạy bên trong nó như DNS hay WebServer, trong khi các hệ điều hành khác có thể có nhiều chức năng tốt hơn như một hệ thống application, database hay email server.
Bước 5: Thực hiện và giáo dục

Ban đầu, sự hỗ trợ cần thiết sẽ được đúc rút lại và lên kế hoạch hoàn chỉnh cho dự án bảo mật. Đây chính là bước đi quan trọng mang tính chiến lược của mỗi công ty về vấn đề bảo mật. Các chi tiết kỹ thuật của bất kỳ sự mô tả nào cũng sẽ thay đổi theo môi trường, công nghệ, và các kỹ năng liên quan, ngoài ra có một phần không nằm trong việc thực thi bảo mật nhưng chúng ta không được coi nhẹ, đó chính là sự giáo dục. Để đảm bảo sự thành công bảo mật ngay từ lúc đầu, người sử dụng phải có được sự giáo dục cần thiết về chính sách, gồm có:

* Kỹ năng về các hệ thống bảo mật mới, các thủ tục mới.
* Hiểu biết về các chính sách mới về tài sản, dữ liệu quan trọng của công ty.
* Hiểu các thủ tục bắt buộc mới, chính sách bảo mật công ty.

Nói tóm lại, không chỉ đòi hỏi người sử dụng có các kỹ năng cơ bản, mà đòi hỏi học phải biết như tại sao và cái gì họ đang làm là cần thiết với chính sách của công ty.
Bước 6: Tiếp tục kiểm tra, phân tích và thực hiện

Hầu hết những gì mong đợi của một hệ thống bảo mật bất kỳ là chạy ổn định, điều

khiển được hệ thống và nắm bắt được các luồng dữ liệu của hệ thống. Quá trình phân tích, tổng hợp các thông tin, sự kiện từ firewall, IDS's, VPN, router, server, và các ứng dụng là cách duy nhất để kiểm tra hiệu quả của một hệ thống bảo mật, và cũng là cách duy nhất để kiểm tra hầu hết sự vi phạm về chính sách cũng như các lỗi thông thường mắc phải với hệ thống.

Các gợi ý bảo mật cho hệ thống và mạng

Theo luận điểm này, chúng tôi tập trung chủ yếu và các bước mang tính hệ thống để cung cấp một hệ thống bảo mật. Từ đây, chúng tôi sẽ chỉ ra một vài bước đi cụ thể để cải thiện hệ thống bảo mật, dựa trên kết quả của việc sử dụng các phương thức bảo mật bên ngoài và bảo mật bên trong của hệ thống. Chúng tôi cũng giới hạn phạm vi của các gợi ý này theo các vấn đề chung nhất mà chúng tôi đã gặp phải, để cung cấp, mô tả vấn đề một cách chính xác hơn cũng như các thách thức mà mạng công ty phải đối mặt ngày nay. Để mang tính chuyên nghiệp hơn về IT, các gợi ý này được chia thành các phần như sau:

Đặc điểm của bảo mật

*Tạo bộ phận chuyên trách bảo mật để xem xét toàn bộ các vấn đề liên quan tới bảo mật

*Thực hiện các thông báo bảo mật tới người sử dụng để đảm bảo mọi người hiểu và thực hiện theo các yêu cầu cũng như sự cần thiết của việc thực hiện các yêu cầu đó.

* Tạo, cập nhật, và theo dõi toàn bộ chính sách bảo mật của công ty.

Windows NT/IIS

* Hầu hết 95% các vấn đề bảo mật của NT/IIS, chúng ta có thể giải quyết theo các bản sửa lỗi. Đảm bảo chắc chắn toàn bộ các máy chủ NT và IIS được sửa lỗi với phiên bản mới nhất.
* Xoá (đừng cài đặt) toàn bộ các script từ Internet.

Cisco Routers

* Loại bỏ các tính năng như finger, telnet, và các dịch vụ, cổng khác trên thiết bị định tuyến (router).
* Bỏ các gói tin tài nguyên IP dẫn đường trong router.
* Chạy Unicast RPF để ngăn chặn người sử dụng của bạn sử dụng việc giả mạo IP.
* Sử dụng router của bạn như một firewall phía trước và thực hiện các ACL tương tự theo các luật trong firewall của bạn.

Quy định chung về cầu hình firewall

* Cấu hình của firewall nên có các luật nghiêm ngặt. Chỉ rõ các luật đối với từng loại truy nhập cả bên ngoài lẫn bên trong.
* Giảm thiểu các truy nhập từ xa tới firewall.
* Cung cấp hệ thống kiểm soát tập luật của firewall.
* Kiểm tra lại các luật.

Cisco PIX Firewalls

* Không cho phép truy cập qua telnet
* Sử dụng AAA cho việc truy cập, điều khiển hệ thống console

Kiểm soát Firewall-1

* Loại bỏ các luật mặc định cho phép mã hoá và quản lý của firewall, thay thế các luật không rõ ràng bằng các luật phân biệt rạch ròi trong công việc thực thi của bạn.
* Không sử dụng mặc định luật “allow DNS traffic” - chấp nhận luật này chỉ cho các máy chủ cung cấp DNS cho bên ngoài.

DNS bên trong

* Bất kỳ máy chủ nào cung cấp DNS bên trong và các dịch vụ mang tính chất nội bộ phải không được cung cấp DNS bên ngoài.
* Kiểm tra với nhà cung cấp DNS của bạn để cấu hình bảo vệ từ thuộc tính “cache

poisoning”

==========
====== HcE Gr0up ======
&ksvthdang(HCE)
Vì sao bạn bị "nhồi" e-mail spam? - 23/8/2006 5h:40

Mỗi ngày mở hòm thư điện tử ra bạn thấy rất nhiều những bức thư lạ không biết của ai. Có những bức thư được gửi đi với nội dung quảng cáo, nhưng cũng có những bức thư không có nội dung gì cả. Bạn băn khoăn không hiểu làm sao những người này biết được địa chỉ email của bạn khi mà bạn chỉ cho một số người địa chỉ email của bạn mà thôi.

Đó chính là cái được gọi là *SPAM - những bức thư rác*. Nhưng làm thế nào SPAM biết được địa chỉ email của người dùng Internet? SPAM đã được gửi đi như thế nào? Trong bài viết này chúng tôi sẽ giúp bạn tìm hiểu rõ hơn về một vấn nạn của Internet. Đó là SPAM.

SPAM là gì?

Thư rác, một vấn nạn của Internet.

SPAM thực sự gây ra rất nhiều khó chịu cho người dùng Internet, nhất là khi nó được gửi đi với số lượng lớn. Hàng ngày một địa chỉ email có thể phải nhận rất nhiều email SPAM cho dù có sử dụng một bộ lọc SPAM tốt đi chăng nữa. Tuy nhiên, SPAM nổi tiếng là thế, nhưng cũng có không ít người không biết thực sự SPAM là gì.

SPAM là những email không được sự cho phép của người nhận (Unsolicited email) được gửi đi với số lượng lớn tới hòm thư của người dùng Internet.

SPAM đôi khi còn được xem là những email thương mại không được sự cho phép của người nhận (UCE - Unsocilited Commercial E-Mail).

Tuy nhiên, không phải mọi vụ gửi SPAM đều là nhằm mục đích quảng cáo thương mại. Một số vụ gửi SPAM lại nhằm mục đích bất chính hoặc cũng có những kẻ gửi SPAM chỉ để bày tỏ quan điểm chính trị hoặc tôn giáo. Hình thức gửi SPAM nguy hiểm nhất là hình thức gửi đi những thông điệp để lừa người dùng tiết lộ thông tin tài khoản ngân hàng trực tiếp, số thẻ tín dụng … - hay đây chính là một dang phổ biến của lừa đảo trực tuyến.

Nguồn gốc của SPAM

Một trong số những vấn đề nhức nhối của SPAM đồng thời cũng là nguyên nhân lý giải tại sao lại có SPAM là "để tạo ra SPAM hay trở thành SPAMMER là một điều qua dễ dàng".

Bất cứ ai cũng có thể trở thành SPAMMER Ví dụ, bạn có một món hàng độc đáo cần bán ngay. Nhưng để mọi người biết đến món hàng đó thì bạn phải làm thế nào. Bạn quyết định trước hết phải thông báo cho bạn bè biết bằng cách gửi email cho 100 người nằm trong sổ địa chỉ của bạn. "Wow!" bạn nghĩ "thế là mình không mất một đồng nào mà vẫn có thể gửi đi 100 email quảng cáo sản phẩm của mình. Nếu có người biết để mua hàng mình sẽ lời to. Tại sao mình không gửi email cho nhiều nhiều người khác nữa? Mình sẽ có thể thu được nhiều lợi nhuận hơn?" Rồi bạn sẽ tìm tòi ứng dụng các giải pháp để gửi đi được nhiều email cho cả những người bạn không quen biết hơn. Vậy là bạn đã trở thành SPAMMER.

> SPAM là một tai hoạ đối với thư điện tử và nhóm thảo luận (newsgroup) trên Internet. SPAM có thể gây trở ngại đến sự hoạt động của các dịch vụ công cộng. Đấy là chúng ta còn chưa nói đến tác động của nó đối với hệ thống email. Những kẻ chuyên gửi SPAM lấy đi những nguồn tài nguyên của người dùng và nhà cung cấp dịch vụ mà không phải đền bù bất cứ cái gì."
>
> ***(Vint Cerf – Cha đẻ của Internet)***

Đó mới chính là vấn đề thực sự của SPAM. Nó quá dễ để ai cũng có thể gửi đi trong khi chi phí bỏ ra chẳng đáng là bao, có khi là chả mất đồng nào. Và cho dù tỉ lệ bán hàng quảng cáo không cao, nhưng SPAM vẫn có một sức hút đặc biệt với giới tiếp thị.

Gửi SPAM như thế nào?

Để gửi SPAM, SPAMMER thường phải đi qua 2 bước cơ bản: Thu thập địa chỉ email và Gửi SPAM.

1. Thu thập địa chỉ email

Những kẻ chuyên gửi SPAM – hay còn gọi SPAMMER – có rất nhiều cách để thu thập địa chỉ email. Phổ biến nhất là những cách sau đây:

Cách thứ nhất là thông qua nhóm thảo luận (newsgroups) hoặc phòng chat (chat rooms) trên Internet, đặc biệt là các trang web cổng thông tin điện tử như AOL hay

Yahoo. Với những dịch vụ như thế người dùng thường vẫn sử dụng địa chỉ email thực để đăng ký tài khoản. SPAMMER chỉ cần dùng một phần mềm đặc biệt là đã có thể lấy được địa chỉ email của rất nhiều người.

Cách thứ hai là khai thác trực tiếp từ Web. Hiện đã có tới hàng triệu trang web trên Internet và SPAMMER chỉ cần sử dụng các phần mềm tìm kiếm có khả năng lần tìm ký tự @ trong các trang web – như bạn biết, đây là ký tự đại diện cho địa chỉ email. Kết quả là SPAMMER cũng dễ dàng có được vô vàn các địa chỉ email trong tay. Những phần mềm như vậy thường được gọi là các SPAMBOT.

Một cách khác là SPAMMER tạo ra các trang web đặc biệt chuyên dùng để thu thập địa chỉ email. Ví dụ, SPAMMER có thể tạo ra một trang web với tựa đề "Win $1 million!!! Just type your e-mail address here!" (Bạn đã trúng giải thưởng 1 tỉ USD!!! Hãy để lại địa chỉ email của bạn!). Đã có không ít người trở thành nạn nhân của trò lừa đảo này. Hậu quả là hòm thư của họ đã bị chất đầy thư rác.

Chuyện thư rác đầy ắp hòm thư email không chỉ còn là chuyện xứ người, mà đã phổ biến cả ở Việt Nam.

Hay có những trang web tạo ra danh sách lựa chọn email "*Would you like to receive e-mail newsletters from our partners*?" (Bạn có muốn nhận tin thư từ đối tác của chúng tôi không?) Nếu bạn trả lời "Yes" thì ngay lập tức địa chỉ email của bạn sẽ được bán cho SPAMMER.

Hoặc SPAMMER có thể thành lập một trang web cho đăng ký thành viên sử dụng, mà yêu cầu cung cấp địa chỉ email xác thực là yêu cầu cốt lõi của việc đăng ký. Trên thực tế đó chỉ là một cách để thu thập địa chỉ email. Trước đây, đã từng có rất nhiều các trang web lớn rao bán địa chỉ email của các thành viên.

Có lẽ cách thức phổ biến nhất chính là cách thức được gọi là "*dictionary attack*". Đây là phương thức liên quan đến việc lập trình cho một chiếc máy tính có thể tạo

ra rất nhiều biến thể từ một địa chỉ email bằng cách thay đổi các ký tự - ví dụ *mike1@yahoo.com, mike2@yahoo.com, mike3@yahoo.com…*

Có một mô tả "*dictionary attack*" như sau: "*Dictionary attack sử dụng một phần mềm để tạo một kết nối đến một máy chủ thư điện tử để gửi lên hàng triệu địa chỉ email bất kỳ. Rất nhiều trong số những các địa chỉ đó chỉ là những biến thể của một địa chỉ email – ví dụ jdoe1abc@hotmail.com và jdoe2def@hotmail.com. Phần mềm đó sẽ kiểm tra xem địa chỉ email nào "còn sống", địa chỉ đó sẽ "lọt vào mắt xanh" của SPAMMER".*

Các thức cuối cùng và cũng là cách dễ nhất chính là việc mua một chiếc đĩa CD có chứa hàng trăm hàng nghìn các địa chỉ email từ các SPAMMER khác.

Và rồi một khi SPAMMER có được một số lượng địa chỉ email tương đối, chúng sẽ trao đổi với các SPAMMER khác và sẽ có được nhiều đại chỉ email hơn. Chúng bắt đầu gửi SPAM.

Gửi SPAM

SPAMMER cũng có rất nhiều cách khác nhau để có thể gửi đi hàng nghìn hàng triệu các bức thư rác – hợp pháp có mà bất hợp pháp cũng có.

Các thứ nhất là SPAMMER phải bỏ tiền đầu tư trang bị cho mình rất nhiều hệ thống máy tính, modem và kết nối mạng Internet để gửi SPAM. Đây là một cách thức hoàn toàn hợp pháp nhưng có chi phí cao. Tuy nhiên, kết quả đem lại sẽ có thể là hàng chục nghìn đô la tiền lợi nhuận thu về.

Cách thứ hai rẻ hơn nhiều nhưng lại bất hợp pháp và cũng là cách thức nguy hiểm nhất đối với người dùng. Đó là cách gửi SPAM thông qua những máy chủ uỷ nhiệm mở (open proxy servers). Nói đến phương thức gửi SPAM này thì cũng là nói đến cách thức SPAMMER bí mật đột nhập bắt cóc hệ thống máy tính của người khác để xây dựng một cái được gọi là botnet.

Trước hết SPAMMER sẽ sử dụng công nghệ và các thủ đoạn cần thiết để bí mật cài đặt một phần mềm lên hệ thống của người dùng. Đó là phần mềm cho phép SPAMMER có thể kiểm soát được hệ thống máy tính của nạn nhân từ xa - hay nói

Zombie PC

một cách khác là SPAMMER đã bắt cóc được chiếc máy tính đó. Chiếc máy tính đó đã trở thành một thứ được gọi là “Zombie” (thây ma). Khi có nhiều Zombie, SPAMMER sẽ tiến hành xây dựng một hệ thống mạng các

Zombie – hay đây chính là hệ thống mạng botnet. Đến đây cách thức thứ hai đã giống với cách thức thứ nhất, chỉ khác một điều là SPAMMER không phải có tiền ra mua các hệ thống máy tính mà chúng đi "bắt cóc" máy tính của người khác.

Cách thức gửi SPAM thứ hai cũng nói lên một điều là tại sao SPAMMER ngày nay lại trở thành một mối đe doạ đối với mọi người dùng Internet và tại sao SPAM cũng được xem là độc hại không kém gì các phần mềm độc hại khác như virus, sâu máy tính hay trojan.

Bạn nên biết để có thể đột nhập thành công và bắt cóc hệ thống máy tính của người dùng thì SPAMMER phải sử dụng các kỹ thuật tấn công khai thác lỗi bảo mật không khác gì hacker hay các kiểu cách lừa đảo không thu kém gì các phisher. Phần mềm giúp SPAMMER tấn công và bắt cóc máy tính của người dùng từ xa cũng chính là các loại phần mềm độc hại virus, sâu máy tính hoặc trojan. Nói một cách khác giờ đây dường như không còn danh giới giữa hacker và SPAMMER nữa, SPAM trở thành công cụ phát tán virus, sâu máy tính, trojan và ngược lại chính những phần mềm độc hại đó là công cụ để gửi SPAM.

Bạn tưởng tượng xem nhé với một lượng SPAM vô cùng lớn gửi đi trên toàn thế giới mỗi ngày thì nếu hệ thống máy tính của bạn trở thành một Zombie thì sao? PC của bạn sẽ liên tục phải gửi đi các email SPAM, đường truyền Internet và PC của bạn sẽ chậm đi rất nhiều vì mọi tài nguyên đều đã được SPAMMER khai thác sử dụng. Mặt khác đôi khi bạn còn có thể trở thành nạn nhân của các cơ quan bảo vệ pháp luật. Vì họ có thể dễ dàng phát hiện ra PC của bạn đã sử dụng trong các vụ tấn công gửi SPAM bất hợp pháp nhưng để phát hiện được SPAMMER thì lại là vấn đề rất khó. Bạn trở thành nạn nhân bất đắc dĩ.

Bạn hay xem một SPAM KING – ông vua trong việc gửi SPAM – nói gì nhé: "*Tôi chiếm quyền điều khiển tổng cộng 190 máy chủ email – 110 chiếc ở Southfield, 50 chiếc ở Dallas và 30 chiếc khác ở Canada, Trung Quốc, Nga và Ấn Độ. Mỗi chiếc máy tính đó có thể gửi đi 650.000 email mỗi giờ, tương đương với khoảng hơn 1 tỉ email một ngày*."

Ngoài ra còn có những công ty được thành lập để chuyên nhận các hợp đồng nhận gửi SPAM với giá rẻ. Nhưng công ty này tuyên bố họ hoàn toàn không phải là SPAMMER vì những khách hàng của họ chấp nhận nhận những email do họ gửi đi. Những địa chỉ email như thế này thường được thu thập bằng cách thức thu thập địa chỉ email thứ 3 như đã nói ở trên.

Chống lại SPAM

Cảnh báo thư rác bằng công cụ Spam Alarm.

Công nghệ tốt nhất để chống lại SPAM hiện tại là sử dụng các phần mềm lọc SPAM. Bạn có thể tìm được rất nhiều phần mềm lọc SPAM trên Internet, tốt nhất là bạn nên vào trang web như pcworld.com hoặc download.com để tải về những phần mềm này.

Tuy nhiên, như bạn biết SPAMMER đôi khi còn quyền điều khiển hệ thống của bạn để gửi đi SPAM, chính vì thế mà phần mềm lọc SPAM chưa phải là tất cả. Bạn còn cần phải thường xuyên cài đặt các bản cập nhật bảo mật cho hệ điều hành để vá các lỗi bảo mật tránh bị SPAMMER khai thác tấn công, bạn còn cần thêm một phần mềm tìm diệt các phần mềm độc hại, và tốt nhất bạn nên cần thêm một phần mềm tường lửa cá nhân.

Nhưng cho dù công cụ nào đi chăng nữa cũng không thể bằng con người. SPAM đã được xem là vấn đề xã hội liên quan đến con người, vậy chỉ có con người mới có thể chống lại được nó. Bạn hãy thật sự cẩn thận khi sử dụng Internet và trang bị cho mình những kiến thức cần thiết về bảo mật và sử dụng Internet an toàn. Có như thế bạn mới tránh được SPAM và những hiểm hoạ khác trên Internet.

Trang Dung

Theo VietNamNet

Giải mã Windows XP

Chỉ cần thực hiện vài tinh chỉnh đơn giản với Registry của Windows XP, bạn có thể tùy biến để hệ điều hành phù hợp hơn với nhu cầu sử dụng. Và nếu ?ang có ý định nâng cấp lên Windows Vista, đừng quên "ghé mắt" qua phần giới thiệu về chàng "tân binh" mới của Microsoft.

PHƯƠNG THUỐC REGISTRY

Có nhiều cách làm cho Windows hoạt động nhanh hơn, thông minh hơn và an toàn hơn. Tất cả những gì bạn cần làm là đương đầu với hàng loạt thông số cấu hình trong Registry.

Hình 1: Đóng nhanh các ứng dụng bị treo bằng cách nhập vào một giá trị thời gian thấp hơn.

Việc chỉnh sửa các thông số Registry đòi hỏi phải được thực hiện hết sức cẩn trọng vì chỉ một sơ suất nhỏ cũng có thể khiến Windows hành xử bất thường, thậm chí không thể đăng nhập được. Do vậy, trước khi tiến hành bất kỳ một chỉnh sửa nào, hãy sao lưu lại cấu hình Registry hiện tại theo các hướng dẫn được trình bày trong bài biết "Chăm sóc và bảo dưỡng Windows Registry" (ID: A0205_90).

Ngoài ra, còn một cách khác nhanh hơn: nhấn Start.Run, gõ vào lệnh regedit và ấn để mở tiện ích Registry Editor. Tiếp đến, chọn mục My Computer trong khung cây thư mục ở cửa sổ bên trái và chọn trình đơn File.Export, đặt tên và chọn vị trí cần lưu tập tin này (có thể là đĩa CD-RW hay thiết bị lưu trữ di động như USB).

Nếu chẳng may xảy ra sự cố, bạn hãy tham khảo bài viết "Làm thế nào để phục hồi Windows Registry" (ID: A0304_106) để biết cách khắc phục. Cũng trong bài viết này, bạn sẽ được hướng dẫn cách sử dụng các công cụ chỉnh sửa, quản lý Registry của một hãng thứ 3.

TĂNG TỐC TRÌNH ĐƠN

Hình 2: Phân chia rõ ràng hình nền và các biểu tượng.

Chỉ cần thực hiện một chỉnh sửa Registry hết sức đơn giản, bạn có thể làm cho thanh trình đơn Start (hay các trình đơn con bên trong) trở nên "linh hoạt" hơn. Hãy mở cửa sổ Registry Editor, tìm và chọn mục HKEY_CURRENT_USER\Control Panel\Desktop (hay HKEY_CURRENT_USER\Control Panel\desktop). Trong khung cửa sổ bên phải, nhấn đúp chuột vào biểu tượng MenuShowDelay và đổi giá trị tại mục "Value data" từ giá trị mặc định là 400 (miligiây) sang một con số khác nhanh hơn, ví dụ 0 chẳng hạn. Tương tự, bạn có thể làm chậm tốc độ xuất hiện của các trình đơn này đến 4.000 miligiây (4 giây) nếu muốn. Sau khi hoàn tất, ấn để kết thúc.

ĐÓNG NHANH ỨNG DỤNG

Đang cố thoát khỏi một ứng dụng (hay trong vài trường hợp chính là Windows) nhưng bạn buộc lòng phải chờ đợi một hay nhiều ứng dụng khác kết thúc trước. Sau một thời gian chờ đợi, Windows lại tiếp tục mời bạn "ngồi chơi xơi nước" và sau đó hiển thị hộp thoại End Program cho phép bạn ép buộc một (hay nhiều) ứng dụng nào đó phải kết thúc.

Sự nhẫn nại là điều cần thiết, nhưng nếu Windows mất quá nhiều thời gian để đóng những ứng dụng "cứng đầu" trên thì bạn có thể yêu cầu Windows hiển thị hộp thoại End Program sớm hơn so với bình thường. Thực tế, bạn có thể thiết lập để Windows đóng nhanh các ứng dụng đang bị "treo" mà không cần thao tác qua hộp thoại End Program. Tuy nhiên, nên nhớ nếu sử dụng tùy chọn này (không được Windows nhắc nhở), bạn có thể làm hỏng những cài đặt hệ thống do chấm dứt quá nhanh các tiến trình Windows đang được thực thi. Có một biện pháp để giải quyết vấn đề này là tiếp tục sử dụng tùy chọn nhắc nhở và thiết lập thời gian time-out ngắn hơn.

Để Windows tự động đóng các process bị treo, mở tiện ích Registry Editor và chọn mục HKEY_CURRENT_USER\Control Panel\Desktop. Sau đó, nhấn đúp chuột vào biểu tượng AutoEndTasks ở khung cửa sổ bên phải, đổi giá trị ở mục "Value data" sang 1 và ấn . (đổi giá trị này lại 0 nếu muốn quay lại cách thức đóng các ứng dụng đang thực thi một cách thủ công).

Kế đến, nhấn đúp chuột vào biểu tượng HungAppTimeout cũng ở khung cửa sổ bên phải này, chỉnh lại giá trị tại mục "Value data" để thiết lập thời gian (tính bằng đơn vị miligiây, Hình 1). Giá trị mặc định là 5.000 miligiây (5 giây). Để thiết lập thời gian chờ một ứng dụng đóng lại khi Windows kết thúc, bạn nhấn đúp chuột vào biểu tượng WaitToKillAppTimeOut cũng ở khung cửa sổ trên, sau đó thay đổi giá trị mặc định 20.000 miligiây (20 giây) sang con số mà bạn muốn và sau cùng ấn để kết thúc.

Tuy nhiên, ứng dụng không phải là nguyên nhân duy nhất khiến bạn phải chờ đợi trong quá trình Windows kết thúc. Nhiều tiến trình đang thực thi của hệ điều hành (hay còn được gọi là dịch vụ – service) cũng có thời gian kết thúc riêng. Để chỉ định thời gian chờ tối đa trước khi Windows đóng (hay nhắc nhở bạn) các dịch vụ vào thời điểm tắt máy, mở tiện ích Registry Editor, chọn mục HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control. Nhấn đúp chuột vào biểu tượng WaitToKillServiceTimeOut ở khung cửa sổ bên phải và đổi giá trị ở mục "Value data" (mặc định là 2.000 miligiây) sang một con số thấp hơn, sau đó ấn để kết thúc. Lưu ý, trong vài trường hợp, những giá trị mới có thể không

có tác dụng do một số dịch vụ sẽ tự động tăng giá trị này lên để có đủ thời gian hoàn thành công việc.

ĐỔI KÍCH THƯỚC HÌNH NỀN

Nếu bạn vừa chuyển sang sử dụng một màn hình khổ lớn (wide-screen) thì hình nền (wallpaper) cũ sẽ không còn vừa vặn nữa, hay có lẽ bạn chỉ muốn thực hiện một chỉnh sửa nhỏ trên hình nền hiện có của mình. Để điều chỉnh kích thước hình nền, chọn mục HKEY_CURRENT_USER\Control Panel\Desktop trong tiện ích Registry Editor và nhấn đúp chuột vào biểu tượng WallpaperOriginX ở khung cửa sổ bên phải. Nếu không thấy biểu tượng này, nhấn phải chuột lên khung cửa sổ bên phải và chọn New.String Value, nhập vào tên WallpaperOriginX và ấn . Sau đó, nhập vào một giá trị (đơn vị tính là pixel) cho vị trí bắt đầu ở hàng ngang (tính từ cạnh trái hình nền) và ấn . Tiếp đến, nhấn đúp chuột vào biểu tượng WallpaperOriginY (nếu chưa có thì thực hiện các bước tạo mới như trên) và nhập vào một giá trị cho vị trí bắt đầu hàng dọc (tính từ cạnh trên hình nền). Nếu như hình nền lớn hơn kích thước màn hình, bạn hãy nhập vào một số có giá trị âm (ví dụ -200 chẳng hạn) để đẩy cạnh trên hay cạnh trái hình nền vào trong.

Để kiểm tra hiệu ứng này, trước hết là bạn hãy thu nhỏ tối đa (minimize) cửa sổ Registry Editor (hay bất kỳ cửa sổ nào đang mở), nhấn phải chuột lên màn hình nền Windows và chọn Properties, sau đó nhấn OK hay Apply để kích hoạt những thông số vừa thay đổi. Lặp lại những bước trên cho đến khi hình nền được hiển thị chính xác trên màn hình (Hình 2). Những cài đặt này cũng có tác dụng với những chế độ hiển thị hình nền có trong Windows.

TÌM KIẾM MỌI TẬP TIN

Khi bạn tiến hành tìm kiếm một tập tin trong Windows (chọn Start.Search.For Files or Folders, hay ấn phím trong bất kỳ cửa sổ thư mục nào), Windows đều chỉ tìm kiếm những dạng tập tin mà hệ điều hành này có thể nhận dạng được. Những dạng tập tin không được liệt kê trong danh sách "Registered file types" sẽ bị bỏ qua trong quá trình tìm kiếm (để xem danh sách này, bạn mở Explorer, chọn Tools.Folder Options và nhấn vào thẻ File Types). Ví dụ, những tập tin với phần mở rộng khá lạ như .xyz chẳng hạn sẽ không được Windows để mắt đến trong quá

trình tìm kiếm dù chúng thực sự tồn tại trên máy tính của bạn. May mắn, một chỉnh sửa đơn giản với Registry có thể giúp bạn hóa giải tình trạng này, giúp Windows nhận biết được tất cả mọi tập tin bất kể chúng có phần mở rộng như thế nào. Trong tiện ích Registry Editor, tìm và chọn mục HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlPanelSet\Control\ContentI

ndex. Sau đó, nhấn đúp chuột vào biểu tượng FilterFilesWithUnknownExtensions ở khung cửa sổ bên phải và đổi giá trị ở mục "Valua data" từ 0 sang 1, cuối cùng là ấn .

Thủ thuật: Để đảm bảo Windows XP tìm kiếm tất cả định dạng tập tin, chọn All Files and Folder trong danh sách thả xuống Type of files ở khung cửa sổ Search Companion (nếu không thấy tùy chọn này, nhấn More Advanced Options). Tiếp đến, đánh dấu chọn các mục Search system folders, Search hidden files and folders và Search subfolders. Trong Windows 2000, nhấn Search Options, đánh dấu mục Type, và đảm bảo mục All Files and Folders được chọn ở trình đơn thả xuống. Tiếp đến, đánh dấu mục Advanced Options và đảm bảo Search Subfolder được chọn. Cuối cùng, để đảm bảo Windows 2000 có thể tìm kiếm tất cả tập tin hệ thống và tập tin ẩn, chọn Tools.Folder Options và nhấn vào thẻ View. Trong danh sách Advance settings, chọn Show hidden files and folders, bỏ tùy chọn Hide protected operating system files (Recommended), sau đó nhấn Yes để chấp nhận cảnh báo và cuối cùng nhấn OK để kết thúc.

LỘ DIỆN TÀI KHOẢN QUẢN TRỊ

Thông thường, chỉ có vài người dùng được trang bị những kiến thức rõ ràng và đầy đủ về tài khoản quản trị của Windows XP (tên đầy đủ là "Administrator"). Tài khoản này sẽ không được hiển thị trừ khi máy tính của bạn không có bất kỳ một tài khoản nào khác hay khởi động ở chế độ Safe Mode. Để loại bỏ sự ngụy trang của tài khoản quản trị và bổ sung tài khoản này vào màn hình Welcome khi khởi động Windows XP, bạn chọn mục HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList trong tiện ích Registry Editor và nhấn đúp chuột vào biểu tượng Administrator trong khung cửa sổ bên phải. (Nếu không thấy biểu tượng này, nhấn phải chuột lên khung cửa sổ bên trái, chọn New.DWORD Value, đặt tên là Administrator và ấn). Sau đó, nhập vào mục "Value data" giá trị là 1 và ấn . Từ lúc này trở đi, khi bạn mở của sổ User Accounts trong Control Panel (chọn Start.Run, gõ vào lệnh Control userpasswords và ấn), bạn sẽ thấy xuất hiện tài khoản Administrator. Bạn có thể dễ dàng đổi hình tượng trưng hay mật khẩu cho tài khoản này. Ngoài ra, ở những lần đăng nhập sau, bạn sẽ thấy màn hình Welcome của Windows XP xuất hiện thêm lựa chọn tài khoản Admistrator bên cạnh các tài khoản người dùng khác (Hình 3).

GIÁM SÁT THAY ĐỔI REGISTRY

Nếu bạn muốn biết Windows Registry đã có những thay đổi gì thì tiện ích Regmon chính là công cụ bạn cần (tải về tại www.pcworld.com.vn, ID: 51394). Cửa sổ chính của công cụ này sẽ nhận dạng tất cả những khóa Registry có sự thay đổi, thời điểm và tiến trình (hay phần mềm) nào thay đổi khóa này. Tuy nhiên, chỉ có những người dùng chuyên nghiệp mới có thể hiểu được những thông tin mà Regmon cung cấp, nhưng người dùng có thể sử dụng bộ lọc để giới hạn các báo cáo (chỉ hiển thị những thông tin cần thiết hay có thể hiểu được). Ví dụ, để giám sát những thay đổi do ứng dụng khởi động cùng Windows, bạn chọn Options.Filter/Highlight. Trong phần Include, nhập vào nội dung HKEY_Current_User\Software\Microsoft\Windows\CurrentVersion\Run; HKEY_Local_Machine\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run. Hay trong phần Exclude, bạn có thể nhập vào đường dẫn đến các khóa mà muốn Regmon bỏ qua (ví dụ HKEY_Current_User\Software\Microsoft\MediaPlayer).

TÌM NHANH REGISTRY

Nếu thường xuyên chỉnh sửa Registry trong Windows 2000 hay Windows XP, bạn có thể lưu lại quá trình tìm kiếm đầy khó khăn những thông số thường dùng bằng cách bổ sung chúng vào trình đơn Favorites của tiện ích Registry Editor. Để thực hiện, nhấn chuột lên khóa Registry cần lưu và chọn Favorites.Add to Favorites, sau đó đặt tên và cuối cùng nhấn OK. Ở những lần chỉnh sửa Registry sau, để di chuyển nhanh đến khóa Registry này, bạn chỉ cần đơn giản mở tiện ích Registry Editor và chọn mục cần thiết từ trình đơn Favorites.

Hình 3: Tài khoản Administrator sẽ xuất hiện ở màn hình Welcome của Windows XP.

Nếu bạn thường xuyên chuyển đổi giữa 2 cài đặt cho cùng một khóa Registry, bạn có thể tiết kiệm được nhiều thời gian bằng cách lưu mỗi phiên bản (giá trị khá nhau) của một khóa thành một tập tin Registry khác và tạo một shortcut để tải cài đặt này vào Registry.

Trước hết, tìm đến khóa Registry mà bạn cần thực hiện chuyển đổi. Sau đó chọn File.Export, đảm bảo tùy chọn Selected Brache được đánh dấu, đặt tên và chọn vị trí cần lưu tập tin này và nhấn nút Save. Kế đến, nhấn phải chuột lên tập tin .reg vừa tạo, chọn Edit để mở tập tin này bằng Notepad. Bạn đừng thay dổi bất kỳ nội dung gì ở dòng văn bản thứ 1, dòng trống sau đó cũng như dòng thứ 3 (có các tựa đề được đặt trong dấu ngoặc đơn) mà hãy tìm dòng văn bản chứa thông tin liên

quan đến khóa Registry mà bạn cần thay đổi. Hãy giữ nguyên dòng này và xóa tất cả các dòng còn lại bên dưới tiêu đề đặt trong dấu ngoặc đơn để tập tin này không thay đổi những cài đặt khác. Sau đó, chọn File.Save. Cũng với tập tin này, bạn hãy thay đổi giá trị của khóa Registry vừa tìm được (ví dụ từ "1" thành 0, hay từ "no" thành yes) và nhấn File.Save as, đặt một tên tập tin mới (nhớ bổ sung phần mở rộng .reg vào cuối tên tập tin).

Hình 4: Dễ dàng tạo một shortcut để chuyển đổi giữa 2 cài đặt Registry.

Tiếp đến, bạn phải tạo một lệnh tắt (shortcut) để chèn những cài đặt này vào Registry. Nhấn phải chuột lên màn hình Windows hay trong một thư mục và chọn New.Shortcut. Trong hộp thoại văn bản vừa xuất hiện, nhập vào lệnh regedit /s và đi ngay sau đó một khoảng trắng là đường dẫn đến tập tin .reg vừa tạo (ví dụ regedit /s testregistry "C:\My Documents\reg1.doc", Hình 4). Sau đó, nhấn Next, đặt tên cho shortcut này và chọn Finish. Lặp lại các bước trên cho tập tin .reg thứ hai.

Từ đây trở đi, bất cứ khi nào cần chuyển đổi giá trị của một khóa Registry, tất cả những gì bạn cần làm là kích hoạt shortcut vừa tạo ở trên. Để khôi phục lại trạng thái cũ, hãy kích hoạt shortcut thứ 2. Bạn có thể đặt những shortcut này vào trình đơn Start hay thanh QuickLaunch hay các thanh công cụ khác. Ngoài ra, để tạo phím tắt cho mỗi tập tin, nhấn phải chuột lên biểu tượng shortcut đó và chọn Properties, gõ vào tổ hợp phím tắt theo ý riêng của bạn vào mục "Shortcut key" ở nhãn Shortcut, cuối cùng nhấn OK.

ĐỔI TIÊU ĐỀ TRÌNH DUYỆT

Mặc định, thanh tiêu đề của trình duyệt Internet Explorer sẽ hiển thị tên website mà bạn đang truy cập và theo sau đó là câu "Microsoft Internet Explorer", trong vài trường hợp có thể là tên công ty hay tên nhà cung cấp dịch vụ ISP. Để thay đổi dòng thông tin quen thuộc này, tìm đến mục HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main trong tiện ích Registry Editor và nhấn đúp chuột vào biểu tượng Windows Title ở khung cửa sổ bên phải. (Nếu không thấy khóa này, nhấn phải chuột lên cửa sổ bên trái và chọn New.String Value, đặt tên Windows Title, sau cùng là ấn). Tiếp đến, nhập vào nội dung mà bạn muốn được xuất hiện trên thanh tiêu đề của trình duyệt (hay không nhập gì nếu chỉ muốn tên website được hiển thị). Khi nạp lại Internet Explorer, bạn sẽ thấy sự thay đổi (Hình 5).

SAO LƯU REGISTRY

Việc sao lưu Registry sẽ giúp bạn an toàn hơn trong quá trình thay đổi những thông số cài đặt đầy rắc rối hay khi cài đặt và sử dụng các phần mềm khác. Tiện ích miễn phí ERUNT (Emergency Recovery Utility NT) cho phép dễ dàng sao lưu các thông số Registry trong Windows 2000 và Windows XP, bạn chỉ cần xác định nơi cần đặt dữ liệu sao lưu. Bạn có thể thiết lập để tiện ích tạo bản sao lưu mỗi khi khởi động Windows. Mỗi thư mục sao lưu đều đi kèm một chương trình khôi phục đơn giản. Ngoài ra, ERUNT còn đi kèm tiện ích NT Registry Optimizer có khả năng cải thiện hiệu quả hoạt động của hệ thống bằng cách loại bỏ các vùng dữ liệu bị phân mảnh xuất hiện trong quá trình cài đặt và gỡ bỏ các ứng dụng. Cả hai tiện ích này có thể tải về từ www.pcworld.com.vn, ID: 51392.

CHIA SẺ REGISTRY

Khả năng gửi những thay đổi Registry cho người dùng khác cho phép bạn thiết lập tất cả máy tính trong mạng có cùng cấu hình mà không cần sử dụng đến các công cụ quản trị nâng cao của Windows. Một biện pháp để thực hiện điều này là trích xuất (export) một hay nhiều tập tin .reg, nếu cần thiết bạn có thể chỉnh sửa chúng bằng tiện ích Notepad. Sau đó, bạn có thể lưu các tập tin .reg này trên máy chủ, hay gửi chúng qua email cho những người dùng cần đến những thông số cài đặt này. Người nhận có thể nhấn đúp chuột các tập tin .reg trên (hay nhấn phải chuột lên từng tập tin và chọn Merge), nhấn Yes khi được yêu cầu.

Hình 5: Thay đổi nội dung thanh tiêu đề của trình duyệt IE.

Khi tiến hành chỉnh sửa Registry theo cách này, bạn phải đảm bảo những cài đặt này không quá "đặc biệt" cho máy tính. Những chỉnh sửa liên quan đến Windows có thể xem là một "ván bài" đầy may rủi để giúp máy tính vận hành "mạnh mẽ" hơn, tuy nhiên những thay đổi khóa Registry cho phần cứng và ứng dụng xác định chỉ có tác dụng trên những máy tính có cấu hình tương tự. Cuối cùng, hãy luôn chắc chắn là đã tiến hành sao lưu Registry của hệ thống trước khi bạn thay đổi bất kỳ thông số Registry nào.

ĐÓN CHÀO VISTA

Giao diện mới chỉ là phần mở đầu, còn sự cải tiến về bảo mật và hiệu quả hoạt

động chính là những điểm nổi bật được dự đoán sẽ có mặt trong phiên bản Windows tiếp theo. Theo đó, Vista sẽ trở thành phiên bản Windows nhanh nhất, an toàn nhất và đáng tin cậy nhất trong thập kỷ này. Hầu hết mọi thành phần dự kiến có mặt ở phiên bản cuối đã xuất hiện trong phiên bản Beta 2 được giới thiệu vào tháng 12 vừa qua (dù chưa thật hoàn hảo). Bạn có thể tham khảo lại bài viết "Windows Vista bóng bẩy và an toàn hơn" (ID: A0510_12).

Bảo mật là lý do chính thúc đẩy hầu hết người dùng Windows sẽ tiến hành nâng cấp hệ điều hành ngay khi có cơ hội. Vista tăng cường khả năng chống đỡ của Windows trước các mối đe dọa trực tuyến mà đa phần có khả năng đánh sập Windows XP. Vista sắp xếp hợp lý hơn quá trình khởi động và tắt máy, khai thác sự dồi dào của bộ nhớ RAM trên các máy tính đời mới để tăng tốc độ thực thi các ứng dụng thông qua tiện ích quản lý bộ nhớ Superfetch mới. Hệ điều hành cũng hứa hẹn cung cấp nhiều tính năng hơn, bao gồm khả năng nhận dạng giọng nói. Giao diện Aero sử dụng các tính năng làm mờ (transparency), tạo bóng (shading) và tô màu (color) để cung cấp cho người sử dụng nhiều thông tin hơn cũng như khả năng kiểm soát đến từng biểu tượng, cửa sổ và hộp thoại.

WINDOWS AN TOÀN HƠN

Hình 1: Chỉ cần nhập vào mật khẩu của một tài khoản quản trị, người dùng thông thường sẽ có khả năng thực hiện các tác vụ đòi hỏi quyền hạn cao.

Về cơ bản, Vista an toàn hơn người tiền nhiệm Windows XP. Nếu bạn cài đặt phiên bản đầu của Windows XP trên một máy tính có kết nối Intermet, sâu Blaster có thể khai thác lỗ hổng trên hệ điều hành này để tắt (shutdown) hệ thống của bạn trong tích tắc. Microsoft đã quan tâm nhiều đến vấn đề bảo mật hơn trong phiên bản XP Service Pack 1 và 2, mặc định kích hoạt tính năng tường lửa Windows Firewall và tự động cập nhật.

Vista kiên cường hơn trước các cuộc tấn công từ Internet bằng cách trang bị những công cụ chống spyware và nâng cấp khả năng bảo mật mặc định của trình duyệt Internet Explorer. Mục Spyware Protection trong tiện ích Windows Security Center tiến hành lập các báo cáo bất kể tính năng Windows Defender và tiện ích phòng chống spyware của Vista (trước đây gọi là Microsoft AntiSpyware) đang thực thi. Mục General Security mới có nhiệm vụ theo dõi có hay không sự thay đổi cài đặt bảo mật trong IE được giảm xuống mức không an toàn, hay mở "cửa hậu" để tin tặc tấn công hệ thống. Phiên bản trình duyệt IE trong Vista sẽ không cho phép bạn xem một trang

web cho đến khi bạn tăng mức độ bảo mật ở mục Internet Zone đến mức "Medium-High" – tương tự mức "High" trong Windows XP SP2.

Tuy nhiên Vista vẫn bỏ sót một lỗ hổng bảo mật, chí ít là đối với người dùng thông thường. Windows cần có tường lửa có khả năng khóa những luồng dữ liệu không được phép để ngăn chặn virus, spyware, sâu máy tính hay các phần mềm độc hại khác. Giống với Windows XP, tính năng tường lửa ở Vista thực hiện xuất sắc nhiệm vụ ngăn chặn sâu Blaster và những tấn công khác từ bên ngoài. Khi bạn cài đặt một ứng dụng được phép sử dụng các kết nối từ bên ngoài (như trình duyệt hay tiện ích gửi nhận tin nhắn IM), firewall sẽ hỏi bạn cho phép hay ngăn chặn thực hiện kết nối này. Nhưng bạn đừng phạm sai lầm với những yêu cầu cho phép thực hiện kết nối đi ra ngoài.

Hình 2: Máy tính sử dụng Windows Vista có khả năng kiểm soát khởi động và mã hóa đĩa cứng.

Tính năng tường lửa ở Vista có thể kiểm soát việc những chương trình cá nhân bắt đầu thực hiện các kết nối ra ngoài nhưng tính năng này không dành cho người dùng bình thường. (Microsoft cho rằng chỉ có bộ phận IT mới có lý do để sử dụng cài đặt này). Ngoài ra, với mục Local Security Policy Settings trong cửa sổ tiện ích Administrator Tools, người dùng có thể thiết lập khả năng ngăn chặn các kết nối ra ngoài và tạo sự chấp thuận cho các tiện ích cá nhân. Tuy nhiên, những cài đặt này lại quá "khó hiểu" đối với hầu hết người dùng. Nếu tính năng tường lửa vẫn giữ hiện trạng này trong phiên bản Windows Vista chính thức sắp được ra mắt, thì có lẽ người dùng nên trang bị phần mềm tường lửa của một hãng thứ 3 như ZoneAlarm (miễn phí) của ZoneLabs chẳng hạn.

HẠN CHẾ QUYỀN NGƯỜI DÙNG

KHỞI ĐẦU TỪ NÚT START

Trình đơn Start mới trong Vista thay thế trình đơn tìm kiếm bằng một hộp thoại tìm kiếm một chạm. Hệ điều hành cũng cung cấp tùy chọn Lock mới, sẽ kích hoạt chương trình bảo vệ màn hình có sử dụng mật khẩu. Nút Power Off ở góc phải bên dưới màn hình kết hợp chế độ ngủ đông trong Windows XP với chế độ chờ an toàn.

Bạn cũng có thể giảm được sự đe dọa từ những phần mềm nguy hiểm bằng cách giới hạn khả năng truy xuất đến các thông số cài đặt hệ thống và thiết bị phần cứng. Hiện tại, Linux, Mac OS, Unix và các hệ điều hành tương tự đều hạn chế sử dụng tài khoản với quyền hạn cao (hay chính xác là tài khoản quản trị) để thực hiện công việc hàng ngày. Bằng cách này, khi một chương trình nào "ngã ngựa" thì sự phá hoại do việc này gây ra sẽ ở mức thấp nhất. Khi có tác vụ đòi hỏi quyền quản trị với một cửa sổ pop-up, bạn chỉ đơn giản nhập vào mật khẩu để thực thi tác vụ đó.

Windows cũng cung cấp vài tài khoản cấp thấp hơn nhưng chúng khó sử dụng, đặc biệt khi cần thực hiện các tác vụ đòi hỏi quyền quản trị (ví dụ như cài đặt phần mềm hay thay đổi các thiết lập bảo mật) thì bạn phải thoát khỏi quyền người dùng hiện tại và đăng nhập lại hệ thống với tài khoản quản trị.

Các tài khoản có quyền giới hạn của Vista dễ dàng thay đổi: tài khoản người dùng thông thường (trong Windows XP gọi là tài khoản Limited) và bất kỳ ứng dụng "lừa đảo" nào được thực thi với quyền của tài khoản này vẫn bị ngăn chặn ở nhiều tác vụ nhạy cảm. Nhưng giờ đây, Windows hiện một hộp thoại cho phép bạn nhập vào mật khẩu của tài khoản quản trị để có thể hoàn thành tác vụ (Hình 1). Không may, trong phiên bản Beta 2, dù đã đăng nhập hệ thống với tài khoản quản trị, một hộp thoại tương tự vẫn xuất hiện và yêu cầu bạn xác nhận trước khi thực hiện mỗi tác vụ đòi hỏi quyền hạn cao.

Chế độ đăng nhập bảo mật và tính năng mã hóa đĩa cứng của Windows XP làm khó khăn hơn việc "ngó trộm" dữ liệu trên máy tính. Tuy nhiên, nếu có đủ thời gian và những công cụ cần thiết thì vẫn có thể giải mã toàn bộ dữ liệu trên máy tính. Tính năng Secure Startup của Vista di dời khóa mã hóa khỏi đĩa cứng và lưu

thông tin này vào chip bảo mật Trusted Platform Module (TPM) trên bo mạch chủ, trên bút nhớ USB hay đơn giản chỉ là ghi trên giấy.

Hình 3: Phụ huynh có thể kiểm soát những gì con trẻ xem, chơi game và thậm chí thiết lập thời điểm có thể sử dụng máy tính.

Bạn vẫn có thể mã hóa các ổ đĩa và thư mục như trong Windows XP Professional, nhưng tính năng Secure Startup sẽ đi theo bạn trong suốt quá trình mã hóa và lưu một khóa giải mã 48 bit vào một tập tin trên máy tính khác, bút nhớ USB hay in ra giấy (Hình 2). Sau đó, không ai có thể khởi động được Windows Vista trên máy tính mà không phải trước tiên là truy xuất qua chip bảo mật TPM (không thể thực hiện điều này khi đĩa cứng được tháo rời khỏi hệ thống), hay gắn bút nhớ USB vào máy tính hay nhập vào khóa 48 bit trực tiếp từ bàn phím. Theo Microsoft, Secure Startup chỉ xuất hiện trong phiên bản Enterprise Edition của hệ điều hành này, giới hạn tính năng cho người dùng công sở.

EXPLORER ĐA NĂNG

Với tiện ích Explorer mới trong Windows Vista, bạn có thể xem nhiều thông tin hơn về các tập tin và thư mục thông qua khung Preview nằm ngang ở phía dưới mỗi cửa sổ thư mục. Bên cạnh kích thước tập tin, ngày tạo tập tin và các thông số khác, bạn còn thấy một danh sách các từ khóa và cấp độ đánh giá mà bạn đã thiết lập. Đối với tập tin nhạc, tên album và thể loại cùng nhiều siêu dữ liệu khác cũng sẽ được hiển thị trong khung cửa sổ này.

AN TOÀN CHO TRẺ NHỎ

Các phiên bản trước đây của trình duyệt Internet Explorer có khả năng kiểm soát và lọc các nội dung không lành mạnh, nhưng Vista mở rộng tính năng này bằng cách cho phép nhà quản trị kiểm soát những gì mà các tài khoản người dùng thông thường (không phải tài khoản quản trị) có thể xem được trên máy tính bất kể đó là trình duyệt, tiện ích gửi nhận tin nhắn IM hay trò chơi.

Hình 4: Vista sử dụng bút nhớ USB để tăng tốc thực thi ứng dụng.

Tính năng kiểm soát website trong Windows Vista có khả năng ngăn chặn các trang web có nội dung liên quan đến rượu, thuốc lá, ma túy, bạo lực... cũng như trong các email và tin nhắn dựa trên nền web. Bạn có thể cấm hoặc cho phép những trò chơi dựa

trên phân loại Entertainment Software Rating Board, kể cả các trò chơi đã được cài trên máy tính (Hình 3). Hơn thế nữa, các bậc phụ huynh (thường không thể thường xuyên theo dõi mục đích sử dụng máy tính của con trẻ) có thể sử dụng tính năng Parental Control, cho phép xác lập những thời điểm mà một tài khoản có thể sử dụng. Vista thậm chí có khả năng giám sát hoạt động của một tài khoản và tạo báo cáo những gì mà tài khoản này đã thực hiện, ví dụ danh sách các website đã truy cập, thời gian sử dụng của từng ứng dụng cụ thể.

Không may, trong phiên bản Beta 2, Vista không thể ngăn cản người dùng xem một số trang web "đen", cũng như không tạo các báo cáo ghi nhận quá trình lướt web và sử dụng máy tính.

KHỞI ĐỘNG VÀ TẮT MÁY NHANH HƠN

Hình 5: Windows Media Player 11 với giao diện rõ ràng và đơn giản.

Máy tính hoạt động ngày một nhanh hơn nhưng dường như việc khởi động và tắt Windows ngày càng kéo dài hơn. Vista sẽ tăng tốc quá trình khởi động hệ thống chỉ khi hệ thống của bạn có phần cứng hỗ trợ giao tiếp Extensible Firmware Interface. Dù vậy, hệ điều hành mới này chuyển qua chế độ tiết kiệm điện năng nhanh hơn. Microsoft cho biết khả năng khởi động lại nhanh hơn là nhờ việc Vista loại bỏ các trình điều khiển thiết bị và ứng dụng không thực sự cần thiết.

Trình đơn Start trong Vista thay thế tùy chọn Turn Off Computer trong Windows XP bằng một nút nhấn mới có khả năng yêu cầu hệ điều hành ghi nội dung hiện tại trong bộ nhớ sang một tập tin trên đĩa cứng và chuyển máy sang chế độ chờ (standby). Không may, khi PCW Mỹ thử nghiệm với phiên bản Beta 2, một thiết bị phần cứng không tương thích làm cho hệ điều hành khởi động lại máy thay vì chuyển sang chế độ chờ. Ngoài ra, một nút nhấn khác cho phép bạn khởi động lại hay tắt máy tính như trong Windows XP, nhưng tùy chọn để chuyển sang chế độ ngủ đông (hibernate) không được hỗ trợ từ phiên bản này.

TĂNG TỐC ỨNG DỤNG

Các phiên bản Windows cũ thường tiến hành nạp trước vào bộ nhớ vài tập tin của một ứng dụng để có thể khởi động nhanh ứng dụng này, nhưng tính năng Superfetch trong Vista xử lý việc này ở một cấp độ khác. Trong khi Windows XP

tải trước các tập tin mà một ứng dụng đã mở gần đây vào bộ nhớ trước khi ứng dụng này được thực thi thì tính năng Superfetch theo dõi tất cả ứng dụng mà người dùng đã sử dụng trong một tháng qua và giữ những tập tin được thường xuyên sử dụng nhất luôn có mặt trong bộ nhớ.

Do bộ nhớ máy tính thường có hạn, Vista cho phép sử dụng bút nhớ USB hay đĩa cứng gắn ngoài như không gian lưu trữ Superfetch bổ sung. Chỉ cần cắm một bút nhớ USB vào máy tính, Vista sẽ hỏi bạn muốn sử dụng một phần hay tất cả dung lượng bút nhớ này để tăng tốc độ máy tính (Hình 4). Phân vùng Superfetch mà Vista tạo trên bút nhớ sẽ được mã hóa, tuy nhiên bút nhớ rất dễ bị thất lạc nên người dùng làm việc với những dữ liệu "nhạy cảm" có lẽ không muốn sử dụng biện pháp này. Ngoài ra, kết quả thu được tốt nhất nếu bạn sử dụng bút nhớ tốc độ cao (tốc độ đọc khoảng 30 MB/giây).

REGISTRY WORKSHOP

Nếu thường xuyên phải thực hiện chỉnh sửa Registry, bạn ắt hẳn sẽ nhận ra vài nhược điểm của tiện ích Registry Editor của Windows: đối với người mới bắt đầu sử dụng thì tiện ích này xử lý quá chậm và không cung cấp tùy chọn cho phép phục hồi thao tác trước đó (undo). Tiện ích Registry Workshop (30 USD, tải về bản dùng thử tại find.pcworld.com/51416) sử dụng tài nguyên hệ thống ở mức tối thiểu và qua đó có thể thực hiện tìm kiếm nhanh chóng. Tiện ích cũng có khả năng so sánh các tập tin Registry, cung cấp nhiều cấp undo/redo. Registry Workshop còn có thanh công cụ và có thể mở nhiều tập tin Registry trong giao diện dạng thẻ (tab) để chỉnh sửa các khóa Registry bằng cách kéo thả.

TỰ ĐỘNG NÂNG CẤP

Trong khi Windows XP cho phép bạn nâng cấp các trình điều khiển thiết bị thông qua dịch vụ Windows Update và đó chỉ là những lựa chọn tải về khi bạn ghé qua trang web Windows Update. Vista tự động tải về các trình thiết bị mới và cung cấp cho quá trình cài đặt đã được đồng ý từ phía người dùng. Điều này có thể xem là một tiến trình nâng cấp hiệu quả cho các thiết bị phần cứng không được hỗ trợ trong phiên bản Vista đầu tiên.

Khả năng báo cáo lỗi trong Vista cũng được thực hiện tự động hơn so với trước đây. Khi ứng dụng gặp sự cố, bạn sẽ được hỏi có muốn gửi báo cáo đến Microsoft hay không, nhưng đó không có nghĩa là Microsoft sẽ gửi lại một bản sửa lỗi. Ngược lại, khi Vista gặp phải một lỗi, bạn sẽ được tự quyết định để gửi báo cáo và sẽ nhận được câu trả lời cùng với giải pháp (nếu có).

DỌN DẸP REGISTRY

Hiện tại, có nhiều tiện ích có khả năng làm sạch các cài đặt Registry đã lỗi thời còn sót lại sau khi đã gỡ bỏ cài đặt các ứng dụng như: đường dẫn sai, phần mở rộng tập tin không còn dùng đến, shortcut hỏng, v.v... Một công cụ chỉnh sửa Registry tốt sẽ tiến hành sao lưu trước vì việc "dọn sạch" Registry thường có độ rủi ro cao. Đối với người dùng thông thường, tiện ích miễn phí CCleaner (www.pcworld.com.vn, ID: 51396) có thể là một lựa chọn hợp lý và đáng tin cậy. Tiện ích có thể quét toàn bộ Registry của máy tính và cho bạn tùy chọn xóa bỏ những thứ không cần thiết. Trong khi không có tùy chọn để khôi phục các đối tượng đã xóa thì việc sao lưu tập tin .reg có thể được thực hiện dễ dàng bằng cách nhấn đúp chuột lên tập tin đó.
CCleaner cũng tìm kiếm và dọn sạch tất cả tập tin tạm của Windows và xóa mọi thông tin trong bộ nhớ đệm của trình duyệt và trình đơn Start.Run, danh sách cookie và nhiều thứ khác. Ngoài ra, tiện ích còn chạy các chương trình gỡ bỏ cài đặt và xóa đi các mục còn sót lại. CCleaner còn cho phép bạn lựa chọn và hiển thị danh sách các tập tin sẽ được xóa.

GIAO DIỆN BÓNG BẨY

Giao diện Aero mới của Vista trông mượt mà và ý nghĩa, làm cho Windows và các ứng dụng dễ sử dụng hơn bởi những thành phần trên màn hình có độ sâu, màu sắc sặc sỡ, mịn màng và có độ trong suốt. Đi cùng với giao diện Aero là vài tiện ích mới trông giống các ứng dụng có trong hệ điều hành Mac OS X của Apple.

Tiện ích Windows Media Player 11 có giao diện hợp lý, với khả năng lựa chọn thư viện đơn giản, nút điều khiển lớn và màu sắc sáng (giống với iTunes, Hình 5). Tiện ích quản lý hình ảnh Windows Photo Gallery mới áp dụng cùng giao diện để xem hình ảnh, đơn giản hóa việc in ảnh, ghi lên đĩa DVD hay thực hiện slide-show trên máy tính.

Hiện giờ, Windows Movie Maker có thể ghi phim lên đĩa DVD nhờ chương trình Windows DVD Maker của Vista (tuy nhiên, để hỗ trợ khả năng xem DVD cho tiện ích Windows Media Player, bạn sẽ phải trả tiền tải về codec cần thiết). Vista cũng giới thiệu tiện ích lịch Windows Calender mới, hỗ trợ chuẩn iCal và cho phép bạn thao tác trên web.

Nhìn chung, có thể Windows XP là một hệ điều hành tốt, tuy nhiên với những tính năng bảo mật cải tiến, giao diện mới hấp dẫn hơn và các công cụ hữu ích hơn được hứa hẹn xuất hiện trong Vista thì phiên bản mới này của Windows sẽ còn xuất sắc hơn nữa.

XEM TRƯỚC NỘI DUNG THƯ MỤC

Việc chuyển đổi giữa những ứng dụng đang mở trong Windows Vista sẽ được thực hiện dễ dàng hơn so với các phiên bản Windows trước vì bạn có thể xem hình thu nhỏ (thumbnail) nội dung của từng cửa sổ khi di chuyển chuột qua shortcut trên thanh tác vụ (taskbar). Thậm chí, bạn có thể nhìn thấy phim đang phát hay ứng dụng đang chạy trong cửa sổ thu nhỏ.

Hồng Vy

Khởi động DOS và Windows XP trên 1 máy tính

Nguồn: Echip.com.vn

Hiện tại bạn đang sử dụng WinXP_SP2 nhưng bạn muốn sử dụng thêm MS_Dos. Vậy có cách nào để Windows đưa ra hai lựa chọn: Windows XP hay DOS mỗi khi khởi động máy? Bài viết này sẽ hướng dẫn bạn một cách đơn giản để làm được điều đó.

Trước tiên, bạn chép các file khởi động của DOS là **Io.sys**, **Msdos.sys**, **Command.com**, **Config.sys**, **Autoexec.bat**... vào ổ cứng C. Sau đó, thêm dòng **C:\="DOS"** vào file **Boot.ini**, thí dụ:

```
[boot loader]
timeout=2
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft WindowsXP"
/fastdetect
```

C:\="DOS"

Sau đó mỗi khi khởi động máy sẽ xuất hiện tùy chọn cho phép bạn khởi động bằng DOS hay WinXP.

4 cách đăng nhập vào Windows

Cách 1:

Cách này được dùng nếu trước đây, khi tạo password trong "User accounts", bạn đã có thêm vào dòng "Password hint"cụm từ gọi ý trong trường hợp quên password. Khi bạn gõ nhầm password, Windows sẽ nhắc giúp bạn câu này để có thể giúp bạn nhớ lại password.

Cách 2:

Đối với cách này, bạn cần tạo đĩa mềm cứu hội khi quên password gọi là "Password reset disk". Bạn cần lưu ý là đĩa mềm này phải được format lại. Bấm tổ hợp phím Ctrl+Alt+Del để làm hộp hội thoại Windows Security hiện ra.

Nếu khi bấm tổ hợp phím này mà không thấy hộp hội thoại Windows Security hiện ra, mà thay vào đó là Windows Task Manager thì bạn hãy làm theo cách sau: Vào User Account trong Control Panel, bấm chọn Change the way user log on or off và bỏ đánh dấu chọn vào Use the Welcome Screen.

Bây giờ bạn bấm lại tổ hợp phím Ctrl+Alt+Del và vào Change password (hãy bấm phím Shift+C). Chọn vào Backup và làm theo hướng dẫn trên màn hình. Chú ý: Trong phần Current user account passowrd là pasword hiện thời của bạn. Nếu như bạn chưa thiết lập thì bạn hãy bỏ trống phần này. Sau quá trình hoàn tất, trê đĩa mềm của bạn sẽ có một file userkey (dung lượng khoảng 2KB)

Sử dụng đĩa mềm này cũng rất đơn giản: Khi vào Windowws, một khi bạn đã gõ sai password thì hộp thoại "Login Failed" hiện ra, bạn chọn Reset. Trình Password reset wizard sẽ giúp bạn tạo mới một password hit vào phần reset the user account password rồi bấm nút OK.

Sau khi quá trình này hoàn tất, bạn trở lại hộp thoại đăng nhập và login bằng password vừa mới tạo. Nếu bạn để trống, có nghĩa bạn chọn đăng nhập vào windows mà không cần password.

Một vào lưu ý khi sử dụng Password reset disk:

Đối với hệ điều hành Windows XP sẽ có một file riêng. Do vậy, bạn không thể dùng đĩa password reset disk của máy tính này để reset password cho máy tính khác.

Bạn cũng có thể dùng đĩa password reset đík để thay đổi tài khoản trên máy chủ trong mạng LAN

Cách 3:

Cách này là đăng nhập bằng tài khoản quản trị (administrator) để reset lại password cho user. Với tài khoản quản trị này, sau khi vào Windowws, bạn bấm tổ hợp phím Win+R. Sau đó, bạn gõ vào control userpassword2. Tiếp theo, bạn chọn vào reset password trên account đã quên password. Giờ bạn chỉ cần chọn một password mới cho user này và confirm (xác nhận) là hoàn tất! hoặc bạn có thể vào User account để thay đổi (change) trực tiếp password cho account này.

Cách 4:

Bạn cũng đăng nhập vào hệ thống với tài khoản administrator. Sau đó bấm tổ hợp phím Win+R và chạy compmgmt.msc. Vào thư mục User trong Local User and Gróup. Bấm phải vào user đã mất password, chọn Set Password. Bấm chọn Proceed. Tiếp theo, bạn chỉ cần gõ password và xác nhận lại. Bấm nút OK để kết thúc.

Theo Làm bạn với máy vi tính

Sao lưu và phục hồi dữ liệu trong WinXP

(04/03/2004, 00h32 GMT+7)

Bạn đã mỏi mệt với việc cài lại WinXP sau mỗi trận oanh tạc của virus? Bạn đang phải đối mặt với nguy cơ dữ liệu quý giá lưu trong ổ cứng sẽ tan theo mây khói?

Thực tế cho thấy có rất nhiều trường hợp ổ cứng máy tính đột nhiên ngừng hoạt động, hay nói đơn giản là "đã chết", mà chẳng có nguyên nhân rõ rệt nào. Và khi điều này xảy ra, kể cả ổ cứng của bạn vẫn trong thời gian bảo hành, bạn vẫn là người thiệt thòi vì không có một nhà sản xuất nào lại bảo hành cho dữ liệu được lưu trữ trong ổ đĩa. Giải pháp duy nhất của bạn là nhờ tới dịch vụ phục hồi dữ liệu, nhưng số tiền bạn phải trả cũng khá đắt đỏ. Chính vì vậy, khi sự an toàn của dữ liệu được đặt lên hàng đầu thì việc sao lưu (backup) chúng trở nên vô cùng quan trọng.

I. Sao lưu dữ liệu

* Phương pháp sao lưu 1: *Chụp hình ổ đĩa*

Phương pháp chụp hình ổ đĩa để sao lưu dữ liệu thực chất là tạo ra một bản copy phân ổ tương tự (một phần hoặc tất cả không gian ổ cứng để hệ điều hành có thể truy cập dưới dạng ổ logic, như ổ C: chẳng hạn) và lưu trữ chúng ở vị trí nào đó. Thường những file hình khi tạo ra bằng phương pháp này đều ở dạng nén, do vậy nó chiếm ít dung lượng hơn so với các file gốc. Trong trường hợp xảy ra sự cố, các file này có thể hồi phục thành một ổ cứng mới; và trong hầu hết trường hợp, chúng sẽ hồi phục lại nguyên trạng ổ đĩa cũ tại thời điểm file hình được tạo ra.

"Chụp hình" thường là tính năng của một số sản phẩm phần mềm như Norton Ghost của Symantec. Chúng được dùng để cài đặt và cấu hình một lượng lớn máy tính trong mạng LAN với các tính năng tương tự nhau. Một quản trị viên sẽ cài đặt hệ thống và những chương trình cần thiết trên một máy tính, đảm bảo sao cho mọi thứ hoạt động trong tình trạng bình thường, và sau đó sẽ tạo ra một file hình của hệ thống đó để lưu trữ trên máy chủ.

Khi sử dụng đĩa khởi động với phần mềm chụp ổ đĩa, các máy tính trong mạng sẽ truy cập tới file hình hệ thống của máy chủ và "bắt chước" cấu hình tương tự. Bằng cách làm này, quản trị viên sẽ tiết kiệm được rất nhiều thời gian thay vì phải cài đặt từng máy riêng rẽ trong hệ thống.

Chụp ổ đĩa là phương pháp tốt nhất để bảo vệ dữ liệu trước nguy cơ hệ thống "sụp đổ" không thể cứu vãn. Ảnh được tạo ra sẽ hoàn toàn tương tự với bản gốc. Tuy nhiên, mỗi phương pháp đều có hạn chế chung, chẳng hạn như phương pháp này còn tồn tại 2 hạn chế:

+ Thứ nhất, các file hình có dung lượng khá lớn và mất thời gian tạo ra. Nếu sử dụng ổ ghi CD-R để tạo một file hình hoàn chỉnh, bạn có thể sẽ phải mất vài chiếc đĩa CD.

+ Thứ hai, quan trọng hơn cả là các file hình chỉ chụp được trạng thái máy tính khi nó được tạo ra; còn nếu sau khi bạn đã cài đặt thêm phần mềm hoặc tiến hành một vài thay đổi, thì file hình đó sẽ không thể lưu được các thay đổi này.

Nâng cấp file hình hàng ngày không phải là phương pháp mang tính thực tiễn. Để giải quyết vấn đề này, giải pháp tốt nhất là kết hợp giữa chụp hình ổ đĩa với các phương pháp sao lưu dữ liệu truyền thống.

*** Phương pháp sao lưu 2**: ***Lưu file và đường dẫn***

Về cơ bản, lưu trữ có nghĩa là sao chép các file và thư mục ra một số phương tiện dự phòng như: ổ cứng, đĩa mềm, đĩa CD... . Phần mềm sao lưu sẽ tạo ra một file nén để lưu trữ tất cả các file và đường dẫn được backup. Phương pháp này có thể tiết kiệm được không gian ổ đĩa và ngăn không cho truy cập vào các file sao lưu trừ khi cần thiết. Thuận tiện lớn nhất của phương pháp này là dễ tiến hành mà không cản trở những thao tác bạn đang tiến hành trên máy. Sao lưu dữ liệu quan trọng từ các đường dẫn cụ thể rất dễ tiến hành, và hầu hết các phần mềm sao lưu (gồm cả những công cụ được tích hợp sẵn trong WinXP) đều cho phép bạn có thể lên kế hoạch triển khai công việc backup. Thậm chí nếu muốn, bạn có thể "giao" cho máy tính đảm nhận công việc này. Hầu hết các phần mềm backup sẽ theo dõi các đường dẫn và file bạn cần lưu, và chỉ lưu các thay đổi kể từ lần sao lưu cuối cùng.

*** Sao lưu trong Windows XP**

Windows XP được trang bị những tính năng sao lưu và phục hồi dữ liệu khá hiệu quả. Người dùng XP Professional sẽ tìm thấy chương trình này tại thư mục: Start/programs/accessories/system tools/backup; trong khi đó, người dùng XP Home phải cài đặt chúng từ đĩa CD.

Tính năng này sẽ cho phép bạn có thể sao lưu các file lựa chọn trước, hoặc chỉ định

rõ từng file. Bạn cũng có thể tạo một backup toàn hệ thống, gồm cả "Đĩa mềm khôi phục hệ thống tự động" (ASR). Cách tốt nhất là kết hợp giữa hai phương pháp.

Đầu tiên, bạn cần tạo một backup toàn hệ thống (đặc biệt là chụp ảnh ổ đĩa). Ảnh này sẽ cho phép bạn có thể phục hồi hệ thống về trạng thái ban đầu trước khi máy tính bị hỏng hóc.

- Tạo file backup ảnh hệ thống:

Để backup toàn bộ hệ thống, bạn cần chạy trình hướng dẫn backup, sau đó chọn: "backup files and settings" (sao lưu file và cài đặt), và cuối cùng là: "all information on this computer".

Chú ý: Phương pháp backup này sẽ tạo ra một ảnh tất cả các ổ đĩa trên máy tính. Nếu bạn chỉ muốn backup ổ hệ thống (Csmile_image, thì thay vì sử dụng trình hướng dẫn, bạn nhấn vào "advanced mode" (chức năng nâng cao) khi bắt đầu chương trình backup, và sau đó chọn "automated system recovery wizard" (trình phục hồi hệ thống tự động). Phương pháp này sẽ tiến hành các bước tương tự với phương pháp trên, nhưng nó sẽ chỉ backup ổ đĩa chính.

Bạn có thể lưu file ảnh backup hệ thống ngay trên ổ cứng hoặc các phương tiện khác (như đã nói ở trên). Chính vì file backup khác lớn, nên bạn cần phải có kế hoạch sao lưu hợp lý.

Ngay sau khi bạn chỉ định vị trí đặt file hình hệ thống, máy tính sẽ tiến hành thực hiện công việc của mình. Khi quá trình này kết thúc, bạn sẽ thấy một thông báo hiện ra, yêu cầu bạn sao lưu các thông tin hồi phục hệ thống trên một đĩa mềm 1.44MB (đã format). Chiếc đĩa này rất quan trọng khi bạn cần phục hồi lại hệ thống. Sau khi thực hiện xong các bước này, bạn sẽ tiến hành backup từng phần dữ liêu cá nhân.

- Backup dữ liệu cá nhân:

Do chiếm một dung lượng khá lớn, nên không phải lúc nào phương pháp tạo file hình hệ thống cũng mang tính thực tiễn. Có một cách làm hay là bạn tạo các tệp tin nén nhỏ, chứa file và tài liệu cần backup.

Khi hệ thống gặp vấn đề, việc đầu tiên bạn cần làm là hồi phục ảnh toàn bộ hệ thống (đã được tạo ra trước đó), và tiếp đến là phục hồi các file lưu gần nhất. Cách làm này có thể tránh mất mát dữ liệu ở mức tối đa.

OK, đã đến lúc bạn sao lưu các file dữ liệu quan trọng, chẳng hạn như "My documents, các shortcut và cài đặt màn hình... Để thực hiện thao tác căn bản này, bạn có thể dùng tính năng backup của Windows: Khởi động trình backup và chọn lựa phần "backup files and settings" và tiếp đến là "my documents and settings".

Chọn vị trí cần lưu file và nhớ rằng trình backup Windows không hỗ trợ ghi trực tiếp vào đĩa CD, do vậy, nếu bạn muốn tiến hành theo cách này, bạn có thể copy file lưu vào một vị trí trên ổ cứng và sau đó burn (ghi) chúng vào đĩa CD.

Khi trình backup hoàn tất, bạn cần tái khởi động lại quá trình. Lần này cần sử dụng lựa chọn: "let me choose what to back up". Hãy đánh dấu vào các file hoặc folder bạn cần backup.

Nếu bạn không muốn mất thời giờ với các thao tác backup, bạn hoàn toàn có thể giao "nhiệm vụ" này cho máy tính thực hiện. Chọn "Advanced mode" và chọn tab "schedule jobs". Kích đúp vào ngày bạn muốn trình backup tự động khởi tạo, và chọn "back up selected files, drives or network data", tiếp đến là đánh dấu vào các file hoặc đường dẫn muốn lưu.

*** Thẩm định quá trình backup**

Chọn vị trí file backup lưu và chọn loại backup. Nói chung, trừ khi bạn cần backup một lượng lớn dữ liệu, còn nếu không chỉ sử dụng các cài đặt bình thường ("normal") để backup tất cả các file. Những cài đặt khác sẽ chỉ backup các file đã

thay đổi kể từ lần backup cuối cùng.

Nếu bạn lựa chọn chức năng "thẩm định" quá trình backup sau khi nó được hoàn tất, bạn có thể sẽ được yêu cầu bổ sung thêm dữ liệu backup vào file lưu hoặc viết đè lên các file cũ với phần backup mới.

Trong hầu hết trường hợp, viết đè bao giờ cũng là lựa chọn tốt hơn cả, trừ phi bạn muốn phục hồi các bản copy dữ liệu cũ hơn. Còn bổ sung thêm dữ liệu sẽ chỉ tăng dung lượng file cho mỗi lần thao tác, và hậu quả là dung lượng ổ đĩa sẽ nhanh chóng bị "ngốn" hết.

OK, bạn cần đặt tên và khởi tạo kế hoạch cho trình backup. Hãy chắc chắn rằng nút "later" được chọn lựa, và tiếp đến là nhấn "set schedule". Từ đây, bạn có thể lựa chọn khoảng thời gian hoặc thời gian bạn muốn sử dụng cho trình backup (hàng ngày, hàng tuần, hàng tháng...) và một số cài đặt khác đối với trình backup tự động. Hãy đặt thời gian, nhấn vào nút "OK" và tiếp đến là nút "Next".

Hãy nhập mật khẩu cho tài khoản vì hệ thống sẽ cần chúng để chạy trình backup tự động cho mỗi khoản riêng.

II. Phục hồi dữ liệu

OK, bạn đã làm quen với quá trình backup, công việc bây giờ là phục hồi chúng.

Đầu tiên, đối với trường hợp ổ cứng của bạn bị "chết", bạn sẽ cần phục hồi ảnh hệ thống bằng cách sử dụng đĩa CD Windows XP và đĩa mềm ASR đã được tạo ra trước đó.

Khởi động hệ thống bằng đĩa CD Windows XP. Ngay sau khi màn hình máy tính hiện màu xanh, một dòng thông báo sẽ hiện thị ở cuối màn hình yêu cầu bạn ấn F2 để khởi động chế độ hồi phục hệ thống tự động. Nhấn F2 và đưa đĩa mềm vào ổ. Nếu bạn bỏ qua bước này, bạn cần thực hiện lại, thường thì cũng phải 2-3 lần mới thành công.

Hãy chắc rằng ổ đĩa mà bạn muốn là ổ chính của hệ thống cần phải được chọn. Vì những lý do hiển nhiên, nên ổ đĩa này không thể là ổ đĩa bạn lưu ảnh hệ thống. Quá trình cài đặt sẽ format tất cả ổ đĩa và tự động quá trình cài đặt.

Khi màn hình phục hồi hệ thống xuất hiện, bạn chọn chính xác các file backup và

Windows sẽ tự động phục hồi hệ thống về thời điểm trước đây. Quá trình này có thể sẽ mất khoảng vài phút.

Giả dụ bạn có dữ liệu cá nhân được lưu trữ tại các vị trí riêng biệt, bạn cần khởi tạo trình backup. Chọn "restore files and settings", một danh sách các file lưu được tạo ra trước đây sẽ hiển thị bên cửa sổ phía phải. Kích đúp vào file bạn cần phục hồi và hãy đánh dấu vào file đó bên cửa sổ tay trái. Kích vào nút Next. Hệ thống sẽ thông báo cho bạn rằng nó sẽ phục hồi file. Nếu bạn muốn khôi phục chúng vào các vị trí khác nhau, hoặc thẩm định các cài đặt khác, chẳng hạn như viết đè, bạn hãy chọn tab "advanced"; còn nếu không, bạn chỉ cần kích vào "Next" để phục hồi các file và đường dẫn.

*** Một số tiện ích backup miễn phí**

Nếu bạn không muốn sử dụng những tính năng backup có sẵn trong Windows, bạn có thể dùng một số tiện ích backup miễn phí khác. Tuy nhiên, hầu hết các tiện ích backup này chỉ có chức năng lưu, chứ không có chức năng chụp ảnh hệ thống.

1. **ASCOMPBackUpMaker** (Download)

BackUp Maker là một tiện ích backup miễn phí tuyệt vời. Nó cung cấp khả năng nhanh chóng tạo ra các file backup hoặc tạo lập kế hoạch backup tự động. Tuy nhiên, tính năng vượt trội hơn cả của tiện ích này chính là cho phép ghi file backup trực tiếp vào đĩa CD mà không cần phải sử dụng các trình burn đĩa của bên thứ ba.

2. **BASK** (Download)

Một công cụ tốt để backup, hồi phục dữ liệu. Tuy giao diện có hơi khó nhìn, nhưng bù lại, BASK lại có những thanh công cụ dễ sử dụng. Nhược điểm của trình phần mềm này là không thể ghi backup trực tiếp ra đĩa CD.

3. **Aethia DBackup** (Download)

Dễ sử dụng với các chức năng khởi tạo và phục hồi file nén backup, đặc biệt là khi bạn đã chán ngấy với quá nhiều chức năng trong trình backup của Windows. Tuy nhiên, Aethia DBackup không thể tạo lập tác vụ backup định sẵn trong một khoảng thời gian.

Van Han

TẮT BỚT CÁC DỊCH VỤ CỦA WINDOWS ĐỂ TĂNG TỐC

Các dịch vụ của Windows (Services) là một trong những thành phần cốt lõi của mọi ứng dụng trên Windows. Với việc sử dụng hợp lý (đóng - ngắt hoặc tạm dừng) sẽ giúp bạn khai thác Windows một cách hiệu quả nhất. Ngoài ra sự hiểu biết các dịch vụ này sẽ giúp bạn tối ưu hóa Windows, tăng cường bảo mật và giảm thiểu virus khi mà các dịch vụ không cần thiết được loại bỏ.

Những nguy cơ tiềm ẩn khả năng tấn công của máy tính thường nằm trong sự thiếu hiểu biết 1 phần nào đó của Windows mà bạn đã vô thức để cho hệ thống tự chạy. Hơn nữa hệ thống có thể sẽ nặng nhọc hơn khi mà phải "gồng mình" khởi động các dịch vụ này. Để truy cập vào các dịch vụ (Services) từ Start bạn chọn --> Control Panel --> Administrative Tools --> Services --> Kích phải chuột vào từng dịch vụ và chọn Properties bạn chọn General --> Startup Type sẽ có 03 lựa chọn Automatic (Sẽ tự khởi động theo mặc định Windows), Manual dùng trong trường hợp bạn tự cấu hình chạy hoặc không chạy mà không phụ thuộc vào cấu hình mặc định Windows, Disabled để đóng dịch vụ khi mà bạn không cần thiết dịch vụ này.

Cũng trong General tab còn có các lựa chọn Start - Stop - Pause - Resume giúp bạn quyết định khởi động hay dừng nhưng bạn phải chú ý rằng khi bạn không lựa chọn Startup Type ở trên thì các chức năng này chỉ có tác dụng trong phiên làm việc hiện tại của Windows mà sau đó khi bạn khởi động lại máy hệ thống lại trả về trạng thái ban đầu vì vậy khi quyết định ngừng hoặc khởi động dịch vụ bạn phải chọn lựa Startup Type.

Cảnh báo: Khi bạn đóng ngắt dịch vụ nào đó tức là bạn đã vô hiệu hóa chức năng bất kỳ trong Windows mà có thể bạn sẽ dùng sau này vì vậy chúng tôi đề nghị bạn đọc kỹ các tính năng trước khi ngắt bỏ (Disabled). Một số tính năng khi mà bạn ngắt bỏ có thể làm cho máy tính báo lỗi do hệ thống đang sử dụng nó cho các ứng dụng được bạn cài đặt

Alerter: Dịch vụ này giúp thông báo cho các máy tính và người dùng được chọn

những sự cảnh báo mang tính chất hành chính. Bạn để nó nếu bạn cảm thấy nó cần thiết với bạn. Nếu không thì hãy tắt nó đi.

Application Layer Gateway : Cần thiết nếu bạn muốn dùng Firewall trong Windows (Internet Connection Firewall) hoặc Chia sẻ thông tin mạng của Windows (Windows Internet Connection Sharing). Sẽ rất vô dụng nếu như bạn không dùng 2 ứng dụng trên.

Application Management : Bạn không dùng chung 1 mạng với ai đó ? Bạn không không có ý định điều khiển 1 trình nào đó thông qua mạng ? Nếu không hãy vô tư mà Disable nó.

Automatic Updates : Bạn muốn máy tự động cập nhật Windows. 1 số trường hợp quay số kết nối để cập nhật mà chủ nhân không biết. Trả tiền cước hàng triệu đồng... Nếu cập nhật mà không mấy hiệu quả thì không cần cập nhật, ngọai trừ các lổ hổng bảo mật lớn thì tự vào website microsoft cập nhật thôi.

Background Intelligent Transfer : Hỗ trợ Windows Update, nếu bạn tắt Automatic Update ở trên thì vô hiệu hóa dịch vụ này nhằm giảm sức nặng hệ thống phần nào.

Clipbook : Cho phép bạn xem những gì lưu trữ trong Clipboard, sắp xếp chúng có trật tự để có thể thi hành tác vụ những gì trong Clipbard. Bạn có thể không cần làm quan trọng mọi việc đến như vậy. Tắt nó đi sẽ giúp các lệnh Copy-Paste-Cut nhanh hơn. Bạn có thể xem nó hoạt động như thế nào qua cách đánh clipbrd.exe vào lệnh Run trong Start Menu.

COM+ : Cả hai Event System và System Application Services giúp quản lý và nắm quyền Microsoft's Compoment Object Model. Nếu như bạn cần tìm hiểu về vấn đề này, chỉ Microsoft mới có câu trả lời tốt nhất tuy là bằng tiếng anh _www.microsoft.com/com/tech/complus.asp. Nói chung, có thể một phần mềm nào đó sẽ cần đến dịch vụ này để chạy, tốt nhất bạn thiết lập nó ở chế độ Manual

Computer Browser : Không hề liên quan gì đến trình duyệt web thân yêu của bạn. Ý nghĩa dịch vụ này là theo dõi những hệ thống khác kết nối vào máy bạn qua

1 mạng chia sẻ. ...Quyết định tùy bạn

Cryptographic services: Dịch vụ chứng nhận - đánh giá trong WinXP. Cho dù bạn cảm thấy không cần thiết với nó, nhưng khuyên bạn nên để nó chạy vì vài tính năng khác của nó khá hữu ích như kiểm tra chứng nhận trình điều khiển các thiết bị của winxp.

DHCP Client: Khi bạn lên mạng hoặc không, dịch vụ này sẽ lấy 1 địa chỉ IP cho bạn. Bạn có thể thử tắt nó. Nhưng nếu bạn bắt đầu gặp những vấn đề lỗi, hiệu hóa nó lại. ***(Ý kiền cá nhân:*** *Nên tắt nó đi nếu bạn không dùng mạng hoặc bạn dùng mạng nhưng lại đặt IP tĩnh****.)***

Distributed Link Tracking Client : Quản lý các Shortcut đến tập tin trên Server nào đó . Nếu bạn đã vô hiệu hóa 2 dịch vụ trên thì cũng nên bỏ luôn cái này.

DNS Client: Dịch vụ này giải đáp và thiết lập một bộ đệm về tên miền để hỗ trợ cho máy tính bạn đang sử dụng. Nếu bạn không sử dụng Internet thì nên tắt dịch vụ này đi.

Error Reporting : Tự động thông báo lỗi có thể là 1 tính năng khá tốt nhưng đôi khi lại quá làm phiền và vô dụng.

Event Log : Bỏ. Nhiệm vụ của nó chỉ là ghi lại những báo cáo đôi khi khó hiểu. (***Ý kiền cá nhân:*** *Không nên tắt dịch vụ này vì nếu tắt không những không làm cho máy khởi động nhanh hơn mà còn làm cho máy khởi động cực chầm.*)

Fast User Switching Compatibility : Nếu bạn không dùng máy chung với nhiều người thì vô hiệu hóa cái này tăng năng lực cho máy rất nhiều.

Help and Support : Sự trợ giúp là 1 điều quý báu nhất là khi ta gặp khó khăn. Nhưng nếu bạn không rành Tiếng anh và không biết nó nói cái gì.... vậy thì nên tắt nó đi thì hơn.

HTTP SSL: Kết nối từ client đến server được thực hiện bằng giao thức HTTPS (HTTP + SSL). Chỉ sử dụng dịch vụ này khi bạn chạy Web Server.

Human Interface Device Access Service: Mở rộng và điều khiển những phím nóng trên các thiết bị nhập. Ví dụ những nút bấm trên bàn phím Play-Next-Internet-Search. Nếu bạn không thường dùng nó, tắt dịch vụ này đi và tận hưởng 0.85% hệ thống nhanh hơn.

IIS Admin: Cho phép bạn quản lý dịch vụ Web và FTP thông qua dịch vụ Internet Information Services (IIS). Nếu bạn không dùng đến những dịch vụ trên thì hãy tắt nó.

IMAPI CD-Burning COM Service : Thật sự ra dùng Nero ghi đĩa trực quan hơn dịch vụ có sẵn trong WinXP này.

Indexing services: Tự động tra sóat thông tin trên ổ cứng nhằm giúp các ứng dụng như Search của windows, Office XP chạy nhanh hơn. Tuy nhiên nó chiếm nhiều tài nguyên và thật sự không xứng đáng với tính năng nó hoạt động.

IPSEC services: Nếu như máy tính của bạn thuộc vào loại viễn thông và kết nối với máy khác bởi VPN thì Internet Protocol Security (IPSEC) có thể cần thiết. Tuy nhiên tôi không dám mơ tưởng máy mình dữ dội đến vậy. Tạm thời tắt nó đi.

Logical Disk Manager : Nếu như bạn muốn quản lý đĩa cứng của mình (bấm phải trên biểu tượng My Computer, chọn Manage rồi đến Disk Management), thì dịch vụ này không thể bị vô hiệu hóa. Vì trình Disk Management phụ thuộc dịch vụ này để chạy. Tuy nhiên, có lẽ bạn không sài đến thường xuyên Disk Management , thiết lập nó sang Manual sẽ là tốt nhất.

Messenger: Vào năm trước , những kẻ Spammer đã nhận ra 1 cách có thể gửi hàng triệu Spam đến người dùng WinXP thông qua Messenger này. Loại bỏ dịch vụ này là lựa chọn sáng suốt

MS Software Shadow Copy Provider/Volume Shadow Copy: Hỗ trợ Microsoft Backup hay các trình sao lưu ảnh đĩa khác. Một lần nữa, bạn có thể thử qua việc tắt nó, nếu có sai sót nào trong việc sao lưu thì khởi động lại nó sẽ giải quyết vấn đề.

Net Logon:Hỗ trợ việc chứng thực để đăng nhập vào một máy tình thuộc miền.

NetMeeting Remote Desktop Sharing : Không muốn chia sẻ với ai bất cứ cái gì trên máy bạn thông qua NetMeeting ? Không = Disable

Network Connections: Quản lý những đối tượng trong kết nối mạng và kết nối mạng quay số, trong đó bạn có thể thấy được cả mạng cục bộ và những kết nối từ xa.

Network DDE: Cung cấp việc truyền tải và an toàn mạng cho sự trao đổi dữ liệu động (Dynamic Data Exchange(DDE)). Cho những chương trình chạy trên cùng một máy tính hoặc trên những máy tính khác nhau.

Network Location Awareness (NLA):Tập hợp và lưu trữ thông tin về cấu hình và vị trí mạng. Đưa ra thông báo khi những thông tin này thay đổi.

Network Provisioning Service: Quản lý cấu hình của file XML trên một miền cơ sở cho mạng được cung cấp tự động. (*XML được thiết kế để thực hiện lưu trữ dữ liệu và phát hành trên các Web site không chỉ dễ dàng quản lý hơn, mà còn có thể trình bày đẹp mắt hơn. XML cho phép những người phát triển Web định nghĩa nội dung của các tài liệu bằng cách tạo đuôi mở rộng theo ý người sử dụng*)

Plug and Play : Bạn cần dịch vụ này để nhận biết các thiết bị mới gắn vào Pc, bên trong hay bên ngòai, PCI hay USB, Fire wire đều sẽ cần đến nó, hay chỉ đơn giản là WinXP cần giao tiếp tìm kiếm lại phần cứng nào đó trong 1 số lý do.

Print Spooler: Nếu bạn không dùng máy in thì hãy tắt nó đi thì hơn.
Remote Desktop Help Session Manager : Đừng để ai đó điều khiển máy bạn nếu bạn không muốn bị vậy

Remote Procedure Call : Trong winXP, các ứng dụng được phân chia trong công thức Cá thể tiến trình. Không 1 trình nào ảnh hưởng đến trình nào. Khi 1 phần mềm bị đứng, treo hay không trả lời, nó sẽ không ảnh hưởng đến tòan bộ máy như Win98. Để quản lý hết tất cả những phần mềm này 1 cách thuận tiện, RPC là dịch

vụ cần thiết sắp xếp phân vùng bộ nhớ phát cho từng ứng dụng. Nếu tắt nó sẽ gây ra lỗi hệ thống rất nghiêm trọng. Vì vậy bạn đừng làm điều đó.

Remote Registry Service : Bạn có thích cho người dùng khác trên 1 mạng máy tính thay đổi các thiết lập trong Registry, trái tim của hệ điều hành trên máy bạn ? Bạn sẽ không tìm ra được nguyên nhiên ngày nào đó WinXP bị..vỡ tim đâu. Dịch vụ này là 1 dạng của sự bất bảo mật cho máy.

Security Accounts Manager: Dịch vụ Lưu trữ những thông tin bảo mật cho tài khoản của người dùng tại chỗ.
Security Center: Theo dõi và quản lý những thiết lập và những cấu hình an toàn của hệ thống

Server: Hỗ trợ file, máy in và tên dùng để chia sẻ thông tin qua mạng cho máy tính bạn đang sử dụng. Nếu bạn không dùng chung mạng với ai đó thì nên tắt nó đi.

Smart Card và Smart Card Helper : Nếu bạn không dùng các thẻ nhớ thì bạn biết phải làm gì với dịch vụ này.

SSDP Discovery : một thành phần của Universinal Plug and Play sắp nói đến. Cho dù bạn tắt hay mở nó, bạn cũng sẽ làm cùng chung 1 việc cho SSDP Discovery.

System Restore : Mừng hết lớn khi có thể bay về quá khứ trước khi bạn cài đặt 1 driver lỗi hay phần mềm làm hại hệ thống là ví dụ thực tiễn cho bạn gợi ý nên tắt ứng dụng này hay không. Tuy nhiên vô hiệu hóa nó sẽ tiết kiệm cho bạn rất nhiều dung lượng đĩa. Lưu ý là nếu bạn đã chọn tắt nó thì tất cả những thiết lập sao lưu sẽ bị xóa hết.

Task scheduler : Đôi khi không mấy hữu dụng đối với bạn, Có thể bạn sẽ không cần phải lập lịch dồn đĩa trong đêm, nhưng Task Scheduler có thể cần thiết với và người khác. Tắt nó hay không tùy vào yêu cầu của bạn có cần hoặc không.

TCP/IP NetBIOS Helper :Là 1 đòi hỏi bình thường nếu hệ thống mạng nội bộ của bạn dùng NetBIOS bởi TCP/IP. Tắt nó nếu bạn cảm thấy không cần thiết. Tuy nhiên khởi động lại nếu như mạng nội bộ của bạn (thậm chí mạng Internet) có trục trặc liên quan đến việc tắt dịch vụ này.

Telephony :Bạn vô cùng cần - nói cách khác không thể thiếu nó nếu bạn muốn vào Internet thông qua phương thức quay số = Modem. Nhưng nếu là kết nối ADSL, bạn thử thiết lập nó qua Manual để xem nếu có lỗi nào xảy ra vì có thể nó vẫn đòi hỏi dịch vụ này. Nếu không bạn đã giúp máy có thể tài nguyên hệ thống khá là không ít...

Telnet : Cho phép người dùng máy khác dang nhập vào máy bạn và chạy các chương trình. Nếu như bạn có bao giờ nghe đến việc tấn công qua IP thì Telnet là 1 trong những kẻ 2 mặt tiếp tay cho giặc quậy phá thành của bạn. Tắt nó đi, trừ khi bạn cần nó cho 1 lý do nào đó

Uninterruptible Power Supply : An tòan để vô hiệu hóa. Trừ khi bạn có cục UPS cho máy tính mình. **Universinal Plug and Play :** Tự hỏi bạn có muốn máy mình kiểm tra và tìm hiểu các thiết bị có trên máy người khác trong 1 mạng máy tính nội bộ ? Có thể nó cần thiết nếu như bạn xài Internet Connection Sharing và cho phép người ngòai hiệu chỉnh kết nối cho máy bạn. Dù sao đi nữa, nếu như thật sự không biết gì, bạn có thể tắt nó cũng được.

Webclient : Theo sự mô tả, dịch vụ này cho phép bạn duyệt qua "Network Places" , thực chất đó là mạng Internet. Nó cho phép các chương trình Windows tạo, xâm nhập và thiết lập tập tin trên nền Internet. Theo như 1 số thử nghiệm, nếu như bạn không có kết nối Internet, dịch vụ có thể làm chậm lại máy và cách bạn duyệt web. Vô hiệu hóa để nhận ra và xem xét những sai sót có thể gây phiền cho bạn, nếu không thì bạn đã tiếp tục giảm gánh nặng cho hệ thống.

Windows Audio: Bạn muốn nghe tiếng - âm thanh thỏ thẻ của Pc phát ra từ 2 giàn loa 480 Watts của bạn thì nên để cho dịch vụ này khởi động bình thường. Đối với nó, bạn chỉ nên vô hiệu hóa khi máy không có sound card hoặc chip sound trên bo mạch.

Windows Image Acquisition : Nếu như đơn giản là bạn không có Webcam hay máy Scan hình thì tắt dịch vụ này đi. Tuy nhiên cho dù bạn có, tắt ứng dụng này chắc cũng không ảnh hưởng, vì vậy hãy tắt nó đi cũng được. (Hay thay nó thành Manual để thử nghiệm trước khi bạn thật sự tắt nó .

Windows Installer : Trợ giúp cho các trình cài đặt .MSI có thể phân phối dữ liệu trong nó cho máy bạn. Nhưng thật chất không phải lúc nào bạn cũng cài-cài-cài phần mềm vào máy mình liên tục. Thay cách khởi động của nó vào Manual sẽ giảm tối thiểu dung lượng Ram bị chiếm.

Windows Management Instrumentation :Dịch vụ này cho phép sự giao tiếp các phần mềm có thể xâm nhập và dùng những tính năng trong Windows có thể diễn ra trọn vẹn. Bản thân windows cũng dùng đến Windows Management Instrumentation, như những trình khác làm, tốt nhất bạn để nó hoạt động.
Windows Time :Đồng ý là thời gian là vàng là bạc là hàng loạt thứ một đi không quay lại. Nhưng nếu như bạn không muốn Windows phải chú trọng đến điều đó cho bạn, nếu như bạn không cp1 1 máy tính luôn kết nối mạng thì không đồng bộ hóa giờ giấc không có nghĩa là bạn có tội.

Wireless Zero Configuration : Bạn dùng mạng không dây? Nếu không, nên vô hiệu tính năng này.
WMI Performance Adapter : Windows Management Instumentation (WMI) là 1 ứng dụng rất có ích nhưng nó có thể làm chậm máy.Nếu như bạn không phải là 1 nhà thiết kế chương trình thì không cần quan tâm đến việc này. Ngòai ra bây giờ bạn có thể tắt nó đi.

note:mỗi máy tính đều khác nhau, có dịch vụ ở máy này không cần nhưng có thể ở máy khác lại cần (chẳng hạn giữa máy nối mạng internet với máy không nối mạng chẳng hạn), cho nên bạn nên cẩn thận khi disable dịch vụ nào đấy bởi nó có thể làm cho máy tính không khởi động được. Cách tốt nhất là chọn manual.

Loại Bỏ Các Dịch Vụ (service) Của Windows Xp., Các dịch vụ không cần thiết.

Windows XP và Server 2003 chạy rất nhiều dịch vụ theo mặc định mà điều này là vô nghĩa nếu bạn không ở trong một mạng cộng tác, những dịch vụ này là những cái bạn có thể loại bỏ an toàn, do đó giải phóng bộ nhớ, nhưng cần kiểm tra xem mỗi cái đó làm những gì trước khi bạn chắc chắn không sử dụng nó:

Vào Start -> Run và gõ services.msc, click chuột phải vào mỗi dịch vụ, vào properties và chọn disable.

Alerter
Application Layer Gateway Service,
Application Management
Automatic Updates
Background Intelligent Transfer
Clipbook
Distributed Link Tracking Client
Distributed Transaction Coordinater
Error Reporting Service
Fast User Switching Compatibility
IMAPI CD-Burning
Indexing Service
IPSEC Services
Messenger
Net Logon
Net Meeting
Remote Desktop Sharing
Network DDE
Network DDE DSDM
Portable Media Serial Number
Remote Desktop Help Session Manager
Remote Registry
Secondary Logon
Smartcard
SSDP Discovery Service
Telnet Themes
Uninterruptible Power Supply
Universal Plug and Play Device Host
Upload Manager
Webclient
Wireless Zero Configuration
WMI Performance Adaptor

17 Service Cần thiết:

Apllication Management
Event Log
IMAPI CD-Burning Cdrom Sevice
Network Connection
Plug and Play
Print Spooler
Remote Access Connection Manager
Remote Procdure Call
Shell Hardware Detection
Telephony
Themes
Universal Plug and Play Device Host
Windows Audio
Window Firewall/ICS
Window Installer
Windows Management INstrumentation
Windows Time

Sưu Tầm.

Cài đặt Windows XP Pro toàn tập

PHẦN I:

1. Một đĩa Windows XP Home CD
2. Một máy tính có ổ CD-ROM.

Để có thể bắt đầu cài đặt, bạn phải kiểm tra trong BIOS xem CD-ROM có phải là thiết bị để khởi động đầu tiên không (first boot).
Phần 1:

Cho đĩa Windows XP vào trong ổ CD-ROM và khởi động lại máy tính của bạn. Windows sẽ tự động kiểm tra phần cứng và cấu hình của máy bạn.

Windows bây giờ chuẩn bị cài đặt vào máy bạn.

Bạn nhấn "ENTER" dể bắt đầu quá trình cài đặt.

Nếu đồng ý với thông báo của Windows bạn nhấn F8 để tiếp tục còn nếu không đồng ý bạn nhấn "ESC" để thóat. Nếu bạn không đồng ý, quá trình cài đặt sẽ kết thúc.

Phần 2:

Bây giờ bạn chọn nơi mà bạn muốn cài đặt Win XP. Bạn nhấn "ENTER" để xác nhận phân vùng mà bạn muốn cài đặt Win.

Bây giò bạn cần phải định dạng (format) ổ cứng, NTFS được khuyến khích sử dụng. Bạn cũng có thể chọn FAT32. sau đó bạn nhấn ENTER.

Ổ cứng sẽ được format.

Phần 3:

và sau đó Windows sẽ bắt đầu copy những file cần thiết cho quá trình cài đặt.

Windows sẽ nhận cấu hình của Win XP.

Giờ là lúc để khởi động lại Win XP, bạn nhấn "ENTER" để quá trình xảy ra nhanh chóng nếu không Windows sẽ tự động khởi động lại sau 15 giây.

Khi khởi động lại, màn hình có hiện thông báo nhấn một phím bất kì để khởi động bằng ổ CD-ROM, bạn đừng làm gì cả hãy để nó trôi qua.
Windows đang được khởi động.

Windows đang được khởi động.
Phần 4:

Quá trình cài đặt được tiếp tục.

Bây giờ là lựa chọn ngôn ngữ và vùng. Chuột của bạn lúc này đã hoạt động vì thế bạn dùng chuột nhấn vào "CUSTOMIZE"

Bây giờ bạn chọn định dạng chuẩn khu vực của bạn và nhấn OK.

Bây giờ bạn nhấn vào Deltails

Tiếp đó chọn ngôn ngữ mặc định sau đó nhấn "OK" để thoát ra

Bây giờ bạn đã có tất cả sự thay đổi cần thiết, bạn nhấn "NEXT".

PHẦN II và HẾT

Phần 5:

Bây giờ là lúc ghi thông tin cá nhân của bạn. Bạn điền tên và có thể điền thêm nơi công tác, làm việc. Bạn nhấn "NEXT" khi đã sẵn sàng.

Tiếp đó bạn điền vào khóa sản phẩm. Sau khi điền chính xác xong bạn nhấn NEXT.

Bây giờ bạn đặt tên cho máy tính của bạn và pasword của admin. Xác nhận lại password và nhấn "NEXT".

Hệ thống giờ và ngày là phần tiếp theo, bạn thay đổi nếu thấy cần thiết, và nhấn "NEXT".

Windows sẽ tiếp tục được cài đặt ngay sau đó.

Phần 6:

Nếu card mạng được tìm thấy trong máy của bạn thì bảng sau sẽ hiện ra. Bạn chọn "TYPICAL SETTINGS" và nhấn NEXT.

Thay đổi tên nhóm làm việc nếu bạn thấy cần thiết và nhấn "NEXT".

Windows sẽ tiếp tục cài đặt.

Quá trình cài đặt kết thúc.

Bây giờ là lúc để Windows XP khởi động lại lần nữa, bạn nhấn"ENTER" để quá trình diễn ra nhanh chóng, mặt khác bạn cũng có thể đợi 15 giây để Windows tự động khởi động lại.

Khi khởi động lại sẽ có thông báo nhấn một nút bất kì để máy tính khởi động bằng CD-ROM, bạn đừng nhấn bất kì nút nào, cứ để mặc cho nó trôi qua.

Windows sẽ tiếp tục được nạp.

Phần 7:[b]

Windows bấy giờ sẽ nhận cấu hình máy tính của bạn. Bạn nhấn OK để tiếp tục.

Nếu bạn đồng ý với sự thay đổi bạn nhấn "OK" không thì bạn nhấn "CANCEL" để qấy lại với cấu hình cũ.

Bây giờ WINDOWS sẽ cập nhật thay đổi. Bạn hãy kiên nhấn chờ đợi.

Màn hình WELCOME hiện lên.

và kết thúc là Desktop của Windows XP. Windows đã được cài xong.

Nếu may mắn bạn sẽ không cần phải cài đặt driver cho các thiết bị. Nếu không bạn vào "device manager" để cập nhật driver cho các thiết bị như: card sound, card màn hình, card mạng....
Các main đời mới nếu có đĩa Driver của các thiết bị như:soud,card màn hình,card mạng,v....v..v.... thì bạn lên cài đặt vào để cho các driver này điều khiển các thiết bị đó thay cho Win và hiệu suất sử dụng cũng tăng lên rất nhiều.

Cài lại Windows không làm mất dữ liệu

Thực hiện: Bùi Xuân Toại

Làm việc quá lâu, Windows sẽ mất ổn định. Dùng một máy tính quá hai năm, tới lúc nào đó bạn có thể gặp trục trặc và phải cài lại Windows từ đầu. Nhưng không như suy nghĩ phổ biến của nhiều người, bạn không cần phải định dạng (format) lại ổ đĩa cứng (trừ trường hợp sẽ trình bày dưới đây). Những thứ tồi tệ cần loại bỏ đều nằm trong thư mục Windows của bạn.

Trước khi bắt đầu, phải tập hợp trong tay các CD-ROM chứa Windows và các ứng dụng. Sao lưu các tập tin dữ liệu (chỉ để cho an toàn), và... dành ra hai ngày làm việc. Nếu mọi việc suôn sẻ, bạn có thể cài lại Windows trong vài giờ. Tuy nhiên bạn phải tính đến một số trục trặc có thể xảy ra: Không tìm được CD cần thiết nào đó, dữ liệu không nằm đúng chỗ, hoặc một cái gì đó không chịu hoạt động.

Có sự khác nhau giữa việc cài lại để sửa chữa và cài lại mới hoàn toàn. Việc cài sửa chữa cho phép giữ lại các thiết lập đang dùng, trong khi đó cài lại mới hoàn toàn sẽ trao cho bạn một bản Windows mới 'sạch sẽ' thực sự. Việc cài sửa chữa tuy nhanh chóng và dễ dàng nhưng không khắc phục được khi có quá nhiều trục trặc. Những hướng dẫn dưới đây dùng cho cài lại mới hoàn toàn, trừ những trường hợp ngoại lệ có chú thích.

Đĩa CD phục hồi của nhà sản xuất

Hầu hết các máy tính đều có kèm theo CD phục hồi của nhà sản xuất, ngoài CD MS Windows (nếu bạn chỉ có CD MS Windows, hãy chuyển tới mục phiên bản Windows tương ứng).

Một số CD phục hồi cung cấp tất cả các tùy chọn của CD MS Windows đầy đủ, hướng dẫn rõ ràng và có sẵn các trình điều khiển (driver) phần cứng phù hợp. Một số khác có thể không làm gì ngoài việc format lại ổ đĩa cứng và phục hồi đúng tình trạng như khi mới mua (đây là ngoại lệ cần phải format lại).

Hình 1: Chuyển các folder vào 'old-stuff' trước khi cài lại HĐH

Nếu đĩa CD phục hồi của bạn là loại chỉ có công dụng format lại, bạn phải sao lưu các tập tin dữ liệu lên mạng hay một phương tiện lưu trữ tháo lắp nào đó trước khi cài lại Windows. Nếu đang dùng Windows 98 hoặc Me, bạn sao lưu C:\My Documents cùng với các folder chứa trong C:\Windows sẽ được nói đến trong mục 98/Me bên dưới. Nếu đang dùng Windows 2000 hoặc XP, bạn sao lưu C:\Documents and Settings. Đồng thời bạn cũng phải sao lưu cả các folder nào có chứa các tập tin dữ liệu của mình.

CD Windows 98 và ME

Các phiên bản Windows này lưu giữ một số dữ liệu quan trọng trong folder Windows mà bạn sẽ xoá, cho nên phải chép một số folder con của nó vào chỗ khác. Bạn nhấn phải My Computer và chọn Explore. Nhấn đúp biểu tượng ổ đĩa C: (trong Me, bạn có thể phải nhấn View the entire contents of this drive). Nhấn phải trong khung bên phải rồi chọn New folder. Đặt tên cho folder mới là oldstuff.

Chuyển đến folder Windows (có thể phải nhấn View the entire contents of this drive), nhấn giữ phím <Ctrl> và chọn các folder con sau: All Users, Application Data, Desktop, Favorites, Local Settings, Profiles, SendTo, và Start Menu. Nếu không nhìn thấy tất cả chúng, bạn chọn View.Folder Options (Tools.Folder Option trong Me), nhấn nhãn View, chọn Show all files, và nhấn OK (nếu vẫn chưa nhìn thấy tất cả chúng, bạn đừng lo). Ấn phím <Ctrl> và kéo các folder này vào C:\oldstuff (xem hình 1).

Khởi động lại Windows bằng đĩa khởi động trong ổ đĩa mềm (để tạo đĩa mềm khởi động, bạn đưa đĩa mềm vào ổ, chọn Start.Settings.Control Panel, nhấn đúp Add/Remove Programs, nhấn Startup Disk.Create Disk, và làm theo các thông

báo). Trong Startup Menu, bạn chọn Start computer with CD-ROM support. Trong khi các driver được nạp, bạn đưa đĩa CD Windows vào ổ.

Trừ trường hợp thực hiện một cài đặt lại để sửa chữa, còn bạn cứ việc gõ lệnh c:\windows\ command\deltree /y c:\windows và ấn phím <Enter>. Việc xóa các tập tin cũ có thể mất nhiều thời gian, nhưng khóa chuyển đổi /y sẽ triệt bỏ các nhắc nhở cần xác nhận, nên bạn hãy nghỉ giải lao một chút.

Khi quay lại dấu nhắc A:, bạn gõ x:Setup, trong đó x là tên chữ ổ CD của bạn (thường đó là ký tự sau tên chữ của nó trong Windows, nếu trong Windows là D: thì nhiều khả năng ở đây là E:). Ấn <Enter> và làm theo các thông báo.

Khi quay lại trong Windows, bạn cài đặt lại driver của card màn hình. Nếu cài đặt Windows cho nhiều người dùng, bạn còn phải tạo lại từng tài khoản cho từng người dùng. Chọn Start.Settings.Control Panel.Users để thực hiện việc đó. Điều quan trọng là tên người dùng phải khớp với tên trong cài đặt cũ. Nếu không chắc chắn, bạn mở Windows Explorer và đi đến C:\oldstuff\profiles. Ở đó bạn sẽ tìm thấy các folder ứng với từng tên người dùng đã đăng ký (xem hình 2). Bạn đừng bận tâm về password. Bạn thoát ra và đăng nhập lại với từng người dùng. Sau khi thực hiện xong, bạn thoát ra và đăng nhập lại một lần nữa, nhưng thay vì chọn tên người dùng và password, bạn ấn phím <Esc> để vào Windows không dùng người dùng cụ thể nào.

Chọn Start.Programs.MS-DOS Prompt (trong Windows 98) hoặc Start.Programs.Accessories.MS-DOS Prompt (trong Windows Me). Gõ xcopy c:\oldstuff*.* c:\windows /s/h/r/c và ấn <Enter> (nếu muốn biết về các khoá chuyển đổi của xcopy, bạn nhập lệnh xcopy/?). Khi xcopy hỏi có ghi đè lên một tập tin nào đó hay không, bạn ấn a (All) cho tất cả. Khi xcopy thực hiện xong, bạn khởi động lại và đăng nhập (dưới tên một người dùng cụ thể nào đó, nếu cần). Mở My Documents để biết chắc tất cả các tập tin dữ liệu của bạn đều nằm đúng chỗ, kể cả các địa chỉ Web ưa thích trong Internet Explorer và các shortcut menu Start tùy biến.

Giờ thì bạn có thể nhảy thẳng đến mục 'Kết thúc công việc'.

CD Windows 2000 và XP

Khởi động máy tính với đĩa CD Windows trong ổ. Khi thấy hiện thông báo 'Press any key to boot from CD' (ấn phím bất kỳ để khởi động bằng CD), bạn thực hiện theo. (Nếu không nhìn thấy thông báo này trước khi Windows khởi chạy, bạn khởi động lại Windows, ấn phím mà bạn được nhắc nhở để vào chương trình PC Setup, và thay đổi trình tự khởi động để ổ CD là lựa chọn đầu tiên).

Hình 2: Sau khi cài lại WinXP,tạo lại tài khoản người dùng

Ở màn hình 'Welcome to Setup', bạn ấn <Enter>. Tùy chọn R (repair - sửa chữa) sẽ đưa bạn vào Recovery Module rất có ích khi Windows không khởi động, nhưng không giúp ích gì cho việc cài đặt lại. Bạn sẽ được báo ngay rằng mọi thứ đã sẵn sàng cho việc cài đặt Windows lên máy tính. Ấn r đối với cài đặt sửa chữa hoặc <Esc> để bắt đầu cài lại mới hoàn toàn. Đối với phục hồi hoàn toàn, bạn chọn phân vùng đĩa C: và ấn <Enter>. Khi thấy xuất hiện cảnh báo là có một hệ điều hành đang nằm trên phân vùng đĩa đó, bạn ấn c. Khi được hỏi về sự chọn lựa phân vùng đĩa, bạn chọn Leave the current file system intact (no changes - không thay đổi). Khi được báo đã có folder Windows (hoặc Winnt đối với Windows 2000), bạn ấn l để xóa nó và tạo một folder mới. Thực hiện theo các thông báo. Khi chương trình cài đặt hỏi tên của bạn, nhập temp.

Khi cài đặt xong, hệ thống của bạn sẽ khởi động lại vào Windows, và bạn sẽ được đăng nhập với tên người dùng Temp. Nếu màn hình khó đọc, bạn cài đặt lại driver của card màn hình.

Nếu cài đặt lại Windows XP, bạn bỏ qua mục 'Đối với cả Windows XP và 2000'.

Nếu cài đặt lại Windows 2000, bạn thoát ra khỏi tên Temp và đăng nhập lại với tên Administrator. Xong thoát ra và đăng nhập một lần nữa với tên Temp. Mở Windows Explorer và đến C:\Documents and Settings. Một trong hai folder con sẽ được đặt tên là Administrator (người quản trị hệ thống). Folder kia sẽ được đặt tên đại khái là Administrator computername.

Bạn chọn Start.Programs.Accessories.Command Prompt. Gõ cd '\documents and settings' và ấn <Enter>. Sau đó gõ xcopy administrator*.* administrator.computername /s/h/h/c, thay computername bằng phần cuối của tên folder đó (sau 'Administrator.') trong Documents and Settings. Bây giờ bạn ấn <Enter> và khi được hỏi về việc ghi đè các tập tin hoặc folder, bạn ấn a (All) cho tất cả.

Nếu có bất kỳ tên người dùng nào trong cài đặt cũ ngoài Administrator, bạn tiếp tục thực hiện theo mục 'Đối với cả Windows XP và 2000' bên dưới. Nếu không có, bạn mở Windows Explorer và kiểm tra để chắc chắn các tập tin dữ liệu đã nằm đúng chỗ. Sau đó dùng applet Users và Passwords của Control Panel và xoá tên người dùng Temp trước khi đi đến mục 'Kết thúc công việc'.

Đối với cả Windows XP và 2000

Hình 3: Duyệt Website Windows Update của Microsoft sau khi cài đặt lại

Mở lại Windows Explorer. Chọn ổ đĩa C: (có thể phải nhấn Show the contents of this folder). Nhấn chuột phải trong khung bên phải, chọn New folder và đặt tên cho folder mới là oldstuff. Trong khung bên trái, chọn folder Documents and Settings. Nó phải có các folder con ứng với từng người dùng từ cài đặt trước cộng thêm một folder cho Temp và một số folder khác. Di chuyển các folder con ứng với những tên người dùng trước sang oldstuff.

Chọn Start.Control Panel.User Accounts (Start.Settings.Control Panel.Users and Passwords trong Windows 2000). Tạo tài khoản cho từng người dùng đã được đăng ký trước khi cài đặt lại. Kiểm tra lại để bảo đảm sử dụng đúng các tên. Chúng cũng trùng tên các folder bạn vừa di chuyển vào oldstuff (hình 2). Trong Windows XP, ít nhất một người dùng phải có quyền của người quản trị. Bạn thoát ra và đăng nhập lại với tên của từng người dùng, trước khi đăng nhập lại dưới tên Temp. Dùng Log Off chứ đừng dùng Switch User (chuyển đổi người dùng) ở hộp thoại Log Off của Windows XP (điều này không có trong Windows 2000).

Đăng nhập dưới tên Temp, chọn Start.Programs.Accessories.Command Prompt (Start.All Programs.Accessories.Command Prompt trong XP), gõ xcopy c:\oldstuff*.* 'c:\documents and settings' /s /h /r /c, và ấn <Enter>. Ấn phím a khi được hỏi có muốn ghi đè lên một tập tin hay không. Thoát khỏi Temp và đăng nhập vào từng tài khoản đã được phục hồi để kiểm tra chắc chắn tài liệu và dữ liệu của mọi người dùng đều nằm đúng chỗ. Đăng nhập là người quản trị và chạy applet User Accounts của Control Panel một lần nữa để loại bỏ người dùng Temp.

Kết thúc công việc

Đến đây bạn đã có Windows hoạt động, nhưng còn thiếu nhiều thứ khác. Có thể còn phải cài đặt lại máy in, card âm thanh v.v... Rất may, nếu driver cho các phần

cứng này có kèm theo trong Windows hoặc trong CD phục hồi của nhà sản xuất, chắc chắn nó đã được cài đặt lại một cách tự động.

Bạn còn phải cài đặt lại các ứng dụng. Một số thiết lập của các ứng dụng sẽ không bị thay đổi bởi việc cài đặt lại, nhưng những thiết lập trước đây được lưu giữ trong Registry đều bị loại bỏ hết.

Khi kết nối Internet hoạt động trở lại, bạn đến windowsupdate.microsoft.com để tải xuống tất cả các bản cập nhật quan trọng cho phiên bản Windows của mình (hình 3). Sau đó đến thăm các Wesite của các hãng sản xuất phần cứng của bạn để cập nhật các driver.

Sau khi cài đặt lại, một số dữ liệu của bạn có thể xuất hiện không đúng chỗ. Tìm kiếm trong các folder Application Data và oldstuff và xem có thể chuyển chúng vào folder mà Windows hoặc các ứng dụng của bạn sẽ tìm chúng không. Nếu tìm thấy folder mang tên Identities có hai folder con mang tên dài và khó hiểu, hãy thử chuyển dữ liệu của 1 folder sang folder kia và xem dữ liệu của bạn có xuất hiện lại không.

Có thể bạn nghĩ bước kết thúc là xóa folder C:\oldstuff và cả folder Administrator trong Windows 2000. Hãy để việc đó lại sau. Bạn đợi vài ngày, vài tuần, thậm chí vài tháng sau, cho đến khi nào tin chắc tất cả các tập tin cần thiết đều có thể truy cập được.

Bùi Xuân Toại
PC World Mỹ 7/2003

Tăng tốc độ mở Start Menu – Windows XP

Cách 1:

+ Chạy **Regedit** từ **Start\Run**
+ Tìm đến khóa **Hkey_Current_User\Control Panel\Desktop**
+ Thay đổi value của key **Menu ShowDelay** thành **0**

=> Chắc chắn nó sẽ nhanh hơn hẳn đấy.

Cách 2:

- Nếu bạn có dùng TuneUp Utilities thì làm như sau:

+ Bật TuneUp Utilities lên, chọn TuneUp SystemControl

+ Trong box **Usage** > chọn **Start Menu**
+ Trong thẻ **Behavior** > tích chọn vào **Open menus automatically after indicated delay** > kéo con chạy về hết bên trái (phía **Short delay**), có giá trị **= 0 ms**

P/s: Hai cách trên là như nhau, 1 cách là dùng sẵn của phần mềm, cách còn lại thì dựa vào Win.
Đây là 1 thủ thuật nhỏ của việc chỉnh sửa ***Registry***. Nếu bạn quan tâm đến những thủ thuật về ***Registry*** thì vào đây:
Code:

```
http://www.updatesofts.com/forums/showthread.php?t=65524
```

Enjoy !
Ptt(UDS)

Thủ thuật Windows XP

Dịch thuật: hungquocle
Thủ thuật nguồn từ các website nướcngoài:
Update theo ngày:

TẮT TÍNH NĂNG ERROR REPORTING

1: Mở Control Panel
2: Nhấn vào Performance và Maintenace
3: Nhấn vào System
4: Rồi nhấn vào Advanced tab
5: Nhấn vào nút error-reporting phía dưới của Windows
6: Chọn Disable error reporting
7: ok và ok.

LÀM BIẾN MẤT MŨI TÊN TRONG ICONS TRÊN DESKTOP

1: Mở Regedit
2: Tìm đến dòng HKEY_CLASSES_ROOTlnkfile
3: Xóa IsShorcut registry

4: Khởi động lại máy để có hiệu lực.

LÀM HÌNH ẢNH NHỎ HƠN KÔ THẤY

Khi bạn thử gửi hình ảnh qua email,bạn cần có thêm chức năng làm chúng nhỏ hơn. Nếu chức năng này kô có, một file DLL cần phải được đăng ký.
1:Start
2:Run
3:regsvr32 shimgvw.dll

MỞ PORTS VÀ THÊM CHƯƠNG TRÌNH VỚI SP2'S FIREWALL

1: Nhấn Start/Run
2: Điền firewall.cpl
3: Nhấn vào thẻ Exception tab
.....
ADDING A PORT FOR INTERNET ACCESS

1: Nhấn vào nút Add port
2: Đặt bất cứ tên gì
3: Điền Ports mà bạn muốn mở
ADDING A PROGRAM FOR INTERNET ACCESS

1: Nhấn vào nút ADD PROGRAM
2: Một dãy chương trình hiện ra
3: Bôi đen chương trình bạn chọn
4: Nhấn OK

ẨN COMPUTER TRÊN MỘT NETWORK

Chạy: Run/ net config server /hidden:yes

Thủ thuật Windows XP 2

Gõ overclockers vào thanh địa chỉ của IE sau đó giữ phím ctrl và ấn enter. Sau đó nó sẽ vào www.overclockers.com. (cảm ơn kendan!)

Ctrl + D sẽ tự động biến trang bạn đang xem thành trang chủ của trình duyệt.....cũng như việc kéo chữ E nhỏ màu xanh dương trong địa chỉ vào nút Home.

Để có một hình chụp màn hình, ấn phím PrintScr, sau đó mở Paint (hoặc một chương trình tương tự), Click vào menu edit-> paste. Làm như vậy sẽ chụp một ảnh của tất cả mọi thứ (bao gồm cả thanh công cụ) trên màn hình của bạn. Nếu bạn muốn chụp hình một cửa sổ cụ thể, giữ phím alt và ấn phím Print Scrn.
Thay đổi nội dung hiển thị trong System Properties (click chuột phải vào my computer...click properties) Trong windows NT/2K/XP vào start.....click run và gõ vào Regedit. Đến khóa:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Cu
rrentVersion và thay đổi giá trị của RegisteredOrganization's thành bất cứ thứ gì bạn muốn. Bạn cũng có thể thay đổi RegisteredOwner cũng như vậy.
WinXP di chuyển những ứng dụng dùng nhiều nhất đến một phần nhanh hơn trên ổ cứng. Nhưng nó chỉ làm như vậy mỗi 3 ngày một lần. Để di chuyển chúng vào phần nhanh nhất "on call", vào Start -> run và gõ **Rundll32.exe advapi32.dll, ProcessIdleTasks**
(c) by Shadow O`O'@ocforums.com

Bạn đã từng kết thúc một tác vụ và phải đợi 30 giây để cửa sổ End Now xuất hiện? Vào Start....Run....gõ vào in regedit, Enter. Đến khóa HKEY_Current User\Control Panel\Desktop điểm sáng vào desktop ở cửa sổ bên phải. Bây giờ tìm giá trị HungAppTimeout và double click vào nó. Thay đổi giá trị thành 3000 (3000miligiây=3 giây). Click chuột phải vào một khoảng trống ở cửa sổ bên phải và tạo một giá trị String mới là WaitToKillAppTimeout (giống như tôi gõ nó). Double click vào khóa mới và thiết lập giá trị là 3000.

Windows có sẵn một sự trì hoãn với thời gian nó mất để menu start thực sự hiển thị cái bạn muốn. Để thoát khỏi sự trì hoãn này và tăng tốc menu start, Vào Start...run...regedit. Trong khóa HKEY_CURRENT USER\Control Panel\Desktop, tạo một giá trị string mới là MenuShowDelay. Thiết lập giá trị từ 0 đến 999 (mili giây).

Một cách dễ dàng để xem và biên tập tất cả các file **autoexec.bat, config.sys, win.ini, system.ini, and protocol.ini** cùng một lúc là vào menu Start>>Run...gõ "sysedit", Enter Dễ dàng hơn nhiều so với cách mở chúng trong một trình biên tập văn bản độc lập IMO cho mỗi cái, và đặc biệt là bằng tay Nếu bạn cần thay đổi nhiều hơn một file cùng một lúc.

Có trang dslreports.com giúp kiểm tra tốc độ băng rộng.

Dọn dẹp taskbar:

Trong regedit:
Đến khóa
[hkey_local_machine][SOFTWARE][Microsoft][Windows][Current Version]

Sau đó đến khóa:
[Run]
[Run Once]
[Run Services]

Tìm thứ bạn không cần và/hoặc muốn trong taskbar và xóa chúng.

Khởi động lại và hưởng thụ taskbar được dọn dẹp!

Mike

Uhhhhhhhh.... Còn cái này thì sao?
Gõ vào 'MSCONFIG' trong menu Start >> Run để biên tập các tính chất khởi động trong máy của bạn và loại bỏ những chương trình không dùng đến.

Các tiện ích dòng lệnh của WindowsXP
Added 1/5/02

Trong khi có rất nhiều tiện ích dòng lệnh trong WindowsXP, đây là vài chương trình mà tôi đã dùng gần đây.

bootcfg - Cấu hình, truy vấn, hoặc thay đổi các thiết lập trong file boot.ini.

driverquery - Hiển thị một danh sách của tất cả các trình điều khiển thiết bị đã được cài đặt và thuộc tính của chúng.

getmac - Trở lại địa chỉ media access control (MAC) và liệt kê các giao thức internet liên kết với mỗi địa chỉ cho tất cả các cạc mạng trong mỗi máy tính

gpresult - Hiển thị các thiết lập chính sách nhóm(Group Policy) và tổng hợp các chính sách (RSOP) cho một người hoặc một máy tính.

netsh - Bạn có thể sử dụng các lệnh trong giao diện Netsh ngữ cảnh IP để cấu hình giao thức TCP/IP

schtasks - Sắp xếp các lệnh và chương trình để chạy định kỳ hoặc vào một thời gian cụ thể

systeminfo - Hiển thị thông tin cấu hình chi tiết về một máy tính và hệ điều hành của nó

Hai cách để gỡ bỏ trình nhắn tin MSN Messenger:

Dòng lệnh(vào Start>> Run và gõ vào):
RunDll32 advpack.dll,LaunchINFSection
%windir%\INF\msmsgs.inf,BLC.Remove

Batch File(*.BAT):
1. Sao chép mã này vào tài liệu văn bản của bạn và lưu lại với phần mở rộng là *.bat

```
@echo off
echo Removing Microsoft Messenger...
rundll32 advpack.dll,LaunchINFSection %WinDir%\inf\msmsgs.inf,BLC.Remove

echo Disabling it from running in the future...
echo REGEDIT4>%temp%\nomsngr.reg
echo
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Mes
senger\Client]>>%temp%\no
msngr.reg
echo "PreventRun"=dword:00000001>>%temp%\nomsngr.reg
echo "PreventAutoRun"=dword:00000001>>%temp%\nomsngr.reg
echo "PreventAutoUpdate"=dword:00000001>>%temp%\nomsngr.reg
echo "PreventBackgroundDownload"=dword:00000001>>%temp%\nomsngr.reg
echo "Disabled"=dword:00000001>>%temp%\nomsngr.reg
regedit /s %temp%\nomsngr.reg
```

2. double click vào file *.BAT và khởi động lại máy
3. msn messenger sẽ bị gỡ bỏ khỏi hệ thống của bạn

Và có một cách sửa dễ dàng hơn:
Đến thư mục: C:/Program Files/Messenger. Đổi tên thư mục Messenger thành

"MessengerOFF" Cách này không làm chậm OutLook hay cản trở hiệu suất của hệ thống.

All work

Max

Nếu mũi tên của shortcut trong các biểu tượng hiển thị trên màn hình nền làm bạn khó chịu, thì đây là một giải pháp cho bạn. Tôi tin rằng hầu hết các bạn biết nó nhưng tôi vẫn nói ra đây.

Vào regedit-->Đến khóa HKEY_CLASSES_ROOT--> Tìm thư mục "lnkfile" và "piffile". Xóa khóa mà hiển thị cái gì đó dọc theo dòng của "shortcut" trên mỗi cái.

Khởi động lại và mũi tên nhỏ biến mất. =)

Biên tập lệnh "Send To" trên menu ngữ cảnh (aka menu hiện ra khi ấn chuột phải) trong WinXP (Cũng làm được với các hệ điều hành khác, nhưng bạn phải đến một thư mục khác):

Đến thư mục C:\documents and settings, sau đó click vào username của bạn, Sau đó mở thư mục SendTo. Tại đây bạn có thể thêm các shortcut cho thư mục, ứng dụng ...v.v

Thêm vào "Copy to folder..." và "Move to folder..." vào menu ngữ cảnh: Bạn có thể tự làm thông qua Registry hoặc copy/paste văn bản này vào một file *.reg và nhập vào Registry (sao lưu registry trước...Tôi không chịu trách nhiệm cho những tai nạn!)

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemO
bjects\shellex]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemO

bjects\shellex\ContextMenuHandlers]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemO

bjects\shellex\ContextMenuHandlers\Copy To]
@="{C2FBB630-2971-11D1-A18C-00C04FD75D13}"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemO
bjects\shellex\ContextMenuHandlers\Move To]
@="{C2FBB631-2971-11D1-A18C-00C04FD75D13}"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemO
bjects\shellex\ContextMenuHandlers\Send To]
@="{7BA4C740-9E81-11CF-99D3-00AA004AE837}"

(Tôi lấy cái này ở đâu đó trong một Website tweak...Tôi nghĩ đó là ntfs.org)

Mỗi lần bạn dùng IE4 hoặc hơn để vào một web site nó(IE4) chỉ tạo một kết nối để mã html và một kết nối khác để download đồ họa.

Tăng số kết nối có thể sử dụng tốt hơn băng thông và nâng tốc độ lên đáng kể các trang xuất hiện trong trình duyệt của bạn. Tất nhiên tinh chỉnh này không có hiệu quả nếu site bạn đang thăm được thiết kế để ngăn cản nhiều hơn 2 kết nối.

Sao lưu registry sau đó chọn start, run, gõ vào regedit và ấn <Enter> trong cửa sổ cây ở bên trái tìm đến

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\Internet Settings. Với Internet Settings được chọn ở bên trái, Tìm kiếm một biểu tượng có nhãn MaxConnectionsPer1_0Server và một cái khác có nhãn MaxConnectionsPerServer. Nếu bạn không thấy chúng, click chuột phải ở ô bên phải và chọn New > DWORD Value. gõ vào MaxConnectionsPer1_0Server và ấn <ENTER>, Click chuột phải lần thứ hai và tạo một giá trị DWORD có tên MaxConnectionsPerServer. Bây giờ double click vào MaxConnectionsPer1_0Server . Giá trị mặc định là 4, Nhưng nếu bạn muốn tăng giá trị này lên, Nhập vào một giá trị lớn hơn trong hộp 'Value data' (số thập phân) là 8. (Một số web sites có thể có giá trị cao đến 20 vì vậy hãy tự do thử nghiệm) Bây giờ click okay ,double click MaxConnectionsPerServer và thay giá trị thành 4 (mặc định là 2) Một số người đặt nó bằng 10.

Click ok và thoát khỏi registry. Nếu may mắn bạn sẽ lướt Web nhanh hơn đáng kể.

Hope this helps

Đây là một cách khác để gỡ bỏ Windows messenger trong Windows XP

Start -> Run , gõ regedit ,click ok, tìm đến khóa: HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\Run. Với khóa run được chọn ở bên trái, chọn biểu tượng MSMSGS ở bên phải và ấn <Delete>. Click Yes để xác nhận xóa và thoát khỏi registry editor.

Biểu tượng sẽ biến mất ở khay hệ thống khi bạn đăng nhập lần sau.

Tuy nhiên có một cách dễ hơn để kiểm soát Windows messenger

Chỉ cần mở outlook express vào options, vào nhãn general và bỏ chọn log on to windows messenger.

chúc vui!

Tăng tốc Shutdown nhanh chóng

Sao lưu registry của bạn sau đó chọn start, run, gõ vào regedit và ấn <Enter> Trong ô vuông cây bên tái tìm đến khóa HKEY_CURRENT USER\CONTROL PANEL\DESKTOP

và double click vào giá trị AutoEndTasks. Giá trị mặc định của nó là 0. Thay đổi bằng cách gõ 1 vào trường DATA và click OK.

Bạn có thể giảm nhiều hơn lượng thời gian mà WinXP mất để đóng cả hai ứng dụng hoạt động và ứng dụng treo bằng cách double-clicking vào giá trị HungAppTimeout (cũng ở khóa HKEY_CURRENT USER\CONTROL PANEL\DESKTOP và xác nhận rằng trường dữ liệu của giá trị được thiết lập ở 5000. Thoát khỏi hộp thoại Edit String, double-click vào giá trị WaitToKillAppTimeout, thiết lập giá trị của nó là 4000 và click OK và thoát khỏi registry editor.

Chúc may mắn

Để các File *.DLL ngòai bộ nhớ Cache

Mặc dù các file DLL (dynamic-Lynk library - thư viện liên kết động) có tính quyết định đối với sự điều hành hệ thống, Không cần thiết để WinXP phải giữ chúng đóng trong trường hợp chúng cần thiết. Mặc dù thực tế các file DLL dùng bộ nhớ cache mà có thể còn dư cho dữ liệu quan trọng hơn, WinXP làm chính xác như vậy.

Để thay đổi điều này thông qua the registry, Tìm đến khóa

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENT VERSION\EXPLORER

Với khóa Explorer được điểm sáng, tạo một khóa khác bằng cách click vào Edit, New and Key. gõ **AlwaysUnloadDLL** để đặt tên cho khóa, ấn <ENTER>, double-click vào giá trị mặc định của nó, gõ 1 vào trường dữ liệu của giá trị và click ok.

Đóng Registry Editor lại và khởi động lại máy.

WinXP bây giờ sẽ giải phóng các file DLL khỏi bộ nhớ cache khi nó ngừng sử dụng chúng.

Dành cho WinXP:

Một điều mà mọi người chưa nói đến khi bạn sử dụng System Restore nó thực sự làm phân mảnh đĩa cứng của bạn. Tôi dùng Norton Systemworks và nói báo cho tôi biết hầu hết các file bị phân mảnh đều là file của system restore. Cách sửa là tắt system restore trên ổ C đi để dọn dẹp folder đó, sau đó lại bật nó lên và tạo một điểm phục hồi mới (để đề phòng). Ổ cứng của tôi giảm phân mảnh từ 23% xuống còn 2%.

Cũng vậy, Bật System Restore trên một ổ cứng khác ổ chứa file hệ thống thì sẽ rất lãng phí dung lượng trống(space).

Phím Win+M cực tiểu hóa tất cả các cửa sổ, nhưng cái hay là Shift+Win+M phục hồi tất cả các cửa sổ mà bạn vừa cực tiểu hóa.

Làm thế nào để tinh chỉnh WinXP để đạt hiệu suất cao nhất

Những bài hướng dẫn này có sẵn ở Tutorial Town và Tutorial Town Forums. Nếu bạn cần trợ giúp thì gửi bài ở đây hoặc ở phần Help hoặc ở diễn đàn TutorialTown.

Phần lớn những mẹo & tweaks này đã được gửi bởi Nikeus & Co ở FTC vì vậy công lao là của họ, các chú thích cũng là của họ !

Trước khi chúng ta bắt đầu đi qua những mẹo và tinh chỉnh mà tôi đã thu thập được cho đến nay , tôi xin cảnh báo với bạn rằng một số trong đó bao gồm sửa đổi registry. Luôn luôn sao lưu registry trước khi sửa đổi nó. Bạn có thể làm điều này bằng cách vào Start >> Run & gõ Regedit. Trong Registry Editor vào menu File -> Export và lưu lại vào nơi an toàn. Nếu bạn muốn quay trở lại như lúc ban đầu chỉ cần double click vào file đã lưu và nó sẽ trở lại như ban đầu. Có thể thay thế việc sao lưu registry bằng cách thiết lập một điểm phục hồi hệ thống trong System Restore để nếu như có rắc rối bạn có thể quay lại như lúc đầu.

Để tăng hiệu suất của hệ thống

Click chuột phải vào my computer. Click properties.
Click nhãn advanced.
Click settings (under performance).
Click chọn Adjust for best performance.
Cuộn xuống dưới và check vào ô cuối “use visual styles on windows and buttons”.

Làm sao để loại bỏ trình ghi đĩa sẵn có của WinXP

Click vào nút start.
Chọn Run.
Gõ services.msc và click ok.
Tìm đến IMAPI CD-Burning Com Services Mở nó ra và click vào start up type, đổi thành "Disabled".

Những thiết lập này sẽ chỉnh tốt nhất bộ nhớ hệ thống của bạn

Bạn cần ít nhất 256MB ram để làm việc này:

Vào start\run\regedit -và đến khóa sau:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Contro l\Session

Manager\Memory Management

1.DisablePagingExecutive -double click nó và cho giá trị thập phân bằng 1 - cái này cho phép XP để dữ liệu trong bộ nhớ thay vì để trong phần hoán chuyển của Ram tới ổ cứng làm tăng hiệu suất hệ thống.

2.LargeSystemCache- double click nó và thay đổi giá trị thập phân bằng 1 -cái này cho phép nhân của XP chạy trong bộ nhớ và cải thiện hiệu suất hệ thống rất nhiều.

3.Tạo một giá trị dword mới và đặt tên nó là IOPageLockLimit - double click nó và đặt giá trị hexa là - 4000 nếu bạn có 128MB RAM hoặc đặt giá trị 10000 nếu bạn có 256MB RAM ,đặt giá trị là 40000 nếu bạn có nhiều hơn 512MB -tinh chỉnh này sẽ tăng tốc bộ nhớ cache của đĩa.

Khởi động lại

Không thể xóa file AVI khỏi ổ cứng

XP giữ các file trong bộ nhớ ngay cả khi bạn đã đóng ứng dụng sử dụng chúng làm cho chúng không thể bị xóa khỏi ổ cứng. Để sửa nó:

Start -> Run -> Regedit
Đến khóa HKEY_CLASSES_ROOT\SystemFileAssociations\.avi\shel lex\PropertyHandler\ directory và xóa khóa "DEFAULT".

Tinh chỉnh tập tin hoán đổi (SWAP FILE hay Page File)

Với những người dùng có 256 MB RAM hoặc hơn, tinh chỉnh này sẽ nâng hiệu suất của Windows và Game lên.
Nó sẽ làm gì: nó bảo Windows đừng sử dụng Swap file cho đến khi thực sự không còn RAM trống nữa.

Mở System Configuration Utility bằng cách gõ msconfig trong hộp RUN, ấn Enter

. Trong file System.ini bạn phải thêm dòng: "ConservativeSwapfileUsage=1" dưới phần 386enh.

Khởi động lại Windows và thưởng thức hiệu suất Game tốt hơn.

Loại bỏ các dịch vụ(Service)

XP Pro chạy rất nhiều dịch vụ theo mặc định mà điều này là vô nghĩa nếu bạn không ở trong Một mạng cộng tác, những dịch vụ này là những cái bạn có thể loại

bỏ an toàn do đó giải phóng bộ nhớ, nhưng cần kiểm tra xem mỗi cái đó làm những gì trước khi bạn chắc chắn không sử dụng nó:

Vào Start -> Run và gõ services.msc, click chuột phải vào mỗi dịch vụ, vào properties và chọn disable.

Alerter
Application Layer Gateway Service,
Application Management
Automatic Updates
Background Intelligent Transfer
Clipbook
Distributed Link Tracking Client
Distributed Transaction Coordinater
Error Reporting Service
Fast User Switching Compatibility
IMAPI CD-Burning
Indexing Service
IPSEC Services
Messenger
Net Logon
Net Meeting
Remote Desktop Sharing
Network DDE
Network DDE DSDM
Portable Media Serial Number
Remote Desktop Help Session Manager
Remote Registry
Secondary Logon
Smartcard
SSDP Discovery Service
Telnet Themes
Uninterruptible Power Supply
Universal Plug and Play Device Host
Upload Manager
Webclient
Wireless Zero Configuration
WMI Performance Adaptor

Tăng tốc hệ thống FILE

NTFS là một hệ thống file tuyệt vời, nhưng bộ những tính năng của nó đi kèm với sự giảm hiệu suất nhỏ. Bạn có thể khắc phụ điều này với những mẹo sau:

* Theo mặc định NTFS sẽ tự động cập nhật tem giờ mỗi khi một thư mục được truy cập. Đây không phải là một tính năng cần thiết,và nó giảm tốc độ những ổ đĩa lớn. Loại bỏ nó bằng cách vào Run và gõ regedit:
Đến khóa:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Contro l\FileSystem và thiết lập giá trị 'DisableNTFSLastAccessUpdate' bằng 1.

* NTFS dùng các file chính rất khác nhau kiểm soát các bảng để lưu trữ thông tin về hệ thống file của các ổ đĩa. Cùng với thời gian những file MFT này lớn lên và bị phân mảnh, làm chậm tất cả các truy cập đến ổ đĩa. bằng cách thiết lập dự trữ một khoảng trống nhỏ, MFT's có thể lớn lên mà không bị phân mảnh.

Trong cùng khóa với nơi bạn đã loại bỏ tính năng truy cập trước đây, tạo một giá trị DWORD mới là 'NtfsMftZoneReservation' và cho giá trị bằng 2.

Hủy bỏ DLL Caching (lưu trữ DLL)

Windows Explorer vẫn lưu trữ các DLL (Dynamic-Link Libraries) trong bộ nhớ trong một thời gian sau khi ứng dụng sử dụng chúng đã được đóng. Điều này có thể làm việc sử dụng bộ nhớ không hiệu quả. Cách hủy bỏ:
Vào Registry(Start -> Run -> gõ Regedit, Enter)

1. Tìm đến khóa
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Explorer].

2. Tạo một giá trị DWORD mới tên là 'AlwaysUnloadDLL' và thiết lập giá trị bằng 1 để hủy bỏ DLL caching trong bộ nhớ.

3. Khởi động lại Windows để các thay đổi có hiệu lực.

Tweak The Prefetch
1. chạy "Regedit"

2. Đến khóa [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher]

3. Thiết lập giá trị 0-hủy bỏ, 1-App launch prefetch, 2-Boot Prefetch, 3-Both (đề nghị dùng số "3").

4. Khởi động lại.

Nó sẽ giảm thời gian khởi động nhưng gấp đôi và tăng hiệu suất của WinXP.

Tăng tốc kết nối Internet đến 20% (Cable Users Only)

1.Đăng nhập với tài khoản "Administrator".
2. Start -> Run -> gõ gpedit.msc ,Enter
3. Mở nhánh "Local Computer Policy".
4. Sau đó mở nhánh "Administrative Templates" (dưới user Configuration).
5. Mở nhánh "Network".
6. Điểm sáng "QoS Packet Scheduler" ở ô bên trái.
7. Trong ô cửa sổ bên phải double-click vào thiết lập "Limit Reservable Bandwidth".
8. Trong nhãn settings chọn "Enabled".
9. Thay đổi "Bandwidth limit %" bằng 0.
10. Và đến các kết nối mạng của bạn Start=>Control Panel>Network & Internet connections>Network Connections và click chuột phải vào kết nối của bạn. Sau đó trong nhãn General hay Networking , (Nơi nó liệt kê các giao thức của bạn) chắc chắn rằng QoS packet scheduler được kích hoạt.

Nó có thể có hiệu quả ngay lập tức trên một vài hệ thống. Để đảm bảo chắc chắn hãy khởi động lại.

Tôi không khuyên bạn làm tất cả cũng một lúc, làm một động tác sau đó khởi động lại để chắc chắn, Tôi không chịu trách nhiệm về những gì xảy ra với máy của bạn. Hy vọng mọi người thấy nó hữu ích.

Ok, Đây là cách để thay đổi chữ Start trong nút Start thành chữ khác.

Tôi đã hoàn thành nó trong **Windows XP Pro SP1**

Để thay đổi chữ Start trong nút Start:

1. Tạo một bản sao của Explorer.exe
2. Mở file Explorer.exe mới sao trong một trình biên tập
Hexa.(WinHex,hexWorkshop, Hiew)
3. đến Byte 4208Eh và thay đổi "s t a r t" thành bất cứ gì bạn muốn. Bạn phải để các khoảng trống(Space) ở giữa. Nếu từ bạn muốn thay thế cho Start ít hơn 5 ký tự thì cứ điền vào ký tự còn lại bằng khoảng trống.

Nếu từ bạn muốn thay thế Start có hơn 5 ký tự, tìm một byte có giá trị 05h trực tiếp trước chuỗi "s t a r t". Thay đổi các giá trị của Byte đó bằng với chiều dài của chuỗi mới(chuỗi thay thế Start). Để thêm chuỗi vào bạn phải thêm các bytes vào, đừng tiếp tục gõ dữ liệu nhiều hơn Sau 5 bytes đầu tiên trong chuỗi start.
(c) www.ocforums.com
Tổng hợp và biên dịch bởi Freewarez

Thủ thuật tối ưu Windows XP

"Là phần mềm tăng tốc Windows XP Professional tốt nhất hiện nay ? Bảo đảm 100% rằng có thể nâng 200~300% tốc độ hiện tại của máy bạn ? Hàng ngàn người đã sử dụng và được nhiều rất nhiều trong số họ khuyên dùng ? Buy now để đón lấy tiện ích quý báu này trước khi bạn đánh mất nó trong tương lai !".....
Nghe nhiêu đó, bạn và Silvery Hat Hacker đủ biết là quảng cáo nhảm. Nhưng chúng ta đôi khi vẫn cứ tin và xài thử. 1 số may mắn không có vấn đề gì, 1 số kết cuộc bị lấy hậu quả năng nền như không thể vào lại Windows, hệ thống hoạt động không ổn định như trước, máy chậm hẳn, màn hình nổ cái đùng...Nói không phải giỡn nhưng, Silvery Hat Hacker chắc chắn đôi khi bạn gặp tình huống như thế.
Silvery Hat Hacker cũng đồng ý rằng 1 số phần mềm đáng giá như TweakUI, PowerToys là cần thiết để thiết lập cho máy bạn những tính năng mở trong Windows XP - giúp máy hoạt động đúng hiệu suất và cải thiện tốc độ. Nhưng đôi khi khó cho người sử dụng vì chúng bằng Tiếng Anh, giải thích mập mờ,...1 bước nhầm lẫn sẽ dẫn đến hư hại không ngờ trước được. 1 lần nữa, theo câu hỏi của các người bạn và ý kiến của họ, Silvery Hat Hacker cố gắng viết lại hầu hết các kinh nghiệm sử dụng Windows XP của mình , nhưng thủ thuật đã học được đã chia sẻ cho nhưng bạn chưa biết rành có cơ hội học tập lại. Silvery Hat Hacker mong rằng công sức bỏ ra trong bộ bài viết này sẽ không là uổng phí...

A\ TỰ TAY TĂNG TỐC WINDOWS :

1/Lấy trình điều khiển mới nhất đi bạn :

-Có 1 lý do vì sao Silvery Hat Hacker luôn đề cập đến vấn đề này trong hầu hết các câu trả lời về tăng tốc windows XP. Là bước đầu tiên phải đạt được , khi bạn có trình điều khiển mới nhất đồng nghĩa với việc giúp cho Windows quản lý phần cứng tốt hơn và tránh bị lửi hơn. Trong suốt qua trình sử dụng driver mới , bạn đã cho tăng tốc cho Windows rất nhiều. Tuy nhiên , nếu không có điều kiện để cập nhật driver cho tất cả các phần cứng , bạn cố gắng tìm cho ra trình điều khiển cho 1 số hardware được xem là cực kỳ cần thiết theo thứ tự sau : Card màn hình, Driver cho Chipset trong mainboard (còn gọi là FirmWare). Còn nhưng phần cứng khác như bàn phím , chuột , hay các thiết bị USB thì không cần phải tiến hành thường xuyên. Chúng chỉ nên được thay thế driver khi bạn đã có kinh nghiệm xử lý các vấn đề phần cứng nâng cao.

+Cố giải quyết :

- Bạn gắn 1 thiết bị USB vào cổng USB 2.0 trên máy mình. . . . . .không có gì xảy ra. Không có hiện tượng nào cho thấy Windows XP nhận ra phần cứng bạn vừa gắn vào. Bạn rút ra , gắn vô lại. . . . . .vô ích. Thất vọng , bạn để sang 1 bên tiếp tục vào Device Manager để tìm hiểu. Bạn nhận thấy Windows trở chậm hơn , hình bị giật , chuột di chuyển chậm chạp , shutdown lâu hơn....Rốt cuộc cái gì đang xảy ra ? Mặc dù được cho là hử trợ tốt USB 2.0 , tuy nhiên Windows XP vẫn còn gặp rất nhiều lửi trong việc quản lý chính các cổng USB 2.0 có trên bo mạch. Điều này có thể khiến bạn tương nhần thiết bị mình gặp vấn đề nhưng thật ra là do Windows đã không hoạt động với driver mặc định của nó đối với cổng USB 2.0. Nếu bạn bắt gặp USB 2.0 Enhanced Host Controller Driver trong phần driver USB , bạn chắc chắn không sử dụng được 1 số thiết bị HighSpeed USB 2.0. Lý do là vì trình điều khiển này không hoạt động với 1 số USB 2.0 của mainboard Intel. Bạn nên sớm vào www.microsoft.com tìm bản sửa lửi hay driver để sửa vấn đề này. Nếu bạn không tìm ra hay khi download về báo thiếu Service Patch 1 thì bạn hãy liên hệ với để nhận được bộ driver sửa lửi này.

-Bạn vô tình cài nhầm driver cho chuột hay bàn phím và bây giờ chúng không hoạt động ? Nhấn F8 trong quá trình khởi động máy để vào chế độ Safe Mode , cài lại driver cho chúng. Mọi thứ bạn cần là sự bình tĩnh. Thế thôi.

2/Hiệu ứng hình ảnh trong giao tiếp giữa Windows và người dùng :

-Bạn đừng suy nghĩ nhiều về cái tên khá dài bên trên ấy. Thật ra nó chỉ là hiệu ứng đồ họa trong Windows XP thôi. Như là bóng mờ trên Menu Start , cửa số động , bóng mờ trên trỏ chuột...Tất cả những thiết lập ấy tạo cho Windows một dáng vẻ

hòan mỹ. Nhưng sự hòan mỹ ấy chẳng phải là hòan hảo. Hiệu ứng càng chi tiết , công sức của Card màn hình bỏ ra càng nhiều khiến hệ thống bị trì trệ. Nếu là người dùng đòi hỏi tốc độ và không cần rườm ra , bạn hãy loại bỏ nhưng thiết lập mặc định của Windows XP này.

+Đầu tiên , bạn vào System Properties bằng phím Windows + Pause/Break hay trong Control Panel/System hoặc chọn Properties trong Menu chuột phải của biểu tượng My Computer trên màn hình. Tiếp đến , bạn nhìn lên tìm thẻ Advanced , mục Settings của khung Performance. 1 menu mở ra , bạn tìm đến Visual Effects , đánh dấu chọn cho "Adjust for best performance". Vậy là xong. Bạn cũng có thể tự đánh dấu chọn cho một số hiệu ứng, không bắt buộc phải bỏ hết.
+ Ý nghĩa các hiệu ứng

*Animated windows when minimizing and maximizing : Hiệu ứng cho cửa sổ Windows mửi khi đóng hoặc mở

*Fade or Slide menus into view : Hiệu ứng mờ-rõ dần hay lướt qua-dừng khi xuất hiện của các Menu (Danh sách)

*Fade or Slide Tooltips into view : Hiệu ứng mờ-rõ dần hay lướt qua-dừng khi xuất hiện của các Tooltip (các thông báo chỉ dẫn , trợ giúp)

*Fade out menu menu items after clicking : Hiệu ứng rõ-mờ dần khi bạn đóng hay thực thi 1 lệnh trong Menu

*Show shadows under menus : Bóng mờ bên dưới menu

*Show shadows under mouse pointer : Bóng mờ bên dưới trỏ chuột

*Show translucent selection rectangle : Hiển thị khung hình chữ nhật xuyên suốt khi chọn các biểu tượng

*Show window content while dragging : Hiển thị nội dung cửa sổ khi kéo

*Silde open combo boxes : Rớt xuống từ từ-dừng đối với hộp danh sách đổ xuống

*Slide taskbar button : Hiệu ứng lướt qua-dừng đối với các cửa sổ hiển thị trên thanh Task bar

*Smooth edges of screen fonts : Làm sắc nét font chữ

*Smoot-scroll list boxes : Làm sắc nét thanh cuộn các hộp danh sách lựa chọn

*Use a background image for each folder tyoe : Sử dụng hình nền cho các loại folder , như MP3 , hình ảnh , Text ...

*Use common task in folders : Dùng menu tiện ích bên trái cho các folder

*Use drop shadows of icon labels on the desktop : Dùng hiệu ứng bóng đổ cho các nhãn của những biểu tượng trên màn hình

*Use windows visual styles on windows and buttons : Hiệu ứng giao diện chung cho tòan bộ cửa sổ , nút bấm.. của windows
- Silvery Hat Hacker đã liệt kê ra hết các tính năng tùy chọn của việc thiết lập hiệu ứng hình ảnh của Windows XP , một số nên bỏ đi , còn 1 số bạn nền giữ lại cho tiên lợi trong quá trình dùng Windows. Tùy theo mửi người chúng ta mà có 1 cách chọn khác nhau. Điều này không gây nguy hại cho hệ thống.

+ Thủ thuật :

-Ngọai trừ bỏ bớt hiệu ứng hình ảnh , bạn nên dọn bớt những biểu tượng trên màn hình , phần giúp dễ nhìn hơn và một phần giảm bớt sức năng cho card màn hình. Nếu không dùng đến chúng , theo ý kiến riêng , Silvery Hat Hacker đề nghị bạn đem Shortcut của các ổ đĩa có trong máy bạn để vào thanh Quick Lauch , trên màn hình , nhấn phải vào Arrange Icons , bỏ chọn mục "Show Desktop Icons". Vậy là công việc đồ họa trên màn hình Desktop được giảm đi rất nhiều. Nâng cao quá trình xử lý các vấn đề khác của CPU...

3/Đóng các ứng dụng đang chiếm tài nguyên hệ thống :

-1 số nhiều các phần mềm được lập trình không chuyên hiện nay có đầy trên mạng. Bạn vô tình tải nó về và sử dụng nhưng càng chạy lâu bao nhiêu thì máy càng trở nên chậm chạp bấy nhiêu....Windows bạn khởi động vào quá chậm vì phải tải nhưng phần mềm định sẵn. Nhiều lý do khiến cho máy bạn chậm chạp năng nề , nhưng yếu tố chính vẫn liên quan 1 phần lớn đến tài nguyên hệ thống. Khi bạn đóng bớt những ứng dụng không cần tới thì bạn đã giải phóng 1 lượng lớn năng lực họat động của CPU. Vì vậy , ngòai việc cài đúng Driver , giảm công việc cho Card màn hình , bạn cũng luôn phải chú ý đến CPU , bộ não của tòan bộ máy nữa.
-Để dẹp mấy chương trình này , một cách tận gốc , bạn phải ghé thăm Registry và thư mục StartUp và dọn tất cả những khóa , tập tin linh tinh. Nghe như dành cho

người dùng chuyên nghiệp vậy , bạn đừng lo , Silvery Hat Hacker khuyên bạn , nếu là người mới , đừng nên đụng chạm đến Registry mà hãy dùng Msconfig để mà hiệu chỉnh. Từ Menu Start , lệnh RUN , bạn đánh vào msconfig.exe. Một ứng dụng sẽ xuất hiện gồm có 6 thẻ , đó là :
+General : chọn kiểu khởi động

*Normal StartUp : khởi động bình thường

*Diagnostics StartUP : chỉ khởi động máy kèm theo những dịch vụ , thiết bị cần thiết. Không gọi các ứng dụng nào khác

*Selective StartUP : Tự chọn thành phần khởi động - Bạn đừng nên đụng đến cái này nếu không biết rõ mình đang làm gì.

2 nút bấm ở dưới Launch System Restore - hồi phục bản sao lưu cuối cùng và Expand file - hồi phục 1 tập tin bị hư hỏng nào đó.

+System Ini , Win Ini , Boot Ini : Tốt nhất là để yên cho chúng bạn àh.

+Services : Những dịch vụ chạy theo Windows. Đây là 1 trong những tác vụ tốn nhiều tài nguyên hệ thống nhất. Chúng ta sẽ trở lại đề tài này trong chủ đề kết tiếp

+StartUP : Nơi chứa những phần mềm sẽ được gọi khi Windows khởi động.

Cốt lõi của Phần 3 này tập trung vào đây. Bạn bỏ chọn những trình nào không cần thiết và nhấn Ok hay Apply , đơn giản. Nhưng mà , lựa chọn để bỏ 1 phần mềm không phải là đều dễ dàng. Bạn đừng vội vàng mà bỏ hết. 1 số dịch vụ cần thiết cho phần mềm nào đó. Trước khi quyết định bỏ 1 phần mềm , trong bảng StartUP đó , bạn đọc mục Location ở dưới 1 chút. Tìm hiểu kỹ đường dẫn đó được liên kết đến tập tin nào. Từ đó có cơ sở rõ ràng để an tâm loại bỏ nó. Nếu thủ thuật trên vẫn chưa đưa cho bạn 1 lợi ích nào , cố thử tìm tập tin đó , nhấn phải , chọn mục Properties , thẻ Version. Từ đây bạn có thể tìm hiểu về Nhà sản xuất , phiên bản , tên thật của tập tin đó.

-Một chú ý nho nhỏ , bạn đừng bao giờ bỏ các ứng dụng nào có liên quan đến chữ RUNDLL32. Bạn có thể sẽ phá hoại 1 tác vụ nào đó của Windows.

-Sau khi đã bỏ nhưng thứ không cần thiết , bạn khởi động lại máy là xong. 1 chút khó khăn nhưng bù lại kết quả nhận được rất xứng đáng với công sức bỏ ra.

4/Loại bỏ các dịch vụ không cần đến :

-Như Silvery Hat Hacker đã nói qua ở Phần 3 - Services (các dịch vụ) là 1 trong những tính năng mới của Windows XP nhằm hử trợ tôt hơn cho các nhóm người dùng WinXP như hử trợ mạng không dây, quản lý SmartCard.... Nhưng nếu bạn không thuộc nhóm người dùng chuyên nghiệp thì bạn đâu cần đến nhưng dịch vụ chuyên nghiệp phải không ? Đã đến lúc tắt bớt một vài trong số chúng rồi. Theo Control Panel để vào được Administrative Tools, nhìn trong cửa sổ bạn nhận thấy nhiều biểu tượng, tìm đến Services và click chúng. 1 menu mới mở ra , cẩn thận bạn từng bước mở lớn của số này ra...Trong màn này , 1 số tác vụ bạn phải biết trước khi vượt qua được bao gồm như sau :

-Muốn bỏ 1 dịch vụ , bạn 2 lần nhấn trái lên dòng hiển thị dịch vụ đó .Menu mới lại xuất hiện. Ngay giữa tầm nhìn mắt bạn , có dòng chữ nằm phía bên trái ghi là Startup type. trong hộp danh sách đổ xuống bên cạnh, bao gồm 3 lựa chọn Disable (Vô hiệu hóa) , Manual (Người dùng quyết định cho chạy hay không) và cái đầu tiên là Automatic (Tự chạy). Vô hiệu hóa 1 dịch vụ nào đó dẫn đến rắc rối về sau ,bạn lập tức trở lại khu vực này , mở lại dịch vụ đó để tránh gặp thêm nhiều phiền phức. Nếu còn do dự không biết nên đóng dịch vụ nào ,Silvery Hat Hacker sẽ liệt kê 1 số có thể được-bị vô hiệu hóa :
*Clipbook : Bạn có muốn chia sẽ những gì lưu trong Clipboard của mình cho một ai đó thông qua mạng không ?

*Application Management : Bạn không dùng chung 1 mạng với ai đó ? Bạn không không có ý định điều khiển 1 trình nào đó thông qua mạng ? Nếu không hãy vô tư mà Disable nó.

*Distributed Link Tracking Client : Quản lý các Shortcut đến tập tin trên Server nào đó . Nếu bạn đã vô hiệu hóa 2 dịch vụ trên thì cũng nên bỏ luôn cái này.

*Error Reporting : Tự động thông báo lửi có thể là 1 tính năng khá tốt nhưng đôi khi lại quá làm phiền và vô dụng.

*TPC/IP NetBIOS Helper : Bạn chỉ dùng cài này khi bạn dùng NetBIOS trên hệ mạng TCP/IP của mình.

*Messenger : Vào năm trước , những kẻ Spammer đã nhận ra 1 cách có thể gửi hàng triệu Spam đến người dùng WinXP thông qua Messenger này. Loại bỏ dịch vụ này là lựa chọn sáng suốt

*Remote Registry : Bạn có muốn ai khác ngòai bạn quản lý bộ não của WindowsXP không ?

*Telnet : Cho phép ai đó đăng nhập vào máy bạn và làm bất kỳ cái gì họ muốn xem ra là một ý kiến tuyệt vời đáng lưu truyền cho hậu thế ?

*Event Log : Bỏ. Nhiệm vụ của nó chỉ là ghi lại những báo cáo đôi khi khó hiểu.

*Fast User Switching Compatibility : Nếu bạn không dùng máy chung với nhiều người thì vô hiệu hóa cái này tăng năng lực cho máy rất nhiều.

*Help and Support : Sự trợ giúp là 1 điều quý báu nhất là khi ta gặp khó khăn. Nhưng nếu bạn không rành Tiếng anh và không biết nó nói cái gì....

*IMAPI CD-Burning COM Service : Thật sự ra dùng Nero ghi đĩa trực quan hơn dịch vụ có sẵn trong WinXP này.

*NetMeeting Remote Desktop Sharing : Không muốn chia sẻ với ai bất cứ cái gì trên máy bạn thông qua NetMeeting ? Không = Disable

*Remote Desktop Help Session Manager : Đừng để ai đó điều khiển máy bạn nếu bạn không muốn bị vậy

*Smart Card và Smart Card Helper : ...Nếu bạn không dùng các thẻ nhớ thì bạn biết phải làm gì với dịch vụ này.

*Task Scheduler : Quản lý các dịch vụ chạy theo định kỳ hay xếp sẵn. Tùy bạn thôi

*Wireless Zero Configuration : Bạn dùng mạng không dây ? Sướng nha. Nhưng Silvery Hat Hacker phải vô hiệu hóa nó.

*Automatic Updates : Bạn muốn máy tự động cập nhật Windows. 1 số trường hợp quay số kết nối để cập nhật mà chủ nhân không biết. Trả tiền cước hàng triệu đồng...Ơ...Thôi để Silvery Hat Hacker dẹp cái này vậy. Nếu cập nhật mà không mấy hiệu quả thì không cần cập nhật, ngọai trừ các lổ hổng bảo mật lớn thì tự vào website microsoft cập nhật thôi.

B\BẢO MẬT CHO MÁY TÍNH

1/Thiết lập tường lửa :

-Bạn không biết tường lửa là gì ? Hãy vào bài viết "Tường lửa là gì ?" để tham khảo. Trong tài liệu này , Silvery Hat Hacker chỉ gợi ý những phương thức bảo mật chứ không đi sâu vào tính năng của mửi phần mềm.

-Trong hầu hết chúng ta hiện nay liên kết vào hệ thống mạng lưới máy tính tòan cầu đều sử dụng kết nối thẳng , cho dù sử dụng Modem hay Boardband , đều nên thiết lập cho riêng mình 1 hệ thống tường lửa tốt nhằm ngăn chặn các xâm nhập vào-ra bất hợp pháp , mà nạn nhân ở đây đôi khi là chính bạn chứ không phải là máy tính. Silvery Hat Hacker khuyên bạn dùng Zone Alarm và luôn để nó trong chế độ hoạt động mửi khi bạn vào Internet. Đây là 1 công cụ không thể thiếu đối với chúng. Hết

2/Cài đặt trình chống Virus :

-Trình Anti-Virus đã trở nên rất cần thiết cho máy tính hiện nay. Trái với việc xâm nhập bất hợp pháp ở trên , nạn nhân ở đây là máy tính chứ không phải là bạn. Nên 1 ngày nào đó bạn chạy 1 tập tin nhận được từ bức email trông rất quan trọng rồi mới nhận ra "Hình như cái này là Virus" thì nếu không có trình Anti-Virus ở đó , rất có thể trong lần khởi động kế bạn không còn gặp được WinXP của mình nữa. Hiện tượng này là căn bệnh thường gặp ở nhiều bạn vì vậy sở hữu 1 trình Chống Virus ở đây được xem là cấp bách. Vào năm trước , Silvery Hat Hacker đề nghị trình tốt nhất là Norton Anti-Virus 2003, nhưng vì Silvery Hat Hacker chưa có cơ hội dùng qua bản 2004 nên không thể đưa ra được ý kiến nào cả. Thay vào đó , AGV 7.0 Free Edition của www.grisoft.com , khá mới mẻ nhưng bạn hãy thử qua. 1 bài viết chi tiết về AGV 7.0 sẽ được Silvery Hat Hacker trình bày trong tháng tới. Nếu bạn không muốn đợi lâu hãy vảo website để tải bản miễn phí về xài trước.

C\TĂNG TỐC ĐỒ HỌA:

-Đây chỉ là 1 phần nhỏ trong bộ tài liệu này , Silvery Hat Hacker sẽ lướt qua khá nhanh. Bạn chỉ cần xem qua cho biết vì việc overclock , cho dù bằng phần mềm cũng khá nguy hiểm cho máy bạn nếu không cẩn thận.

-Hầu hết các Card màn hình hiện nay dư sức để đàm nhiệm một nguồn lớn việc xử

lý điểm ảnh và năng lực để quản lý nhiều dữ liệu gửi đến , vì thế việc tăng tốc Clock sẽ không những mang đến chất lượng hình ảnh tốt hơn mà việc xử lý sẽ lại càng nhanh hơn. Nhưng hãy nhớ rằng việc việc overclock sẽ mang bạn ra khỏi Chế độ bảo hành , chỉ vì Silvery Hat Hacker chưa nghe có ai đã nướng chín Card màn hình của họ qua việc Overclock nên mới bổ sung 1 phần nhỏ về Tăng tốc Đồ Họa cho tài liệu này cho các bạn tham khảo.
-Ngòai trừ các trình Overclock của ATI hay nVidia đã có sẵn , 1 trong những trình Silvery Hat Hacker thích nhất đó là PowerStrip. Tải từ www.powerstrip.com hay trong Website Learning Hacking For Viet , bạn cài đặt nó vào máy rồi khởi động lại. Một khi PowerStrip đã được chạy , 1 biểu tượng Icon sẽ xuất hiện trên System Tray , bạn click phải , chọn Performance\Configure. Lúc này cửa sổ mới nên hiện ra, nổi bật với hai thanh dọc nhiều màu bên trái, thể hiện tốc độ hiện tại của tần số của CPU (Aka core) và tần số xung nhịp của bộ nhớ trên Card (Memory clock). Thanh trượt cho phép bạn di chuyển lên hoặc xuống. Đối với việc tăng tốc xung nhịp này (Core clock) , bạn nên làm theo từng bước của em bé. Chậm , từng khỏang 5MHz 1 lần . Bạn xác nhận lần nữa (Ok) rồi khởi động máy lại. Chạy thử 1 game hay trình Benchmark , chắc chắn rằng không có sự cố nào thì bạn tiếp tục đi lên 5Mhz nữa. Đến khi bạn đã đến sự giớn hạn cho phép và không gặp rắc rối nào, chuyển sang tăng tốc cho bộ nhớ (Memory clock).
Đừng bao giờ tăng Memory clock nhiều như Core clock vì có thể dẫn Card màn hình bạn đến bờ vực núi lửa. Hơn thực tế hơn là hoạt động chập chờn và không ổn định. Đó là tất cả của phần Tăng tốc Đồ Họa này. Bạn hỏi tại sao silvery Hat Hacker không đề cập đến việc Overclock nóng - thay đổi Jumper hay thiết lập cord cho mainboard. Lý do vì nó không đơn giản và cũng không phù hợp với tài liệu này. Nên đành hẹn bạn lại khi khác.
D\SẮP XẾP GIAO DIỆN WINDOWS:

Bên dưới đây có những những thủ thuật có liên quan đến Registry mà Silvery Hat hacker đã có dịp tìm ra hay sưu tầm được. Trước khi thực thi những chỉ dẫn , bạn nên sao lưu cẩn thận Registry - bộ não Windows vào 1 thư mục để đề phòng bất trắc còn có thể phục hồi lại được.

-Khởi chạy Registry , bạn vào Start , lệnh RUN , đánh vào regedit.exe

-Sao lưu tòan bộ, bạn chọn File\Export từ menu file của trình Registry Editor mới hiện ra. Trong Menu bạn thấu sau khi click Export , phía dưới , mục Export Range , bạn nhớ đánh dấu All rồi cẩn thận lựa tên , đường dẫn và sao lưu bản dự phòng này vào 1 thư mục nào đó. Trái lại với việc sao lưu tòan bộ nếu bạn chỉ muốn 1 khóa con thì đừng chọn All mà chọn Select Branch. Mọi thứ chuẩn bị đã hòan tất. Hãy để cho nhưng khám phá được bắt đầu.

1/Lọai bỏ các thư mục lưu trữ không cần thiết :

-Bạn chắc chắn biết rằng Windows có bao gồm các thư mục như My eBooks , My Videos và My Music. Đôi khi bạn không cần thiết dùng đến chúng và bạn muốn xóa nó đi - cho đỡ chướng mắt đó mà. Nhưng chỉ ít phút sau khi bị deleted , trở lại , bạn vẫn còn thấy chúng còn nằm đầy ở đó :

Vào Start , lệnh Run lần nữa , bạn đánh hay copy dòng sao vào :

Regsvr32 /u mydocs.dll

Một thông báo sẽ xuất hiện sau khi bạn click Ok. Từ lúc này trở đi bạn có thể xóa các thư mục My eBooks , My Videos và My Music. Chúng sẽ không quay lại nữa đâu.

2/Dấu Recycle bin từ Desktop :

-Bạn chạy Registry Editor , tìm khóa HKEY_Current_User\Software\Microsoft\Windows\Curre ntVersion\Explorer\HideDesktopIcons\NewStartPanel. Click phải trong khu vực hiển thị thông tin của khóa , bạn con New\DWORD Value. Đặt tên khóa mới là {645FF040-5081-101B-9F08-00AA002F954E}. Thiết lập giá trị cho là 1.

-Nếu bạn muốn phục hồi đặt giá trị lại là 0

3/Đổi màu cho màn hình Logon :

-Khóa HKEY_Users\.Default\Control Panel\Colors , giá trị BackGround. Đổi giá trị hiện tại thành 3 thông số màu sắc RGB mà bạn muốn. Mửi thông số Red , Blue và Green cách nhau bởi khỏang trắng. Ví dụ :

*Màu đen : 0 0 0

*Màu đỏ : 255 0 0

*Màu Silver - Bạc : 241 241 241

4/Dấu các biểu tượng trong System Tray :

-Bạn muốn làm cho Windows trông giống như không có chương trình nền nào đang chạy hay chỉ đơn giản là muốn giao diện dễ nhìn hơn ?

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\Policies\Explorer và đặt 1 khóa DWORD mới với tên "NoTrayItems Display". Gán giá trị 1 để che các Icons trên system Tray và trong lần khởi động kế đến bạn sẽ không còn thấy chúng nữa.

5/Vô hiệu hóa tính năng xem trước ảnh

-Xóa khóa HKEY_CLASSES_ROOT\SystemFileAssociations\image\She llEx\ContextMenuHandlers\ShellImagePreview. Nhưng bạn nhớ sao lưu trước.

6/Học các phím tắt của Windows :
Alt + Tab : Chuyển đổi giữa các cửa sổ
Alt + d : di chuyển dấu nhắc trong cửa sổ IE đến khu vực Address bar
Shift trong suốt quá trình để CD vào ổ nhằm tạm thời vô hiệu hóa tính năng tự động AutoPlay
Phím Windows + Pause/Break dẫn bạn đến system Properties
Phím Windows + f mở cửa sổ tìm kiếm
Phím Windows + e mở cửa sổ Explorer
Phím Windows + d : thu nhỏ tất cả cửa sổ tác vụ
E\TỐI ƯU HIỆU SUẤT WINDOWS XP NGÀY-QUA-NGÀY:

1/Giám sát hiệu suất CPU trực quan trên System Tray :

-Chỉ đơn giản là đánh dấu chọn Option\Hide when minimized trong menu file của tác vụ Task Manager(Ctrl +Alt + Delete) . Nếu bạn muốn luôn giám sát hiệu suất CPU thì có thể tạo 1 shorcut để vào StartUp là xong

2/Tự động dọn dẹp ổ cứng :

-Bạn muốn đĩa cứng lúc nào cũng gọn gàng , luôn sẵn sàng chạy ầm ầm mửi khi bạn ngồi vào máy ? Silvery Hat Hacker cũng thế. Vậy thủ thuật đơn giản hiệu quả mà ai cũng biết là cái gì đó ở đầy chính là Dọn dẹp đĩa cứng. Nhưng nếu bạn đã đọc đến đầy của tài liệu này , đã thao tác thành thạo những thủ thuật ở trên , giờ đây Silvery Hat Hacker nên gọi bạn là người Sành điệu rồi. Đối với bạn , ngồi để nhấn Dọn dẹp đĩa cứng bằng tay thật mất thời gian. Tại sao không để cho máy tự

động ? Bạn có thể xếp lịch nhưng không biết.....Vậy muốn được thế ta phải đánh dòng sau vào (Chỉ Silvery Hat Hacker đánh thôi , bạn copy rồi paste)...

```
C:\windows\system32\cleanmgr.exe /dc /sagerun: 1
C:\
D:\
e:\
cd\
cd c:\windows\prefetch
del *.* /q
```

Thế đấy bạn àh. Sao khi đã copy và dán vào 1 tập tin Text nào đó , bạn nhớ đổi kiểu tên file thành *.bat. Mục đích của file Bat trên là dọn dẹp tất cả những tập tin không cần thiết có trên các ổ cứng của bạn 1 cách tự động 95% (Vì bạn phải click nó mới chạy). Tất nhiên bạn có thể để nó vào StartUp là trở thành 100% đó thôi.

3/Tắt Windows nhanh :

-Nếu đã hiểu qua từ trước , chắc chắn bạn biết Silvery Hat Hacker muốn nói đến cái gì. 1 shorcut.
+Nhấn phải trên Desktop , bạn chọn New\Shorcut.

+Trong Menu trước Đường dẫn (Location) , bạn copy vào :

```
shutdown.exe -s -t 0
```

+Đó là tất cả. Nhưng thủ thuật ở đây Silvery Hat Hacker đã trích lược ra đến mức dễ dàng nhất có thể. Bạn đừng lo nó sẽ mang đến nhưng rắc rối cho mình. 1 chút khám phá và tìm hiểu sẽ mang lại cho bạn nhiều kinh nghiệm sử dụng máy tính hơn.

+Bạn có thể đổi Icon cho Shorcut tắt máy này như sau : Click phải lên Shorcut - Properties , mục Change Icons trong thẻ Shortcut. Thông báo lửi sẽ xuất hiện nhưng bạn đừng lo cứ tiếp tục. Menu mới sẽ chứa các biểu tượng Icon bạn có thể tùy chọn.

+Bạn có muốn biết Shortcut khởi động nhanh ? Không ! Vậy thì nó đây :

shutdown.exe -r -t 0

Đừng nói dối nữa , Silvery hat Hacker biết bạn thích và muốn tìm hiểu mà.

F\TỐI ƯU HIỆU ỨNG ÂM THANH CHO WINDOWS

1/Thiết lập đúng dạng xuất âm thanh :

-Nếu bạn giống Silvery Hat Hacker, bạn nghe nhạc suốt ngày bên máy tính ngay cả khi làm việc , khi ăn , uh , khi ăn. Nhưng cuối cùng bạn cũng phải có lúc chuyển sang dùng Headphone-Tai nghe để thưởng thức âm nhạc vì vợ bạn ngủ , bồ bạn ngủ (đừng nghĩ lung tung).....Nói dài dòng như thế để có câu mở đầu dẫn đến chủ đề chính của chương này. Đó là bạn phải hiểu rõ việc đổi giữa Jack cắm âm thanh của Speaker qua Headphone không chỉ đơn giản là rút ra-cắm vô. Các Sound card hiện đại ngày nay sử dụng những thuật tóan nâng cao cực kỳ phức tạp để mã hóa xuất ra âm thanh. Định dạng đầu ra này đòi hỏi sự thiết lập tương thích chính xác với các lọai Speakers thông thường hiện nay. Nhưng Headphone là vật khác Speakers mà. Vì vậy hiện tượng bị bóp méo chất lượng hay nhiễu cũng là điều hiển nhiên.
Để chỉnh đúng , nếu không có trình đi kèm sẵn (như Mixer của Creative) , bạn đi qua Control Panel đến Sounds and Audio Devices. Trong khung Speaker Settings , bạn nhấn Advanced và chọn kiểu đầu xuất tương thích với thiết bị gắn vào.

2/Hiệu chỉnh chế độ âm thanh Stereo :

-Nếu bạn đã đặt loa 5.1 hay 7.1 vào máy thông qua sự hử trợ của Sound card , bạn vẫn nhận thấy rằng hình-như-có-lẽ-là âm thanh chỉ đến từ 2 kênh mà thôi.

Chẳng có gì lạ đâu bạn , vì hầu hết các tập tin âm thanh MP3 hay từ đĩa CD hầu hết chỉ là Stereo mà thôi, chúng không thể đạt được chất lượng như DVD hay các trò chơi game Playstation 2 đâu. May mắn thay , hầu như tất cả các thiết bị Sound card ngày nay đều có tính năng khuyếch đại âm thanh , được xem như 1 bộ chuyển đổi và lọc lại đầu vào của file âm thanh đó. Trong những bộ khuyếch đại này , 1 số chia tiếng hát và tiếng bè lên 3 loa trước , nhạc cụ được chuyển qua cac loa sau. Một số khác lại nhân đôi kiểu âm thanh Stereo lên và chia ra cho tất cả các loa. Bạn đã nắm được kiến thức tổng quát về cách thức hoạt động của các sound card 4.1;5.1 đến 8.1 hiện nay. Nếu như bạn đã có 1 bộ đồ chơi âm thanh tuyệt như vậy , để kích hoạt tính năng khuyếch đại này bạn nhìn vòng vòng hộp đựng Sound card , nếu tìm thấy dấu chọn cho mục CMSS hay CMSS2 nghĩa là tự khắc Sound card của bạn đã có tính năng này.

3/Đầu vào âm thanh tốt , đầu ra quá tệ :

-Các chương trình khá nổi tiếng như WinAmp và nhiều trình chơi DVD mặc định sử dụng phần Wave-out cho âm thanh. Không may thay , Wave-out , tác vụ này là thông qua phần mềm để xử lý và ngốn rất nhiều tài nguyên hệ thống lẫn năng lực của CPU. Có thể điều đó không thành vấn đề nếu bạn đặt vào mainboard con Pentium 4 3.2 Ghz hoặc Athlon 64 FX. Nhưng bỏ tiền ra mua Sound card tốt như Creative, nForce2 có chip giải mã âm thanh xịn để làm gì ? Thay vào đó bạn làm tốn thêm sức lực CPU để tự giải mã âm thanh, Silvery Hat Hacker nhận thấy đó không là quyết định sáng suốt....Bây giờ bạn chắc chắn hiểu rồi, giải pháp ở đây là dùng DirectSound (Âm thanh truyền thẳng , tạm dịch vậy). Nếu trong bất kỳ trình Multimedia nào có thiết lập âm thanh liên quan đến DirectSound , bạn nên chọn tính năng này nhằm giảm bớt công việc phải xử lý âm thanh của CPU.
G\THỦ THUẬT MỘT VÀI ỨNG DỤNG

1/Chạy nhanh trình gửi email của Outlook :

-Thỉnh thoảng , bạn chỉ muốn gửi 1 email nhanh chóng mà không phải mất công chạy ứng OuTLoOk khá nặng nề. Để chạy tác vụ gửi mail nhanh của Outlook , bạn tạo 1 Shortcut , trong mục Location , bạn gõ vào "mailto:". Đó là tất cả.

2/Trình TweakMP :

-MP là chữa viết tắt của Media Player. Và chính xác như tên gọi của nó bạn àh. Nếu bạn đã khám phá đầy đủ với TweakUI, phần mềm để hiệu chỉnh các thông số ẩn cho hệ thống Windows XP và những phiên bản khác. Nhưng không , đối TweakMP này, bạn sẽ sắp thay đổi các thiết lập cho trình nghe nhạc khá nổi tiếng được đi kèm theo WinXP - Windows Media Player.Bạn có thể chỉnh cho thời gian xuất hiện thanh công cụ trong chế độ Tòan màn hình tắt nhanh hay chậm hơn, hay vài hiệu chỉnh nhỏ trong việc copy âm thanh từ CD . Tuy rằng những hiệu chỉnh có trong TweakMP không nhiều những bản update sẽ hứa hẹn nhiều tính năng mới hơn.

3/X-Setup :

-Xuất hiện chỉ mới 1 năm trở lại đây tính từ đầu năm 2003 đến đầu năm 2004
-Vượt qua mặt cả TweakXP về số lượng thiết lập các thông số ẩn trong WinXP
-Khó hiểu và dễ dùng
-Không dành cho nhưng bạn chưa rành lắm về Registry

-Mức độ "có thể gây nguy hiểm" cho máy bạn là 3/5
http://www.majorgeek.com/esselbachfp.php?in=allinone/xsp-setup-en.zip,1075643716O934b535800b1cba8f96a5d72f72f1611df5354693177e83e8ba089e94b7b6b55%20 (4.2 Mb)

H\TĂNG TỐC KHỞI ĐỘNG CHO WINDOWS

Sau đây là một số thư mục có thể xóa được và không ảnh hưởng gì tới Windows mà còn làm Windows khởi động nhanh hơn nhiều.

1.C:\WINDOWS\DOWNLOADED INSTALLATION xóa nó đi không ảnh hưởng gì cả.

2.C:\WINDOWS\DRIVER CACHE (hoặc trong system32\drivercache) làm giảm quá trình khởi động của XP thì việc gì mà không xóa nó đi.

3.C:\WINDOWS\SYSTEM32\DLLCACHE cũng thế xóa nó còn tiết kiệm được vài trăm MB (chỉ với XP Pro)

4.C:\ WINDOWS\REGISTEREDPACKAGES hãy xóa toàn bộ tệp tin và thư mục trong đó, tốc độ tăng đáng kể.

5.C:\WINDOWS\PREFETCH xóa hết các tệp tin trong đó tốc độ nhanh hơn khoảng 5->7 giây.

6.C:\WINDOWS\REPAIR cũng không thật cần thiết hãy xóa tất cả những gì trong đó thì tốt hơn.

7.C:\WINDOWS\SYSTEM32\REINSTALLBACKUPS xóa hết nó đi chỉ mất dung lượng mà không được gì.

8. Ngoài ra người nào hay Update XP tren mạng thi trong C:\WINDOWS sẽ tự động tạo ra một thư mục có tên là LASTGOOD thực chất thì thư mục này sao lưu những gì của Windows bao gồm DRIVECACHE, SYSTEM32... xóa nó đi mà không ảnh hưởng gì, tiết kiệm được vài trăm MB đấy

*****Sưu tầm bởi ghost1982@updatesofts.com*****

Thuần phục Windows

Thực hiện: Phương Uyên

---

50 thủ thuật giúp bạn thuần phục Windows, trừ khử sự lộn xộn trong PC và ngăn chặn những phiền toái ngay từ đầu.

Khi gặp điều phiền toái thì có 2 khả năng: hoặc là bạn nổi điên hoặc cam chịu. Tuy nhiên còn có lựa chọn thứ ba: thuần phục nó. Loại bỏ những chương trình, biểu tượng và các dịch vụ Windows không cần thiết và bạn sẽ tống khứ được nhiều phiền toái. Hầu hết những công cụ cần thiết đều có sẵn, chủ yếu là những thủ thuật tinh chỉnh Windows và các chương trình để chúng chỉ làm những gì bạn muốn. Bạn cũng nên thay các chương trình thông dụng nhưng cồng kềnh và tốn kém bằng những chương trình đơn giản hơn. Nếu lỡ quá đà và làm cho PC trở nên 'đờ đẫn', cũng có cách giúp bạn quay lui.

KHỞI ĐỘNG VÀ KẾT THÚC TRƠN TRU

Nhờ sự ổn định của Windows 2000 và XP, giờ đây bạn không còn phải thường xuyên khởi động PC nữa. Nhưng dù sao, với mục tiêu thuần phục Windows, bạn cũng cần tìm hiểu qui trình khởi động. Càng ít chương trình thừa nạp lúc khởi động, Windows càng được kích hoạt nhanh hơn và càng có nhiều vùng nhớ hơn dành cho các ứng dụng. Hơn nữa, kiểm soát các chương trình nạp lúc khởi động sẽ giúp bạn tránh được những phiền toái do phần mềm gián điệp hay virus gây ra.

Bước đầu tiên để giảm tải lúc khởi động là gỡ bỏ các chương trình không dùng đến, đặc biệt là những chương trình luôn đặt biểu tượng ở khay hệ thống (góc dưới trái, chỗ hiện giờ hệ thống). Trước hết hãy tìm trong menu Start biểu tượng gỡ cài đặt (uninstall) ở chung chỗ với biểu tượng chính của chương trình. Nếu không thấy biểu tượng này, hãy dùng công cụ Add or Remove Programs trong Control Panel của Windows, chọn chương trình không cần thiết và nhấn nút Remove hay Change/Remove để thực hiện gỡ bỏ.

Tiếp theo, có thể bạn cần để mắt đến các chương trình vẫn muốn giữ lại nhưng

không phải lúc nào cũng cần chạy. Ví dụ chương trình QuickTime của Apple luôn nạp tập tin qttask.exe lúc khởi động, mỗi khi bạn xem phim QuickTime, chương trình sẽ tự nạp lại vào khay hệ thống. Hãy loại bỏ những chương trình như vậy để giảm tải quá trình khởi động (bạn vẫn có thể dùng chúng khi cần). Để thực hiện việc này, hãy tìm trong tất cả những nơi Windows dùng để gọi các chương trình lúc khởi động và cấm những chương trình không cần.

Giảm tải quá trình khởi động

Có 4 cách để Windows gọi chạy các chương trình tự động lúc khởi động: khai báo shortcut chỉ đến chương trình trong mục Startup của menu Start (Start.All Programs.Startup); khai báo trong registry; khai báo theo kiểu cũ trong tập tin system.ini hay autoexec.bat; hay khai báo trong Computer Management console (nếu chương trình thuộc loại đặc biệt gọi là service - dịch vụ).

Bạn duyệt qua từng nơi và cấm hay gỡ bỏ các tham chiếu đến chương trình không cần chạy mỗi khi khởi động. Một cách dễ dàng để thực hiện công việc này là dùng tiện ích System Configuration của Windows, nó có thể gỡ bỏ những tham chiếu như vậy ở cả 4 nơi (nếu dùng Windows 2000, trước hết hãy tải về công cụ msconfig ở địa chỉ www.perfectdrivers.com/howto/msconfig.html và lưu vào folder c:\winnt\system32).

Hình 1: Gỡ bỏ khỏi menu Startup các chương trình không thật sự cần thiết chạy lúc khởi động Windows

Chọn Start.Run, gõ vào msconfig trong vùng Open và nhấn OK để gọi chạy công cụ. Các chương trình liệt kê ở mục Startup lấy từ registry; mặc dù ít có trường hợp chương trình dùng system.ini hay win.ini để tự khởi chạy, nhưng bạn cũng nên duyệt qua các mục này nếu không tìm thấy ở những nơi khác. Bạn cũng có thể dùng msconfig để quản lý các service, tuy nhiên có cách thức tốt hơn để tắt chúng nhanh chóng.

Để cấm một chương trình khởi chạy, hãy xóa ô đánh dấu chọn ở kế bên nó, nhấn OK và khởi động lại máy. Nếu xảy ra trục trặc, hãy vào lại System Configuration Utility và đánh dấu chọn lại chương trình.

Bạn có thể rút ngắn thời gian khởi động và giải phóng thêm bộ nhớ bằng cách ngừng các service không cần, sau đó thiết lập để chúng không khởi chạy cùng với Windows. Mở Services Console: nhấn phải chuột lên My Computer và chọn Manage. Khi cửa sổ này mở, ở khung bên phải bạn nhấn đúp Services and Applications (hay nhấn vào dấu cộng kề bên) để mở khoản mục này, kế tiếp chọn Services xuất hiện bên dưới.

Services Console hiển thị các service đang chạy ('Started') và cách thức service được kích hoạt: Automatic (kích hoạt mỗi khi hệ thống khởi động, bất chấp bạn có cần hay không), Manual (không chạy lúc khởi động nhưng Windows có thể kích hoạt dịch vụ khi cần), hay Disabled (hoàn toàn không chạy, ngay cả khi Windows cần).

Tất nhiên, việc cấm một hay nhiều dịch vụ mà Windows có lúc cần đến có thể gây nên một vài trục trặc. Bạn có thể tham khảo danh sách các dịch vụ Windows cùng với thông tin chi tiết ở website UK Security Online (www.uksecurityonline.com/husdg/windowsxp/disableservices.htm) để biết những dịch vụ nào có thể cấm an toàn.

Stanby để tăng tốc

Hình 2: Ngưng các service không cần thiết

Dù bạn có loại bỏ bao nhiêu chương trình và dịch vụ, hệ thống vẫn mất nhiều thời gian để khởi động (startup) và kết thúc (shutdown). Có một cách thức tốt hơn để trị bệnh cho PC của bạn: Đưa PC về chế độ Stanby hay Hibernate thay vì tắt hoàn toàn. Stanby tắt nguồn màn hình và các ổ đĩa nhưng vẫn duy trì nguồn cho CPU và bộ nhớ, cho phép bạn 'đánh thức' PC và quay lại với công việc đang làm chỉ trong vài giây. Hibernate ghi thông tin trong bộ nhớ xuống đĩa và tắt PC hoàn toàn; khi khởi động lại, PC sẽ đọc lại thông tin của phiên làm việc được lưu trên đĩa, nhờ vậy bạn có thể vào ngay công việc đang làm trước đó.

Chế độ Hibernate thích hợp cho máy tính xách tay (để tối ưu thời gian dùng pin), còn Stanby thích hợp cho máy tính để bàn. Nhấn đúp biểu tượng Power Options trong Control Panel; chọn mục Power Schemes; thiết lập các tùy chọn màn hình, đĩa cứng và Stanby; sau đó nhấn OK. Để bật chế độ Hibernate, nhấn thẻ Hibernate, đánh dấu chọn Enable hibernation, và nhấn OK. Một số PC, nhất là những PC cũ,

có thể không hỗ trợ chế độ Stanby hay Hibernate; nếu vậy bạn sẽ không thấy thẻ Hibernate.

THANH LỌC DESKTOP VÀ MENU

Đôi khi thật khó biết hiện Windows có những công cụ gì. Để dễ dàng tìm thấy công cụ cần thiết, hãy loại bỏ các biểu tượng trùng trong menu Start, trong thanh công cụ Quick Launch và trên desktop. Có thể bạn muốn một vài biểu tượng xuất hiện ở nhiều nơi, tuy nhiên để đơn giản, chỉ nên bố trí biểu tượng ở nơi thích hợp nhất.

Thanh lọc biểu tượng

Việc gỡ bỏ các phần mềm có tính năng hạn chế hay dùng thử thường không xoá đi shortcut trên desktop. Thật may, Windows XP có cung cấp một công cụ tiện lợi để xoá sạch các biểu tượng desktop không dùng đến. Nhấn phải chuột trên desktop, chọn Properties, nhấn thẻ Desktop và nhấn nút Customize Desktop. Nhấn Clean Desktop Now để kích hoạt wizard tìm các biểu tượng mà gần đây bạn không dùng đến và chuyển chúng vào folder Unused Desktop Shortcuts. Khi chỉ còn lại một ít biểu tượng trên desktop (chẳng hạn như Recycle Bin), hãy liên kết chúng với thanh tác vụ để bạn không phải thu nhỏ các ứng dụng đang làm việc chỉ để nhìn thấy chúng: Nhấn phải chuột lên thanh tác vụ và chọn Toolbars.Desktop. Kế tiếp nhấn chuột phải tên thanh công cụ mới (nếu 'Lock the Taskbar' được đánh dấu chọn, hãy bỏ chọn nó, nhấn chuột phải thanh tác vụ lại để thêm thanh công cụ desktop). Trên menu hiện ra, bạn sẽ thấy các tuỳ chọn thay đổi kích thước biểu tượng và bật/tắt hiển thị tựa đề của thanh công cụ hay tên của biểu tượng.

Menu Start của Windows có khả năng cấu hình cao - nhấn phải chuột nút Start, nhấn Properties, chọn thẻ Start Menu, chọn hoặc là Start menu (mặc định của XP) hoặc là Classic Start (đổi sang dạng menu giống Windows 2000), rồi nhấn nút Customize để hiển thị các tuỳ chọn. Tuỳ sở thích riêng, tuy nhiên bạn có thể loại bỏ 2 biểu tượng trùng trong menu Start mặc định bằng cách bỏ chọn các tuỳ chọn Internet và E-

Hình 3: Dùng Desktop Cleanup Wizard để dọn sạch các icon không dùng đến khỏi desktop

mail (mặc định, các liên kết đến các chương trình này xuất hiện trong thanh công cụ Quick Launch). Nhấn thẻ Advanced để xem thêm các tùy chọn tinh chỉnh. Nếu bạn ít dùng đến các mục sau của menu Start: Favorites, Search, Set Program Access and Default, Help and Support... bạn có thể làm biến mất chúng bằng cách bỏ chọn chúng trong danh sách 'Start menu items' và nhấn OK.

Thanh Quick Launch, nằm ở bên phải nút Start, là phương thức kích hoạt ứng dụng thường dùng thuận tiện nhất - bạn có thể gọi chạy các chương trình ưa thích chỉ với một nhấn chuột (nếu không thấy thanh Quick Launch, nhấn chuột phải lên thanh tác vụ và chọn Toolbars.Quick Launch).

Hãy loại bỏ các biểu tượng ít dùng đến (nhấn chuột phải lên biểu tượng và chọn Delete). Bạn cũng có thể thay đổi kích thước thanh công cụ Quick Launch (kéo thanh ở bên phải thanh công cụ với điều kiện không khoá), sắp xếp các biểu tượng (kéo từng cái một) và giấu đi tựa đề của thanh công cụ và tên của các biểu tượng. Hầu hết chương trình, khi cài đặt với thiết lập mặc định, sẽ đặt biểu tượng trên desktop, trong Quick Launch và trong menu Start - quá 'phung phí'. Để ngăn tình trạng hỗn độn biểu tượng về sau, nên chọn tùy chọn 'custom' khi cài đặt ứng dụng mới để có thể quyết định nơi đặt biểu tượng.

Thanh lọc khay hệ thống

Gỡ bỏ các ứng dụng không cần thiết sẽ làm giảm số biểu tượng trong khay hệ thống, nhưng bạn còn có thể thanh lọc thêm nữa: Windows, các thiết bị phần cứng và các tiện ích hệ thống cài đặt biểu tượng để cho phép truy cập nhanh các thiết lập hoặc để hiển thị trạng thái. Thanh lọc khay hệ thống sẽ giải phóng không gian trên thanh tác vụ để dành chỗ cho những ứng dụng quan trọng hơn (xem phần '15 biểu tượng có thể bỏ'). Thao tác trên khay hệ thống dễ dàng hơn khi tất cả biểu tượng của nó đều được hiển thị: Trong Windows XP, nhấn phải chuột lên nút Start, chọn Properties, nhấn thẻ Taskbar, bỏ chọn Hide inactive icons, và nhấn OK (có thể bạn sẽ muốn bật lại tính năng này khi thực hiện xong). Nhấn chuột phải hay trái trên từng biểu tượng để hiện các tùy chọn cấu hình (mỗi biểu tượng hành xử khác nhau). Ngay cả khi phần mềm không cho phép tắt biểu tượng ở khay hệ thống, Windows vẫn có thể giấu nó đi với tính năng tuỳ biến khay hệ thống (xem mục Outlook trong phần '15 biểu tượng có thể bỏ').

LOẠI BỎ NHỮNG ỨNG DỤNG VÔ ÍCH

Cũng như bản thân Windows, các ứng dụng bạn dùng hàng ngày theo thời gian sẽ trở nên 'mất trật tự'. Bạn cần giải phóng khỏi hộp thư đầy tràn, menu 'láu táu' che đi các lệnh cần dùng và các thanh công cụ không bao giờ dùng đến. Sau đây là cách thức để loại bỏ những thứ không cần thiết.

Đơn giản việc bảo mật

Hiện nay, việc bảo mật máy tính là quan trọng. Tuy nhiên, việc bật mọi tính năng bảo mật trên PC có thể làm ảnh hưởng đến hiệu suất làm việc. Ví dụ, việc bật tính năng bảo vệ bằng mật khẩu (password) của trình tiết kiệm màn hình (screen-saver) cho phép bạn rời khỏi PC mà không lo có ai đó tò mò xem những thông tin nhạy cảm.

Hình 4: Tăng thời gian kích hoạt screen saver bằng cách dùng Tweek UI tăng 'grace period'

Nhưng screen-saver cũng có thể kích hoạt khi bạn bận nói chuyện điện thoại hay bận suy nghĩ gì đó và 'lơi là' máy tính. Có một khoảng thời gian chuyển đổi ('grace period') từ lúc screen-saver kích hoạt đến khi chế độ bảo vệ yêu cầu password có hiệu lực (trong khoảng thời gian này, khi bạn rê chuột hay nhấn phím bất kỳ thì screen-saver sẽ kết thúc ngay), mặc định là 5-10 giây. Bạn có thể tăng thời gian này lên để tránh phiền toái nhập đi nhập lại password. Công cụ miễn phí TweakUI PowerToys for Windows XP của Microsoft (find.pcworld.com/42714) có thể thực hiện công việc này. Chạy TweakUI, nhấn dấu cộng kế bên Logon ở khung bên trái, và nhấn Screen Saver bên dưới. Bạn có thể tăng 'grace period' đến 99999 giây, tuy nhiên chỉ cần trong khoảng 30-60 giây là đủ. Một cách khác, bạn có thể chỉnh sửa thẳng trong registry với công cụ regedit có sẵn (nhớ sao lưu registry trước khi chỉnh sửa). Duyệt đến khoá HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, tạo mới biến DWORD đặt tên là 'ScreenSaverGracePeriod' (nếu đã có thì chỉ cần chỉnh sửa) và thiết lập Value thích hợp trong khoảng 0-2147483 (giây).

Windows XP SP2 bổ sung nhiều tính năng bảo mật hấp dẫn, đáng kể nhất là Windows Firewall. Khi bạn cài đặt SP2, một biểu tượng nhỏ có hình dạng giống

cái khiên sẽ xuất hiện ở khay hệ thống. Biểu tượng này liên kết đến Security Center Control Panel, công cụ này cho phép bạn quản lý các thiết lập bật/tắt Automatic Updates và Windows Firewall. Nếu bạn dùng phần mềm firewall khác, Microsoft khuyến cáo nên tắt firewall tích hợp sẵn của Windows. Nhưng nếu làm như vậy, bạn sẽ nhận được hàng đống cảnh báo phiền toái ở khay hệ thống yêu cầu bật lại firewall. Để chấm dứt các cảnh báo này, hãy nhấn đúp lên biểu tượng để mở Security Center, nhấn liên kết Change the way Security Center alerts me ở bên trái, và bỏ chọn Firewall Alert. Cùng cách thức này cũng có thể giúp bạn tránh được phiền toái cảnh báo của Automatic Update, nếu bạn thực hiện cập nhật Windows thủ công và cấm Automatic Updates.

MS Office và nhiều chương trình khác dùng menu để giấu những lệnh thường dùng. Được thiết kế nhằm giúp sử dụng ứng dụng đơn giản nhưng trớ trêu là tính năng này lại làm khó tìm những lệnh ít dùng. Nếu thấy phiền toái, bạn có thể cấm tính năng menu tùy biến trong Outlook, Word, Excel hay Access bằng cách chọn Tools.Customize, đánh dấu Always show full menus
rồi nhấn Close.

Có thể đôi khi bạn không muốn thấy toàn bộ menu. Một số ứng dụng như IE và Outlook cho phép kéo và thả (hay thay đổi kích thước) các thanh công cụ đến không gian tối thiểu. Các chương trình khác như trình duyệt Mozilla cho phép bỏ những thành phần ít dùng. Sau khi di chuyển hay thay đổi kích thước các thanh công cụ của IE, chốt chúng lại ở vị trí hiện tại bằng cách nhấn chuột phải lên thanh công cụ hay menu và chọn Lock the Toolbars.

Hình 5: Loại bỏ các menu tùy biến trong MS Office để nhìn rõ ràng hơn

Tinh giảm hộp thư

Khi số lượng thư trong hộp thư lên đến hàng trăm hay hàng ngàn, bạn sẽ dễ bỏ sót những thư quan trọng, ngoài ra việc tìm một email nào đó cũng mất nhiều thời gian. Vấn đề này có thể khắc phục.

Trước hết, dùng các công cụ lọc thư rác để loại bỏ những thư vớ vẩn có thể ẩn chứa virus (tham khảo bài 'Chống spam cho hộp thư' - TGVT A 6/2004, tr.84). Có thể bạn cần lưu giữ một vài thư để tham khảo sau này nhưng không nhất thiết để 'thường trú' trong Inbox. Hãy chuyển chúng sang các folder con và dùng tính năng lưu trữ của trình email để chuyển các thư cũ trước thời gian nào đó (ví dụ trước 3 tháng) vào một tập tin lưu trữ.

TỐI ƯU PHẦN CỨNG

Về lý thuyết, bất kỳ phần cứng nào được lắp và làm việc trên PC đều yêu cầu nguồn (điện), bộ nhớ và sự điều khiển của bộ xử lý. Loại bỏ những thiết bị không dùng đến có thể giúp cải thiện hiệu suất làm việc của hệ thống. Một số phần cứng, như adapter nối mạng không dây, cũng có thể làm giảm thời gian dùng pin (đối với MTXT) đáng kể, ngay cả khi bạn không nối mạng, ngoài việc tạo ra nguy cơ về

bảo mật.

Nếu ít khi dùng modem, kết nối hồng ngoại, cổng Serial hay Parallel, bạn có thể dùng các thiết lập phần cứng để cấm một số hay cấm chung nhóm phần cứng này nhằm tiết kiệm pin. Nếu sau này cần dùng phần cứng đã cấm (chẳng hạn như cổng Serial), bạn có thể khởi động lại máy và chọn profile cho phép phần cứng này.

Để tạo một profile phần cứng mới, nhấn phải My Computer (trên desktop hay trong menu Start), chọn Properties, nhấn Hardware rồi nhấn Harware Profiles. Chọn profile hiện có (có thể bạn chỉ có một) và nhấn Copy, rồi nhấn OK (chép profile có sẵn là cách dễ nhất để tạo profile mới). Để thiết lập profile mặc định, dùng các nút mũi tên ở bên phải để di chuyển profile được chọn lên đầu danh sách. Windows sẽ sử dụng nó từ lần khởi động kế. Để cấm phần cứng trong profile hiện tại, nhấn phải My Computer, chọn Properties, nhấn Hardware và nhấn Device Manager. Nhấn phải chuột mục phần cứng mà bạn muốn cấm trong danh sách Device Manager (có thể bạn cần mở danh sách này trước), và chọn Disable (lưu ý: đừng cấm bất kỳ phần cứng nào được liệt kê bên dưới danh mục System Devices).

Bạn cũng có thể tiết kiệm nguồn pin của MTXT bằng cách tháo ra các phụ kiện như PC Card, thẻ nhớ Flash, các thiết bị USB và FireWire. Để tránh xảy ra rắc rối mạng và tăng độ bảo mật, mỗi lúc chỉ nên dùng một mạng - cấm kết nối mạng không dây nếu đã nối mạng dùng dây. Hầu hết MTXT đời mới tích hợp Wi-Fi đều có nút bật/tắt ở bên ngoài.

Hình 6: Hardware Profile cho phép cấm phần cứng không cần

Một đề xuất quan trọng: không phải mọi PC đều cần kết nối Internet. Nếu bạn có 2 hay 3 PC, hãy dành một máy để chơi game và những công việc khác không đòi hỏi kết nối Internet - chỉ việc tháo cáp điện thoại hay cáp mạng, hoặc cấm phần cứng mạng trong Device Manager. Nếu PC không nối mạng, nó sẽ ít bị virus tấn công.

Ngốn sạch không gian đĩa cứng sẽ ảnh hưởng đến hiệu suất làm việc của hệ thống và dĩ nhiên bạn không thể cài đặt thêm phần mềm hay tạo thêm tài liệu mới. Bạn có thể giải phóng không gian đĩa đáng kể bằng cách xóa các file rác do các ứng dụng hay trình duyệt web tạo ra. Mở My Computer, nhấn phải ổ đĩa cài đặt Windows, chọn Properties rồi nhấn Disk Cleanup. Sau khi duyệt qua ổ đĩa, Windows sẽ hiện ra danh sách các mục có dung lượng đôi khi lên đến hàng trăm MB. Chọn những mục mà bạn muốn xóa và nhấn OK.

Từ bỏ trình dồn đĩa

Và đây là thủ thuật cuối cùng: Đừng mất thời gian dồn phân mảnh đĩa cứng. Trước đây, việc dồn liên tục các sector của file có thể giúp tăng tốc truy xuất đĩa. Việc dồn phân mãnh sẽ tăng không gian trống liên tục (cho phép bạn cài đặt các chương trình lớn) nhưng không giúp cải thiện tốc độ đáng kể đối với hầu hết PC hiện nay (xem bài 'Sao lưu để an toàn' - TGVT A 2/2004, tr.60). Thay vì vậy, hãy dành thời gian quí giá để thực hiện việc khác nếu bạn muốn tăng tốc PC.

MẶT TRÁI CỦA VIỆC THUẦN PHỤC WINDOWS

TUY VIỆC LOẠI BỎ các service, ứng dụng và những thứ lộn xộn khác trong PC là tốt, nhưng nếu làm quá đà có thể biến PC chỉ bị đôi chút phiền toái thành cỗ máy vô dụng. Nếu dùng Windows XP, công cụ System Restore có thể hậu thuẫn cho bạn phòng khi lỡ đà bước qua lằn ranh giữa việc thuần phục với việc 'tẩy não' PC.

Nói chung, nếu bạn không biết chắc gỡ bỏ hay cấm một chương trình hay service giải pháp nào tốt hơn thì hãy để nó lại (Google là công cụ tốt để tìm hiểu về một chương trình nào đó, chỉ việc tìm theo tên của nó), nếu không bạn có thể cấm nhầm chức năng Windows cần để khởi động.

Để đề phòng trường hợp này, hãy tạo đĩa CD cứu hộ (có thể khởi động) trước khi thực hiện (xem hướng dẫn ở TGVT A 11/2003, tr.116). Sau khi tạo đĩa CD, hãy kiểm tra thử và cất nó vào nơi an toàn và hy vọng không bao giờ phải dùng đến.

Bạn chỉ nên cấm những chương trình hay dịch vụ mà bạn biết là không cần thiết, sau đó giám sát hoạt động PC trong 1 ngày nhằm đảm bảo không gây sự cố gì. Luôn tiến hành thật cẩn thận, mỗi lần cấm một dịch vụ hay chương trình, sau đó khởi động lại máy để xem có trục trặc gì lúc khởi động không. Nếu mọi việc đều ổn thỏa, hãy tạo điểm phục hồi mới

dùng công cụ System Restore, công cụ này sẽ lưu lại cấu hình hệ thống và cho phép bạn khắc phục việc chỉnh sửa Windows sai chỉ với vài nhấn chuột. Việc tạo điểm khôi phục với công cụ này rất dễ dàng: Chọn Start.All Programs (hay Programs). Accessories.System Tools.System Restore, chọn Create a restore point, nhấn Next, nhập thông tin mô tả điểm khôi phục (ví dụ như 'cấu hình chạy tốt trước ngày 11/9'), sau đó nhấn Create.
System Restore cũng có thể dùng để tạo điểm khôi phục trước khi cài đặt phần mềm mới, cho phép bạn rút lại bất kỳ thay đổi nào mà chương trình mới đã làm trên hệ thống. Với System Restore và đĩa CD cứu hộ, bạn có thể khá thoải mái thực hiện việc thuần phục Windows mà không phải lo mạo hiểm biến PC thành cỗ máy vô tri.

Phương Uyên

Trẻ hóa Windows

Thực hiện: Anh Thư

Máy tính của bạn trở nên chậm chạp, Windows chạy ì ạch. Đó chính là những dấu hiệu của sự lão hóa. Đã đến lúc bạn cần ra tay khôi phục lại sự nhanh nhẹn vốn có của Windows.
Việc cài đặt mới hoàn toàn Windows có thể giải quyết triệt để các trục trặc tích lũy dần trong quá trình sử dụng, nhưng cũng có những giải pháp khác giúp "hồi sức" Windows nhanh chóng hơn.

Hồi sức cho Windows

Trong trường hợp Windows gặp trục trặc nhưng chưa đến mức "ngã quỵ" thì bạn không cần thiết phải cài đặt lại Windows mà chỉ phải thực hiện tinh chỉnh vài thứ. Trên thực tế, những lỗi phát sinh trong quá trình khởi động Windows đều có thể được khắc phục dễ dàng. (Nếu hỏng hóc xảy ra trước khi Windows khởi động, hãy làm theo các hướng dẫn được đề cập trong bài "5 phút - thế là xong" - TGVT A tháng 01/2005, t.84).

Tinh giảm các ứng dụng tự khởi động

Bạn sẽ ngạc nhiên khi biết số lượng các chương trình được nạp tự động khi Windows khởi động và hoạt động "ẩn" trong suốt quá trình hệ điều hành làm việc. Người dùng rất khó nhận biết được sự hiện diện này vì hầu hết biểu tượng của các chương trình này không hề xuất hiện trên khay hệ thống. Tất cả chương trình này đều chiếm bộ nhớ và những tài nguyên khác của máy, thậm chí có thể gây xung đột với một số chương trình khác.

Để liệt kê danh sách các chương trình khởi động cùng với Windows, bạn vào Start.Run, gõ vào msconfig và nhấn OK để mở cửa sổ System Configuration Utility. Do trong Windows 2000 không có tính năng này nên bạn cần dùng đến tiện ích bổ sung Startup Control Panel miễn phí của hãng Mike Lin (www.pcworld.com.vn, Download, ID: 46260). Trong giao diện System Configuration Utility, chọn nhãn Startup (hình 1), bỏ chọn chương trình mà bạn không muốn nạp trong quá trình khởi động.

Hình 1: Kiểm soát các ứng dụng được nạp trong quá trình khởi động Windows bằng tiện ích System Configuration Utility.

HĐH Windows 2000 không cần nạp một chương trình nào trong quá trình khởi động, còn Windows XP chỉ cần duy nhất một. Nếu không sử dụng Microsoft Messenger, hãy bỏ "msmsgs". Tuy nhiên việc làm này có thể phát sinh vài trục trặc với Outlook, Internet Explorer hoặc các phần mềm khác của Microsoft.

Ngược lại, Windows 98 (hay Win Me) lại yêu cầu nạp một số chương trình trong quá trình khởi động hệ thống. Vì vậy, đừng bỏ những chương trình như LoadPowerProfile, SystemTray, ScanRegistry, PCHealth và TaskMonitor kể cả khi các tên này xuất hiện hai lần vì có thể chương trình được dùng cho một quá trình khác trong lúc khởi động Windows. Nếu bạn cần đến tính năng Scheduled Tasks của Windows thì đừng bỏ Scheduler Agent. Bạn có thể chọn Start.Program.Accessories.System Tools.Scheduler Task để xem những chương trình nào đang sử dụng tính năng này. Với Win Me, bạn nên nhớ giữ lại StateMgr.

Với các chương trình nạp tự động khác, bạn cần kiểm tra để quyết định có giữ lại hay không. Bạn có thể đoán được ứng dụng đã đăng ký vào danh sách tự khởi động bằng cách đọc thông tin ở cột Command của nhãn Startup. Ví dụ, nếu thấy tập tin chương trình thuộc thư mục Roxio, gần như chắc chắn đó là chương trình Roxio. Ngoài ra, bạn cũng có thể sử dụng những dịch vụ tìm kiếm như Google chẳng hạn để tìm ra nguồn của những chương trình này. Đưa vào từ khóa là tên tập tin, chắc chắn bạn sẽ tìm thấy manh mối.

Hãy giữ lại tất cả chương trình liên quan đến ứng dụng tường lửa (firewall) và chống virus để đảm bảo chúng luôn hoạt động bảo vệ hệ thống. Mặt khác, một số ứng dụng tự động đặt biểu tượng trên khay hệ thống để dễ dàng khởi động thay vì phải kích hoạt từ Start, việc này gây lãng phí tài nguyên hệ thống, do đó hãy loại bỏ chúng.

Đôi khi bạn phải cân nhắc: nếu một tiện ích giúp cải thiện Windows, nó đáng được nạp. Nhưng nếu hệ thống hoạt động không ổn định, hãy thử vô hiệu tiện ích đó – ít nhất là tạm thời – để tìm hiểu xem có phải là nguyên nhân hay không.

Một số chương trình có khả năng xuất hiện lại trong danh sách tự khởi động dù bạn đã bỏ nó. Nguyên nhân là do những chương trình này có khả năng tự chỉnh sửa lại các thiết lập về mặc định (những phiên bản cũ của chương trình nghe nhạc Real Networks là một ví dụ điển hình). Để khắc phục tình trạng này, bạn hãy khởi động ứng dụng đó, kiểm tra các menu và bỏ tùy chọn “Load at startup”.

Trường hợp không tìm thấy tùy chọn này, hãy thử kiểm tra thêm thông tin tại trang web của nhà sản xuất hoặc liên hệ bộ phận hỗ trợ kỹ thuật. Nếu vẫn tiếp tục không có giải pháp để tắt tính năng này cũng như không có nhiều lý do để bạn sử dụng chương trình đó nữa, hãy gỡ bỏ chúng khỏi hệ thống.

Loại bỏ những ứng dụng không cần thiết

Những ứng dụng không dùng đến có thể làm xáo trộn và giảm hiệu suất của Windows. Hãy gỡ cài đặt (uninstall) các chương trình đó ra khỏi hệ thống càng sớm càng tốt, dù việc này không phải đơn giản.

Hình 2: Gỡ cài đặt những chương trình không còn sử dụng.

Đa số các chương trình đều có sẵn thủ

tục gỡ cài đặt nhưng không thể gỡ bỏ hoàn toàn mọi thứ đã cài vào hệ thống. Các nhà phát triển phần mềm đều muốn phần mềm của họ được sử dụng, vì vậy những thủ tục gỡ bỏ cài đặt thường được tạo một cách miễn cưỡng.

Dù vậy sử dụng thủ tục gỡ cài đặt có sẵn của chương trình vẫn là sự lựa chọn tốt nhất. Nếu không tìm thấy thủ tục đó, hãy chọn Start.Control Panel.Add or Remove Programs (trong Windows XP) hoặc Start.Settings.Control Panel.Add/Remove Programs (các phiên bản Windows khác). Tìm chương trình muốn gỡ bỏ trong danh sách Currently installed programs hoặc Install/Uninstall (trong Windows 98). Nhấn Add/Remove hoặc Change/Remove (hình 2) và thực hiện theo hướng dẫn.

Tuy nhiên, bạn vẫn chưa hoàn toàn gỡ bỏ chương trình khỏi hệ thống. Hãy mở cửa sổ System Configuration Utility để xem liệu tập tin tự khởi động của ứng dụng đó đã thật sự được xóa chưa? Nếu tập tin đó vẫn còn, bạn vô hiệu hóa chúng (xem mục " Tinh giảm các ứng dụng tự khởi động"). Kế đến, mở cửa sổ Windows Explorer, tìm và xóa thư mục chứa ứng dụng đó trong "C:\Program Files" (nếu ứng dụng được cài đặt vào thư mục này). Và nếu biểu tượng của ứng dụng trên vẫn còn trong trình đơn Start, nhấn phải chuột lên biểu tượng đó và chọn Delete.

Để chỉ định lại chương trình dùng để mở các tập tin liên quan thay thế cho chương trình vừa bị gỡ bỏ, mở Windows Explorer, chọn Tools.Folder Options (trong Windows 98 là View.Folder Options), sau đó nhấn vào nhãn File Types. Trong mục Registered file types, kiểm tra phần mở rộng tập tin của chương trình đã gỡ bỏ. Nếu tìm thấy, nhấn Change và chọn chương trình thay thế để mở dạng tập tin đó. Ví dụ: nếu đã gỡ bỏ một phần mềm biên tập ảnh, bạn có thể chỉ định lại tiện ích Paint của Windows để mở những tập tin có phần mở rộng .bmp hoặc chọn Delete để yêu cầu Windows nhắc nhở người dùng chọn chương trình mở các tập tin định dạng này vào những lần sau.

Ngoài ra, bạn cũng cần xóa sạch những thông tin của chương trình này được lưu trong Windows Registry (xem mục "Dọn dẹp Registry").

Phòng chống Spyware

Bạn nên thường xuyên kiểm tra các phần mềm gián điệp (spyware) nhiễm vào hệ thống, nhất là khi Windows hoạt động một cách khác thường.

Thực tế, không có một phần mềm nào thật sự hiệu quả vì thế bạn nên kết hợp sử dụng nhiều chương trình với nhau. Trong số những phần mềm miễn phí thì Ad-Aware (www.pcworld.com.vn, Download, ID: 42748) và Spybot Search &

Destroy (www.pcworld.com.vn, Download, ID: 42746) được đánh giá có khả năng phát hiện và quét phần mềm gián điệp tốt nhất. Bạn nên tải về các bản cập nhật mới nhất trước khi tiến hành kiểm tra toàn bộ hệ thống.

Bạn cũng có thể tham khảo website SpywareGuide (www.spywareguide.com, hình 3), nơi cung cấp nhiều thông tin hữu ích với cơ sở dữ liệu hơn 800 phần mềm gián điệp hoặc đọc thêm các hướng dẫn để phát hiện và phòng chống phần mềm gián điệp tại find.pcworld.com/46320.

Hình 3. Tham khảo thông tin về spyware trên website của SpywareGuide.

Cập nhật trình điều khiển

Một biện pháp hữu dụng để Windows luôn hoạt động suôn sẻ là thường xuyên kiểm tra và cập nhật các trình điều khiển thiết bị. Những phần mềm này sẽ giúp Windows làm việc tốt hơn với các thiết bị phần cứng trên hệ thống.

Hình 4. Chọn Update Driver trong hộp thoại Properties để cập nhật trình điều khiển thiết bị.

Nếu máy tính của bạn vẫn đang làm việc tốt thì không có lý do gì để cập nhật các trình điều khiển. Tuy nhiên nếu máy gặp trục trặc, việc này có thể giúp bạn khắc phục vấn đề. Trước hết, hãy mở cửa sổ Device Manager bằng cách nhấn phải chuột lên biểu tượng My Computer và chọn Properties. Tiếp đến trong Windows XP, bạn chọn nhãn Hardware và nhấn nút Device Manager (với Windows 98, chọn Device

Manager).

Tìm các liệt kê được đánh dấu hỏi màu vàng hoặc dấu chấm than màu đỏ. Dấu hỏi thông báo cho bạn biết Windows đang sử dụng trình điều khiển cơ bản cho thiết bị đó thay vì sử dụng trình điều khiển chuyên biệt. Dấu chấm than thông báo thiết bị đó không còn hoạt động trong Windows. Thông thường, trình điều khiển của card đồ họa, card âm thanh và máy in cần được cập nhật thường xuyên trong khi trình điều khiển của những thiết bị hiển thị dưới các mục Computer, Disk drives, Floppy disk drives và Keyboards hiếm khi cần phải cập nhật.

Để cập nhật trình điều khiển, hãy nhấn đúp vào thiết bị tương ứng. Chọn Driver.Update Driver trong hộp thoại Properties (hình 4). Tính năng Hardware Update Wizard sẽ tự động tìm kiếm và cập nhật nếu tìm thấy trình điều khiển thích hợp trên đĩa cứng hay website Windows Update của Microsoft. Nếu không tìm thấy trình điều khiển cần thiết, hãy thử tìm một phiên bản mới tại website của nhà sản xuất hoặc dùng các website tìm kiếm với từ khóa là tên đầy đủ của sản phẩm và thêm từ khóa "driver". Khi tìm thấy bản cập nhật, bạn phải chắc chắn rằng nó tương thích với phiên bản Windows đang sử dụng. Tải trình điều khiển đó về máy và kích hoạt nó.

Cũng có thể việc cập nhật một trình điều khiển mới làm mọi thứ trở nên tồi tệ hơn. Tuy nhiên với Windows XP, bằng cách chọn Roll Back Driver từ nhãn Driver của hộp thoại Properties sẽ giúp bạn khôi phục lại trình điều khiển cũ. Trong trường hợp đang sử dụng Windows 98, Me và 2000, do không có tùy chọn trên nên bạn phải thay thế bằng trình điều khiển cơ bản cho đến khi nhà sản xuất cung cấp bản sửa lỗi mới.

Dọn dẹp Registry

Cứ mỗi lần cài đặt phần mềm, thay đổi thiết bị phần cứng hoặc tải xuống thứ gì đó từ Internet, bạn đều tác động đến cơ sở dữ liệu hệ thống điều khiển mọi hoạt động của Windows. Đó chính là Registry. Việc dọn dẹp Registry sẽ giúp cải thiện hiệu quả hoạt động của hệ thống. Trước khi bắt đầu, bạn cần đảm bảo có thể phục hồi Registry trở lại trạng thái cũ nhằm đề phòng trường hợp xảy ra sai sót. Windows 98, Me, XP (ngoại trừ Windows 2000) đều có tính năng tự động sao lưu Registry

tuy nhiên lại không có tính năng mở rộng như tự sao lưu trước khi người dùng thực hiện việc cài đặt hoặc thay đổi cấu hình máy. Với dữ liệu cá nhân, bạn có thể sao lưu vào một phân vùng đĩa cứng khác để đề phòng sự cố nhưng điều này không thể thực hiện với Registry. Nếu ổ cứng của bạn bị hỏng, việc phục hồi Registry cũng trở nên vô dụng với một phiên bản Windows hoàn toàn mới.

Trong Windows XP và Me, bạn có thể sử dụng tiện ích System Restore để sao lưu Registry bằng cách chọn Start.All Programs.Accessories.System Tools.System Restore.Create a restore point và thực hiện theo các hướng dẫn trên màn hình. Để sao lưu Registry trong Windows 98, bạn hãy nhấn Start.Run, gõ vào scanreg và nhấn OK. Nếu không có thông báo lỗi nào xuất hiện thì nhấn Yes và OK để tiếp tục.

Windows 2000 không được tích hợp tính năng sao lưu Registry, vì thế bạn phải sử dụng phần mềm của một hãng thứ ba như Emergency Recovery Utility NT, một tiện ích miễn phí của hãng Lars Hederer (www.pcworld.com.vn, Download, ID: 42636).

Thay vì sử dụng tiện ích chỉnh sửa Registry có sẵn của Windows, sẽ dễ dàng và an toàn hơn khi tinh chỉnh Registry với tiện ích Reg Organizer giá 30USD của hãng ChemTable Software (www.chemtable.com). Các khóa Registry được hiển thị trực quan, rõ ràng với những thông tin như loại tập tin, chương trình liên quan... Thậm chí bạn có thể tạo một danh sách những khóa Registry thường dùng và truy cập nhanh chóng chỉ bằng một thao tác nhấn chuột.

Công cụ Registry Cleanup của Reg Organizer sẽ tìm kiếm trong Registry và hiển thị tất cả thiết lập lỗi. Qua đó, bạn có thể tùy thích sửa lỗi hoặc xóa hẳn. Nếu vừa gỡ bỏ một phần mềm, bạn cần sử dụng tính năng Search and Replace để xóa sạch tất cả những liệt kê có chứa tên phần mềm.

Nếu đủ tự tin và kinh nghiệm, bạn có thể sử dụng công cụ chỉnh sửa Registry có sẵn trong Windows là Registry Editor. Ngoài ra bạn cũng có thể tham khảo bài

“Chăm sóc và bảo dưỡng Windows Registry” - TGVT A tháng 5/2002, t.90.

Làm mới Windows

Đôi lúc bạn không thể phục hồi “phong độ” cũ cho Windows có quá nhiều trục trặc. Hãy mạnh dạn cài mới lại Windows. Việc này có thể giúp bạn “giũ sạch” những trục trặc cũ và tạo ra một hệ thống mới hoàn toàn “khỏe mạnh”.

Các bước chuẩn bị

Hình 5. Dùng tiện ích True Image của Acronis để tạo bản sao đĩa cứng.

Nếu mọi việc tiến hành suôn sẻ, bạn có thể hoàn tất việc cài đặt chỉ trong vài giờ, tuy nhiên bạn cũng cần tính đến một số trục trặc có thể xảy ra. Do vậy, sao lưu dữ liệu là một bước hết sức cần thiết. Hãy sao lưu tất cả dữ liệu vào thiết bị lưu trữ hoặc ghi đĩa CD. Một giải pháp tốt là sử dụng chương trình tạo bản sao đĩa cứng như True Image giá 50USD của Acronis (hình 5) giúp bạn phục hồi dữ liệu một cách dễ dàng và nhanh chóng.

Kế đến, tập hợp các đĩa CD cài đặt Windows, đĩa phục hồi đi kèm với máy tính hoặc đĩa cài đặt các ứng dụng cần thiết khác. Nếu không có đĩa phục hồi, hãy thử tìm tiện ích phục hồi trong máy. Trong trường hợp có sử dụng những phần mềm chia sẻ tải về từ Internet, hãy kiểm tra để biết chắc mã đăng ký vẫn có tác dụng kích hoạt các phần mềm đó.

Lưu trữ tất cả trình điều khiển thiết bị hiện tại vào một thư mục riêng trước khi tiến hành cài đặt lại (lưu ý là không lưu trong thư mục “C:\Windows”). Bạn có thể tải về tập tin batch thực hiện việc sao lưu này tại www.pcworld.com.vn, Download, ID: 46290. Nếu có trình điều khiển không hoạt động, bạn phải cần đến đĩa CD của nhà sản xuất.

GIAO DIỆN MỚI CHO WINDOWS

Mọi người đều nóng lòng chờ đợi "tân binh" Longhorn, phiên bản tiếp theo của HĐH Windows XP được Microsoft dự kiến phát hành trong năm 2006. Nếu không muốn chờ đợi, chỉ với 40USD bạn có thể sử dụng bốn tiện ích để cải tiến giao diện Windows (tải về tại find.pcworld.com/46288).

Desktop Sidebar: Longhorn sẽ thêm vào màn hình của Windows một thanh tác vụ mới hiển thị các thông tin thu thập từ hệ thống và Internet. Tiện ích Desktop Sidebar cũng có thể thực hiện những tính năng đó. Thanh tác vụ của tiện ích sẽ hiển thị các thông tin về thư điện tử, lịch làm việc, thông tin hệ thống, tin tức trực tuyến và thậm chí slide show các hình ảnh sẵn có của bạn.

Giao diện như Windows Longhorn.

Cũng tương tự thanh tác vụ của Windows, Sidebar có khả năng tự động hiển thị hoặc ẩn theo ý bạn.

Actual Transparent Window: Bạn không muốn cửa sổ hiện hành che khuất các cửa sổ khác kể cả hình nền tuyệt đẹp của mình. Trong HĐH Longhorn, bạn có thể làm trong suốt mọi cửa sổ theo ý thích và dĩ nhiên bạn phải tiếp tục chờ cho đến khi HĐH được chính thức phát hành. Actual Transparent Window (phần mềm chia sẻ, giá 20USD) sẽ giúp bạn thực hiện yêu cầu này. Tiện ích sẽ bổ sung vào thanh tiêu đề của mỗi cửa sổ một biểu tượng để chuyển đổi giữa chế độ hiển thị hoàn toàn (mặc định) và 20% trong suốt. Bạn có thể tùy biến linh hoạt tính trong suốt của từng cửa sổ hoặc áp dụng cho tất cả các cửa sổ bằng công cụ đi kèm.

Spaces: Bạn cần thêm không gian để làm việc? Tiện ích Spaces (20USD) của Spatial Research sẽ thay thế không gian phẳng màn hình Windows bằng một không gian làm việc ba chiều. Các chương trình, ứng dụng khi thu nhỏ sẽ được xếp vào một lưới định vị. Bạn có thể di chuyển, sắp xếp hoặc phóng to, thu nhỏ một cách dễ dàng. Spaces yêu cầu hệ thống phải hỗ trợ .Net Framework được tải về miễn phí tại www.windowsupdate.microsoft.com.

Copernic Desktop Search: Cơ chế tìm kiếm của Windows thật thảm hại. Longhorn cố gắng khắc phục điều này dựa vào việc thu thập các thuộc tính tập tin, thư mục thành những thư viện. Tiện ích Copernic Desktop Search của Copernic Technologies dù không thể đáp ứng các đòi hỏi trên nhưng có

thể tìm kiếm nội dung các tập tin chỉ trong "nháy mắt". Để làm được điều đó, Copernic lập chỉ mục các tập tin tựa như các trình tìm kiếm trên web thực hiện. Tính năng tìm kiếm nâng cao cho phép người dùng thêm vào những các phép toán luận lý AND-OR-NOT giữa các từ khóa.

Thực hiện cài đặt

Đưa đĩa cài đặt (hoặc đĩa phục hồi) vào ổ CD, khởi động lại máy tính và thực hiện từng bước một theo hướng dẫn trên màn hình. Nếu may mắn, những đĩa này sẽ phục hồi lại Windows với đầy đủ các trình điều khiển và ứng dụng cần thiết. Nhưng cũng có thể chúng đưa ổ cứng trở lại tình trạng ban đầu với Windows hoàn toàn không có dữ liệu và ứng dụng nào cả. Nếu đây là lựa chọn duy nhất, bạn phải chắc chắn đã sao lưu toàn bộ dữ liệu lên một thiết bị lưu trữ khác trước khi cài đặt lại máy.

Nếu là đĩa cài đặt đầy đủ của Windows XP hoặc 2000, bạn sẽ thấy thông báo "Press any key to boot from CD". Hãy làm theo chỉ dẫn đó. Nếu không nhận được thông báo này, bạn nên khởi động lại máy tính và tiến hành cài đặt lại CMOS để thay đổi trình tự khởi động với ổ CD là tùy chọn đầu tiên. Trong màn hình "Welcome to Setup", nhấn Enter để chọn chức năng cài đặt lại Windows. Kế đến, nhấn phím F8 sau khi đọc kỹ nội dung và đồng ý với các điều khoản trong cửa sổ "Licensing Agreement".

Trong màn hình lựa chọn phân vùng cài đặt, chọn phân vùng Windows đang sử dụng và nhấn Enter. Tiếp đến nhấn phím C để chấp nhận cảnh báo về việc sử dụng phân vùng và chọn "Leave the current file system intact (no change)". Ngay sau đó, hộp thoại "To use the folder and delete the existing Windows installation in it, press L" xuất hiện và bạn cần nhấn phím L để xác nhận việc xóa thư mục Windows cũ và tạo thư mục mới trong quá trình cài đặt.

Vào cuối quá trình cài đặt, Windows sẽ yêu cầu tên người dùng người dùng (user name). Hãy nhập một tên tạm nào đó – đừng dùng tên thật của bạn, ví dụ như Temp (bạn sẽ xoá sau khi hoàn tất).

Khôi phục dữ liệu

Ở màn hình đăng nhập Windows, nhập vào tên Temp. Dùng Windows Explorer mở thư mục "C:\Documents and Settings". Trong cửa sổ Tools.Folder Options.View, đánh dấu tùy chọn Show hidden files and folders và bỏ tùy Hide protected operating system files (Recommended). Tiếp đến là chọn Yes và OK để thoát ra ngoài.

Bây giờ, bạn sẽ thấy các thư mục như All Users, All Users.WINDOWS, Default User, Default User.WINDOWS, Temp và cả thư mục của những người dùng trước. Mở thư mục "Default User", tìm và xóa những tập tin mang tên NTUSER (kể cả những tập tin khác phần mở rộng) và chuyển các tập tin còn lại sang thư mục "Default User.WINDOWS". Nếu có bất kỳ hộp thoại nào xuất hiện, luôn chọn Yes hoặc Yes to All (hình 6). Khi đã hoàn tất, xóa thư mục rỗng "Default User" này. Cứ như thế lặp lại các bước trên với thư mục "All Users", sao chép tất cả trừ những tập tin NTUSER đã có vào thư mục "All Users.WINDOWS".

Quay trở lại thư mục "Documents and Settings", đổi tên thư mục của người dùng bằng cách thêm vào phần mở rộng .old.

Hình 6. Di chuyển các tập tin và thiết lập cũ sang thư mục mới sau khi cài lại Windows XP/2000.

Để tạo những tài khoản mới, chọn Start.Control Panel.User Accounts (Windows XP) hoặc Start.Settings.Control Panel.Users and Passwords (Windows 2000) và tạo lại chính xác tài khoản các người dùng trước khi cài lại. Lưu ý: phải có ít nhất một tài khoản được thiết lập quyền quản trị (Administrator). Trong Windows 2000, bạn phải đánh dấu tùy chọn Users must enter user name and password to use this computer để tạo mới tài khoản người dùng.

Sau khi hoàn tất việc tạo các tài khoản mới, thoát khỏi tài khoản Temp bằng cách chọn Start.Log Off.Log Off hoặc Start.Shut Down.Log off Temp.OK (Windows 2000). Nếu chỉ có mình bạn sử dụng máy, hãy đăng nhập và thoát khỏi tài khoản của mình. Sau đó đăng nhập lại cũng với tài khoản tạm thời đó một lần nữa. Nếu có nhiều người sử dụng cùng một máy, bạn lần lượt đăng nhập và thoát ra với từng tài khoản một trước khi đăng nhập lại vào tài khoản tạm thời của mình (Temp).

Với người dùng XP, bạn phải hoàn toàn thoát khỏi chứ không phải chuyển đổi giữa các tài khoản người dùng (tính năng Switch User).

Sau khi đăng nhập lại vào hệ thống bằng tài khoản tạm, mỗi tài khoản người dùng trong "Documents and Settings" sẽ có hai thư mục "login name" và "login name.old". Thực hiện xóa những tập tin NTUSER và chuyển tất cả tập tin khác vào thư mục mới của từng người dùng giống như Default User mô tả ở trên (nhưng ở đây là từ "login name.old" sang "login name").

Sau khi hoàn tất, thoát khỏi tài khoản tạm, đăng nhập với tài khoản quản trị và xóa hẳn tài khoản này bằng cách sử dụng tính năng User Accounts trong Control Panel.

Kết thúc công việc

Bước cuối cùng để hoàn tất là cài đặt các trình điều khiển cần thiết. Nếu đã chạy tập tin batch (đề cập ở trên) trước khi thực hiện cài đặt lại, bạn chỉ việc mở Device Manager và tiến hành cập nhật (tham khảo mục "Cập nhật trình điều khiển"). Các liệt kê được đánh dấu hỏi màu vàng là những thiết bị cần được nâng cấp trình điều khiển (hình 7). Tuy nhiên vẫn có một số thiết bị đòi hỏi nâng cấp mặc dù vẫn hoạt động tốt.

Để cài lại trình điều khiển, nhấn đúp vào thiết bị trong danh sách Device Manager, chọn Driver.Update Driver. Hardware Update Wizard sẽ tự động tìm và chọn đúng trình điều khiển cần thiết. Bỏ tùy chọn tìm kiếm trong ổ đĩa mềm, CD hoặc các thiết bị tháo lắp khác, chỉ định tìm kiếm trong thư mục "C:\Olddrivers". Chọn Next và thực hiện theo các hướng dẫn trên màn hình.

Hình 7. Device Manager giúp bạn dễ dàng xác định trình điều khiển nào cần được thay thế sau khi cài lại Windows.

Nếu gặp thông báo yêu cầu đưa đĩa CD có liên quan, chọn OK và tiếp tục chỉ đến thư mục "C:\Olddrivers". Cứ việc bỏ qua và tiếp tục quá trình cài đặt nếu Windows không tìm thấy tập tin cần thiết. Tuy

nhiên, thiết bị phần cứng sẽ không hoạt động, hãy cài đặt trình điều khiển từ đĩa CD đi kèm với thiết bị. Sau khi hoàn tất, bạn có thể xóa hoặc tốt nhất là di chuyển

thư mục "C:\Olddrivers" đến một nơi lưu trữ an toàn cho đến khi hệ thống hoạt động thật sự ổn định.

Với các ứng dụng vẫn còn trên đĩa cứng và được liệt kê trong trình đơn Start (trừ khi sử dụng đĩa CD phục hồi có định dạng lại ổ cứng), hầu hết chúng đều không làm việc khi cài lại Windows do các thiết lập trước đây trong Registry đã bị xóa bỏ. Cài đặt lại các ứng dụng đó hoặc xóa chúng khỏi trình đơn Start và thư mục Program Files nếu không còn nhu cầu sử dụng. Bạn không cần phải sử dụng tiện ích Uninstall trong trường hợp này.

Trong trường hợp cần thiết, có thể bạn phải kích hoạt lại Windows XP. Nếu không có sự thay đổi về phần cứng, mọi việc sẽ diễn ra như bình thường. Cuối cùng, bạn nên cập nhật các bản sửa lỗi cho Windows hay cài thêm các tiện ích cần thiết. Tham khảo những hướng dẫn về việc cài đặt Service Pack 2 cho Windows XP tại find.pcworld.com/46286.

BẮT ĐẦU MỚI CHO WINDOWS 98, Me

Việc cài lại Windows 98 và Me đòi hỏi nhiều "thủ thuật" hơn so với Windows 2000 và XP, nhưng về cơ bản thì quá trình thực hiện như nhau.

Trước hết, bạn hãy sao lưu các thư mục dữ liệu trong C:\windows sang thư mục C:\datawin. Bạn phải xóa thư mục Windows cũ trước khi cài đặt lại và đó là lý do cần sao lưu những dữ liệu quan trọng trong thư mục "C:\Windows" vào nơi khác an toàn hơn. Những thư mục khác cũng cần được sao lưu là All Users, Application Data, Desktop, Favorites, Local Settings, Profiles, SendTo và Start Menu. Bạn không cần sao lưu thư mục "C:\My Documents" vì chúng nằm ngoài thư mục Windows. Nếu máy tính có nhiều người dùng, bạn phải sao lưu thư mục "C:\Windows\Profiles".

Sử dụng lệnh trên để thay thế dữ liệu cá nhân sau khi đã cài lại Windows98/Me. Dùng tiện ích Add/Remove Program để tạo đĩa mềm khởi động (hình dưới).

Khởi động với đĩa mềm

Bạn cần một đĩa mềm có khả năng khởi

động để cài đặt lại Windows 98/Me. Để tạo một đĩa mềm khởi động, chọn Start.Settings.Control Panel.Add/Remove Programs và nhấn Startup Disk.Create Disk và thực hiện theo hướng dẫn.
Khởi động lại hệ thống từ đĩa mềm này. Trong trình đơn Startup, chọn Start computer with CD-ROM support. Sau khi hệ điều hành DOS nạp xong trình điều khiển CD-ROM, đưa đĩa cài đặt Windows vào ổ CD, ở dấu nhắc DOS, gõ lệnh dir x: (với x: là ký tự gán cho ổ CD). Gõ dòng lệnh c:\windows\command\deltree /y c:\windows và nhấn Enter.
Trở lại dấu nhắc A:, gõ lệnh x:setup, nhấn Enter và thực hiện theo các hướng dẫn trên màn hình. Và bạn đừng quên lấy đĩa mềm ra khỏi ổ đĩa trước khi Windows khởi động lại.
Nếu máy tính của bạn có nhiều người dùng, chọn Start.Settings.Control Panel.Users (Windows 98) hoặc Start.Settings.Control Panel.View all Control Panel options.Users (Win Me). Sử dụng các thông tin trong thư mục "C:\Datawin\Profiles" để tạo lại chính xác các tài khoản người dùng.
Cuối cùng, chọn Start.Run, gõ xcopy c:\datawin*.* c:\windows /s /h /r , và nhấn OK. Nhấn phím a (All) để xác nhận chấp nhận việc ghi đè tập tin. Sau khi quá trình chép các tập tin kết thúc, khởi động lại máy và thực hiện theo những chỉ dẫn ở mục "Kết thúc công việc" .

Anh Thư
PC World Mỹ 03/2005

Gỡ bỏ Windows XP SP 2 một cách an toàn

09:01:32, 22/09/2005

Phiên bản windows XP SP2 vừa tung ra thì lại bị lỗi bảo mật. Vả lại có quá nhiều chương trình xung đột không chạy sau khi updates. Những lý do trên có thể cho bạn lời khuyên là gở bỏ XP SP2. Bài viết này giúp bạn một số cách có thể gỡ bỏ Windows XP SP2 một cách nhanh chóng và suôn sẻ nhất.

Cách 1 : Sử dụng Recovery Console

Đầu tiên bạn dùng CD cài đặt WinXP để boot từ CD. Khi gặp màn hình thông báo cài đặt, bạn nhấn R để start Recovery Console. Tiếp tục bạn chọn câu hỏi. Lưu ý bạn phải chọn một số cụ thể trước khi nhấn phím enter.

Ví dụ 1:C:\windows

Sau đó bạn điền vào password của admin. Điều này các bạn thường bỏ qua không thiết lập. Tuy nhiên nếu không biết, thì bạn cứ enter. Đừng cố nhớ, nếu bạn gõ sai bạn sẽ không thể tiếp tục. Tiếp theo tại dấu nhắc bạn gõ cd $ntservicepackuninstall$\spuninst. Nhấn Enter.

Tiếp theo bạn gõ tiếp spuninst.txt (để xem những danh sách những file đang thực thi). Sau khi quá trình remove hoàn tất, bạn gõ exit là restart lại máy tính ở chế độ safe mode (nhấn F8 và chọn chế độ safe mode).

Tuy nhiên nếu thấy màn hình đen thì bạn nên tắt nguồn và restart lại lần nữa. Khi đó bạn sẽ vào hệ thống được. Sau khi máy tính khởi động lại, windows Explorer (explorer.exe) sẽ không hoạt động, các icon đều biến mất, thay vào đó là những icon lạ hoắc không hình dạng. Để giải quyết trường hợp trên, bạn làm như sau. Nhấn CTRL + ALT + DEL để vào TASK MANAGER.

Chọn vào File > New Task, gõ regedit. Sau đó tìm đến từ khóa HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RpcSs
Tạo mới một key mới là ObjectName với giá trị là LocalSystem. Nhấn Ok để hoàn tất. Khởi động lại máy tính.

Cách 2: Sử dụng System restore.

Để thực hiện bạn nhấn WIN + R để mở hộp thoại Run. Sau đó gõ vào %SystemRoot%\System32\restore\rstrui.exe.

Nhấn OK. Hộp thoại System Restore xuất hiện. Bạn chọn Restore My Computer To An Earlier Time. Nhấn Next. Chọn thời điểm bạn updates XP SP2. Nhấn Next và làm theo hướng dẫn trên màn hình để hoàn tất quá trình gở bỏ XP SP2. Restart lại máy tính.

Cách 3: Sử dụng công cụ Add or remove programs trong Control Panel

Nhấn Win + R. Hộp thoại run hiển thị ,bạn gõ vào appwiz.cpl. Nhấn OK để vào Add remove Programs (bạn cũng có thể vào danh sách chương trình cài đặt, khi đó bạn sẽ gặp ngay Windows XP Service Pack 2 trong Program list. Nhấn Remove để gở bỏ ra khỏi hệ thống).

Một vài lưu ý khi thiết lập

Cách 3 đơn giản nhất, tuy nhiên nếu chỉ trình bày cách 3 một cách riêng lẻ thì bạn sẽ gặp trường hợp như cách 1 là các icon không hiển thị. Do vậy cách giải quyết đã trình bày ở cách 1 .

Cách 1 chỉ áp dụng sau khi bước 2 và bước 3 thất bại. Trong trường hợp đó cách 1 vẫn là hiệu quả nhất và gom lại cả ba cách là có chung một giải pháp là đụng tới regedit. Do đó bạn nên sao lưu trước khi thiết lập…

Theo kinh nghiệm thì hoàn toàn không có việc gì xảy ra khi gở bỏ SP2. Ngoại trừ icon không hiển thị và cách giải quyết đều cho kết quả tốt đẹp.

Phạm Lê Minh Định

Gia tăng hiệu suất Windows

(Dân trí) - Sau một thời gian dài hoạt động, bản ghi nhớ các chương trình Windows của bạn sẽ trở nên quá tải với một số lượng lớn các thư mục đã cũ. PC chạy như rùa bò và Windows tốn nhiều thời gian để tải, tìm kiếm và đọc dữ liệu các thư mục. Phần mềm TweakNow RegCleaner sẽ giúp máy tính của bạn đạt hiệu suất làm việc cao nhất.

Giao diện của phần mềm.

Việc cài đặt phần mềm này, có thể nói là tạo dựng được một bản đăng kí được coi là trái tim và linh hồn của bất cứ một hệ thống Windows nào. Nó chứa đựng thông tin điều khiển các hệ thống trong hệ điều hành của bạn xuất hiện ra sao và chạy nó như thế nào. Hầu hết những chương trình ứng dụng hiện nay đều sử dụng đăng kí này để lưu giữ cấu hình và những dữ liệu quan trọng khác. Khi bạn cài đặt các chương trình ứng dụng, mục đăng kí mới này sẽ được tạo lập.

Phiên bản mới của phần mềm này đã chứng minh được hiệu quả của nó với các tính năng ưu việt:

- Nhanh: Sử dụng với hiệu suất máy cao, TweakNow RegCleaner nhanh chóng kiểm tra những mục đăng kí để tìm ra các thư mục cũ đã cất giữ trong hệ thống máy.
- Chính xác: Do sử dụng thuật toán phức hợp TweakNow RegCleaner nhận dạng chính xác các thư mục cũ.
- Đăng kí linh hoạt: TweakNow RegCleaner cho phép hiển thị hai phần: chi tiết hoặc không chi tiết.

Hiện nay phần mềm này đã ra mắt phiên bản mới 2.9.7 với độ bền cải tiến hơn và

hiện thị một cách tối đa, hỗ trợ cao với nền 64x. Tùy vào chức năng mà bạn mong muốn, các phiên bản của phần mềm này sẽ đáp ứng giúp bạn. Tất nhiên, bạn sẽ phải mua nó với giá 26,95 USD hay 69,95 USD cho cá nhân hay cho toàn bộ hệ thống của bạn. Với gói giá 69,95 USD, phần mềm sẽ hỗ trợ máy tính của bạn cài đặt rất nhiều phần mềm với số lượng không giới hạn.
Phần mềm hỗ trợ các hệ điều hành Windows: 2000/XP/XP x64/2003.
Bạn có thể mua phần mềm tại các cửa hàng hoặc tải bản dùng thử 30 ngày tại địa chỉ:
http://www.tweaknow.com/download/RegCleanerPro-t.exe

Quốc Trung

Trang Web về Windows XP

XP Tips, Tutorials, and useful Websites

http://www.labmice.net
http://www.windowsxptutor.com
http://www.webtree.ca/windowsxp/best_xp_sites.htm
http://rain.prohosting.com/~starman2/wxpr_index.shtml
http://www.cnet.com/software/0-6688749.html
http://www.techtv.com/screensavers/supergeek/story/0,24330,3337963,00.html

Windows XP Guide

http://www.windows-help.net/WindowsXP
http://www.windowsxpatoz.com
http://www.tipsdr.com
http://windowsxp.devx.com
http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/xptechov.mspx]
Windows
http://www.winsupersite.com/showcase/windowsXP_tips.asp

Microsoft XP Tips

http://www.microsoft.com/windowsxp/expertzone/tips/moretips.asp

http://www.microsoft.com/technet/prodtechnol/winxppro/tips/default.mspx
http://www.activewin.com/winxp/tips/index.shtm
http://www.neoseeker.com/Articles/Hardware/Guides/winxptweak/]neoseeker.com
http://www.kellys-korner-xp.com/]Kelly's Corner XP
(c) ghost1982@updatesofts.com
Ashampoo AntiSpyWare - Vietnamese Edition !!!
Chống Spyware, Adware, Malware ..... với Ashampoo AntiSpyWare

Với **20.000 nhận diện** về các mối hiểm họa như: Spyware, Adware .... **Ashampoo AntiSpyWare** có thể bảo vệ bạn trước các hiểm họa từ Internet và nay nó đã có phiên bản Tiếng việt để bạn sử dụng dễ dàng hơn !!!!!!!!!

Ashampoo AntiSpyWare có thể bảo vệ bạn trước các hiểm họa sau:

Spyware
Spyware thường được cài đặt chung với các chương trình "bình thường" được cung cấp bởi các công ty **Vô trách nhiệm**. Các Spyware khác thì được cài đặt bởi các hacker. Chúng sẽ thu thập và truyền các thông tin về bạn cho các công ty quảng cáo hoặc là các mục đích phạm tội.

Adware
Adware chứa đựng các loại quảng cáo. Bị nhiễm Adware có thể so sánh như là có chấy, rận trong máy của bạn, nó rất đáng ghét và rất khó thoát khỏi nó.

Hijackers
Chúng chiếm đoạt quyền điều khiển trình duyệt của bạn, hiển thị các trang web mà bạn không muốn và cài đặt các "thanh quảng cáo" vào trình duyệt của bạn.

Tracking Cookies
Hầu hết các Cookie thì vô hại, nhưng có 1 số cái có thể theo dõi tất cả hoạt động của bạn trên net rồi báo về cho các công ty quảng cáo hoặc dùng vào mục đích xấu.

Hidden Dialers
Các chương trình này có thể làm bạn tiêu tốn đến hàng nghìn dollar bằng cách quay số tới Internet thông qua các số mà phải trả tiền cao hơn so với các số bình thường.

Worms
Chương trình sẽ ngăn chặn không cho phát tán các loại virus và malware thông qua máy của bạn.

Key Loggers
Bạn nghĩ sao về chương trình mà ghi lại tất cả những gì mà bạn đã gõ, với những thông tin chi tiết về bạn và số thẻ tín dụng của bạn? Thật không tốt! Hãy thoát khỏi chúng.

Trojan Horses
Trojan Horses hoặc Trojan là chương trình chạy ngầm không trực tiếp gây ra nguy hiểm gì cả. Nhưng chúng cho phép các hacker điều khiển máy của bạn thông qua Internet và thực hiện những gì họ muốn - bật webcam, gửi thư rác, tấn công các máy khác, phát tán văn hóa đồi trụy, sử dụng thông tin ngân hàng .... bằng tên của bạn.

Rootkits
Rootkits là mối hiểm họa mới xuất hiện, và là một trong những thứ tồi tệ nhất. Chúng có thể giấu Trojans, Spyware, Adware và
virus, làm cho các chương trình chống virus không phát hiện được.**Ashampoo AntiSpyware** có thể nhận diện được biến thể mới đặc biệt nguy hiểm của malware này.

System Requirements

The requirements for running Ashampoo AntiSpyWare are very modest:

Operating System:

Windows® 2000 and XP.

Computer:

Any computer that runs one of the above operating systems at a reasonable speed.

RAM and disk space:

128 MB RAM, around 20 MB for the program files. Some additional space for

quarantined files. (depending on the amount of infected files that were quarantined)

Software:

Microsoft® Internet Explorer 5.0 or higher is required.

Other:

Full administrative rights are required to use the program. An internet connection to receive signature updates.

1.Về phiên bản này:

-Được chỉnh sửa lại dựa trên bản việt hóa của **HoangLong** (hoanglong942006) thành viên trẻ tuổi có triển vọng của UDS

2.Yêu cầu:

- Hệ thống (WinXP) phải được thiết lập Tiếng Việt, xem bài này để biết cách làm. Code:
http://www.updatesofts.com/forums/showpost.php?p=78715&postcount=44

3.Hình ảnh về bản này

4.Tồn tại & những phần cần khắc phục / phát triển sắp tới:

-Còn 1 vài chỗ ngôn từ vẫn chưa đc thông suốt

5.Download

MegaPatch

Phiên bản đặc biệt:MegaPatch
Sữa lỗi chính tả và các thành phần trong tab Internet đã hoạt động
Download

Code:
http://www.zshare.net/download/megapatch-rar.html
Code:
Mirror
Code:
http://green.uploadspider.com/file/5338/
Bản exe,không nén
Code:
http://rapidshare.de/files/19908917/AshampooASVN.exe.html

*Mở Ashampoo AntiSpyware,chọn ngôn ngữ là English.Xoá file 109.nlang trong thư mục Translation,giải nén file Patch vào thư mục này ,mở Ashampoo AntiSpyware lên,chọn ngôn ngữ là Vietnamese,khởi động lại chương trình.
*Xin mọi người gửi thư về:hoanglong942006@yahoo.com hoặc PM em,thông báo về những câu bất hợp lý,lỗi chính tả để em đưa ra bản Patch Final!!!

Một lần nữa thay mặt tất cả người dùng cảm ơn em rất nhiều Hoàng Long ạ
Ashampoo Magical Optimizer - Phiên bản Tiếng Việt

Ashampoo Magical Optimizer - Phiên bản Tiếng Việt

- Dọn dẹp toàn bộ hệ thống và Lấy lại dung lượng trống cho máy của bạn : **CHỈ VỚI 1 LẦN BẤM CHUỘT**

Là một điều hiển nhiên! Sau một thời gian sử dụng - bạn có thấy máy của mình chạy chậm đi không
. Đó là do máy của bạn chứa rất nhiều file dư thừa
(Các tập tin tạm của các trình duyệt, các giá trị registry thừa, ...)

==> Và đây chính là cách giải quyết để lấy lại "phong độ" cho máy tính của bạn **Ashampoo Magical Optimizer** - Nay đã có phiên bản Tiếng việt, đem lại sự thuận tiện cho các bạn, làm cho chương trình trở nên dễ sử dụng và thân thiện với người dùng Việt Nam hơn

***Các tính năng chính**

-Sử dụng thật dễ dàng
-Chương trình có 3 chế độ quét cho bạn chọn lựa
+Xóa các thông tin nhạy cảm: Ngay lập tức xóa các tập tin mà khi bạn online để lại (Cookie, Cache, ...)
+Dọn dẹp ổ cứng: Quét toàn bộ ổ cứng rồi lấy lại dung lượng cho ổ cứng của bạn bằng cách xóa các tập tin không cần thiết
+Dọn dẹp Registry: Quét toàn bộ Registry - Thành phần cơ bản của Window - Xóa đi các khóa không đúng hoặc không còn tồn tại, ...
-Sao lưu các tập tin trước khi xóa để bạn có thể phục hồi sau này
-Bảng thống kê cho biết bạn đã xóa các file gì và vào thời điểm nào
-Cập nhật dễ dàng qua Internet
-Đã có Tiếng Việt

***Một số hình ảnh về phiên bản này**

***Thông tin về phiên bản này**

-Phần mềm Ashampoo Magical Optimizer được Việt hóa bởi HoangLong - Thành viên nhóm Việt hóa của Updatesofts.com

-Đã được việt hóa toàn bộ - 100%

***Yêu cầu hệ thống**

-Hệ thống (WinXP) phải được thiết lập Tiếng Việt, **xem bài này** để biết cách làm.

***Cài đặt**

-Đối với Phần mềm Ashampoo Magical Optimizer này, chúng tôi đã gửi bản Việt hóa đến nhà sản xuất và được họ chấp nhận
==> Điều này sẽ giúp bạn cài đặt chương trình một cách dễ dàng hơn

-Bạn download bản cài đặt tại đây
Code:
http://www.ashampoo.com/dl/1406/ashampoo_magicaloptimizer_se.exe
-Nếu bạn không download được về từ địa chỉ trên, bạn hãy download về ở đây
Code:
http://rapidshare.de/files/23797640/ashampoo_magicaloptimizer110_se.exe.html
-Crk:
Code:
http://rapidshare.de/files/23099153/tamo110b-2006-06-15.rar.html
-Sau khi đã cài đặt chương trình xong, ngôn ngữ sẽ là mặc định Tiếng việt. Nếu chưa hiển thị Tiếng Việt, bạn vào Option/Language/Vietnamese

-Các bạn down thêm bản cập nhật
Code:

http://rapidshare.de/files/25150666/42.nlang
Code:
http://d.turboupload.com/d/759846/42.nlang.html

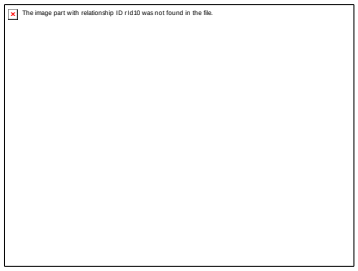
Bạn hãy copy đè file 42.nlang vào thư mục **Translation** trong thư mục của Ashampoo Magical Optimizer

Hy vọng bạn sẽ hài lòng khi sử dụng phần mềm này.

Bạn hãy là người sử dụng các phần mềm được Việt hóa để thấy sự đơn giản và tiện lợi trong sử dụng

=> Hãy ủng hộ cho nhóm việt hóa của chúng tôi

Lướt web an toàn hơn với phần mềm chống Keylog - 24/8/2006 13h:43



Mới đây hãng phần mềm QFX đã đưa ra một phần mềm đính kèm theo trình duyệt Internet Explorer nhằm mục đích chống lại được các phần mềm ghi lại các thao tác bàn phím (keylogger).

Phần mềm này có hai biến thể là KeyScrambler Personal 1.0.1 (miễn phí) và KeyScrambler Professionnal 1.0.1 (có tính phí).

KeyScrambler Professionnal cung cấp cho người dùng đầy đủ các tính năng bảo vệ để tránh khỏi các phần mềm ghi lại các ký tự mà người dùng đã gõ trên bàn phím khi truy cập Web như : thông tin đăng nhập mail, yahoo , các thông tin cá nhân quan trọng (thẻ tín dụng, bảo hiểm xã hội...v.v).

Người dùng có thể tải về dùng bản KeyScrambler Personal 1.0.1 tại đây.

DUYLONG

Theo Softpedia, VnMedia

Những công cụ chống Virus tốt nhất hiện nay

Các chương trình chống virus hiện nay dễ dàng ngăn chặn những kiểu xâm nhập đã biết, nhưng với những hiểm họa chưa biết thì thật khó lường. Kết quả thử nghiệm trên 10 sản phẩm cho chúng ta thông tin để chọn được ứng viên đáng giá đáp ứng hiệu quả nhu cầu thực tế.

Có cả tin tốt và tin xấu về cuộc chiến chống virus máy tính đang diễn ra. Tin tốt: tất cả sản phẩm mà PC World Mỹ đánh giá trong bài viết này đều phát hiện và cô lập 100% các mối đe dọa đã được nhận diện. Tin xấu: các công cụ này không thể bảo vệ bạn hoàn toàn khỏi các mối đe dọa mới xuất hiện đầy dẫy trên Internet.

AV-Test (find.pcworld.com/51168), hãng phần mềm bảo mật của Đức, cộng tác với PC World Mỹ thực hiện bài viết này cho biết, mỗi ngày xuất hiện khoảng 70-100 hiểm hoạ mới. Mặc dù trong số đó có nhiều biến thể của những hiểm họa tồn tại trước đó, nhưng chỉ trong vài giờ chờ đợi các hãng phát hành bản sửa lỗi cũng đủ cho chúng tấn công hệ thống của bạn. Hơn thế, virus không chỉ là vấn đề duy nhất, còn có cả sâu (worm) – một loại không cần tập tin mồi để lây nhiễm - và những chương trình phá hoại khác chẳng hạn như tập tin đính kèm email.

Do những mối nguy hiểm như vậy, chương trình chống virus phải có khả năng không chỉ nhận ra, loại bỏ virus mà còn những dạng hiểm họa khác.

Công cụ chống virus phản công

Giao diện chính của BitDefender

Các công ty phát triển phần mềm chống virus (antivirus) đã thích ứng và nâng cấp sản phẩm của họ bằng nhiều cách khác nhau. Chiến thuật thường thấy là gộp chương trình chống virus truyền thống với các công cụ khác như công cụ chống phần mềm gián điệp (spyware), tường lửa (firewall) nhằm bảo vệ người dùng toàn diện hơn. Thời gian đưa ra bản cập nhật chương trình được rút ngắn để đối phó kịp thời với những hiểm hoạ mới. Kỹ thuật quét thông minh (heuristics) của các công cụ chống virus cũng được hoàn thiện hơn, kỹ thuật này có thể nhận ra hiểm hoạ mới dựa trên dấu vết tương đồng với các hiểm hoạ đã biết.

Ngoài ra, các công cụ antivirus còn được trang bị cơ chế phát hiện dựa vào hành vi để chống lại các hiểm hoạ mới. Kỹ thuật này giám sát những phần của hệ thống có thể bị tấn công, cảnh báo hành vi đáng ngờ và ngăn chặn. Hạn chế của giải pháp này là chương trình độc hại phải hoạt động trên hệ thống thì mới phát hiện được. Vì lý do đó, cơ chế phát hiện dựa vào hành vi sẽ hiệu quả nhất khi nó là lớp bảo vệ bổ sung đằng sau cơ chế quét kiểm tra virus trước khi thực thi.

Công cụ miễn phí, độc lập và bộ công cụ

PC-cillin gộp nhiều thông tin trong một màn hình

Thử nghiệm đánh giá 10 sản phẩm chống virus tốt nhất có thể chống đỡ cả những hiểm hoạ đã biết lẫn chưa biết, từ miễn phí đến 50 USD. Để công bằng, nhóm thử nghiệm (NTN) chỉ kiểm tra thành phần antivirus của các bộ công cụ.

Trong số đó, Avast Home Edition 4.6 của Alwil Software, AntiVir PersonalEdition Classic 6.32 và AVG Free Edition 7.1 của Grisoft là các chương trình độc lập và miễn phí. F-Secure Anti-Virus 2006, Kasperky Anti-Virus Personal 5.0 của Kaspersky Lab, McAfee VirusScan 2006 và BitDefender 9 là các ứng dụng thương mại độc lập. Panda Titaninum 2006 Antivirus + Antispyware của Panda Software và Norton Antivirus 2006 của Symantec đều có kèm công cụ chống spyware. Còn Trend Micro bán sản phẩm chống virus là một phần của bộ PC-cilin Internet Security Suite 2006.

Cách đánh giá

Tổng quát, qui trình thử nghiệm gồm 5 bước.

Thứ 1, kiểm tra khả năng phát hiện 1.518 đoạn mã độc hại được tổ chức WildList nhận diện.

Thứ 2, kiểm tra khả năng phát hiện 136.250 đoạn mã độc hại nằm ngoài danh sách WildList, gồm Backdoor, Trojan và Bot (còn gọi là Zombie). Danh sách này được gọi là zoo, được tập hợp từ người dùng, tạp chí máy tính và các tổ chức nghiên cứu bảo mật.

McAfee VirusScan xếp thứ hai trong kiểm tra heuristic

Thứ 3, đánh giá khả năng heuristics phát hiện những mã độc mới với các chương trình không được cập nhật từ 1-2 tháng.

Thứ 4, kiểm tra khả năng khử 110 virus macro tấn công các ứng dụng Microsoft

Office.

Thứ 5, so sánh thời gian "phản ứng" của mỗi công ty phần mềm đối phó 16 đợt "dịch" diễn ra trong 8 tháng năm 2005.

Để hoàn tất việc thử nghiệm, NTN đã đo tốc độ quét virus của từng chương trình, đánh giá về mức độ dễ dùng, tính năng và chính sách hỗ trợ kỹ thuật.

Người chiến thắng

BitDefender 9 Standard sáng giá nhất, là 1 trong 4 sản phẩm đứng đầu về phép đo tốc độ và giá chỉ có 30 USD. McAfee VirusScan 2006 giá 40USD xếp thứ 2, chương trình có giao diện trực quan và khả năng quét heuristics khá tốt.

PC-cillin Internet Security Suite 2006, kế tục 1 sản phẩm từng đạt Best Buy 2004 của PC World, xếp thứ 9/10 vì kém hiệu quả trong thử nghiệm với zoo và heuristics, giá lại tới 50 USD. Tuy vậy, đây là sản phẩm có thời gian phản ứng nhanh và giao diện người dùng xuất sắc.

Ba chương trình xếp hạng gần kề là AntiVir, Avast lần lượt xếp hạng 7, 8 và AVG ở vị trí "đội sổ". Tất nhiên, với những ai không có chi phí cho phần mềm antivirus thì các sản phẩm miễn phí này chấp nhận được.

Đối đầu trực diện
Norton Antivirus giải thích rõ ràng các thành phần giao diện và chọn lựa của người dùng

Ởcấu hình mặc định và trạng thái cập nhật đầy đủ nhất, tất cả các sản phẩm đều phát hiện 100% virus có trong danh sách WildList ở chế độ bảo vệ thời gian thực và theo yêu cầu.

Các chương trình đều phát hiện và gỡ bỏ thành công các virus macro, chỉ có một vài ngoại lệ. Avast không gỡ bỏ được 10 virus, trong đó có 2 virus tấn công tập tin

PowerPoint phiên bản từ 97 đến 2003 và 4 virus tấn công tập tin World 6. Panda không hoàn toàn khử sạch 2 virus PowerPoint, tuy nhiên các tập tin này vẫn làm việc được. AntiVir thất bại với 10 virus Word 6 và BitDefender bỏ sót 2 virus tấn công tập tin Word phiên bản từ 97 đến 2003. Các virus này không mới nên đúng ra các chương trình phải xử lý được chúng.

Khả năng phát hiện các virus trong danh sách WildList là yêu cầu cơ bản, vì chúng phổ biến; nhưng với danh sách zoo thì vấn đề hơi khác.

Kaspersky Anti-Virus Personal 5.0 là chương trình duy nhất cô lập thành công 100% cả 3 thể loại zoo. F-Secure và Symantec thành công 97%, điểm số vẫn ở mức xuất sắc. PC-cillin cho kết quả rất thất vọng, chỉ có 76% (85% Bot, 82% Backdoor, và 69% Trojan). Lý giải điều này, Trend Micro cho rằng họ không tập trung phát triển sản phẩm để phát hiện toàn bộ danh sách zoo vì những đe dọa này rất ít tác động đối với khách hàng của họ.

Kẻ địch trong bóng tối

Không một sản phẩm nào tỏ ra nổi bật trong các trắc nghiệm heuristics. Tất cả các chương trình đều chưa cập nhật nhận dạng virus 1 tháng, BitDefender hiệu quả nhất, phát hiện 43% worm, 57% Backdoor. McAfee xếp thứ 2, phát hiện 41% worm, 55% Backdoor. F-Secure and Kaspersky theo sát phía sau với 32% worm, 53% Backdoor (tỉ lệ 50% phát hiện được là tốt). PC-cillin một lần nữa gây thất vọng, quét được 5% worm, 7% backdoor.

Trong đợt thử nghiệm thứ 2, thời gian không cập nhật nhận dạng virus mới kéo dài 2 tháng thì hầu hết chương trình đều cho kết quả "rất khiêm tốn".

Tốc độ

Avast có giao diện giống trình chơi nhạc

Sản phẩm được đánh giá theo 2 tốc độ: thứ nhất, tốc độ quét virus và thứ hai quan trọng hơn, tốc độ đưa ra bản cập nhật khi có hiểm hoạ mới. Phần mềm của hãng Panda về đích xuất sắc trong cuộc đua quét virus với thời gian trung bình là 1 phút 43 giây, nhanh gấp 7 lần sản phẩm chậm nhất (Avast).

Về tốc độ xử lý khi virus phát tán, tất cả các hãng đều đưa ra bản cập nhật trong khoảng 12 giờ, Kaspersky nhanh nhất, từ 1-2 giờ, BitDefender và F-Secure theo sát phía sau khoảng từ 2-4 giờ. AntiVir và PC-cillin từ 4-6, Panda cần khoảng 6-8 giờ. Cả 3 sản phẩm AVG, Avast và McAfee đều cần đến 8-10 tiếng và sau cuối đại gia Symantec phải mất 10-12 giờ.

Khác biệt tính năng không nhiều

F-Secure thông báo những nguy cơ bảo mật mới nhất

Một số sản phẩm có thêm những tính năng hay. Tất cả đều có khả năng tự động cập nhật, cho phép thiết lập cấu hình theo ý muốn cá nhân hoặc cho lập lịch quét. Một vài sản phẩm hạn chế tùy biến, chẳng hạn như AVG chỉ cho lập lịch quét trên ổ đĩa và định dạng tập tin nhất định. Không giống như các chương trình khác, Panda chỉ cho phép lập lịch ở phiên bản đầy đủ Panda Platinum 2006 Internet Security Suite.

Nhiều chương trình đã áp dụng màn hình trạng thái giống Windows XP SP2 Security Center, giúp người dùng biết thông tin hiện tại của máy tính. Ví dụ, Norton Protection Center của Symantec báo cho người dùng về mức độ an toàn của PC khi lướt web hay sử dụng email. F-Secure và Panda cung cấp tin nóng về bảo mật tại khay hệ thống. BitDefender hiển thị một cửa sổ đồ thị nhỏ (File Zone) ngay trên màn hình làm việc cho biết số tập tin đã quét vài phút trước đó (người dùng có thể tắt chức năng này).

Tất cả các sản phẩm đều có hỗ trợ kỹ thuật qua email. BitDefender, F-Secure, Kaspersky, Panda và TrendMicro có hỗ trợ miễn phí 1 tuần qua điện thoại. Symantec tính phí 30USD cho 1 lần giải quyết sự cố, McAfee tính 3USD/phút trả lời điện thoại (dịch vụ hỗ trợ qua điện thoại chỉ có hiệu lực tại Mỹ).

Tính dễ dùng

PC-cillin của TrendMicro là sản phẩm dễ dùng nhất, gộp nhiều thông tin về bảo mật trong một giao diện rất thuận tiện. Giao diện trực quan giúp cho người mới làm quen dễ điều khiển, nhưng cũng có những thiết lập dành cho người dùng có kinh nghiệm.

Avast của Alwil nổi bật với màn hình chính hào nhoáng độc đáo có thể thay đổi lớp "áo" (skin) tương tự như các trình chơi nhạc.

Giao diện của các chương trình khác khá đơn giản. BitDefender bật màn hình thông báo chỉ khi kích hoạt tính năng tự động cập nhật tự động và bảo vệ chống virus. Những tính năng quan trọng hơn nằm trong các màn hình được truy cập ở phía bên trái của cửa sổ.

Giao diện chính của Grisoft AVG gây thất vọng, các tính năng hạn chế và một số chức năng cần thiết chỉ có ở phiên bản thương mại AVG Professional.

Mặc dù không có một sản phẩm nào có thể bảo vệ PC tuyệt đối trước những mối hiểm hoạ chưa biết, nhưng chọn lựa 1 trong 4 sản phẩm đầu bảng sẽ giúp bạn bảo vệ PC tốt nhất lúc này.

MICROSOFT ONECARE LIVE

Microsoft sẽ sớm gia nhập danh sách các công ty cung cấp phần mềm bảo mật tất cả trong một. Chúng ta hãy xem qua phiên bản beta của Windows OneCare Live, một trong nhiều dịch vụ cung cấp trực tuyến có thể tải về ở trang Windows Live Ideas (http://ideas.live.com/).
OneCare Live là bộ công cụ và tiện ích bảo mật mà người dùng có thể quản lý chỉ bằng một giao diện duy nhất. Thành phần chống virus hiện tại của bộ ứng dụng này cho phép người dùng quét theo yêu cầu, lập lịch quét, cấu hình tập tin hay thư mục muốn quét. Hiện tại nó chưa quét được email nhận/gửi và chỉ có thể quét tin nhắn từ MSN Messenger. Microsoft đang có kế hoạch kết hợp khả năng quét e-mail và xem xét khả năng quét bổ sung các trình nhắn tin khác.Một lớp bảo vệ theo cơ chế hành vi sẽ theo dõi các tập tin có động tịnh khả nghi, chẳng hạn như thay đổi khóa trong Registry.

Tường lửa của Windows OneCare Live có cảnh báo dễ hiểu

Tường lửa trong OneCare kiểm soát cả đầu vào và ra của mạng, đây là phiên bản

nâng cấp của Windows Firewall. Lần đầu tiên sử dụng OneCare sẽ hỏi những hoạt động phần mềm mà nó không nhận biết được, chẳng hạn như hoạt động cập nhật phần mềm iTunes hay hoạt động mạng của Lotus Notes.
Cài đặt dễ dàng, mặc dù đòi IE6. Một wizard giao diện web sẽ kiểm tra xem hệ thống có đủ yêu cầu tối thiểu không cũng như phát hiện nguy cơ xung đột với các ứng dụng khác trước khi tiếp tục cài đặt OneCare. Microsoft cho rằng OneCare sẽ dò trên máy người dùng để đảm bảo không "đụng độ" với các chương trình chống virus đang chạy. Mặc dù vậy trong thử nghiệm sản phẩm này đã không nhận ra phiên bản client của bộ Symantec Norton Antivirus Corporate. Một kinh nghiệm khác được chia sẻ trên blog của PC World (find.pcworld.com/51360) là OneCare phát hiện và gợi ý gở bỏ phiên bản của Norton Antivirus.
Microsoft chưa định giá cho sản phẩm này nhưng nút Purchase Now (hãy mua ngay) cho thấy OneCare sẽ không miễn phí mãi.

BitDefender 9 - Vietnamese Edition !!!!
Diệt Virus, Chống thư rác, Thiết lập tường lửa với
BitDefender 9 - Vietnamese Edition !!!!

1> Đặc điểm của phiên bản (Việt hóa) này:
Tỷ lệ việt hóa 98% (đã việt hóa phần trợ giúp) -- Thế thôi

2> Một số hình ảnh

3> Cài đặt:
Sau khi download bạn được 2 file Lang -I Và Lang - II bạn cần clik đúp vào là chương trình tự chạy

4> Rắc rối:
Nếu bạn không hiển thị đúng tiếng việt xin hãy xem bài này
http://www.updatesofts.com/forums/sh...5&postcount=44

5> Tồn tại:
Có 1 số chỗ chưa việt hóa được vì khi việt hóa cho KQ thế này

Sẽ cố gắng tìm cách khắc phục sớm nhất

6> Cám ơn
- Cám ơn Softwin đã làm ra soft này

- Cám ơn tôi

- Cảm ơn tất cả mọi người, những ai đã từng tin tưởng & dùng **BitDefender 9 - Vietnamese Edition** !!!!, ủng hộ cho phong trào Việt hóa phần mềm, "người Việt dùng hàng Việt". Sự động viên, cổ vũ của các bạn là chính là nguồn động lực giúp cho những sản phẩm thuần Việt không ngừng ra đời.

Hy vọng mọi người sẽ hài lòng với phiên bản này. Rất mong nhận được ý kiến đóng góp của mọi người để sản phẩm ngày càng hoàn thiện hơn.
LINK
Code:
http://rapidshare.de/files/17150187/Lang_-_I.exe.html
http://rapidshare.de/files/17150220/Lang_-_II.exe.html

Bản cập nhật cho Bitdefender:
+Đây là file ngôn ngữ cập nhật cho Bitdefender phiên bản

+Cập nhật tiếng việt cho:
-Phần quét Spyware + Riskware ....
-Tính năng nhận dạng "OutBreak Detection"

Download
Code:
http://d.turboupload.com/d/618900/BitDefender9_-_7.068687_.rar.html

An toàn hơn cho máy tính với Cyberhawk - 22/8/2006 6h:51

Các phần mềm gây hại cho máy tính ngày càng nhiều và ngày càng "hiểm độc" hơn. Vì vậy, cài đặt một vài công cụ phòng chống các phần mềm độc hại ấy là điều cần thiết cho máy tính.

Hãng Novatix cung cấp cho chúng ta một phần mềm miễn phí giúp đem lại an toàn cho máy tính bằng cách phân tích và giám sát hoạt động của các file, các ứng dụng nền, các tiến trình từ đó có những cảnh báo và sự phong tỏa cần thiết nếu máy tính bị "nhiễm độc". Cyberhawk có dung lượng 6,45 MB, tương thích Windows 2000/XP, tải về từ địa chỉ www.novatix.com.

Cửa sổ làm việc chính của Cyberhawk gồm phần bên trái là 5 nút chức năng, khi bấm vào một nút thì phần bên phải sẽ hiển thị các thông tin tương ứng.

1/ Security Status: Gồm Your Protection và Cyberhawk SecureCommunity Protection cung cấp các thông tin về việc Cyberhawk đang thực hiện để bảo vệ máy tính.

2/ Protection Log: Những báo cáo về tất cả các tiến trình mà Cyberhawk đã giám sát, kiểm tra

3/ Undo: Khi Cyberhawk dò tìm và nghi ngờ một hoạt động nào đó đang xảy ra trong hệ thống có thể gây hại, sẽ đưa ra cảnh báo để chúng ta quyết định có cho phép nó hoạt động hay không.

4/ Ruler Setting: Bấm nút Custom Rule Settings ở cửa sổ bên phải để có hộp Cyberhawk Settings.

- Thẻ Custom Rules đánh dấu chọn Check All. Có thể tạo mới bằng cách bấm nút New và làm theo các bước hướng dẫn của Rules Wizard.

- Thẻ File Blocking: Bấm nút Check All, có thể bấm nút New thông qua hộp File Blocking Group.

- Thẻ Process Lists: Chấp nhận sự mặc định của chương trình.

5/ Options: Cả ba tùy chọn theo mặc định đều trong trạng thái mở. Nếu muốn tắt thì bấm vào Turn Off Cyberhawk hoặc Turn Off Automatic Updates hoặc Disable Community Contributions. Để kích hoạt cũng bấm vào vị trí của những hàng chữ ấy.

Theo Thanh Niên

D32 với kỹ thuật nhận dạng virus hướng tiếp cận máy học

Kể từ bản cập nhật D32 phát hành ngày 8/8/2004, cơ sở dữ liệu (CSDL) virus của phần mềm đã được thiết kế lại theo hướng áp dụng các kỹ thuật Khai Khoáng Dữ Liệu (Data Mining). Đây là bước khởi đầu trong lộ trình triển khai các kết quả từ đề tài nghiên cứu hệ chống virus thông minh hướng tiếp cận máy học (Machine Learning) của tác giả.

Thay vì nhận dạng truyền thống từng mẫu virus xác định như trước đây, D32 (8/8/2004) nhận dạng virus theo đơn vị lớp (class) sử dụng kỹ thuật NNSRM-Nearest Neighbor Structural Risk Minimization - một giải thuật phân lớp tiên tiến trong Khai Khoáng Dữ Liệu và Máy Học, được các nhà nghiên cứu công bố trên tạp chí Elsevier (www.elsevier.com), tháng 9/2003.

Giống như tên gọi của nó, NNSRM dựa trên đặc trưng giống nhau giữa các điểm dữ liệu của một lớp để xây dựng quyết định phân lớp. Tính chất này được tính bằng tỷ lệ nghịch khoảng cách giữa các điểm dữ liệu trong tập chẩn đoán. Điểm dữ liệu chưa phân lớp sẽ được gán vào lớp chứa các điểm có khoảng cách gần nó nhất, với độ rủi ro thấp nhất. Khi quét dữ liệu, D32 sẽ tính toán "khoảng cách" của file so với các đặc trưng của lớp virus cần chẩn đoán để phân bổ tập dữ liệu này vào các lớp lân cận nhất của nó. Tuy phải tốn thêm giai đoạn phân lớp khá công phu và phức tạp, nhưng kết quả lại rất khả quan. Nếu như trước đây D32 phải chạy đủ 300 thủ tục nhận dạng 300 sâu trình (worm), đến nay số thủ tục nhiều nhất mà D32 phải triệu gọi khi chẩn đoán 1 file EXE là 10 thủ tục!

Một đặc điểm nữa của kỹ thuật này là CSDL được rút gọn, đặc biệt quan trọng khi kích thước tập mẫu gia tăng đáng kể. Điều này lý giải sự "giảm sút" số lượng virus của D32 (800 virus ở các phiên bản 7-2004 đến 700 virus ở phiên bản 8-2004). Ngoài ưu điểm nổi bật về gia tăng tốc độ và tiết kiệm không gian lưu trữ, NNSRM còn được đánh giá là một giải thuật triển vọng cho các bài toán phân lớp dữ liệu tuyến tính với độ chính xác cao. Trước khi công bố D32 (8/8/2004), chúng tôi đã chạy thử nghiệm song song 2 phiên bản (D32 cũ-800 virus và D32 mới-700 virus) trên bộ sưu tập virus thu thập từ trước đến nay. Kết quả nhận dạng là như nhau nhưng phiên bản mới chạy nhanh và ít nhầm hơn.

NNSRM là kỹ thuật khá mới, có nhiều ưu điểm vượt trội nhưng cần thời gian khẳng định. Vì vậy chúng tôi chỉ áp dụng thử nghiệm cho các quá trình chẩn đoán worm và trojan horse cho D32. Trong thời gian tới, chúng tôi sẽ mở rộng giải thuật này cho quá trình chẩn đoán các loại mã gây hại (harmful code) khác (như backdoor, malware, spyware...)

Chúng tôi hy vọng trong thời gian không xa sẽ tiếp tục công bố các nghiên cứu mới nhất trong lĩnh vực nhận dạng virus thông minh, từng bước cải tiến D32 trở thành phần mềm chống virus trí tuệ của Việt Nam.
Cần Thơ, thng 8/2004

Trương Minh Nhật Quang

CẬP NHẬT D32

Bản nâng cấp phần mềm D32 (08/08/2004) bổ sung virus Mydoom.o.exe, Mydoom.o.gen và Mydoom.o.zip.
Bản nâng cấp phần mềm D32 (24/08/2004) cập nhật sâu Ratos.a.gen.worm.W32, Ratos.a.exe.worm.W32 và Ratos.x.worm.W32. Ratos lây theo email với các đặc điểm như sau:
Subject:Photos
Body: LOL ! ;)))
Attachment: photos_arc.exe
Khi kích hoạt, Ratos chép vào thư mục hệ thống thành các file rasor38a.dll và winpsd.exe.
D32 (24/08/2004) còn cập nhật các loại sâu Lovgate.hx.worm.W32, Lovgate.hz.worm.W32, Lovgate.r5.worm.W32, Lovgate.rx.worm.W32. Đây là loại sâu có nhiều biến thể, kích thước từ 120 KB đến 140 KB, chuyên làm tràn các hộp thư mail.

Norton Ghost 10 và tạo đĩa Symantec Recovery Disk

Norton Ghost là phần mềm chuyên dùng để sao lưu, phục hồi dữ liệu trên máy tính. Norton Ghost giúp đơn giản hóa cài đặt phần mềm cho nhiều máy tính có cùng cấu hình (rất thích hợp cho các quán nét). Norton Ghost có khả năng sao lưu toàn bộ ổ đĩa hay một phân vùng lên ổ cứng khác (phân vùng khác), lên DVD, CD, lên các phương tiện lưu trữ di động USB. Norton Ghost đã có phiên bản mới nhất là Norton Ghost 10, ở phiên bản này bạn có thể sao lưu và phục hồi dữ liệu ngay trong hệ điều hành Windows, bạn không cần phải khởi động lại máy như các phiên

bản trước. Norton Ghost 10 chỉ được cài đặt trên hệ điều hành Windows XP và Windows 2000 SP4. Norton Ghost 10 được chạy trên nền Microsoft Frame Net 1.1. Phiên bản này giao diện được cải thiện đẹp đẽ hơn so với các bản trước, không tối tăm như các phiên bản 8.*, không sợ nhầm lẫn nữa. Phù hợp với những người mới làm quen với Ghost.
+ Cài đặt:
Các bản có thể tải tại:

http://www56.fixdown.com/endown/lz04oq06-2006-03-13.rar

Nếu không tải được thì bạn có thể thử với các link khác:

http://www422.fixdown.com/lz04oq06-2006-03-13.rar
http://www414.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www408.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www10.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www21.fixdown.com/endown/lz04oq06-2006-03-13.rar
http://www36.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www82.fixdown.com/lz04oq06-2006-03-13.rar
http://www400.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www412.fixdown.com/keydown2003/lz04oq06-2006-03-13.rar
http://www420.fixdown.com/lz04oq06-2006-03-13.rar

Với dung lượng 142 MB. Sau khi tải về bạn giải nén file lz04oq06-2006-03-13.rar bằng WinRaR và chạy file norton_ghost_v10.exe để giải nén tiếp. Sau khi giải nén bạn chạy file SETUP.EXE để cài đặt Norton Ghost 10. Sau khi cài đặt Norton Ghost 10 bạn nên tiếp tục cài Microsoft Frame Net 1.1 ở thư mục SUPPORT\DOTNET và khởi động lại máy tính.
+ Đăng ký
Sau khi khởi động lại Norton Ghost 10 sẽ "Activation".

Khi được hỏi bạn chọn "Activate later". Bạn click Next một vài lần rồi click Finish để kết thúc. Sau đó bạn chạy file "patch.exe" để đăng ký.
Khi gặp thông báo thì bạn đã đăng ký thành công.

+ Sao lưu dữ liệu:
Sau khi cài đặt chương trình sẽ có biểu tượng

trong khay hệ thống. Để sao lưu bạn clich chuột phải và chọn Back Up Now, tại đây có 2 tùy chọn sap lưu:
Back Up All Drivers: Sao lưu toàn bộ ổ đĩa.
Define New Back: Lựa chọn phân vùng cần sao lưu.
Các bạn chọn Define New Back, click Next để tiếp tục. Sau khi chọn phân vùng cần sao lưu bạn click Next. Tại đây có 2 lựa chọn:
Recovery Point set (recommended): Tạo điểm phục hồi
Independent recovy point: tạo bản sao lưu của một phân vùng.

Bạn click Next để tiếp tục.
Tại đây bạn cần phải chỉ ra nơi lưu bản sao. Bạn click vào Browse… để chọn nơi lưu. Các bạn có thẻ đổi tên bằng cách click vào Rename. Sau đó bạn click Next để tiếp tục.
Ở bước này bạn có thể đổi tên, lựa chọn mức độ nén. Bạn cũng có thể đặt mật khẩu, chia file sao lưu thành nhiều file bằng nhau, bỏ qua Bad sectors (nếu máy bạn có Bad sectors). Bạn click Next để tiếp tục.
Nếu bạn muốn sao lưu ngay thì chọn Manually, để đặt lịch sao lưu thì chọn Scheduled. Click Finish để bắt đầu sao lưu.
+ Phục hồi dữ liệu:
Bạn clich chuột phải lên biểu tượng
trong khay hệ thống. Để phục hồi có 2 lựa chọn:
Recover My Computer: phục hồi cả ổ đĩa hay một phân vùng.
Recover My Files: chỉ phục hồi một file hay một thư mục.
Các bạn chọn Recover My Computer, nếu bạn có nhiều bản sao lưu hãy lựa bản sao lưu các bạn muốn rồi click Recover My Computer, tiếp theo đánh dấu vào dấu kiểm Express (recommended), click OK để tiếp tục. Sau đó có một bảng thông báo hiện ra. Bạn click Yes.

Khi các bạn chỉ muốn phục hồi một vài file hay một thư mục thì bạn chọn Recover My Files. Nếu có nhiều bản sao lưu bạn hãy chọn bản bạn cần và click vào Browse Contents.

Tại đây bạn hãy lựa chọn file hay thư mục bạn muốn phục hồi, click chuột phải vào file hay thư mục và chọn Recover (Ctrl + R), tiếp theo bạn click vào Browse …để lựa chọn nơi phục hồi, click Recover để phục hồi.

+ Tạo đĩa Symantec Recovery Disk:
Như bạn biết Norton Ghost 10 này không hề cung cấp một công cụ nào để có thể làm ra đĩa CD boot dùng để phục hồi ổ cứng hay phân vùng từ file sao lưu khi không thể vào Windows. Nếu bạn muốn có đĩa này thì bạn phải mua từ Symantec. Tôi sẽ hướng dẫn bạn làm ra đĩa Symantec Recovery Disk mà không phải mất tiền mua. Nếu bạn để ý sẽ thấy sau khi bung file norton_ghost_v10.exe, sẽ có một số thư mục trong đó có thư mục I386. Bạn đã nhận thấy có gì lạ không? Thật ra đây đã là một đĩa Symantec Recovery Disk rồi nhưng chưa được đóng gói thành file ISO để có thể ghi ra CD làm đĩa boot Symantec Recovery Disk. Các bãn hãylàm theo các bước sau đây :
- Dùng UltraISO để mở một file ISO của bất kỳ một file ISO của bộ cài Windows XP nào hoặc của bất cứ file ISO nào của Win PE (ERD Commander 2005, Reatogo PE, BartPE). Bạn chỉ trích lấy file Boot bằng cách dùng UltraISO mở file ISO và trong Tap Bootable chọn Save Boot File, bạn lưu lại với tên XP.bif.
- Bây giờ bạn dùng UltraISO tạo một file mới bằng cách click vào tap File\New\Bootable CD\DVD Image, tại đây bạn hãy mở ra file XP.bif mà lúc trước đã lưu.
- Bạn hãy mở lại thư mục chứa bộ cài Norton Ghost 10 và chọn tất cả các file và thư mục (có thể bỏ qua file norton_ghost_v10.exe), các bạn kéo và thả vào UltraISO. Nếu không các bạn có thể dùng cách nhớ từng file và thư mục vào trong UltraISO, các bạn chọn tap Actions chọn Add Files … để nhớ file, Add Directiry… để nhớ thư mục, cách này thủ công và lâu hơn so với việc kéo và thả vào UltraISO. Sau khi đã kéo và thả các file và thư mục bạn Save lại thành một file *.ISO với tên gì thì tùy bạn. Bạn có thể dùng UltraISO để ghi ra đĩa CD luôn hoặc các chương trình ghi đĩa khác.
Nếu bạn cẩn thận bạn có thể dùng các chương trình tạo máy ảo (VirtualPC, VMware Workstation) để kiểm tra.
Đi kèm với Symantec Recovery Disk còn có các chương trình sau: Ghostxp V.2003, Ghost 32 V 8.2, Norton AntiVirus PRESCAN, NDD
Lưu ý để chạy được đĩa Symantec Recovery Disk này máy bạn phải có dung lương RAM nhiều hơn 200 MB và Norton Ghost 10 chỉ mở được file có phần mở rộng là *.v2i, không thể mở được đối với file *.gho.

Cài Hiren bootCD7.9 vào ổ cứng để cứu hộ ?

I) Đặc điểm của bài viết này:
Bạn đã biết qua việc cài Hiren boot CD vào USB để cứu hộ, nhưng để Hiren boot trong cây viết USB như vậy khá bất tiện : Ngoài chuyện mất chỗ khá nhiều hơn 50MB, việc cứu hộ, lại lâu lâu mới có .
Do vậy tốt và tiện cho bạn nhất, là cài sẵn Hiren boot CD ngay trong ổ cứng cùng XP và khi cần sẽ dùng, tiện hơn là có trong đĩa CD (đôi lúc còn bị trầy).
II) Bằng cách nào bạn chuyển mọi file từ Hiren boot CD 79 mới nhất vào ổ

cứng? :

A) Điểm quan trọng để làm được là XP của bạn trong C phải đã có sẵn DOS thực. Nếu ổ C hoàn toàn chưa có, hay đang ở NTFS , bạn cần thực hiện từng bước những điểm sau đây:

1) Nếu ổ C của bạn đang là NTFS, phải chuyển trước về FAT 32, mới cài Hiren CD trong ổ cứng cùng với XP được .

Có hai trường hợp đặt ra cho bạn :

a) Nếu XP có cài sẵn Partition magic 805 : Bạn có thể chọn convert C partition sang FAT 32 ngay trong XP , và khi chọn xong, nó sẽ reboot lại để ra môi trường PE*(trước khi vào XP) mới làm được .

b) XP của bạn chưa cài PM 805 , bạn buộc phải để đĩa CD Hiren 79 vào ổ CDROM, chọn first boot device trong CMOS là CDROM .

Xong vào PM 805 ở trong Hiren 79 để convert ổ C từ NTFS thành ra FAT 32 .

2)Tải 2 file dạng zip sau đây từ Megaupload , rồi bung ra từng file trong ổ cứng ở ổ E, hoặc ổ F :

a) Winimage 80 dạng zip : ở
http://rapidshare.de/files/22669102/WinImage_80.zip.html

b) Boot98. IMA dạng zip: http://rapidshare.de/files/19898933/BOOT98.rar.html

3) Bắt đầu chạy Winimage 80 và đặt 1 đĩa mềm mới tinh và ổ A: Chọn vào open để tìm ra nơi đã lưu file boot98.ima.

Sau đó, bạn chọn vào disk rồi write disk: nó sẽ ghi file hình ảnh boot98.IMA vào đĩa mềm mà bạn chuẩn bị xong trong ổ đĩa .

4) Đĩa mềm này sau khi làm xong sẽ tự boot được, nhưng khác với các đĩa mềm khác là nó có sẵn NC 5 để coi file bên trong và có sẵn 3 dụng cụ để giúp bạn tạo ra được DOS thực cho XP.

5)Chọn lại trong CMOS , first boot device là Floppy disk: Để đĩa mềm mới làm ra tự boot vào ổ đĩa. Reboot máy lại và lần này ở ngay dấu nhắc A:\>

6)Bạn đánh lần lượt 3 lệnh như sau:

a) sys A: C: bạn sẽ thấy dòng chữ system transferred là thành công . Bạn sẽ boot được vào dấu nhắc C:\> nhưng hết boot vào Win XP được nữa.

b)debug< read.scr, để tạo ra bootsect cho DOS.

c) sysXPfat C: máy bạn sẽ reboot lại vào WinXP được như cũ .

d) Trong và trường hợp, lệnh sysXPfat C thất bại không giúp vào XP, bạn đánh lại một lệnh khác tư ødấu nhắc A là bootpart winnt boot: C:

e) Chép file boot.ini từ ổ đĩa mềm A vào C .

B)Chuẩn bị các file Hiren boot CD 79 chép vào ổ C nhằm boot được cùng XP như

sau:
1)Để đĩa Hiren boot CD 79 vào ổ CDROM và boot bằng đĩa này: Trong Hiren, chọn bất cứ chương trình Files manager nào cũng được từ Volkov commander 49 hay File Wizard, để chép tất cả file từ ổ A vào ổ E hay F trong đĩa cứng với một thư mục tạo sẵn là Hiren 77 , ngoại trừ 2 file file jo.sys và command.com(không chép).
2)Vẫn để đĩa CD Hiren 797 trong ổ CDROM, tìm ra ồ CDROM chép hết thư mục BOOTCD từ đĩa CD Hiren 79 vào thư mục Hiren 79 trong ổ E hay F .
3)Chép lần cuối toàn bộ các file, folder có trong Hiren 79 vào ổ C đang có sẵn Win XP.
C) Với phiên bản mới nhất 79 này Hiren có thêm điểm khá đặc sắc là có thêm Win98 thu nhỏ dể dễ dành chép file dài qua lại các ổ đĩa.
Không còn dùng Windows quá xưa là Win3.11 như các phiên bản cũ trước đây 75 hay 76 .

III) Hưởng thụ thành quả có XP và Hiren boot CD 79 cứu hộ có trong ổ cứng:

Bạn giờ reboot máy lại , bạn sẽ không cần đến CD nào nữa, nhờ file boot.ini trong XP, bạn sẽ chọn vào XP hay Hiren 79 mỗi khi bạn cần cứu hộ bằng ghost83 , PM 805; hay khi cần xoá file nào đó mà XP không cho phép làm trong XP.
Lưu ý, điểm khác nhau giữa Hirenboot trong ổ cứng cùng XP, là bạn vẫn ghost thoải mái cho mọi ổ đĩa khi cần backup vì nguyên tắc Hiren làm việc là dùng RAM disk ở ở R, chứ không phải trên ổ C nên Ghost ổ C thoái mái không sợ gì trục trặc nữa.

Dr Hoàng
Hiren boot CD 8.1
http://files.9down.com:8080/HBCD81-%...own.com%5D.rar
[*]Tổng Quan Hiren's Boot 8.0 ^_<
Tổng Quan Hiren's Boot 8.0
*By **anhtu9a@yahoo.com** với giúp đỡ của 45h thực hành trên máy ^_!^*

Thạch Bàn - LB - Hà Lội 22/04/2006
Updatesofts.com

Hirent's Boot - cái này ai cũng biết hay từng nghe nói đến : Nó mạnh mẽ vô cùng với cả trăm chương trình - hàng ngàn chức năng đa dạng phong phú, cao thủ có, thấp thủ cũng có, đơn giản có , phức tạp có… gì cũng có . Với phiên bản 8.0 đã có

sự chuyển biến về giao diện cũng như chức năng rất mạnh mẽ - tăng cường khả năng ổn định của các chương trình + mức độ cập nhật cực nhanh so với các bản 7.x trước đó .
Hiren's Boot chia thành các mục riêng biệt để cho người dùng ko bị hoa mắt khi lạc vào mê hồn trận của nó - có trên 10 mục lớn à mỗi mục lớn có vô số các chương trình cùng loại với nhau.
Việc sử dụng đến 20% các phần mềm có trong này là một điều hiếm thấy vì ngay cả các vọc sĩ chuyên nghiệp cũng thường chỉ dùng đến tầm 10 chương trình là nhiều (dùng thường xuyên). Nhân dịp UDS tổ chức Tutorial Contest - em đã dành 5 ngày để dạo quanh một vòng gần như tất cả các phần mềm có trong Hirent nhằm mang đến cho các bác một cái nhìn khái quát gần như toàn bộ các chương trình có trong này - mục đích chính của chúng ta sẽ tuyển chọn ra các chương trình hay nhất để dùng vào các mục đích riêng của mỗi người .

I) Disk Partition Tools

+1) Partition Magic Pro 8.05

Cái này chắc mình ko phải nói nhiều vì nó gần như quá quen thuộc với bất cứ ai thích chia chác: Nó dùng để chia ổ mà KO MẤT DỮ LIỆU - đánh giá là số một hiện nay. Giao diện rất trực quan -> nhưng mà nhiều khi sự kết hợp nó với các chương trình khác ko phải là một điều tồi vì biết 2 hay 3 phần mềm cùng loại luôn hay hơn là 1 vì hiếm khi nó có vấn đề nhưng cũng thi thoảng xảy ra, lúc đó việc biết thêm các phần mềm khác phát huy tác dụng.

+2) Acronis Disk Director Suite 9.05

Có thể chia ổ nhưng mà ko thể Merge được

+3) Paragon Part Manager Server 7.0

Cũng chia ổ nhưng mà mình ko thấy chức năng Merge của nó đâu cả.

+4) Partition Commander 9.01

Mình rất chú ý đến thằng này (nó có giao diện như Win ấy)
Phần Tool của nó có các chức năng Resize, Delete, Format, Copy, Validate, Hide, Convert FAT, NTFS, Boot Fixer .. nói chung thằng này khá đơn giản, dễ hiểu, hỗ trợ rất nhiều định dạng khác nhau. Ngoài các dạng phổ biến như FAT, NTFS, Ext2, Ext3, Swap, Reiser (Linux) còn có Fat-auto, HPFS, BeOS, Customize.
Có chức năng quét ổ để xem có lỗi ko. Mình ko thấy chức năng Merge của bản trên DOS nhưng chắc là bản trên Win sẽ có cái này. Tốc độ của nó cũng ko nhanh

lắm .
Không hiểu sao mình ko dùng được chức năng Move của nó - vì mỗi lần dùng là nó báo lỗi đỏ lòe .
Trong menu Start của nó có Backstep Wizard đấy à đừng ai dại mà đụng vào - nó để delete ổ đấy ạ .
Nói chung em đánh giá thằng này 5 lạng nửa cân so với PQ Magic - nếu chăng chỉ kém chút cíu .

+5) Ranish Partition Manager 2.44

Cái này giao diện xanh lè như VC và NC ấy - chả thấy các chức năng nó đâu àmình nghĩ nó chỉ để dùng xem các Cylinder, Size … của HDD mà thôi vì khi dịch chuyển bằng các mũi tên qua các ổ các bác sẽ thấy thông tin của nó hiện ra trong ô chữ nhật phía dưới (như kiểu lý lịch ấy ạ)

+6) The Partition Resizer 1.34

Nó có vài chức năng như:
_Resize/Move Partition
_Change Partition Cluster Size
_Partition Information
_Exit
Khi chọn resize thì các thao tác khi thực hiện toàn dùng bàn phím để chia ổ như left, right, home, end, tab, shift …
Nhưng được cái chia ổ bằng thằng cũng hay phết các bác ạ - nhanh ghê - tuy rằng nó ko có giao diện graphics.

+7) Smart Fdisk 2.05

Cái này chỉ có tạo ổ Primary, Logical, Delete, Boot Manager thôi - ít chức năng quá, đơn giản quá nhưng cũng ko phải đồ bỏ vì nó có chức năng test đĩa xem có bị lỗi gì hay ko - cũng được.

+8) Special Fdisk 2000

Cái này chỉ dùng để Boot Manager + Fdisk: chủ yếu dùng để chọn ổ nào để Boot ấy mà.

+9) Extended Fdisk

Cái này cũng có thể tạo HPFS, FAT … vài định dạng đơn giản.

+10) Gdisk 1.1

Mình dùng nó thấy nó báo fix mấy cái active mà ko active ổ.

+11) Free Fdisk

Vài chức năng:

_Creat Partition …
_Set active partition …
_Delete Partition …
_Display Partition Information

+12) Delete Partition

Xóa ổ - nó chỉ có mỗi chức năng ấy

II) Disk Clone Tools

+1) Image Center 5.6 (trước là Drive Image 2002)

Các bác đã biết đến nó với cái tên Drive Image 2002 nhưng nay nó đã bị bọn Symantec "thịt" mất rồi à chương trình backup dễ dùng nhất, tương thích phiên bản tốt - tốc độ nhanh - nén cũng khá tốt - giao diện trực quan (ko biết em khen thế đã hết các ưu điểm của nó chưa nhỉ ?)

(diễn đàn mình đã có tuts về thằng này)

+2) Ghost 8.3

Em ko khoái nó lắm vì ngày xưa thời NewBie dùng nó tí nữa bị nhầm - nó dùng backup ổ khá tốt, tương thích phiên bản thì lại ko cao, bản 9.0 chạy rất chuối vì phải cần cả 1 CD để Boot à bản 9 này cũng là phiên bản được trông đợi nhưng lại gây thất vọng nhiều nhất. Nói chung em thích các phiên bản chạy trên Dos của nó dạng đơn giản hơn là các bản chạy trên Win - bản trên win em hay dùng bản 2003 thôi.

Khi vào trong DOS sẽ thấy có bản Gh hỗ trợ USB, ghost ổ SCSI (máy chủ), Gh thường, Ghost tỉ lệ nén cao, Gh có hỗ trợ chẻ file ra 700 Mb để bắn CD (hé hé hé - thằng này tiến bộ rồi à nó cho ngay vào đây chứ ko phải đi mò như trước, nếu mà ko có cái chức năng này thì còn lâu nó mới kịp Image Center và True Image bởi vì 2 chương trình này có cả phần chọn chẻ file ngay khi quá trình thực hiện mà ko cần phải có chương trình riêng)

Để chạy các file backup thì sau khi cho đĩa Boot vào - chạy chương trình backup - bỏ đĩa Boot ra - cho đĩa thứ nhất vào rồi Browse đến file đó - đợi nó thực hiện - hết đĩa nó sẽ bảo cho tiếp đĩa 2 vào - cứ làm vậy cho đến hết.

(diễn đàn có bài rất chi tiết về Ghost rồi)

+3) Acronis True Image Enterprise Server 8.1.945

Thằng này rất tuyệt - nó mới được cho vào Hiren trong mấy version 7.x gần đây nhưng đã được đánh giá khá cao: Tốc độ cực nhanh - giao diện đơn giản, trực quan - dùng cho Newbie y như thằng Image Center 5.6 rất tốt.

Bản trên Win nó chạy rất tuyệt - nó còn có thể backup bổ xung, tuy nhiên em ko mấy khi dùng bản bổ xung vì em chỉ làm 1 lần rồi cất đi . Bản trên win còn có thể tạo vùng an toàn, check ổ …

(diễn đàn đã có bài chi tiết về nó)

+4) Partition Saving 3.10

Vài chức năng:

_Save an element

_Restore an element

_Copy an element

_Check a saving file

_Copy a saving file

Phần element để lưu vài cái như all sector, master boot record, first sector, partition

table .. nhưng mà các chức năng nó loằng ngoằng bỏ xừ, chả đâu vào đâu à chán quá em té

III) Antivirus

+1) F Prot Antivirus
Thằng này quét khá phết - nhanh - giao diện trực quan - dễ dùng
+2) McAfee 4.4
Em hay dùng thằng này, nó update 08/04/2006 à quá tốt, quét được >185000 loại virus + trojan …
Quét khá hay - chất lượng tốt - giao diện dễ vô cùng - tốc độ quét 160 GB mất chừng ~ 2h - khá lắm à tuy nhiên thỉnh thoảng mấy cái kegen xịn của em lại bị nó xóa mất tiêu (Norton ít/ko bị vậy)

Chú ý: các bác khi click vào các chương trình này trong menu thì thì ngay sau đó cóa lựa chọn về thằng VC - các bác bỏ qua đừng làm gì nó , ko click zdì hết cứ để mặc nó. Nếu click vào là nó nhảy ngay vào VC chả làm ăn gì được nữa đâu.

IV) Recovery Tools

+1) Active@ Partition Recovery v3.0
Nó chán bỏ xừ - giao diện xanh như NC - mình chưa dùng đã bị treo, mà nhìn kỹ chả thấy chức năng gì - chỉ thấy cung cấp vài thông tin về HDD.
+2) Active Uneraser 3.0
Thằng này cũng xanh lè xanh lẹt như thằng trên - nó recover từ ổ này sang ổ kia nhưng mà chắc cũng chuối - mà chờ mãi ko được mình tắt luôn .
+3) Ontrack Easy Recovery Pro 6.10
Cái này đỉnh cao rồi khỏi bàn cãi - nó là lựa chọn Recovery số 1 à giá bán bản trên Win vào ngàn $ đấy các bác ạ - ko rẻ đâu - gần như là phần mềm đắt nhất trong đĩa Hiren (theo em biết cho đến nay) nhưng mà các bác chú ý cái NTFS nhé.
(em thấy đã có bài full về cái này trên diễn đàn - các bác tìm lại là thấy liền)
+4) Disk Commander
Cái này giao diện cũng thân thiện - rất dễ dùng - recovery dữ liệu cũng được.
+5) Test Disk 6.3
Cho biết vài thông tin của ổ đĩa - màn hình đen như DOS ấy. Nó cũng có thể change Type của ổ như FAT, NTFS.
+6) DiyData Recovery Disk Path 2.1.10
Cái này cho phép quét ổ sau đó các bạn có thể chọn từng ổ - để xem nó thuộc loại gì - có lỗi read / write hay ko. Nếu nó xuất hiện màu đỏ là lỗi .

Ngoài ra nó còn có chức năng Editor, có cả công cụ chuyển đơn vị như Hex sang Dec, Dec dang Hex … (ko biết có ai thèm dùng hay ko ?
)
Có cả backup và restore nhưng mà em ko hiểu lắm vì thấy nó ko giống backup thường mà chỉ backup nội dung sau:
Procedure will backup the Partition Table and the associated Boot Sector or LDM database.

+7) Prosoft Media Tools 5.0 v1.1.264

Thằng này Initializing lâu quá làm em chờ sốt hết cả ruột . Nó có chức năng như File Recovery , Boot / Partition repair, Secure Wipe (xóa vĩnh viễn để đảm bảo ko lấy lại được), Format à giao diện xanh xanh trông chán phèo - em nhìn qua list cóc thèm đi sâu thêm nữa .

+8) Lost and Found 1.16

Cái này cứu dữ liệu nhưng mà load lâu ơi là lâu à em loại nó từ vòng gửi xe (dù trước đây nó nổi đình nổi đám, nghe quảng cáo rất oách) : thấy nó thua xa Easy Recovery và Get data back.

+9) Photo Rec 6.3

Cái này dùng để cứu các loại file như 7zip, asf, au, doc, eps, exe, bmp, gif và 1 vài loại khác

+10) Recover

+11) Undelete 0.83

Hai cái này em chả thấy gì mà nó nhảy ngay vào R:\>

V) Testing Tools

+1) RAM Testing Tool (Memory)

a) Doc Memory 2.2b

Dùng để test RAM xem nó có lỗi gì ko - kết quả của nó là Passed và Failed xuất hiện ở phía dưới bên phải màn hình ấy ạ - test xong xem thông báo tại đó.
Cái này test hơi lâu - 512 MB của em nó test mất gần tiếng

b) Gold Memory 5.07

Cũng để test RAM xem thế nào - có thể Manual test hay Quick test - cái bản này chưa đăng kí (sao bọn Hiren này lại ko Reg nhỉ - nếu ko thì mail em một cái em gửi cho bản full có phải hay hơn ko - he he he
) . Mấy chức năng ko xài được vì là Unreg Version (bị đánh dấu hoa thị *)
Nó test lâu quá - em để nó test rồi xuống ăn ốc - hết cả mấy đĩa ốc rồi chạy lên mà nó vẫn chưa xong (45 ') à mãi hết được 100% thì nó lại chạy tiếp 1 phần khác mà em đoán mất ko ít time - tức mình em cancel luôn. Biết vậy là đủ rồi .

c) Memtest86 + Ver 1.65

Mãi mà nó chẳng chạy - cứ xanh như kiểu cài XP ấy - bye nó luôn - time là vàng mà cứ đợi nó thì em đánh rơi nhiều gold quá

+2) Speed Test
Nó cho biết các phần cứng của em như CPU, RAM, BIOS, Card …
Kết quả test RAM của em với kết quả:
Passed
Data Cache L1 (512 KB) - 6015.23 MB/s
Memory Throughout - 973.73 MB/s

Test ổ cứng thì em được biểu đồ kiểu như thế này và vài thông số:

Random seek time: 10.11 / 15.54 ms
Track to track seek: 2.19 ms
Random access time: 16.35 ms
Bufferd read speed: 4792 KB/s
Và mấy cái khác nữa …
+3) PC Check 5.5
Cái này em nhìn thấy có vẻ Pờ rồ (Pro) à nó check RAM, main, chip , FDD, HDD, Keyb, Mouse, Print ….
_Em test thử chip (Processor) thấy nó passed hết - ngoài ra có mấy cái mà chip của em ko có nên nó báo absent (thiếu) như AMD 64 Bit core, 3D! Now Extension.
_Main: cũng passed hết - may quá
DMA Controller
System Timer
Interrupts
Keyboard Controller
PCI bus
CMOS
Em chọn kiểu Test All
_ Test ổ cứng: ôi nhiều mục quá em test sao xuể - chạy thử mấy cái thấy lâu quá - thôi em chuồn

Bác nào thích thì thử nhưng mà em check ổ em ngon rồi nên em bỏ qua cái này (Test bằng đĩa chuyên dụng - ke ke)
_Hic, đến phần Keyboard test (má ơi) tại hôm nọ em tháo hết cả bàn phím ra để đi đánh xà bông cho nó sạch, tháo cả bảng mạch nhựa nên hôm nay nó chập quá - chết mất khối phím nhưng may mà chỉ liệt bên phải - bên phần gõ chữ thì vẫn ko sao . Ai hảo tâm (HN) tài trợ em cái bàn phím đê ..ê..ê..

_Chuột em test ngon
_Các cổng USB sức khỏe vẫn tốt..
Thế thôi nhé - có cái gì còn lại các bác test nốt .

+4) Ontrack Data Advisor

Nó test vài thứ như RAM, SMART check (HDD), Structure Partition , Surface Scan. Bọn này test nhanh lắm - đúng là Ontrack có khác - em test tí đã xong:
Kết quả:
SMART check: Unknow - hí hí tại em đang test con ổ cũ có vài GB thì sao mà có tích hợp sờ mát được .
90-Second Test: Passed
File Structure: Fail (chắc tại em vừa Format nên nó ko có file nào để test nên nó mới báo thế)
Complete Surface Scan: Not Select

+5) The Trouble Shooter

Em thấy thằng này gần hệt như thằng PC Check 5.5 - nó cũng test đủ thứ như main, chip, ram, hdd, keyboard, mouse… tuy nhiên có ít các mục đi sâu chit tiết hơn chút cíu .

+6) PC Doctor 3.0

Trùi ui - nó có nhiều menu kinh khủng gần như máy tính có cái gì nó có chức năng test cái đó .
Các menu đổ xuống dài dằng dặc, các chức năng test của nó đa dạng và đầy đủ nhất trong tất cả các phần mềm test PC.
Nó cung cấp cả Hardware Information để biết rõ về thông tin phần cứng.

+7) CPU-Video-Disk Test 5.6

Chả có gì - chán phèo .

+8) Test Hard Disk Drive 1.0

Nó test mỗi ổ cứng và cung cấp các thông tin về ổ cứng.
Tốc độ Test của em dao động trong tầm 15 - 50 MB/s tùy theo dung lượng ổ cứng - càng lớn tốc độ MB/s càng nhanh . Nhìn quá trình test qua giao diện đồ họa thấy nó cũng Pro.
Kết quả nó báo Errors: 0 à may quá

VI) Hard Disk Tools

+1) Hdd Regenerator 1.51

Nó mà check thì lâu chết đi được - tốc độ tầm < 1MB/s. Sau khi check nó sẽ cho

biết ổ có mấy bad sector mà bao nhiêu trong số đó đã được recover (nôm na là khoanh vùng) để các bác dùng tiếp - em thấy chỉ có vài bad sector thôi là các bác

nên chuẩn bị ổ mới đi - kẻo "nhỡ" thì khổ vợ kon .

+2) Ontrack Disk Manager

Thằng này dùng để cài đặt nhận diện ổ cứng - sẽ bị mất hết dữ liệu . Nó cũng có thể phân vùng các ổ được - chức năng cũng gần như trên DOS à quá Basic, quá ít lựa chọn nhưng mà cơ bản. Ngày xưa thì dùng chứ bây giờ cho em cũng chả dùng .

+3) Spinrite 6.0

Khi chọn các Partition các bác nhớ dùng dấu cách (space bar) nhé . Nhưng mà em lại test trên cái ổ trắng nên nó chả Recovery được cái gì - tốc độ chậm lắm: 1 phút quét được tầm 100 MB ổ cứng.

+4) Active Kill Disk 1.1.1

Nghe tên đã thấy "ghê" - - kill -- nó xóa cả ổ cứng luôn. Vì thằng này nguy hiểm nên nó phải qua một đống thao tác xác nhận (có cả bước gõ KILLDISK bằng chữ hoa để xác nhận)

+5) H Dat2 4.04

Các chức năng sau:

_Drive level test menu: + check and repair bad sector

+ check bad sector only

+ wipe drive …

Phần check có 3 màu: xanh da trời - vàng - đỏ tương ứng với OK - Warning - Bad

Dính kiểu nào đem màu ra so sánh là biết ngay (may mà em xanh da trời)

_File level test menu

_Device Information

_SMART ….

Vài cái khác nữa….

+6) HDD SMART Viewer

Cho biết các thông tin về ổ cứng : Tên, Dung lượng, Primary, Slave, Serial, Buffer…

+7) Victoria 3.33

Loay hoay một hồi từ F1 à F9 thấy nó chả nhảy gì cả: INIT cứ báo Err - tức mình bỏ qua. Em nghĩ nó có chức năng test tốc độ mình chưa mò ra vì có các mốc thời gian (đa số là ms) ở menu bên phải .

+8) Seagate Tool

+9) Western

+10) Maxtor

+11) Fujitsu

+12) Samsung

+13) IBM

Đây là các công cụ tương ứng dành cho các ổ cứng của mỗi hãng khác nhau, em đang test con Fujitsu:

Quét SMART, outer/inner area, buffer write, read test… thấy nó báo OK

Nếu quick test ko lỗi các bác có thể dùng chức năng Comprehensive test để quét kỹ hơn (xuất hiện bảng lựa chọn cái này sau khi quick test)

+14) GW Scan 3.15

Quick test
Extented test
….
Em thích Extended test nên chạy thử - xong thấy báo pass: Okie - vẫn còn ngon .

+15)Excel Stor's Estest

Nó cóc chạy

+16) Norton Disk Editor

Toàn Hex y như Win Hex 12 - em chả dám nghịch ^_<

+17) Norton Disk Doctor

Chủ yếu là Diagnose Disk và Surface Test
Em chạy thử cái Surface Test thấy nó có thể cho các kết quả như:
Used Block
Unused Block
B: Bad Block
= : Block being tested
Test xong em thấy ko dính cái bad nào .

+18) MHDD

Nó có mấy lệnh y hệt như lệnh trong DOS ấy
VD: MHDD>Smart, Fdisk, Eraser, Config, PCI Scan, SCSI Information, Scan à em thử chạy Scan Parameter thấy time out của nó là 240 (s)

VII) System Information Tools

+1) AIDA - Sys Information Tool 2.14

Cho biết các thông tin về CPU, Main, Chipset, BIOS, Memory Size, Video Adapter, Monitor, Sound, PCI Audio, Adaptor, PCI device…. à 44 chi tiết đủ các loại = cách ấn F5 để dịch chuyển qua các số.

+2) PCI AGP Information

Thông tin về thiết bị cắm qua cổng PCI và card đồ họa (của em onb)

+3) System Analyser

Phân tích thông tin hệ thống, cổng, chuột, cpu, dos version, bios…

+4) Navratil Software System Information 0.586

Có phần Detail cho biết thông tin về chip, video, memory, bios, drive, os, port …
Test Printer, Speaker..
Cái test loa có 1 đoạn nhạc hay phết - nghe rất quen nhưng nhất thời em vẫn ko nghĩ ra đó là bài zdì ? (nghe hơi có mùi "chưởng")

+5) Astra System Information

Cũng là cung cấp các thông tin phần cứng - ấn F10 để xem các menu
+6) HW Infor
Thằng này ít thông tin quá - chỉ có main, card, drive, FDD và vài cái vớ vẩn.
Test CPU, nhiệt độ chip, điện áp.
+7) PC Config 9.33
Thằng này lỗi em ko check được.
+8) Syscle 2.46 Beta 7
Có những cái sau: CPU/BIOS , IDE/SCSI , video, speed, CMOS …. Em test thử thấy thông số sau:
CPU: 1818 MHz
Video Speed: 13556 char/sec
HDD access: 9.23 ms Average Seek
Transfer: 869.02 KB/s

Syscheck Rating: 1067.0 Sys chks
+9) CPU Identify Utility
+10) CTIA CPU Infor

Hai cái này cái lỗi, cái ko chạy - em cóc test nữa .

VIII) File Manager

+1) Volkov Commander 4.99
Thằng này hay hơn cái NC là nó có hỗ trợ NTFS à em toàn dùng nó để quản lý file, copy, paste, del… mỗi khi Win bị lỗi ko vào được.
+2) Dos Commander Center
Thằng này giống hệt VC - chả khác chó gì
+3) File Wizard
Cũng tương tự nhưng khác VC chút cíu - nhiều mục lựa chọn hơn 1 tí nhưng mà quản lý cũng khó hơn vì cái giao diện F1-F9 lại treo ngay trên đầu .
+4) File Maven
Giống thằng File Wizard - chả khác mấy
+5) Fast Lynx
Nó có mấy chế độ nhưu
Split Screen mode - chẻ đôi ra hai cửa sổ kiểu VC
Form mode, Command mode, Configuration, Diagnostic à rất chuối, chả thấy các menu chức năng đâu. Ngay cả Split Screen cũng thấy khó chỉnh bỏ xừ à mò 1 lúc em mới thấy Change Dir là F2 à nó viết tắt CHDIR làm em nhầm là check disk - thế mới chuối. Lúc đầu loay hoay Alt + F1 có được .
+6) Lap link

Cái này có thể Copy, move, del được, có thể change cái Skin trắng đen để thành màu sắc khác được. Cái này hình như có Moderm thì có thể có mạng trong này nhưng mà em ko có nên cóc Test được.

+7) DOS Navigator

Cái này y chang như VC nhưng có màu xám.

+8) Mini Windows

Trong phần này sẽ có Windows 311 - cái Win cổ lỗ sĩ này quá cũ rồi chức năng chả có gì - thà em dùng VC còn hơn là dùng nó.

Cái đáng chú ý trong phần này là các phiên bản Hiren gần đây đã bổ xung thằng Win98 vào với các phiên bản 98 khác nhau vô cùng phong phú - Win98 đã có thể xem được cả các ổ NTFS, tích hợp 7Zip để ta có thể giải nén các file RAR, Zip … Quản lý cực kì tiện lợi - hay hơn VC nhiều.

Có các loại Win 98 sau:

Win98 RAM Setting: tùy mức độ RAM mà các bác chọn loại hình Win98 - nó có 7 mức RAM tất cả à RAM em 512 em chọn mức 5 hay 6 là okie chứ 7 đòi trên 700 MB RAM em chịu ko nổi

Nhưng mà em thấy dù em có chọn 1, 2, 3 hay 4 thì thấy chức năng cũng thế - chả biết tại sao ?

Win 98 - này ko thể truy cập ổ CD đâu nhá .

Tiếp theo là các phiên bản 98 có hỗ trợ NTFS và Win98 thường -- loại thường chắc < 100 MB RAM

IX) MBR Tools

Các công cụ ở đây lieenm quan đến Master Boot à cái này hay dính nếu các bác cài linux và win lẫn với nhau.

Em chỉ cài win nên chả biết test nó ra sao .

X) BIOS and CMOS Tools

Các công cụ về BIOS và CMOS à em chả dùng.

XI) Multimedia Tools

+1) Picture Viewer

+2) Quick View Pro

He he he - lúc đầu em tưởng nó chỉ xem được 256 màu là kịch kim ko ngờ bọn này trên DOS mà xem được True Color như trên Win ấy - Kool wa'

+3) Mpx Play Music Play

Hí hí hí à nó chơi nhạc MP3 trên DOS hay đáo để ,
Không biết các bác ra sao chứ em cảm thấy rất xúc động mỗi khi nghe nhạc trên DOS. Cũng bài ấy nhưng nghe trên DOS thấy nó hay và ý nghĩa hơn hẳn nghe trên Win với các chương trình WMP, Winamp, JetAudio.
Ôi cái cảm giác lần đầu nghe nhạc trên luôn làm em bồi hồi mỗi khi nhớ lại .

XII) Password and Reg Tool

+1) Active Pass Change XP, NT, 9X, 2000

Cái này có thể change pass Win hoặc xóa Pass của Win một cách nhanh chóng - test với XP em chỉ mất chưa đến 30 giây cho thao tác .
Giao diện từng phần-các bước rõ ràng, đơn giản à chỉ chọn mấy số 1,2,3 theo hướng dẫn là okie (các bác nhớ **dấu cách** chính là đánh dấu chọn thay cho ta hay dùng chuột để chọn trên win ấy)

+2) Offline Pass NT Change

Em test nó báo:
IDE: Failed Opcode wan unknown rồi treo im re
Cái này trước có trên mấy báo tin học như Echip, LBVMT, Thế Giới @ nhưng mà các thao tác của nó nếu vừa nhìn báo vừa làm thì okie - làm lại ngay thì cũng okie nhưng mà chỉ để tầm 2 tháng ko làm lại là lại quên béng mất à nên em ko khoái thằng này mà hay dùng thằng Active phía trên.

+3) Registry Viewer / Editor 4.2

Em chạy nó nhảy ngay vào ổ R (ram) vì ổ cứng em cóc có win nên nó chả xem, edit được gì .

XIII) NTFS / Ext2 Tools

+1) NTFS DOS Professional 5.0

Chạy nó em chả thấy gì ngoài cái check disk và danh sách FDD, CD

+2) NTFS 4 DOS

Chạy thì nó liệt kê ra 3 ổ: 2 ổ FAT32, 1 ổ NTFS à hết vị

+3) Paragon Mount Everything

Nó xác định có 1 ổ NTFS à hết
(Bọn Paragon có cái backup trên win chạy cũng hay phết - các bác thử mà coi)
+4) EditBINI
Dùng để chỉnh sửa boot.ini của Win (kể là NTFS cũng "chấp" luôn)
+5) NTFS DOS (Read Only)
Cóc chạy

XIV) Other Misc Tool

+ 1) Ghost Walker
Em test nhưng chưa biết chức năng của nó là gì (cũng là của Symantec)
+ 2) DOS CD Roast
Cái này y như trình soạn thảo văn bản NotePad ấy - cũng có menu và lệnh tương tự, có thể save được vào trong máy
+3 +4 +5) Universal TCP/IP Network
Cho biết card mạng và 1 loạt các Enable cho Mouse, CD, NTFS, Time out

XV) DOS
Các bác tự xem đi - cái này ko nói các bác cũng thừa biết .

Vậy qua một loạt các phần mềm em đã giới thiệu thì chúng ta sẽ thấy hoa mắt chóng mặt nhưng mấu chốt của ta chỉ là chọn ra các phần mềm tốt nhất trong số đó và phù hợp với chúng ta để tận dụng được sức mạnh của Hiren's Boot.

Bảng kết luận như sau:

1) Backup toàn bộ 1 phân vùng or HDD
Image Center 5.6 hay **Acronis True Image Enterprise Server 8.1.945** (ko dùng Ghost)

2) Chia ổ, chuyển định dạng FAT, NTFS, Ext2, Ext3
Partition Magic Pro 8.05

3) Cứu dữ liệu bị xóa, format nhầm:
Ontrack Easy Recovery Pro 6.10

4) Test RAM
Doc Memory 2.2b hoặc **Gold Memory 5.07**

5) Ổ cứng:
Test Hard Disk Drive 1.0
GW Scan 3.15
Norton Disk Doctor (đừng nhầm với Editor nhé)
Hdd Regenerator 1.51
Và các chương trình của chính hãng :
Seagate Tool

Western
Maxtor
Fujitsu
Samsung
IBM

6) Thông tin hệ thống:
AIDA - Sys Information Tool 2.14

7) Quản lý file:
Mini Windows 98 và **VC (Volkov Commander 4.99)**

8) Xem ảnh True Color:
Picture Viewer 1.94
Quick View Pro 2.56

9) Nghe nhạc mp3:
Mpx Play Music Play 1.53

10) Change Pass - Xóa Pass
Active Pass Change XP, NT, 9X, 2000

11) Diệt Vitrus
McAfee 4.4

12) DOS

IDM và cách down ngoài hàng net có cài deepfreeze

Mèn ơi, mệt ghê, lâu rồi toàn vọc vô game, giờ viết cái tut cho vui, chắc nhiều người biết rồi nhưng mà tui là tui cứ viết.

Thế này, các bác đôi khi ra 1 quán net thường xuyên nào đó, nhất là để down cái gì nặng nặng mà nhà mình trả thuê bao theo dung lượng. Bác có bực không nếu mỗi lần có acc của rapid hay acc ftp của 1 server nào đó, mà mỗi lần vào quán net đó lại phải nhập từng cái 1. (ý ẹ, có khoảng 10 cái thôi thì chết, như em chỉ có rs.com và rs.de còn không chịu nổi mà)

Thế này để đỡ phải nhập đi nhập lại pass trong
Code:

```
Site Login
```

bác cứ nhập 1 lần đi.

Em đợi .....

Nhập xong chưa, chờ lâu quá, bác nhập xong rồi, nhấp okie roài, thì bác vào registry. chỗ cái ky này

Code:

```
HKEY_CURRENT_USER\Software\DownloadManager\Passwords
```

Bác nhấp phải chọn import, thế roài bác lưu file reg đó vào usb, thế là xong, khi nào qua máy khác, báo nhấn vào file reg đó trước khi chạy IDM. Đảm bảo là có sắn acc khỏi phải nhập lại

Còn khi rời quán net, muốn xoá acc ư, dễ ẹc, xoá cả cái key đó cho em, không thì bác soạn 1 file là cleanreg.reg tương tự như sau:

Code:

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\DownloadManager\Passwords]
[HKEY_CURRENT_USER\Software\DownloadManager\Passwords\http://rapidshare.com]
"User"=hex(0):
"Password"=hex(0):
[HKEY_CURRENT_USER\Software\DownloadManager\Passwords\http://rapidshare.de]
"User"=hex(0):
"Password"=hex(0):
```

Thế rồi cấn xoá thì lại click vào nó, dễ như ăn cháo, đá bát!
Phpdeveloper(UDS)

Tiêu diệt cái easyCafe ở wán net thôi

Hiện nay đa số các Internet Cafe ở VN đều xài một chương trình tính tiền chung là EasyCafe. Những tưởng cách tính tiền trên server có nhiều ưu điểm dù máy tính có bị restart sẽ không bị mất giờ nhưng EasyCafe lại làm thất vọng hơn dự kiến. Kent

nhớ lúc trước hình như pác langtu nhà minh hay pác yeuem dại khờ có một Tut chém thằng này , nay Kent cho thêm một chiêu nữa , nếu có đụng chạm gì đến cách các bác cho em xin lỗi nhá .
Công cụ :
+ PsSuspend
+ PsKill
Bạn có thể tìm thấy cả 2 công cụ này trong bộ công cụ tìm kiếm của google với từ khóa pstool
1. Tình huống 1 : Đóng băng 1 chương trình.
_ EasyCafe hoạt động theo phương pháp sau :
Khi client.exe bị kill, bạn sẽ bị xuất hiện 1 màn hình logout. Sau đó phải nhập lại user/pass mới có thể vào được.
_ Lý do :
EasyCafe chạy 2 process :
+ Client.exe : Dùng để tính tiền, tương tác với user.
+ Guardit.exe : Dùng để hiển thị bảng logout.
_ Như vậy, ta thấy được muốn vô hiệu hoá EasyCafe thì phải vô hiệu hoá cả 2 process trên.
_ Tạo 2 file .bat trong cùng thư mục với 2 công cụ PsSuspend và PsKill có nội dung sau :
--- File Bat 1 (PauseEasyCafe.bat)
Code:

```
@pssuspend.exe client.exe
@pssuspend.exe Guardit.exe
```

--- File Bat 2 (ResumeEasyCafe.bat)
Code:

```
@pssuspend.exe -r client.exe
@pssuspend.exe -r Guardit.exe
```

Mỗi lần bạn muốn "đóng băng" EasyCafe, chỉ việc chạy tập tin PauseEasyCafe.bat
_ Khi muốn kích hoạt lại, chạy file ResumeEasyCafe.bat
2. Tình huống 2 : Triệt tiêu EasyCafe.
_ Nếu bạn muốn "giết" hoàn toàn EasyCafe, hãy thử tập tin .bat sau :
--- File Bat 3 (StopEasyCafe.bat)
Code:

```
@pskill.exe Guardit.exe
@pskill.exe client.exe
```

3. Kết luận :
_ Cả 2 cách trên đều khiến EasyCafe bị treo. Khi bạn cần kích hoạt lại client, chỉ

cần chạy lại bản client (nếu dùng cách 2) hoặc chạy file ResumeEasyCafe.bat (nếu dùng cách 1).
_ Điều thú vị là, sau khi bản client được kích hoạt trở lại (sau thời gian > 1 phút), số tiền bạn đã sử dụng máy sẽ được reset lại thành 0. Hoặc đối với tình huống 1. Sau khi "đóng băng" EasyCafe. Đến khi bạn sử dụng máy xong, kích hoạt lại client, số giờ sẽ hiện lên trên server bằng với giờ lúc bạn "đóng băng" chương trình.
Chúc thành công!
Kent(HCE)

Password recovery kit enterprise 7.0

Password recovery kit enterprise 7.0: Giúp bạn lấy lại mật khẩu của 28 chương trình thông dụng

Đối với các chương trình thông dụng như: Microsoft Word, Microsoft PowerPoint, Adobe Acrobat, WinZip, WinRar... thì chúng ta hoàn toàn có thể tận dụng tính năng tạo mật khẩu được thiết kế sẵn để bảo vệ sự an toàn cho dữ liệu. Tuy nhiên do phải nhớ quá nhiều mật khẩu nên có thể một lúc nào đó bạn sẽ quên mất mật khẩu đã đặt.

Khi đó để lấy lại tài liệu quan trọng đấy thì bạn phải nhờ đến một chương trình dò tìm mật khẩu của hãng sản xuất phần mềm Passware. Mạnh nhất trong các dòng sản phẩm là: Password Recovery Kit Enterprise hỗ trợ đến 28 chương trình gồm: 1-2-3 Key, Acrobat Key, ACT Key, Backup Key, FileMaker Key, Internet Explorer Key, Mail Key, Money Key, MYOB Key, OneNote Key, Organizer Key, Outlook Express Key, Paradox Key, Peachtree Key, PowerPoint Key, Quattro Pro Key, QuickBooks Key, Quicken Key, RAR Key, Schedule Key, WordPerfect Key, WordPro Key và Zip Key.

Cách sử dụng: Tùy theo dữ liệu cần lấy lại mật khẩu bạn được tạo bởi chương trình gì mà chọn Key cho tương ứng. Nói chung cách sử dụng đều tương tự như nhau. Ở bài viết này xin minh họa đối với chương trình WinRar. Sau khi khởi động RAR key, bạn nhấn menu File và chọn Recover. Kế đến chọn file cần phục hồi và nhấn OK. Chương trình sẽ tự động detect và tiến hành thử các mật khẩu đã lập trình sẵn hoặc theo thứ tự các ký tự hay các chữ số để lấy lại tài liệu đó. Nếu thành công bạn sẽ nhận được bảng thông báo của chương trình. Nhấn vào dòng copy để ghi nhớ

mật khẩu đó vào trong Clipboard. Thế là dữ liệu lại trở về với bạn.

Chương trình được cung cấp tại website: -http://www.lostpassword.com/ với dung lượng khoảng 4.3 MB dưới dạng dùng thử, tương thích hoàn toàn với hệ điều hành Windows.

******Sưu tầm bởi ghost1982******

Để máy tính chạy nhanh... như gió!

Làm sao để máy tính chạy nhanh nhất là mong ước chính đáng của hầu hết các "công dân IT". Có rất nhiều cách để làm được việc này, trong đó sử dụng các phần mềm tăng tốc là một trong những cách khả thi và ít tốn kém nhất.

Với WinOptimizer Platinum 3, người dùng có thể yên tâm với chiếc máy tính không những chạy nhanh mà còn ổn định. Chương trình chia làm 4 nhóm công cụ chính là: Cleaning Tools (các công cụ dọn dẹp rác máy tính, giải phóng dung lượng ổ đĩa); Tuning Tools (các công cụ giúp tối ưu các thông số, tăng tốc hệ thống); File Tools (những công cụ chia tách, nối file, xóa file vĩnh viễn, hiển thị dung lượng thư mục dưới dạng biểu đồ hình bánh); Tweaking Tools (công cụ dồn đĩa, xem thông tin về hệ thống, thay đổi các thiết lập Windows).

Ngoài ra, nếu là người mới làm quen với máy vi tính và không biết phải sử dụng các công cụ trên như thế nào, chương trình cung cấp cho bạn một công cụ tự động: 1- Click-Optimization. Chỉ với một cú nhấp chuột, bạn có thể để chương trình thực hiện tối ưu hệ thống một cách tự động từ A tới Z, rất tiện lợi.

WinOptimizer Platinum 3 là phần mềm thương mại của hãng Ashampoo, tương thích với Windows 98, Me, 2000, XP. Bạn có thể xem thông tin và tải bản dùng thử 30 ngày tại website http://www.ashampoo.com/ (dung lượng 13,4 MB) hay tìm mua trên các đĩa CD phần mềm tổng hợp, hiện có bán ngoài thị trường.

Theo **Nguyễn Hồng Hạnh**
Tuổi trẻ

Những công cụ không thể thiếu cho PC

Thực hiện: Hồng Vy

Đôi lúc, những công cụ sẵn có trong Windows đành bó tay trước những trục trặc xảy ra với máy tính. Khi đó, cái bạn cần nhất là phần mềm chuyên dụng có khả năng nhanh chóng vực dậy hệ thống.

BỘ PHẦN MỀM TRỌN GÓI

Nếu không muốn mất nhiều thời gian lựa chọn tiện ích phục vụ công việc bảo trì hệ thống, bạn có thể sử dụng bộ phần mềm trọn gói với các công cụ khôi phục dữ liệu, bảo mật, khắc phục sự cố và nhiều tính năng khác trên duy nhất một đĩa CD. Ba trong bốn bộ phần mềm sẽ được đề cập ở đây đều có khả năng khởi động khẩn cấp từ CD, giúp sửa chữa một máy tính không thể khởi động. Thông thường, những công cụ này được bố trí thuận tiện trên một giao diện chung.

Nhóm thử nghiệm (NTN) đánh giá 4 bộ phần mềm bảo trì hệ thống trọn gói hàng đầu hiện nay là Business Logic WinCleaner Complete PC Care, Iolo System Mechanic 5 Professional, Symantec Norton SystemWorks 2005 Premier và V Communications SystemSuite 5. Các bộ phần mềm được đánh giá về tính năng, dễ cài đặt và dễ dùng, mức độ cải tiến so với phiên bản trước.

Mỗi bộ phần mềm có ưu điểm riêng. Norton SystemWorks của Symantec đoạt danh hiệu "Ưa thích nhất" (Best Buy) vì có nhiều công cụ tốt và dễ sử dụng. System Mechanic có sự cải tiến tốt với việc tích hợp tất cả công cụ vào một giao diện dễ dùng. Tuy SystemSuite của V Communications (đoạt danh hiệu "Best Buy" ở năm trước) không được nâng cấp trong hơn 1 năm qua nhưng nó có công cụ chuẩn đoán rất hữu ích. WinCleaner của Business Logic làm người dùng khó chịu vì màu sắc giao diện quá sáng nhưng có khả năng dọn dẹp hệ thống thực thi trực tiếp từ CD chỉ qua một thao tác nhấn chuột.

Nếu có ý định sử dụng bất kỳ phần mềm nào kể trên nhằm mục đích cải thiện khả năng hoạt động hệ thống thì có thể bạn sẽ thất vọng. Theo ngày tháng, Windows

“tích tụ” lại vô số tập tin không cần thiết như trình cài đặt ứng dụng cũ, tập tin tạm và khóa Registry. Những dữ liệu rác sẽ làm giảm hiệu năng của máy tính. Để khắc phục tình trạng này và giải phóng đĩa cứng, 4 bộ phần mềm trên đều được trang bị công cụ loại bỏ tập tin không cần thiết, xóa và sửa các khóa Registry. Tuy các phần mềm này có khả năng khôi phục không gian đĩa cứng nhưng không cải thiện đáng kể cho hiệu năng.

NTN sử dụng công cụ giám sát màn hình để ghi lại chính xác những gì các bộ phần mềm thực hiện và nhận ra rằng cả 4 phần mềm có những điểm khác biệt trong việc lựa chọn định dạng và số lượng tập tin để xóa. Phần mềm SystemSuite và SystemWorks có chế độ dọn dẹp hệ thống mặc định rất “thô bạo” (SystemWorks xóa hơn 12000 khóa Registry), ngược lại System Mechanic và WinCleaner thực hiện xóa tập tin và khóa Registry có phần dè dặt hơn.

Cả 4 bộ phần mềm đều cho phép kiểm soát nhiều cấp độ khác nhau đối với các tập tin mà chúng xóa. Ví dụ như Symantec cho phép bạn chỉ định cấp độ dọn dẹp với tiện ích Norton Cleanup, CleanSweep và WinDoctors. Có thể việc dọp dẹp hệ thống vô tình xóa một tập tin bạn cần sau đó, vì thế 4 bộ phần mềm đều có công cụ như Undo It của SystemSuite, cho phép sao lưu tập tin và khóa Registry bị xóa để khôi phục về sau.

Nếu máy tính có dấu hiệu hoạt động chậm hay không thể khởi động được thì việc sử dụng những công cụ trên có thể là kế sách cuối cùng dù chúng chưa thật hoàn hảo.

SYMANTEC NORTON SYSTEMWORKS 2005 PREMIER

Dù giá cao (100USD) nhưng SystemWorks 2005 Premier của Symantec vẫn đoạt được danh hiệu “Best Buy” vì đi kèm nhiều công cụ và dễ sử dụng. Bộ phần mềm này được bổ sung tiện ích tạo ảnh đĩa Norton Ghost để sao lưu dữ liệu, khôi phục và nâng cấp hệ thống. Những công cụ hữu ích khác như GoBack giúp khôi phục lại hệ thống về trạng thái “khỏe mạnh” trước đó, CheckIt chuẩn đoán hệ thống và System Optimizer tập hợp thông số cấu hình Windows dưới một cửa sổ. Đáng chú ý nhất, Symantec cung cấp đĩa CD cứu hộ có khả năng khởi động và hỗ trợ định

dạng NTFS.

Tuy nhiên, SystemWorks cũng có vài nhược điểm chẳng hạn như yêu cầu bộ nhớ cao và đây là trở ngại với các máy trang bị RAM dung lượng thấp (kiểm tra các tiến trình thực thi trong Windows Task Manager cho thấy các thành phần của SystemWorks chiếm hơn 87MB bộ nhớ hệ thống). Hơn nữa, quá trình cài đặt tốn nhiều thời gian, đòi hỏi nhiều lần khởi động lại máy và tải về các ứng dụng cập nhật. SystemWorks 2005 thiếu công cụ kiểm soát các ứng dụng khởi chạy cùng với Windows.

IOLO SYSTEM MECHANIC 5 PROFESSIONAL

System Mechanic 5 Professional của Iolo là phần mềm duy nhất tích hợp tất cả công cụ dọn dẹp, sửa chữa, bảo trì, tối ưu và bảo vệ dữ liệu trên cùng một cửa sổ giao diện. Cài đặt nhanh và có nhiều tính năng, System Mechanic được xếp vị trí thứ 2 sau SystemWorks 2005 Premier. Bộ phần mềm cung cấp công cụ tìm kiếm và khôi phục dữ liệu mạnh, cho phép phục hồi các thư đã xóa trong Eudora, Nestcape, Outlook và Outlook Express. System Mechanic chỉ có một khiếm khuyết nhỏ là không cung cấp công cụ khôi phục hệ thống từ đĩa khởi động.

V COMMUNICATIONS SYSTEMSUITE 5

Bộ phần mềm SystemSuite 5 có hầu hết các công cụ cơ bản như chuẩn đoán, tối ưu hệ thống, sửa chữa và khôi phục tập tin. Giao diện của SystemSuite 5 nhất quán nhưng thiết kế màn hình chính không trực quan gây khó tìm các tính năng chính. Quá trình cài đặt nạp một số ứng dụng của hãng thứ 3 vào hệ thống trước khi cài đặt chương trình chính. Một vài công cụ rất ấn tượng, các tính năng PCDiagnostics và SystemExplorer hữu ích trong việc xem cấu hình hệ thống và thực hiện kiểm tra cấp thấp. Phần mềm có công cụ di chuyển ứng dụng khá hay, không chỉ cho phép chuyển ứng dụng đã cài đặt từ thư mục này sang thư mục khác trên cùng hệ thống (PC) mà còn cho phép “đóng gói” ứng dụng để chuyển sang một hệ thống khác. SystemSuite cũng có cung cấp đĩa CD khởi động cứu hộ với các tính năng xử lý đĩa và file hạn chế.

V Communications cho biết phiên bản mới sắp phát hành sẽ có thủ tục cài đặt mới, chuẩn đoán phần cứng tốt hơn và giao diện chương trình được thiết kế lại.

BUSINESS LOGIC WINCLEANER COMPLETE PC CARE

WinCleaner Complete PC Care được trang bị những công cụ tốt nhưng lại thiếu tính năng chuẩn đoán hệ thống thường thấy ở các bộ phần mềm khác. Ngoài ra, giao diện lòe loẹt và không trực quan khiến việc tìm kiếm và sử dụng một số công cụ khó khăn.

Xét về mặt tốt, WinCleaner có tiến trình cài đặt nhanh và giao diện chính được tổ chức hợp lý giúp truy cập nhanh đến các chức năng. Tuy nhiên, giao diện chính không chứa hết tất cả tính năng, nhiều tiện ích được mở ở cửa sổ riêng không thống nhất. Ngoài ra còn có một vài nhược điểm nhỏ, chức năng WinReg Optimizer cho bạn chỉnh sửa Registry nhưng không cảnh báo cần khởi động lại hệ thống (Business Logic cho biết lỗi này đang được sửa chữa). Bạn nên tránh thực hiện dồn đĩa (defrag) đối với những thư mục lớn vì chức năng WinFile Defragmenter có thể sẽ tiến hành việc kiểm tra mất nhiều thời gian và bạn không có cách nào để dừng lại.

Bộ phần mềm cho truy cập nhanh công cụ WinSmart giúp di chuyển các chương trình đã cài đặt và quản lý ứng dụng khởi động cùng Windows. Ngoài ra, chức năng OneClick Cleanup có thể được thực thi trực tiếp từ đĩa CD mà không cần cài đặt. Dù thiếu tính năng dọn dẹp tập tin và khóa Registry nhưng WinCleaner vẫn rất ấn tượng với giá 70USD.

TIỆN ÍCH ĐƠN LẺ
PHỤC HỒI DỮ LIỆU

Phục hồi tập tin đã xóa: Khi lỡ tay xóa đi những tập tin ảnh quí giá hay tài liệu quan trọng, bạn không biết làm thế nào để cứu vãn chúng? Thực tế, bạn có thể khôi phục những tập tin này từ Windows Recycle Bin, nhưng nếu tập tin có kích thước quá lớn hay bạn nhấn phím khi thực hiện lệnh xóa thì tập tin sẽ không tồn tại ở đó. Trong nhiều trường hợp, tiện ích miễn phí Free Undelete cung cấp giải pháp hiệu

quả cho hệ thống định dạng tập tin NTFS thường được dùng trong Windows XP. Windows xóa các tập tin không phải bằng cách "vứt hẳn" chúng ra khỏi đĩa cứng mà chỉ là để riêng vùng không gian trên đĩa của tập tin đó cho một tập tin mới. Nếu nhanh chóng vào cuộc, bạn có thể xem nhanh danh sách các tập tin vừa xóa. Đừng do dự vì nếu Windows ghi chồng một dữ liệu mới lên vùng đĩa ấy thì Free Undelete sẽ chẳng giúp ích gì được cho bạn. Tiện ích có thể tải về miễn phí tại www.pcworld.com.vn, ID:47626.

Sao lưu hiệu quả: Muốn sao lưu dữ kiệu một cách đều đặn nhưng nếu đĩa cứng đã đầy ắp hay có hỏng hóc, bạn phải đương đầu với những phiền toái vì cài đặt và tinh chỉnh lại ứng dụng. Khi ấy, bạn có thể nghĩ đến Acronis TrueImage (50USD). Không đơn thuần là sao lưu dữ liệu, tiện ích mạnh mẽ này nhanh chóng "chụp ảnh" đĩa cứng, bạn có thể lưu và sử dụng dữ liệu đó để khôi phục trạng thái cũ khi hệ thống gặp bất trắc. TrueImage cho phép tạo mới, thu giảm kích thước và di chuyển các phân vùng đĩa cứng trong khi vẫn bảo toàn được dữ liệu. Bạn có thể phân vùng đĩa hiện tại và thực hiện sao lưu ngay trên đó. Giao diện dễ dùng. Để biết thêm thông tin, bạn hãy tham khảo bài viết "Acronis True Image: Đối thủ của Ghost" trong số báo tháng này trang 77.

Sửa máy từ đĩa CD: Ngay cả khả năng khởi động từ đĩa CD của bộ phần mềm Norton SystemWorks cũng không thể sánh được với Winternals ERD Commander 2005 (149USD, www.winternals.com), một tiện ích cho phép bạn truy xuất các tập tin hệ thống, thư mục, dữ liệu "sao lưu" của Windows XP. Tiện ích đi kèm trình duyệt Firefox, giúp bạn có thể truy cập Internet để tải phần mềm và chép tập tin qua mạng. Tiện ích có khả năng nhận dạng cấu hình các thiết bị phần cứng và được trang bị công cụ giống như Registry Editor là Windows Management Console (kèm theo Event Viewer và Disk Manager) và công cụ System Restore. Tiện ích còn có ứng dụng khôi phục tập tin đã xóa, và trình hướng dẫn Locksmith giúp truy cập máy với quyền quản trị (administrator) ngay cả khi bạn quên mật khẩu đăng nhập. Winternals ERD 2005 có thể thực hiện những gì mà đĩa khởi động Windows không làm được. Giá phần mềm khá cao, tuy nhiên nếu máy tính của bạn bị khóa thì mức giá này chấp nhận được.

BẢO MẬT HỆ THỐNG

Trình duyệt an toàn hơn: Thật khó chịu khi ai đó hoặc phần mềm gián điệp kiểm soát bất kì điều gì bạn thực hiện trên máy tính. Tiện ích Windows Washer (30USD, www.webroot.com/products/windowwasher/) sẽ xóa sạch mọi địa chỉ Internet đã truy xuất (history), cookies, bộ đệm trình duyệt và những thông tin khác mà các ứng dụng hoặc Windows lưu lại trên hệ thống. Ngoài việc xóa các tập tin trong thư mục tạm của Windows và bộ nhớ trình duyệt (Firefox, Nescape và IE), công cụ còn có chức năng dọn dẹp đĩa cứng. Sau khi thực hiện dọn dẹp đĩa cứng trong khoảng thời gian 30 giây, hệ thống không còn nhận ra bất kỳ dữ liệu nào đã được xóa đi và thậm chí các chương trình phục hồi tập tin cũng phải "chào thua". Giao diện dễ dùng với nhiều tùy chọn, từ việc dọn dẹp theo kế hoạch cho đến tính năng làm sạch đĩa cứng mạnh mẽ.

Bảo vệ mật khẩu: Tiện ích RoboForm tự động thực hiện công việc điền thông tin cá nhân, hóa đơn và xác nhận thông tin vào các biểu mẫu giao diện web. Bạn chỉ cần tạo mẫu dữ liệu hoàn chỉnh một lần và sử dụng thanh công cụ RoboForm trong trình duyệt để tiện ích điền thông tin thích hợp. RoboForm mã hóa password chính theo chuẩn 3DES, tạo password với độ dài lên đến 512 kí tự. Tất cả những gì bạn cần chỉ là nhớ tên truy cập và password chính. Tiện ích có thể tải về miễn phí tại

www.pcworld.com.vn, ID:47634.

Mã hóa thông tin cá nhân: Máy tính là một kho dữ liệu vô cùng quí báu các thông tin cá nhân. Cách tốt nhất để bảo vệ dữ liệu đó khỏi những cặp mắt tò mò là hãy mã hóa chúng. Tiện ích đơn giản và hiệu quả BestCrypt (60USD, www.jetico.com) cung cấp nhiều chuẩn mã hóa như Blowfish, Twofish và Rijndael, cho phép tạo một hoặc nhiều đĩa mã hoá chỉ mở được bằng cách nhập vào mật khẩu từ bảng điều khiển chính BestCrypt Control Panel. Tiện ích cũng có thể bảo mật nội dung trên đĩa CD-RW hay nhiều thiết bị lưu trữ khác. Hơn thế nữa, BestCrypt có khả năng bảo mật các tập tin tạm thời của Windows.

Che giấu dữ liệu: Nếu đơn giản chỉ muốn bảo vệ các thư mục tập tin, một ứng dụng mã hóa có thể giúp bạn việc đó. Tiện ích Folder Shield 2003 (20USD, www.baxbex.com/foldershield.html) hoạt động như là một phông nền cho các thư mục đó. Chỉ cần nhập vào password, đánh dấu tùy chọn Enable Protection trong cửa sổ chương trình và xác định thư mục muốn giấu đi. Khi đó, bạn không thể sử dụng tính năng Windows Search và các ứng dụng khôi phục tập tin để tìm các thư mục này. Việc sử dụng phím tắt để truy xuất thư mục vừa được đặt thuộc tính ẩn sẽ gặp thông báo lỗi cho biết thư mục đã được chuyển hoặc xóa đi. Tuy nhiên, cũng cần biết rằng Folder Shield sẽ không có tác dụng gì khi một người khác khởi động máy tính từ một hệ điều hành khác.

QUẢN LÝ HỆ THỐNG

So sánh nhanh thư mục: Tiện ích Beyond Compare (30USD, www.scootersoftware.com) giúp bạn quản lý tốt hơn các tập tin trên đĩa cứng dung lượng lớn. Tiện ích với giao diện tương tự Windows Explorer, hiển thị đồng thời nội dung hai thư mục, cho phép so sánh và đồng bộ dữ liệu giữa chúng, cũng như với các thư mục trên máy chủ hay site FTP. Ngoài ra, bạn có thể thiết lập để ghi lại những thay đổi.

Tham khảo cấu hình máy: Chỉ với thông tin từ chủng loại bo mạch cho đến tốc độ và cấu hình RAM hệ thống, Windows không cung cấp đủ thông tin bạn cần để giải quyết trục trặc hay quyết định nâng cấp. Tiện ích miễn phí PC Wizard 2005 có thể giúp bạn điều này. Chỉ với vài phút, bạn sẽ được biết những thông số chi tiết hệ

thống của PC hay máy tính xách tay, từ tốc độ FSB đến thông tin CMOS. Bạn có thể dễ dàng tìm ra bất cứ thông tin nào và kiểm tra tốc độ (benchmark) hệ thống. Tiện ích có thể tải về miễn phí từ www.pcworld.com.vn, ID:47638.

Xem hiện trạng hệ thống: Tiện ích Motherboard Monitor "soi" vào tận những cảm biến cấp thấp trên bo mạch chủ để đo nhiệt độ của bo mạch chủ và bộ xử lý. Bạn cũng có thể giám sát tốc độ quạt làm mát, chỉnh định dạng hiển thị các thông số trên và bật tính năng "cảnh báo" (trên thanh tác vụ Windows hay qua thư điện tử) khi nhiệt độ hay các tham số khác vượt qua mức ngưỡng. Dù vậy, tiện ích Motherboard Monitor không phải dành cho mọi đối tượng người dùng. Khó cài đặt, tính tương thích chưa cao, chẳng hạn như không thể nhận diện các bo mạch chủ ở những dòng máy Compag Presario cũ và máy xách tay Sager đời mới. Nhưng dù sao, tiện ích cũng rất hữu ích cho các game thủ và người dùng ham thích công viêc "ép xung hệ thống". Tiện ích có thể tải miễn phí tại www.pcworld.com.vn, ID:47642.

Chỉnh sửa Registry dễ dàng: Các kỹ thuật viên máy tính thường dựa vào tiện ích Registry Editor để tinh chỉnh tất cả những thông tin quan trọng của Windows, tuy nhiên họ không thích tiện ích này vì giao diện thô sơ. RegWorks (15USD, www.regwrks.com) sẽ giúp bạn có một cái nhìn mới về Registry. Ngoài giao diện đơn giản là tính năng "Undo" hiệu quả, khả năng tìm kiếm tốt hơn, công cụ so sánh khóa và tính năng Favorites nhanh chóng xác định giá trị cho các khóa thường dùng. Tuy nhiên, phần giá trị nhất của tiện ích này là kho dữ liệu các thủ thuật tinh chỉnh hệ thống Tweaks.

CÔNG CỤ CẢI THIỆN TỐC ĐỘ

Kiểm soát card đồ họa: Tiện ích PowerStrip (30USD, www.entechtaiwan.net/util/ps.shtm) cho phép tiến hành ép xung chip đồ họa, đánh giá thời gian đáp ứng bộ nhớ, chỉnh tốc độ làm tươi (refresh) với biên độ 0,1Hz. Bạn cũng có thể dùng phím tắt để tăng giá trị tham số "gamma" giúp quan sát chi tiết hơn những vùng tối khi chơi game. Ngoài ra, bạn có thể sử dụng các mẫu cấu hình (profile) sẵn có hay thư viện tinh chỉnh riêng. Tuy nhiên, việc tinh chỉnh xung nhịp chip đồ họa và bộ nhớ làm giảm chất lượng hình ảnh và có thể làm khởi động lại máy dù việc này giúp tăng tốc hệ thống đôi chút. PowerStrip đặc biệt xuất sắc

trong việc chỉnh tín hiệu hình máy tính để xuất sang tivi màn ảnh lớn, canh theo độ phân giải ti-vi, tần số làm tươi và những thông số khác.

Tinh chỉnh Windows dễ dàng: X-Setup Pro (8USD, www.x-setup.net) đem đến cho bạn hơn 1700 cách tinh chỉnh phần cứng, phần mềm và hệ điều hành Windows. Bạn có thể đổi tên hiển thị của biểu tượng My Computer hay My Network trên màn hình, thay đổi cấu hình cấp thấp hệ thống để chống lại sự tấn công từ Internet. Tiện ích cũng tích hợp một số công cụ của Windows như Registry Editor, Task Manager và Disk Cleanup dưới một trình đơn đơn giản. Những tính năng mà X-Setup Pro có thể giúp ích cho bạn rất nhiều tuy nhiên cũng có lúc chúng đem đến cho bạn những trục trặc thật sự.

NÂNG CẤP TÌM KIẾM

Tìm nhanh thư mục: Bạn muốn truy truy xuất nhanh đến một thư mục, tiện ích Direct Folders (20USD, www.codesector.com/directfolders.asp) có thể giúp bạn chuyện đó bằng cách sử dụng biểu tượng History và Filter trên thanh công cụ tiện ích Explorer. Mỗi chương trình cũng sẽ xuất hiện một biểu tượng có thể cuộn lại. Tuy nhiên, tiện ích không hoạt động được với các ứng dụng Office 2003.

Tạo phím tắt cho thư mục: Tiện ích Folder View giúp bạn truy xuất đến bất kỳ thư mục nào một cách nhanh chóng bằng cách thêm vào biểu tượng trong Windows Explorer. Thay vì phải duyệt qua nhiều cấp thư mục, bạn có thể nhấn chuột vào một biểu tượng và duyệt qua danh sách thư mục như My Documents hay các thư mục truy xuất gần đây. Hộp thoại mở và lưu tập tin hiển thị các thư mục truy xuất gần đây ở cạnh trái, trong khi một biểu tượng khác cho phép truy cập nhanh một thư mục bằng một thao tác nhấn chuột. Bạn có thể tải về tiện ích này từ www.pcworld.com.vn, ID: 46982.

NHỮNG CÔNG CỤ KHÁC

Kiểm soát tình trạng kết nối: Bạn muốn tìm ra lý do mạng hoạt động chậm, hãy sử dụng VisualRoute 2005 (50USD, www.visualroute.com). Chương trình dễ sử dụng, được xây dựng trên nền Java, hiển thị đồ họa giám sát kết nối từ máy tính của bạn đến trang web (giống như lệnh TRACERT của DOS). Chạy chương trình,

gõ địa chỉ URL vào hộp thoại Address và bạn sẽ nhận được thời gian phản hồi từ các máy chủ được kết nối. Tiện ích cần cải tiến thêm đôi chút về giao diện.

Quản lý Clipboard tốt hơn: Như bạn đã biết, clipboard (vùng nhớ tạm lưu trữ thông tin cắt-dán) của Windows ngày càng trở nên nhỏ bé trong thời đại Internet. Tiện ích ClipCache (20USD, www.xrayz.co.uk/clipcache/) biến clipboard thành một thư viện ảo để lưu trữ những tài liệu thường dùng như ảnh số của chữ ký điện tử hay phần cuối thư. Nhấn chuột vào một mục trên cửa sổ ClipCache, bạn có thể ngay lập tức dán chúng vào chương trình đang dùng bằng cách sử dụng tổ hợp phím Ctrl-V. Tiện ích cũng cho phép cài đặt các thư mục thường dùng để thực hiện sao chép tập tin nhanh chóng.

Đánh văn bản chính xác: Tiện ích Insert Toggle Key sẽ giúp người dùng trình xử lý văn bản tránh đánh chồng lên văn bản có sẵn do lỡ tay kích hoạt phím Insert. Tiện ích có thể tải về miễn phí từ www.pcworld.com.vn, ID:47655.

Hồng Vy
PC World Mỹ 6/2005

Khôi phục hệ thống về trạng thái cũ

Tiện ích System Restore của Windows Me/XP sẽ tiến hành "chụp ảnh" cấu hình hệ thống và dữ liệu trên máy, sau đó lưu trên đĩa cứng. Công cụ này có thể đưa máy tính trở lại tình trạng trước khi xảy ra hỏng hóc, dù không có khả năng sửa chữa. Để sử dụng công cụ này, bạn hãy chọn Start.All Programs.Accessories.System Tools.System Restore, và rồi làm theo hướng dẫn để khôi phục lại hệ thống từ dữ liệu sẵn có hay tiến hành sao lưu mới.

Sử dụng tiện ích System Restore để đưa máy tính về lại trạng thái khỏe mạnh trước đó.

THỦ THUẬT WINDOWS

Hạn chế phần mềm gián điệp

Bạn có thể hạn chế hoạt động của phần mềm gián điệp (spyware) bằng cách sử dụng tài khoản giới hạn quyền thay đổi cấu hình hệ thống cũng như cài đặt phần mềm. Để tạo tài khoản dạng này, bạn chọn Start.Control Panel và mở mục User Account. Tiếp đến, nhấn chuột vào chức năng Create a new account, điền vào tên

và nhấn Next. Sau đó, bạn đánh dấu tùy chọn Restricted và nhấn Create Account. Tạo tài khoản giới hạn có thể ngăn cản spyware tấn công hệ thống.

THỦ THUẬT WINDOWS

Chuẩn đoán chi tiết hơn

Trước khi mua một công cụ chuẩn đoán tình trạng hệ thống, bạn dùng thử tiện ích System Information trong Windows XP. Bạn hãy chọn Start.Programs.Accessories.System Tools.System Information để xem chi tiết các thiết bị phần cứng, phần mềm và các thành phần khác của hệ thống. Bạn sẽ không thể truy cập đến những thông tin mà tiện ích PC Wizard 2005 có thể nhưng lệnh System History trong trình đơn View sẽ hiển thị những thay đổi địa chỉ bộ nhớ và vị trí các khóa Registry. Chẳng hạn, bạn có thể dùng công cụ Net Diagnostics từ trình đơn Tools để kiểm tra và khắc phục trạng thái kết nối mạng của hệ thống. Tiện ích System Information thông báo những thay đổi trong hệ thống.

THỦ THUẬT WINDOWS

Tăng tốc hệ thống

Tăng "sức sống" cho máy tính bằng cách tắt đi các hiệu ứng. Bạn hãy nhấn phải chuột lên biểu tượng My Computer, chọn Properties, sau đó chọn thẻ Advance và nhấn nút Settings. Tại thẻ Visual Effects của hộp thoại Performance Options, đánh dấu tùy chọn "Adjust for best performance" hoặc bỏ đi các hiệu ứng được liệt kê bên dưới.

Hạn chế hiệu ứng Windows có thể tăng tốc hệ thống.

THỦ THUẬT WINDOWS

Kích hoạt nhanh ứng dụng

Bạn có sử dụng các phím số để thực thi nhanh một ứng dụng từ trình đơn Start của Windows XP. Nhấn Start.All Programs, chọn ứng dụng bạn thường sử dụng và kéo nó lên trên cùng của trình đơn Start. Nhấn chuột phải lên biểu tượng và chọn Rename, thêm vào con số trước tên chương trình (ví dụ như 1 Firefox, 2 Excel... lưu ý không sử dụng trùng số). Để thực thi những chương trình đó, sau khi nhấn Start hay ÿ, bạn chỉ cần nhấn trực tiếp con số ứng với chương trình. Để gỡ bỏ biểu tượng này, bạn chỉ đơn giản là nhấn phải chuột và chọn Delete (hay Delete from this list với trình đơn mặc định của Windows).
Nhấn phím 1 để kích hoạt Firefox và 2 để chạy Excel.

Recovery Genius - Sự thay thế hoàn hảo cho "thần hộ mệnh"

Lo ngại trước những nguy cơ tiềm ẩn có thể gây sụp đổ hệ thống, rất nhiều cơ quan, trường học, dịch vụ internet và cả người dùng cá nhân đã trang bị cho máy tính của mình một "vị thần hộ mệnh" có cái tên rất quen thuộc - Deep Freeze.

Với sự hiện diện của Deep Freeze, cho dù máy tính của bạn bị tàn phá nặng nề bởi virus, spyware hoặc bị các "vọc sĩ" quậy tưng registry, chỉnh sửa lại những thiết lập nhất quan trọng của hệ thống, cài đặt thêm những phần mềm mang tính phá hoại... thì cũng chẳng có gì phải buồn phiền, bởi chỉ với một thao tác khởi động lại máy là bạn sẽ có ngay một máy tính làm việc ở trạng thái sung sức như thuở ban đầu. Song, chính vì sự "bành trướng" của mình mà Deep Freeze đã khiến cho những tay chơi phần mềm "ngứa mắt" và tung ra một "bí kiếp" có tên Deep UnFreezer nhằm hóa giải Deep Freeze. Trong thời gian chờ đợi theo dõi những tập tiếp theo của bộ phim "Deep Freeze V.S Deep UnFreezer", xin giới thiệu đến bạn đọc một chương trình "đóng băng" máy tính mới mẻ hơn, có chức năng tương tự Deep Freeze nhưng phương thức làm việc thì linh động hơn rất nhiều, đó là Recovery Genius (RG).

Cấu hình hệ thống tối thiểu để cài đặt RG: hệ điều hành Windows 98 trở lên, máy Pentium III có bộ nhớ RAM tối thiểu 64 MB, 20% không gian đĩa cứng còn trống cho phân vùng muốn được sự bảo vệ của RG. Bạn tải về miễn phí phiên bản đầy đủ RG v6.1 tại địa chỉ www.zshare.net/download/rg-rar.html (dung lượng nén 7.54 MB).

Cài đặt chương trình

Lúc bạn giải nén file rg.rar vào một thư mục nào đó (chẳng hạn rg), có thể sẽ có một số chương trình anti-virus cảnh báo là phát hiện một Trojan có tên TR/Slata ẩn nấp trong file YZDLL32.DLL. Đừng quá lo lắng vì thực chất Trojan này hoàn toàn vô hại và nếu để chương trình anti-virus tiêu diệt file YZDLL32.DLL thì quá trình cài đặt RG sẽ không thể hoàn tất. Bạn hãy "lờ đi" bằng cách tắt chế độ bảo vệ tự động của chương trình anti-virus và khi cài đặt xong RG thì có thể tùy ý "xử lý" file YZDLL32.DLL sau. Tiếp đó, bạn mở thư mục rg, kích hoạt file AutoRun.exe để mở giao diện cài đặt RG, rồi bấm vào nút Install.

- Trong hộp thoại đầu tiên xuất hiện, chương trình hỏi bạn có muốn thực thi chế độ tối ưu hệ thống với RG hay không. Việc này vừa làm mất thời gian, vừa chẳng mang lại lợi ích gì nhiều, nên bạn cứ bấm No để bỏ qua.

- Hộp thoại thứ hai xuất hiện với nội dung khuyến cáo bạn nên quét virus, chạy scan disk, dồn phân mảnh ổ đĩa... để có một máy tính ở trạng thái hoạt động ổn định nhất trước khi "đóng băng" với RG. Bạn bấm Next để quá trình cài đặt được tiếp diễn.

- Ở hộp thoại thứ ba, bạn đánh dấu ở mục I agree rồi bấm Next 2 lần liên tiếp.

- Đến hộp thoại thứ năm, với thông điệp "Are there more than one OS on the hard disk?", chương trình hỏi bạn có cài đặt nhiều hệ điều hành khác nhau trên máy hay không. Nếu có, bạn đánh dấu ở mục "Yes, there are many"; bằng không hãy để dấu kiểm mặc định ở mục "No, there is only one", rồi bấm tiếp vào nút Next.

- Hộp thoại xuất hiện kế tiếp đưa ra 2 tùy chọn là: Minimal Protect (chỉ bảo vệ phân vùng đầu tiên với những thông số mặc định của chương trình, thông thường là ổ đĩa C cài đặt HĐH) và Custom Protection (cho phép bạn tùy chọn phân vùng muốn bảo vệ và thiết lập những thông số nâng cao). Bạn nên đánh ở mục Custom Protection và bấm vào nút Next. Trong cửa sổ xuất hiện ngay sau đó, tại hộp Partition Information, bạn đánh dấu kiểm ở những ổ đĩa quan trọng muốn được bảo vệ bởi RG. Tại mục Miscellaneous > Password, bạn nhập vào một mật khẩu quản trị nhằm tránh tình trạng người khác vọc phá chương trình (mật khẩu mặc định là 12345678). Phía bên dưới, bạn đánh dấu luôn ở 2 mục Auto Recover CMOS (tự động khôi phục lại những thông số mà bạn đã cấu hình trong CMOS trước đó) và Prevent HDD I/O (ngăn ngừa đĩa cứng xảy ra những sự cố đáng tiếc như: bad sector, bị virus phá hoại...). Xong, bấm nút Next 2 lần liên tiếp và chờ đợi trong chốc lát.

- Ở hộp thoại xuất hiện sau cùng, bấm vào nút Finish. Ngay sau đó, chương trình sẽ bắt đầu tiến trình tạo ra một thời điểm sao lưu hệ thống "chuẩn" và rồi khởi động lại máy để thay đổi có hiệu lực. Quá trình này thường diễn ra khá lâu nên bạn hãy kiên nhẫn chờ đợi.

Cách sử dụng

- Khởi động lại vào Windows, bạn mở Start > Programs > Recovery Genius > Recovery Genius để kích hoạt RG. Trong hộp thoại xuất hiện, bạn bỏ chọn ở mục Display hint when startup và bấm nút Close. Tiếp đó bấm đôi vào biểu tượng của RG trên khay đồng hồ, rồi nhập vào mật khẩu quản trị trong hộp Check Password để mở giao diện tương tác của chương trình.

- Cách sử dụng RG tương đối đơn giản. Tại hộp Partition Settings > Recovery Type, chương trình cung cấp 3 chế độ phục hồi hệ thống khác nhau để bạn tùy biến là: Auto Recovery (tự động phục hồi hệ thống về thời điểm sao lưu ngay sau khi khởi động lại máy, đây là chế độ đặc biệt "ưa thích" cho các chủ dịch vụ internet), Timer Recovery (phục hồi hệ thống về thời điểm sao lưu theo một chu kỳ thời gian tương ứng với số ngày định trước) và No Recovery (mặc định là giữ hệ thống ở trạng thái bình thường như lúc chưa cài RG). Tùy vào mục đích sử dụng, bạn hãy đánh dấu ở một chế độ thích hợp nhất, rồi bấm vào nút Apply để xác nhận.

- Trong hộp Recover point(s) phía trên, bạn sẽ thấy chỉ có một thời điểm sao lưu "chuẩn" duy nhất vừa được tạo với ngày giờ và thời gian được ghi khá cụ thể. Nút Add Point cho phép bạn tạo thêm những thời điểm sao lưu khác với thời điểm "chuẩn", việc này là cần thiết khi bạn muốn cài đặt thêm những phần mềm mới để sử dụng hoặc cập nhật những bản vá mới nhất cho chương trình anti-virus, anti-spyware của mình. Trong cửa sổ hiện ra ngay khi bấm vào nút Add Point, bạn đánh dấu ở những ổ đĩa muốn được bảo vệ trong hộp Select partitions, nhập vào tùy thích một nội dung mô tả thời điểm sao lưu mới này trong hộp Recovery points description, rồi bấm vào nút Add. Trong hộp thoại xuất hiện, bấm Yes để khởi động lại máy. Cần lưu ý, sau mỗi lần khởi động lại máy ngay khi tạo thêm một thời điểm sao lưu mới, chế độ Auto Recovery ở thời điểm sao lưu mà bạn chọn trước đó sẽ tự động bị hủy bỏ, vì vậy bạn cần thiết lập lại.

- Trong trường hợp muốn cho chế độ Auto Recovery tự động phục hồi hệ thống về một thời điểm mới khác với thời điểm sao lưu "chuẩn" sau mỗi lần khởi động máy, bạn chỉ việc đưa chuột đến thời điểm mới đó trong hộp Recover point(s), bấm đôi chuột vào biểu tượng một ổ đĩa bất kỳ trong hộp Select Partition để làm xuất hiện

hộp Partition Settings phía dưới, tiếp đó đánh dấu lại ở mục Auto Recovery, rồi bấm vào nút Apply để xác nhận việc thay đổi.

- Trong trường hợp không sử dụng chế độ Auto Recovery mà lỡ hệ thống gặp phải sự cố đáng tiếc gì đó, bạn hãy chọn ra một thời điểm sao lưu ưng ý nhất trong hộp Recover point(s), rồi bấm vào nút Recover Data để phục hệ thống bằng tay.

RG là một sự thay thế hoàn hảo cho DF bởi những ưu điểm nổi bật sau: không cản trở đến tốc độ làm việc chung của hệ thống (không chạy nền trong Windows), tốc độ khôi phục hệ thống rất mau lẹ (diễn ra chỉ vài giây trong quá trình khởi động máy), độ bảo mật cao (không thể gỡ bỏ nếu không biết chính xác mật khẩu quản trị), khả năng tùy biến linh hoạt trong phương thức khôi phục hệ thống (hơn hẳn Deep Freeze) và quan trọng nhất là nó không dễ bị "bắt bài", vì trên "giang hồ" hiện nay chưa hề xuất hiện một "bí kíp" thứ hai có tên UnRecovery Genius.

Sửa lỗi file nén Zip bằng "Advanced Zip Repair" - 21/8/2006 9h:23

Bạn không thể nào giải nén được một file Zip có chứa nhiều dữ liệu quan trọng? Bạn đã tải hoàn tất một file nén Zip về từ mạng nhưng vẫn không thể bung ra để sử dụng? Điều này chứng tỏ rằng đã xuất hiện lỗi trong quá trình nén hoặc tải về file Zip.

Công cụ mang tên "Advanced Zip Repair" (AZR) có thể khắc phục được lỗi file Zip kiểu này để cứu lại dữ liệu theo kiểu "còn nước còn tát". Ngoài việc sửa lỗi file nén Zip, AZR còn có khả năng sửa lỗi kiểu file nén tự động bung (Self Extracting file) dạng EXE.

Cách sử dụng AZR cũng vô cùng dễ dàng. Cách thực hiện như sau:

- Sửa lỗi cho file Zip riêng lẻ: Chọn thẻ "*Repair*" trong giao diện chính -> nhấn vào nút có 3 dấu chấm (…) ở ô "*Select Zip or Self Extracting file to be repaired*" để tìm đến file Zip bị hư và nhấp đúp vào để đường dẫn của nó hiện ra -> chọn thư mục chứa file kết quả ở ô "*Output fixed file as*". AZR sẽ tự động chứa file kết quả trong thư mục chứa file Zip bị lỗi -> sau khi chọn lựa xong thì bạn chỉ việc nhấn nút "*Start Repair*" để AZR bắt đầu quá trình sửa lỗi file Zip. Việc sửa lỗi đa số sẽ diễn ra trong thời gian cực nhanh và tên của file kết quả sẽ có thêm từ "*_fixed*" ở phần tên để phân biệt với file gốc bị lỗi.

- Sửa lỗi cho hàng loạt file Zip bị hư: Chọn thẻ "*Batch Repair*" trong giao diện chính -> Nhấn vào nút "*Add files*" -> tìm đến các file Zip bị hư để lần lượt "*Open*" nó ra trong giao diện liệt kê số file Zip cần sửa chữa -> Sau khi đã hoàn tất việc tìm

file, bạn nhấn vào nút "*Start Repair*" và chọn "*Yes to All*" trong giao diện "*Confirm*" để AZR lần lượt sửa chữa toàn bộ các file Zip cho bạn.

Công cụ này tỏ ra rất hiệu quả đối với những file Zip chứa các các gói dữ liệu có nhiều file hoặc dữ liệu văn bản; nó có tác dụng hạn chế đối với những file nhạc số hoặc video, và "bó tay" trước những file Zip có chứa duy nhất một file thực thi dạng EXE, COM…

Công ty DataNumen đang bán ra bản Advanced Zip Repair 1.7 với giá là 29,95 USD. Người dùng có thể vào đây để tải về bản dùng thử với dung lượng chỉ khoảng 788 KB hoặc tìm mua bản chính thức tại các cửa hàng phần mềm.

THỤY KHANH

Theo Tuổi Trẻ Online

Safe Internet (Phần mềm Việt miễn phí)

Safe Internet là phần mềm duyệt Web và cho phép bạn kiểm soát chặt chẽ nội dung truy cập Web. Phần mềm được thiết kế dựa trên nền tảng Microsoft Internet Explorer nên có đầy đủ tính năng duyệt Web và tương thích hầu hết các trang Web trên Internet.

Với Safe Internet, bạn sẽ không còn lo lắng nhân viên sao lãng công việc, học sinh hay con em lướt Web không lành mạnh nữa... Chương trình có giao diện hoàn toàn bằng tiếng Việt, tương thích Windows 2000/XP/2003. Bạn có thể tải miễn phí tại đây (dung lượng 9,3MB).

Ngoài ra, để sử dụng chương trình, bạn cần cài đặt thêm .NET Framework 1.1 trở lên và Microsoft Text-to-speech (nếu máy chưa có). Bạn có thể tải 2 bộ chương trình này tại www.microsoft.com.

1. Các tính năng chính:

- Duyệt Web nhanh, theo Tab.

- Công cụ tìm kiếm tích hợp Google, MSN, Yahoo.

- Tìm địa chỉ và chủ đề nhanh.

- Lọc nội dung Web (chống Web có nội dung xấu rất hiệu quả).

- Lọc địa chỉ, tên miền và từ khóa.

- Lọc chủ đề.

- Lọc File.

- Giới hạn địa chỉ và tên miền được phép sử dụng.

- Nhật ký theo dõi và ghi lại địa chỉ của Web có nội dung xấu.

- Cho phép hoặc cấm download file chương trình.

- Điều khiển tốc độ truy cập Web.

- Lưu trữ tin tức và sách từ nhiều Website khác nhau, xuất ra định dạng XML.

- Tra từ điển khi đang duyệt Web.

- Đọc từ hoặc câu tiếng Anh đã chọn trên Web.

- Sổ lưu niệm cho phép lưu trữ thông tin cá nhân của bạn và khách hàng.

- Điền địa chỉ e-mail hoặc tài khoản tự động vào ô đã chọn trên Web.

...

2. Cấu hình và sử dụng:

Phần mềm được thiết kế phục vụ cho hai đối tượng là người có mật khẩu và người không có mật khẩu.

Với người có mật khẩu khi duyệt Web sẽ không có bất kỳ sự kiểm soát nào về nội dung, tên miền, mở hoặc tải file từ Internet. Thông thường, mật khẩu dành riêng cho người quản lý. Với người không có mật khẩu, phần mềm sẽ kiểm soát chặt chẽ nội dung, tên miền, file, và chủ đề khi đang duyệt Web.

Để vào phần cấu hình, bạn nhập mật khẩu vào ô mật khẩu ở cuối cửa sổ (mật khẩu mặc định là admin) và nhấn Enter. Khi vào trang cấu hình, bạn có thể thay đổi lại mật khẩu này.

- Các loại file chương trình (exe, dll, vbs...) mặc định bị cấm tải hoặc mở từ Internet. Bạn có thể chọn hoặc bỏ ở mục "Cấm Download file chương trình".

- Nếu muốn bỏ qua các thông báo hay yêu cầu do trang Web phát sinh, bạn chọn mục "Bỏ qua các thông báo".

- Nếu muốn khóa lựa chọn Proxy Server của Internet Explorer, bạn chọn mục "Khóa lựa chọn Proxy Server của IE". Khóa lựa chọn Proxy Server trong IE nhằm mục đích cấm các trình duyệt Web khác dựa trên nền IE truy cập Internet.

- Nếu hệ thống có Proxy Server, bạn có thể nhập địa chỉ IP và Port vào mục "Proxy Server". Ví dụ: 192.168.1.5:8080.

- Bạn cũng có thể nhập địa chỉ trang Web mà bạn yêu thích vào mục "Trang mặc định".

- Khi duyệt Web, người sử dụng thường mở nhiều Tab mà ít khi đóng lại, làm lãng phí bộ nhớ máy tính, bạn có thể giới hạn số Tab tối đa được phép mở ở mục "Số trang tối đa".

- Để lướt Web nhanh hơ, bạn có thể chọn tốc độ truy cập ở mục "Tốc độ".

Chủ đề và địa chỉ

Chương trình cho phép bạn tạo thêm chủ đề mới và địa chỉ mới, tiện lợi cho việc truy cập nhanh đến các địa chỉ mà người sử dụng không phải nhớ hoặc nhập địa chỉ.

Web an toàn

Mục "Web an toàn" cho phép nhập các địa chỉ và tên miền mà bạn không muốn chương trình kiểm tra nội dung. Ví dụ: .com.vn, .edu.vn.

Bộ lọc địa chỉ và tên miền

Nếu muốn cấm người sử dụng truy cập đến các địa chỉ nguy hiểm hoặc có nội dung xấu, bạn có thể sử dụng bộ lọc này để cấm. Bạn chỉ cần nhập tên miền vào ô "Từ khóa hoặc tên miền" và bổ sung vào danh sách cấm.

Bộ lọc nội dung Web

Với bộ lọc này, chương trình sẽ tìm các từ khóa trên trang Web, nếu giống với danh sách mà bạn đã nhập nó sẽ tự động đóng trang và trở về trang mặc định. Bạn cũng có thể điều chỉnh số từ khóa xuất hiện trong nội dung Web.

Nếu muốn con em của bạn duyệt Web với nội dung lành mạnh, an toàn thì bộ lọc này rất hữu dụng.

Bộ lọc file

Bộ lọc này không cho phép mở tự động hoặc tải các loại file mà bạn đã quy định. Bạn chỉ cần nhập loại file và bổ sung vào danh sách cấm.

Web được phép truy cập

Nếu muốn người sử dụng chỉ truy cập một số trang Web nhất định, bạn có thể sử dụng mục này để bổ sung địa chỉ. Các địa chỉ nằm ngoài danh sách sẽ bị cấm truy cập.

Nhật ký theo dõi

Nhật ký này sẽ tự động ghi lại các địa chỉ của những trang Web có nội dung xấu mà người sử dụng đã truy cập. Mục này cũng cho phép đưa các địa chỉ đó vào bộ lọc hoặc chủ đề.

Sau khi cấu hình xong, bạn đóng cửa sổ cấu hình lại. Và bây giờ, bạn có thể bắt đầu duyệt Web an toàn với Safe Internet rồi đó.

Phần mềm được cập nhật thường xuyên và cung cấp miễn phí bởi:

Tác giả: Nguyễn Quốc Bảo.

Địa chỉ: 107A C/c Trần Văn Kiểu, P.14, Q.10, TP.HCM.

ĐT: 0903 699709.

E-mail: baothoinfo@hotmail.com.

Nguyễn Quốc Bảo (Q.10, TP.HCM)

Xahoithongtin

Bảo mật hoàn hảo với Invisible Secret 4

Hiện có khá nhiều công cụ hỗ trợ bảo mật máy tính nhưng nếu đã thử sử dụng qua Invisible Secret 4 thì bạn sẽ thích ngay vì công cụ này có khả năng bảo mật hoàn hảo cho những gì mà nó bảo vệ, ngay cả trong trường hợp máy tính bị cài keylogger.
Invisible Secret 4 cung cấp nhiều khả năng như ẩn thư mục, mã hóa file, xóa file ở mức độ không thể phục hồi được, xóa toàn bộ mọi dấu vết của những ứng dụng đã truy cập, bảo mật qua IP, khóa mọi ứng dụng và thiết lập…

1. Chức năng làm ẩn mọi thư mục

Chọn "Hide Files" -> vào Add files để chọn các file cần làm ẩn -> nhấn Next để đặt tên file cần làm ẩn vào ô "Enter the file name…" -> chọn kiểu file phù hợp ở ô "Carrier type" -> nhấn Next và nhập vào các password cần thiết, sau đó chọn thuật toán mã hóa như: AES - Rijndael, Twofish, RC4, Gost, Cast128… -> Nhấn Next và Hide để làm ẩn file. File ẩn sẽ có đuôi là tên file gốc.ISC.

Trong quá trình "Add files", bạn nên chọn chế độ vừa nén (Compress), vừa xóa (Delete, Shred) để dung lượng file ẩn trở nên nhỏ đi nhiều lần và file nguyên thủy sẽ được xóa đi vĩnh viễn. Bạn cũng nên chọn chức năng "New message" để tạo ghi chú cho file cần làm ẩn.

Để file ẩn trở lại hiện trạng ban đầu thì bạn click vào "Unhide Files" -> tìm đến file đã làm ẩn -> nhập vào password cần thiết để làm file nguyên thủy hiện ra.

2. Mã hóa tập tin và thư mục:

Chọn "Encrypt Files". Ở đây bạn có thể mã hóa từng file hoặc nguyên cả một folder bằng cách nhấn vào "Add files" hoặc "Add Folders" -> nhấn Next để gõ vào password và chọn kiểu mã hóa và sau cùng nhấn nút "Enscrypt" đã

mã hóa từng file hay toàn bộ thư mục. Các file đã mã hóa xong cũng sẽ có kiểu đuôi là .ISC và nằm chung trong thư mục gốc của thư mục đã chọn để mã hóa. Nếu muốn giải mã file hoặc folder thì chọn tính năng "Decrypt Files".

3. Xóa file vĩnh viễn ở mức độ không thể phục hồi:

Ghi đè 9999 lần để xóa vĩnh viễn
Chọn "Shred Files" tạm dịch "Bằm file" -> vào "Add files" để chọn những file cần xóa -> chọn "Shred" và nhấn Yes để xóa file vĩnh viễn. Invisible Secret 4 áp dụng công nghệ xóa file triệt để "DoD 5220.22-M" của Bộ Quốc phòng Mỹ nên những file đã xóa đi hầu như vĩnh viễn không thể phục hồi.

Để dọn sạch những dấu vết truy cập Internet cũng như ứng dụng và đồng thời dọn vệ sinh cho máy thì ta chọn chức năng "Destroy Internet Trace" để Invisible Secret 4 xóa sạch toàn bộ cache, cookie, history của Internet Explorer, đồng thời xóa luôn mọi dấu vết truy cập của những ứng dụng khác. Nên check vào ô "Use DoD…" để Invisible Secret 4 áp dụng công nghệ "DoD 5220.22-M" nhằm xóa đi tiệt nọc.

4. IP - To - IP Password Transfer:

Là tính năng độc đáo, giúp chủ nhân của hai máy tính có thể gửi cho nhau mọi password cần thiết một cách hết sức an toàn phục vụ cho việc giải mã file trong Invisible Secret 4.

Để nhận password, chọn ô "Receive Password", sau đó nhập vào địa chỉ IP của máy tính đang dùng -> nhấn Next để đợi password của bạn mình chuyển về máy dưới dạng một thông điệp văn bản.

Để chuyển password cho bạn mình, chọn ô "Transmit Password" -> gõ vào địa chỉ IP của người nhận và password cần chuyển -> nhấn Next để hai chương trình Invisible Secret 4 của hai máy kết nối với nhau qua IP và thực hiện quá trình chuyển password.

5. Khóa mọi ứng dụng đã cài đặt trong máy:

Nhấn vào “Loked Applications” -> nhập vào password cần dùng -> chọn “Lock New Application” để hiện ra bảng liệt kê toàn bộ mọi ứng dụng đã cài đặt trong máy. Chọn các ứng dụng cần khóa lần lượt bằng cách nhấn nút Ctrl và nhấp chuột một lần để chọn. Khi đã chọn xong nhấn nút “Lock”. Khi biểu tượng của chương trình cần khóa đã hiện ra trong bảng thì nhấn “Finish” để hoàn tất quá trình khóa các ứng dụng đã chọn.

Nếu các bạn chú ý kỹ thì trong giao diện sử dụng của tất cả mọi tính năng có trong Invisible Secret 4 đều có một nút chức năng mang tên "Virtual Keyboard". Khi nhấn vào nút này thì một bàn phím ảo sẽ hiện lên và bạn sẽ gõ password bằng cách click chuột vào từng ký tự có trên bàn phím ảo. Chính chức năng này sẽ qua mặt mọi chương trình keylogger đã được bí mật cài đặt vào máy tính mà bạn không biết.

Để sử dụng chương trình một cách hữu hiệu nhất, bạn nên vào "Option" để tìm hiểu và tự tạo ra các thiết lập của riêng mình. Thú vị nhất là bạn có thể chọn cách "tàn sát" dữ liệu triệt để bằng cách ra lệnh cho Invisible Secret 4 vừa xóa vừa tiến hành ghi đè dữ liệu bất kỳ lên vùng dữ liệu đã xóa đến những… 9999 lần, đủ sức làm nản lòng các công cụ phục hồi dữ liệu mạnh nhất thế giới hiện nay. Ngoài ra Invisible Secret 4 cũng cung cấp tính năng quản lý password hết sức hiệu quả (vào Option -> chọn thẻ Password) dù rằng bạn có bao nhiêu password đi nữa.

Công ty NeoByte Solutions đang bán ra Invisible Secret 4 Version 4.4 với giá 39,95 USD. Người dùng có thể vào địa chỉ http://www.gold-software.com/Invisib...-file4092.html để tải về bản dùng thử.

Bộ công cụ bảo mật hàng đầu cho Windows XP SP2

09:56:00, 29/09/2005

Trước những mối đe dọa như virus, spyware, spam, hacker… luôn rình rập người sử dụng mỗi khi vào mạng, vừa qua, hãng BitFantasy đã cho ra mắt phiên bản XPSecurity 2005, một bộ công cụ bảo mật cực mạnh cho Windows XP.

Chương trình XPSecurity 2005 đã được rất nhiều website phần mềm hàng đầu như: Softpedia, TopShareware, FileHeaven… đánh giá là sản phẩm 5 sao. Phiên bản mới nhất XPSecurity 2005c build 1219 có dung lượng 1.54MB, tương thích với mọi phiên bản của Windows XP, có thể tải về bản dùng thử tại địa chỉ http://www.download.com/3000-2094-10309078.html.

Do các tính năng của XPSecurity rất nhiều, nên chỉ xin giới thiệu về những tính năng quan trọng nhất của chương trình. Sau khi thiết lập xong, bạn bấm vào thẻ Apply để thay đổi có hiệu lực.

• **Windows Firewall:** được thiết kế giống với tường lửa của WinXP SP2, giúp bảo vệ máy tính khỏi sự xâm nhập bất hợp pháp từ bên ngoài và giành quyền kiểm soát hệ thống của hacker. Tại tab General, bạn đánh dấu ở thẻ On (recommended) và bấm Apply để thiết lập tường lửa cho WinXP. Nếu muốn hệ thống an toàn hơn nữa, ở tab Exceptions, bạn thêm vào danh sách của XPSecurity những ứng dụng và cổng muốn khóa.

• **Internet Security:** gồm một số tính năng bảo an cho Internet Explorer khi duyệt web, được thể hiện trong 5 tab:
+ Pop-up Blocker: ngăn chặn các trang quảng cáo và pop-up xuất hiện khi duyệt web.
+ IE Apprearance: khóa trang chủ của Internet Explorer, vô hiệu hóa một số tùy chọn trong Internet Options của IE.
+ Privacy: chỉ định trước những website mà bạn không muốn cho ghi lại cookie.
+ Web Content Zone (tương tự tab Security trong IE Options): lựa chọn mức độ bảo mật theo vùng về nội dung của các trang web, hạn chế sự truy cập vào các trang web cấm.
+ Advanced Settings: gồm một số thiết lập tăng cường cho hệ thống, trong đó đáng chú ý như: bật/tắt tính năng autorun của CD/DVD-ROM, không cho save nội dung các trang web bị mã hóa, dọn dẹp temporary files sau khi đóng trình duyệt, kiểm tra chữ ký của các chương trình tải về… Do số lượng tính năng khá nhiều, vì vậy bạn nên thiết lập theo cách nhà sản xuất đã khuyến cáo (chọn thẻ Select Recommended).

• **Email Security:** gồm một số tính năng bảo mật cho Outlook Express, trong đó đáng chú như:
+ Warn me then other applications try to send mail as me: cảnh báo khi có ứng dụng lạ nào đó gửi thư đến.
+ Do not allow attachments to be saved or opened that could potentially be a virus: không cho save hoặc mở các file đính kèm có nguy cơ nhiễm virus từ những lá thư gửi đến.
+ Encrypt contents and attachments for all outgoing messages: mã hóa nội dung lá thư và file đính kèm gửi đi.
+ Digitally sign all outgoing message: đính kèm chữ ký điện tử vào tất cả các lá thư gửi đi.

• **System Security:** gồm một số tính năng bảo mật tăng cường cho hệ thống, được thể hiện trong 6 tab.
+ Windows Update: bật/tắt tính năng tự động cập nhật bản vá của Windows XP.
+ DEP (Data Execution Prevention) Settings: thiết lập một danh sách "đặc biệt"

cho những ứng dụng và dịch vụ chạy nền sẽ được bảo vệ khỏi sự tấn công của virus và các mối đe doạ khác.
+ Startup Run: quản lý các chương trình và dịch vụ nạp chung vào quá trình khởi động Windows.
+ Service Processess: bật/tắt các các dịch vụ chạy nền của Microsoft.
+ Advanced Settings: gồm một số thiết lập tăng cường, trong đó đáng chú ý là: vô hiệu hóa Command Prompt và các batch file, không cho sử dụng Registry Editor, Task Manager; dọn dẹp pagefile lúc tắt máy…

• **Desktop Security:** gồm "hàng tá" tính năng bảo mật cho các thành phần khác của Windows, được thể hiện trong 4 tab:
+ Desktop: ẩn đi biểu tượng của các chương trình trên desktop, vô hiệu hóa tính năng Active Desktop, không cho thay đổi hình nền của desktop…
+ Start menu: bỏ bớt các thành phần trong Start menu như: Search, My Documents, Control Panel, Help and Support, Run…
+ Control Panel: thêm/bớt, làm ẩn đi hoặc vô hiệu hóa một số tác vụ trong Control Panel.
+ Task Scheduler: không thay đổi hoặc tạo ra các task scheduler.
Do trong phần này, số lượng các tính năng là rất nhiều, vì vậy bạn cũng nên thiết lập theo cách nhà sản xuất đã khuyến cáo (chọn thẻ Select Recommended).

• **File System:** gồm một số thiết lập bảo mật dữ liệu trong ổ cứng, được thể hiện trong 2 tab:
+ Drive Accessibility: không cho người khác truy xuất vào các ổ dĩa hệ thống định trước.
+ USB Drive Accessibility: không cho sử dụng các thiết bị di động qua cổng USB để chuyển tải hoặc sao chép dữ liệu trong máy tính.

• **Applications Security:** gồm "hàng tá" tính năng bảo mật cho các ứng dụng, được thể hiện trong 5 tab:
+ Access Control: lập danh sách hạn chế người khác sử dụng một số ứng dụng nào đó.
+ Microsoft Office: tùy biến mức độ an toàn của macro cho các chương trình trong bộ Microsoft Office (Word, Excel, Powerpoint, Outlook), ẩn đi menu trợ giúp Help, bỏ tính năng báo lỗi trong bộ Office XP…
+ MSN Messenger: không cho chat, chia sẽ thông tin trong NetMeeting…

+ Windows Media player: không cho tải codec xem phim, bỏ bớt các tính năng từ menu của Windows Media Player như: Radio Bar, Media Favourites…

• **Anti-Adware:** ngăn chặn các trang quảng cáo, pop-up xuất hiện khi duyệt web; hạn chế sự xâm nhập của ad-ware vào hệ thống, đồng thời cho phép bạn chỉ định trước danh sách những website mà bạn muốn xem quảng cáo...

• **Anti-Virus:** gồm một số tính năng phòng chống virus, được thể hiện trong 2 tab:
+ Sp2 Anti-virus: tích hợp với chương trình diệt virus cài trong máy nhằm tăng thêm tính bảo mật cho hệ thống.
+ Program Self-Protection: tích hợp tính năng tự bảo vệ cho các ứng dụng (mỗi khi ứng dụng nào đó bị nhiễm virus, chúng sẽ tự động được sửa chữa).

• **Preference and Register:** được thể hiện qua 3 tab:
+ Password: tạo ra một password quản trị nhằm tránh tình trạng người khác thay đổi những thiết lập mà bạn đã cấu hình cho chương trình (khi kích hoạt XPSecurity, bạn phải gõ password để đăng nhập).
+ Profile Manager: quản lý chương trình theo chế độ đa cấu hình với các profile chỉnh trước.
+ Register and About: phần giới thiệu của nhà sản xuất và đăng ký sử dụng chương trình.

• **Lưu ý:** Bạn nên đặt chương trình ở chế độ chạy nền để giữ cho Windows XP SP2 của mình luôn ở tình trạng an ninh cao nhất (đánh dấu thẻ Run XPSecurity when starting computer tại thẻ Preferences).

XPSecurity 2005 được đánh giá là vượt trội hơn cả Security Center của Windows XP SP2 về mức độ an toàn và cả số lượng tính năng bảo mật. Chắc chắn XPSecurity 2005 sẽ đem đến là sự hỗ trợ tối ưu nhất cho Windows XP SP2 để bạn tự tin đối phó với những hiểm họa tiềm ẩn có thể xuất hiện bất cứ lúc nào từ không gian Internet.

Phạm Hồng Quân

Dọn dẹp và tối ưu hệ thống với System Cleaner

Giao diện chính của chương trình.

(Dân trí)- Bạn không hiểu tại sao máy tính của bạn sau một thời gian sử dụng ngày một chậm? Bạn muốn chạy một chương trình yêu thích, nhưng máy khởi động rất chậm, khiến bạn bực mình?... Chương trình System Cleaner sẽ giúp bạn tìm lỗi và khắc phục một cách nhanh chóng.

Sau một thời gian sử dụng, máy tính thường có dấu hiệu chậm đi do rất nhiều nguyên nhân như: các ứng dụng thừa, các chương trình đã được gỡ bỏ nhưng chưa hoàn toàn, các lỗi về Registry, các chương trình tự động xâm nhập vào quá trình khởi động …

Chương trình System Cleaner 5, với thiết kế giao diện đơn giản và dễ sử dụng, tất cả các chức năng đều được thiết lập sẵn tạo thuận lợi cho những người mới học tin học, ngoài ra bạn còn có thể vào phần Options nếu bạn muốn hiệu chỉnh lại các thiết lập của chương trình theo ý mình.

Chương trình được chia ra làm 4 mục chính:

+ *Clean up & Repair* (dọn dẹp và sửa chữa –): đây là công cụ giúp bạn dọn dẹp các ứng dụng, các file không cần thiết trên ổ đĩa, Registry. Giúp cho hệ điều hành của bạn quản lý, truy xuất các file và ứng dụng dễ hơn, tiết kiệm được dung lượng ổ cứng của bạn. Ngoài ra chương trình còn kiểm tra và khắc phục các lỗi về Registry.

+ *Optimize & Improve* (tối ưu và cải tạo hệ thống): đây là công cụ giúp bạn sắp xếp lại Registry và kiểm tra các file giống nhau trên ổ cứng để giúp bạn loại bớt các file thừa mà đôi khi vô tình bạn để nhiều nơi khác nhau trên ổ cứng.

+ *Privacy & Security* (sự riêng tư và Bảo mật) : đây là công cụ giúp bạn dọn dẹp và xóa các thông tin cá nhân đã được tự động lưu trên máy tính khi bạn sử dụng như : Cookies, AutoComplete Passwords, URL History, Find File or Folders History …

Ngoài ra còn có một chức năng nữa là Shredder tương tự như chức năng của máy hủy tài liệu. Giúp bạn có thể xóa vĩnh viễn file hoặc folder mà bạn muốn hủy.

+ *System Control* (điều khiển hệ thống): Chương trình đưa ra cho bạn 3 thiếp lập:

Startup Manager: Đây là công cụ quản lý các file tự động chạy khi máy tính khởi động, giúp bạn dễ dàng phát hiện ra các file lạ tự động chèn vào phần startup hoặc loại bớt các file không cần thiết trong quá trình khởi động của máy tính.

Uninstall Manager : Đây là công cụ quản lý các chương trình đã được cài đặt trong máy tính, giúp bạn quản lý một cách chi tiết hơn và còn có thể gỡ bỏ một số chương trình "cứng đầu" mà bình thường bạn không thể uninstall được.

Internet Explorer Extensions Manager : Đây là công cụ giúp bạn quản lý các

chương trình đính kèm Internet Explorer như Yahoo Messenger, Yahoo! Toolbar, Messenger, FlashGet …. Giúp bạn quản lý và gỡ bỏ những chương trình không mong muốn.

+ *Analyze & Compare* (Phân tích và so sánh) : Đây là công cụ giúp bạn phân tích và so sánh các phân vùng, thuộc tính, các vùng trống cũng như đã sử dụng của ổ cứng, đưa ra cho bạn sự tổng quan về ổ cứng đang sử dụng. Quản lý các file có chứa liên kết, giúp bạn quản lý các file này khi nó tự động liên kết và báo cáo cho bạn.

Bạn có thể download bản dùng thử 15 ngày tại địa chỉ :
http://www.pointstone.com/download/

Quốc Trung

Hướng dẫn sử dụng True Image 9

Như chúng ta đã biết từ lâu Acronis True Image là một đối thủ cực kỳ nặng ký của Norton Ghost và từ khi hang phát triển lên phiên bản 9 đã có 1 bước phát triển rất dài với các tính năng ưu việt, nhưng bên cạnh đó phiên bản 9 đã thêm vào 1 số tính năng gây phiền phức và gây hậu quả cực kỳ nghiêm trọng cho người dung (bị mất toàn bộ dữ liệu, Delete các phân vùng trừ phân vùng khởi động…). nhưng một khi làm chủ hoàn toàn được TI thì bạn sẽ thấy đây là 1 công cụ cực kỳ mạnh mẽ và có những tính năng vượt xa Ghost 10. Trong bài viết của tôi dự định chia làm 3 phần như sau:

Phần 1: Hướng dẫn những tính năng cơ bản như cài đặt và sử dụng TI, tạo ảnh dĩa, tạo phân vùng ẩn, chỉnh sửa dĩa…

Phần 2 : Hướng dẫn phục hồi 1 phần hoặc toàn bộ ổ cứng.

Phần 3 : hướng dẫn cách lấy ảnh dĩa của 1 máy và khôi phục trên 1 máy khác có cấu hình hoàn toàn khác (giống như tạo files Ghost cho nhiều máy).

Quote:

PHẦN 1: CÀI ĐẶT VÀ SỬ DỤNG MỘT SỐ TÍNH NĂNG CƠ BẢN.

1. Cài đặt:

Bạn download và tải về dùng thử 15 ngày tại địa chỉ Code:

http://download.acronis.com

Hoặc mua bản Acronis True Image Enterprise Sever 9.1 với giá 999 USD (dung lượng 189Mb).

Double Click vào files TrueImageEnterpriseServer9.1_s_en.exe và màn hình sẽ hiện ra như sau:

Cài đặt True Image Enterprise Server và True Image Agent For Windows.

Hình 1

Khởi động lại máy để hoàn tất việc cài đặt.

Sau khi khởi động xong, boot vào Windows và chạy TI, màn hình TI hiện ra sẽ có giao diện như sau:

Hình 2

1. Tạo một phân vùng ẩn. Click vào **Manage Secure Zone.**

Hình 3

Nhấn **Next** và màn hình **Manage Acronis Secure Zone Vizard** sẽ hiện ra

Nhấn chọn vào phần có ổ cứng nhiều nhất để tạo phân vùng ẩn. (bạn có thể lựa 2, 3

ổ cứng tùy ý nhưng không được phép chọn ổ C)

Hình 4
Nhấn **Next** để tiếp tục, ở màn hình kế tiếp trong ổ **Partiton Size** bạn gõ vào dung lượng phù hợp với ổ cứng của bạn.

Hình 5
và trong hộp thoại tiếp theo

Hình 6
Chú ý: đối với một số máy khi bạn chọn Active Acronis Startup Recovery Manager thì máy tính sẽ không khởi động vào Windows được (do TI đã chép đè lên Master Boot Record), bạn chỉ cần install Standart MBR là xong.), nhấn Process để tiếp tục.
.....
2. Bật, tắt tính năng System Restore của Windows.
Ở màn hình bên trái bạn lựa Manage System Restore, nhấn Next để hiện ra màn hình bật, tắt System Restore, theo tôi nên Lựa Turn Off System Restore.

Hình 7

Hình 8
Nhấn Procees để hoàn tất việc lựa chọn.
---
3. Tạo dĩa CD, DVD cứu hộ.
Như hình trên, bạn bấm vào hình cái dĩa có dòng chữ Create Bootable Rescue Media
Màn hình Acronis Media Builder sẽ hiện ra và bạn nên chọn tất cả các tùy chọn.

Hình 9
Nhấn Next để tiếp tục.
Một điểm mạnh của TI9 so với bản 8 đó là tùy chọn lưu thành files ISO trực tiếp trên ổ cứng, bản 8 bắt buộc bạn phải ghi ngay ra đĩa CD, còn bây giờ bạn có thể lưu trên ổ cứng và 1 chương trình chỉnh sửa files ISO như UltraIso để thêm, bớt files cho đỡ phí dung lượng 1 đĩa CD. Chọn ISO image và nhấn Next để tiếp tục.

Hình 10
Chọn vị trí cần lưu nhấn Next và Process để tiếp tục.
.....
4. Backup hệ thống.
http://i6.tinypic.com/14sp535.png (hình 11)
Nhấn Next 2 lần để tiếp tục.
Hộp thoại **Partition Selection** hiện ra, mặc định ổ C đã được chọn
một hộp hội thoại sẽ hiện ra và bạn cứ nhấn OK để tiếp tục.
Màn hình Backup Archive Location sẽ hiện ra và bạn sẽ có nhiều lựa chọn nhưng bạn chỉ cần quan tâm đến 2 tùy chọn là **Acronis Secure Zone** và **My Computer.**

Hình 12

Hình 13
Có 3 tùy chọn hiện ra, nếu bạn tạo files ảnh lần đầu thì bạn nên lựa tùy chọn ổ trên cùng (Create new full backup archive), tùy chọn thứ 2 (Create incremental backup ì possible) để lưu đè files bạn đã có sẵn trong Acronis Secure Zone, tùy chọn thứ 3 (Create diffenrential backup archive) là bạn sẽ tạo 1 files mới trong Secure Zone.
Nhấn Next, trong ô hội thoại tiếp theo bạn nên chọn tùy chọn : Click here nếu muốn thiết lập nâng cao, còn không thì nhấn Next để tiếp tục với các thiết lập mặc định của nhà sản xuất.

Hình 14
Trong hộp hội thoại Option ta chỉ cần quan tâm đến các tùy chọn : **Compression lever** (chọn Maximum) để nén files với tỷ lệ cao nhất; **Backup Perfomache-Backup Priority** (chọn Hight) để có tốc độ Backup nhanh nhất.

Hình 15
Còn các tùy chọn còn lại thì để mặc định. Nhấn Next 2 lần và Process để tiếp tục. (tỷ lệ nén của Acronis 9.1 thật tốt, ổ C của tôi gần 5Gb mà khi nén xuống Files nén có 1,04 Gb)

(Hình nén)

---
b. Back up vào My Computer. Cũng tương tự bạn chọn My Computer lựa đường dẫn để backup files (phải lựa ổ lưu files backup khác với ổ C), đặt tên files và tiếp tục làm giống như hướng dẫn ở trên.

---
5. Kiểm tra files đã Backup
Chọn Validate Backup Archive, nhấn Next chọn Archive Secure Zone, nhấn Next và Process để kiểm tra, nếu bạn lưu vào My Computer thì chỉ đến đường dẫn đã lưu.

Hình 16
Khi hộp thoại này hiện ra có nghĩa là quá trình Check đã hoàn tất và files Backup của bạn đã hoàn thành.

.....
2. Bật, tắt tính năng System Restore của Windows.
Ở màn hình bên trái bạn lựa Manage System Restore, nhấn Next để hiện ra màn hình bật, tắt System Restore, theo tôi nên Lựa Turn Off System Restore.

Hình 7

Nhấn Procees để hoàn tất việc lựa chọn.
---
3. Tạo dĩa CD, DVD cứu hộ.
Như hình trên, bạn bấm vào hình cái dĩa có dòng chữ Create Bootable Rescue Media
Màn hình Acronis Media Builder sẽ hiện ra và bạn nên chọn tất cả các tùy chọn.

Hình 9
Nhấn Next để tiếp tục.
Một điểm mạnh của TI9 so với bản 8 đó là tùy chọn lưu thành files ISO trực tiếp trên ổ cứng, bản 8 bắt buộc bạn phải ghi ngay ra đĩa CD, còn bây giờ bạn có thể lưu trên ổ cứng và 1 chương trình chỉnh sửa files ISO như UltraIso để thêm, bớt files cho đỡ phí dung lượng 1 đĩa CD. Chọn ISO image và nhấn Next để tiếp tục.

Hình 10
Chọn vị trí cần lưu nhấn Next và Process để tiếp tục.
.....
PHẦN 2 : PHỤC HỒI 1 PHẦN HOẶC TOÀN BỘ HỆ THỐNG

bạn nhấn vào nút Recovery và nhấn Next.
(CHÚ Ý, TRONG PHẦN NÀY BẠN PHẢI THẬT CẨN THẬN, NẾU LÀM SAI 1 TÙY CHỌN THÌ TOÀN BỘ DỮ LIỆU TRÊN Ổ CỨNG CỦA BẠN SẼ MẤT HẾT, KHẢ NĂNG PHỤC HỒI LẠI ĐƯỢC CỰC KỲ THẤP DO ACRONIS SẼ DELETE (DEL Ổ CỨNG KHÁC FORMAT, NÓ SẼ XÓA TÊN Ổ CỨNG VÀ SẼ NHƯ MỘT Ổ CỨNG MỚI MUA) VÀ CHỈ ĐỂ LẠI 1 Ổ C MÀ THÔI.)
a. PHỤC HỒI TỪ Acronis Secure Zone (Đặc biệt chú ý)

Nhấn Next và hộp hội thoại Restore Data Selection sẽ hiện ra:

Sẽ có 3 tùy chọn (tùy chọn Using Snap Restore là tùy chọn mặc định) và bạn KHÔNG được lựa tùy chọn này, nếu không toàn bộ dữ liệu của bạn sẽ bị mất hoàn toàn (bản thân tôi đã bị mất gần 250Gb dữ liệu và thực hành lại một lần nữa mất luôn gần 20Gb dữ liệu trên máy tính của cơ quan) Và tùy chọn chính xác phải là **Restore disk or partitions**

(A) Nhấn Next và chọn ổ C: và tiếp tục nhấn Next

Và hộp hội thoại sau sẽ hiện ra, tiếp tục chọn ổ C, Next.

Và cứ để mặc định các tùy chọn của Acronis tiếp tục nhấn Next cho tới khi hiện ra bảng Process, nhấn Process để Acronis khởi động lại và bạn chỉ việc ngồi chờ và Okie
b. Phục hồi từ files Backup
Chọn vị trí mà bạn đã lưu files bakup trên ổ cứng,

Nhấn Next và chọn

Và lặp lại thao tác (A) cho đến khi hoàn thành.

c. Phục hồi Files từ Acronis Zone.

Nhấn Next

Nếu bạn lựa Orginal location thì Sẽ phục hồi lại toàn bộ Windows, nếu chọn location thì sẽ restore Windows ở một vị trí tùy chọn.
Phục hồi files hỏng từ Files Backup (tương tự).
End phần Backup và Restore.

PDF files Code:
http://www.rapidupload.com/d.php?file=dl&filepath=11652

Tạo PC ảo

Tác giả: trinhh

Hiện nay có 1 số phần mềm cho phép tạo máy ảo trên PC nhưng trong bài viết này mình sử dụng phần mềm Virtual PC 2004 để thực hiện công việc này. Tuy đây là phiên bản cũ nhưng ưu điểm của nó là dung lượng nhỏ và sử dụng rất thuận tiện. Và đây là phần mềm hoàn toàn free. Bạn có thể download tại đây

http://www.microsoft.com/downloads/details.aspx?FamilyID=6d58729d-dfa8-40bf-afaf-20bcb7f01cd1&DisplayLang=en

Sau khi download về cài đặt như bình thường. Chạy chương trình lần đầu tiên máy sẽ hiện ra 1 bảng báo lỗi

Bạn cứ nhấn OK. Sau đó nhấn Next.
Bảng **Options** hiện ra với các lựa chọn
-**Create a virtual machine** (bạn sẽ tạo 1 máy PC ảo theo ý thích của mình)
-**Use default settings to create a virtual machine** (Phần mềm sẽ tự tạo 1 máy PC ảo)
-**Add an existing virtual machine** (Chọn 1 máy PC ảo mà bạn đã có sẵn với dạng file *.vmc)
Chọn mục **Create a virtual machine** và nhấn Next
Ở phần **Name and Location** bạn đặt tên cho máy PC ảo và chọn nơi đặt máy đó bằng cách nhấn vào Browse hoặc cứ để như mặc định. Nhấn Next

Cửa sổ **Operating System** hiện ra cho phép bạn lựa chọn Hệ điều hành cho máy ảo: Windows 95, Windows 98, Windows 2000, Win XP….Nhấn Next.

Ở mục **Memory** bạn có thể để lượng RAM mặc định cho máy ảo là 64MB hoặc nếu muốn thay đổi thì chọn mục Adjusting the RAM và kéo thanh trượt.
Ở mục **Virtual Hard Disk Options** bạn chọn mục **A new virtual hard disk**, nhấn Next và chọn nơi đặt ổ đĩa ảo đó.(Bạn đặt nó ở ổ đĩa nào thì nó sẽ sử dụng ổ đĩa đó để chứa dữ liệu cho máy ảo)
Nhấn Next và Finish là xong.

Cửa sổ **Virtual PC Console** hiện ra. Bạn nhấn Start để chạy máy ảo mà bạn vừa tạo ra.
Sau đó bạn sẽ phải cái hệ điều hành tương ứng lên máy ảo và sử dụng nó như 1 máy tính thật sự.
Bạn có thể cài Hệ điều hành hay dùng các đĩa Boot mà ko cần đĩa CD mà chỉ cần các file ISO = cách vào chạy máy ảo và vào mục CD > Capture ISO Image…

Bộ công cụ chẩn đoán lỗi ổ cứng (Phần I)

Mỗi hãng sản xuất ổ cứng hiện nay đa phần đều phát triển thêm các bộ công cụ, tiện ích dùng để chẩn đoán, bảo dưỡng và sửa chửa các lỗi vật lý trên ổ cứng của mình. Ở phần I, bài viết tổng hợp các công cụ, tiện ích hay liên kết về ổ cứng của Fujitsu, Hitachi (IBM).

Trước khi sử dụng những bộ công cụ, tiện ích này, bạn phải chắc rằng bạn đang sử dụng ổ đĩa cứng của hãng đó và cùng những tính năng, model khác như (IDE, SCSI …) để các tiện ích hoạt động đúng chức năng hơn.

Fujitsu

FJDT (Fujitsu ATA Diagnostic Tool)

FJDT là công cụ phân tích giúp người dùng xác định nhanh chóng ổ cứng EIDE có vận hành đúng hay không. FJDT có thể phân tích những lỗi đáng nghi của ổ đĩa bằng cách kiểm tra dữ liệu thông qua S.M.A.R.T. và song song đó, FJDT cũng dò xét trên bề mặt của ổ đĩa, từng sector để xác định những nhóm môi trường với nhau.

FJDT 6.20 có thể chạy trên đĩa boot MSDOS để xử lý khi hệ điều hành không thể khởi động.

SDIAG (SCSI Diagnostic Tool)

SDIAG là một công cụ đơn giản và đáng tin cậy được phát triển bởi Fujitsu dùng để phân tích các ổ đĩa cứng SCSI Fujitsu. Một lượng lớn các ổ đĩa được gởi trả về nhà sản xuất nhưng với trạng thái thật sự sau khi được phân tích là "No Trouble Found" (Không có trục trặc). Đó có thể là những trường hợp lỗi hệ thống hoặc hệ điều hành nhưng ổ cứng luôn luôn bị đổ trách nhiệm. SDIAG có thể hoạt động mà không cần phải di chuyển ổ cứng ra khỏi hệ thống nên tiết kiệm được tiền bạc và thời gian cho người dùng.

Tùy chọn kiểm tra:

- **Quick: kiểm tra S.M.A.R.T thông tin và khuyết điểm của bề mặt.**
- **Standard: kiểm tra S.M.A.R.T bề mặt, ngẫu nhiên với Đọc/Ghi và Tìm kiếm.**
- **Extended: thực hiện việc Hoạt động hay Ngưng của việc kiểm tra, xác định lại, Đọc/ghi.**

Với tùy chọn "destructive testing" chỉ hoạt động nếu dữ liệu đã được lưu trữ trên ổ cứng.

SDIAG 2.0 vừa được Fujitsu cập nhật, hoat động với hệ điều hành Windows 2000 trở lên.

Hitachi (IBM)

Drive Fitness Test

Phiên bản hiện tại là Drive Fitness Test 4.0, DFT giúp người dùng kiểm tra nhanh chóng các ổ cứng SCSI và IDE và bao gồm cả Serial-ATA IDE. DFT có chức năng thực thi kiểm tra mà không chép đè lên dữ liệu của người dùng. Tuy nhiên, DFT có kèm một vài tính năng khôi phục mà có thể chép đè dữ liệu.

Ở phiên bản 4.0 này, DFT cũng hỗ trợ thêm cho cho các model chipset mới của ThinkPad và có nhiều cải tiến hơn. Ban có thể tải về các phần của DFT ở bên dưới để tạo đĩa khởi động cho Windows hay Linux, nhưng bạn phải khởi động hệ thống của bạn với đĩa khởi động từ DOS để chạy DFT và DFT cũng chỉ hỗ trợ những chip x86:

- **Download Windows diskette creator 4.0 (Đây là phần tạo đĩa boot trong DOS)**
- **Download binary diskette image (non-Windows systems) (Phần tạo đĩa boot trong DOS nhưng ko dành cho HĐH Windows)**
- **Download a CD image v3.73 (Phần tạo CD khởi động cho Windows, Linux và các HĐH khác.**

OGTDT (OGT Diagnostic Tool)

OGTDT là công cụ phân tích lỗi cho các dòng sản phẩm Ultrastar 10K300, Ultrastar 15K73 và DK32XX và nhà sản xuất cũng khuyến cáo các đại lý hoặc người dùng chỉ nên dùng OGTDT cho 3 dòng sản phẩm trên thay vì dùng Drive Fitness Test.

Hoạt động trên hệ điều hành (HĐH) Windows, OGTDT giúp người dùng thực hiện phân tích, kiểm tra lỗi cho ổ cứng.

OGT Diagnostic Tool 7.01 yêu cầu ASPI driver nên bạn có thể tải về phiên bản mới nhất của ASPI driver tại đây.

Bộ công cụ chẩn đoán lỗi ổ cứng (Phần II)

Maxtor là nhãn hiệu nhà sản xuất ổ cứng được ưa chuộng ở Việt Nam, với nhiều dòng sản phẩm ổ đĩa cứng, Maxtor cũng tung ra nhiều bộ công cụ hỗ trợ cho người dùng. Ở phần II, bạn sẽ làm quen với các công cụ, tiện ích của ổ cứng Maxtor và Quantum.

A. MaxBlast 3

MaxBlast 3 là tiện ích đơn giản giúp cài đặt các ổ cứng dạng ATA/IDE. MaxBlast 3 tạo cài đặt và nâng cấp dễ dàng cho người dùng không hiểu biết hay chuyên nghiệp theo cùng một cách như nhau là tự động nhận biết, phân vùng và format bất kỳ ổ cứng Maxtor ATA nào. MaxBlast 3 giúp bạn chuẩn bị mọi thứ chỉ trong vài phút.

Phiên bản MaxBlast 3 thay thế cho tất cả các phiên bản trước như MaxBlast hay MaxPlast Plus.

MaxBlast 3.6 chạy trên hầu hết các phiên bản của HĐH Windows như Windows 95, 98, Me, NT, 2000, Windows XP Home – Professional, hỗ trợ cả 2 định dạng là FAT và NTFS, có khả năng xử lý đến 4 thiết bị ATA trên cùng một hệ thống. Giao

diện thân thiện và hỗ trợ cả in ấn. Để sử dụng MaxBlast 3.6 thì bạn phải có ít nhất một ổ cứng Maxtor ATA được lắp đặt.

Ngoài ra, MaxBlast 3 cũng có một phiên bản cho HĐH Windows là MaxBlast 3 for Windows. Phiên bản này ngoài chức năng kể trên hỗ trợ cho bất kỳ ổ cứng IDE nào, MaxBlast 3 for Windows còn được sử dụng trên hệ thống đã cài đặt HĐH Windows để copy tất cả dữ liệu sang một ổ cứng mới để sử dụng như một ổ đĩa khởi động hoặc cho việc lưu trữ.

Nếu bạn đang cài đặt mới một hệ thống, thì nhà sản xuất khuyến cáo nên sử dụng đĩa mềm khởi động MaxBlast hay CD.

- MaxBlast for Windows (English)

- MaxBlast for Windows (French)

- MaxBlast for Windows (German)

Bạn có thể tải về "MaxBlast Bootable ISO CD" dung lượng khoảng 52MB tại đây. Rồi dung một chương trình như UltraISO hay Nero Burning Rom để burn ra CD.

- MaxBlast Bootable ISO (English)

- MaxBlast Bootable ISO (French)

- MaxBlast Bootable ISO (German)

B. PowerMax

PowerMax là tiện ích được thiết kế để phân tích cho việc đọc/ghi của các ổ đĩa cứng Maxtor và Quantum. Những phần kiểm tra này sẽ quyết định trạng thái của ổ đĩa cứng. Tiện ích PowerMax có thể sử dụng với tất cả những ổ cứng ATA (IDE) với dung lượng lớn hơn hoặc bằng 500MB. Maxtor khuyến cáo người dung thường xuyên sử dụng PowerMax để phát hiện những hư hỏng tiềm tàng của ổ đĩa cứng.

Dung lượng gần 1MB, PowerMax bao gồm 3 thứ tiếng (Anh, Pháp Đức) có thể tải về tại đây.

C. SCSIMax

SCSIMax giúp người dùng phân tích tất cả các ổ đĩa cứng SCSI của Maxtor / Quantum với các chức năng như theo dõi (Self-Monitoring), phân tích và báo cáo.

Việc kiểm tra này sẽ giúp bạn biết về tình trạng của ổ cứng trong thời gian ngắn với mức độ chính xác cao.

Nếu việc kiểm tra hoàn tất mà không có lỗi, thì vấn đề tr ục trặc sẽ nằm ở các linh kiện còn lại trong hệ thống. Kiểm tra lại cáp SCSI, đầu cắm và hệ điều hành. Maxtor cũng khuyến cáo người dùng kiểm tra hỏng hóc của ổ đĩa cứng với SCSIMax không chỉ ở bề mặt vật lý như hư hỏng cluster, sector, các phân vùng hoặc định dạng ổ đĩa … mà còn ở sự nhận diện ổ cứng (trường hợp hệ điều hành không nhận diện đươc ổ cứng).

SCSIMax sử dụng bộ điều khiển SCSI ASPI để gởi tập lệnh *Int13* đến ổ cứng. SCSIMax không phải là tiện ích phá hủy dữ liệu, nhưng nhà sản xuất cũng khuyến cáo nên sao lưu lại tất cả dữ liệu trước khi sử dụng.

Chú ý: SCSIMax không sử dụng được cho các hệ thống máy tính Apple và bộ điều khiển SCSI Ultra320. Tiện ích này cũng không hoạt động trên máy tính để bàn sử dụng HĐH Windows.

Dung lượng nhỏ gọn (70KB), có thể tải về tại đây.

Bộ công cụ chẩn đoán lỗi ổ cứng (Phần III)

Ở phần II, các bạn đã được tìm hiểu về các bộ công cụ, tiện ích dành cho các ổ cứng của Maxtor, với phần III, ta sẽ tiếp tục với 2 hãng sản xuất ổ cứng khác là Samsung và Seagate.

A. Samsung

1. SSDM (Samsung Disk Manager)

SSDM 10.42 là tiện ích giúp xử lý việc giới hạn dung lượng cho các BIOS đời cũ giới hạn dung lượng và việc nhận diện ổ đĩa cứng có dung lượng lớn.

Cách sử dụng SSDM hơi khó nên bạn cần phải xem qua hướng dẫn chi tiết của Samsung tại đây.

2. HUTIL (Diagnostic Utility for New Drives)

Hutil (Drive Diagnostic Utility) được tạo ra với mục đích kiểm tra của ổ đĩa cứng của SamSung trong khi được cài đặt vào trong một PC, bất kể trang thái của hệ điều hành mà người dùng đang sử dụng. Trong quá trình sử dụng ổ cứng, nhà sản xuất khuyến cáo người dùng nên kiểm tra ổ đĩa cứng của mình với Hutil thay vì thay đổi một ổ cứng mới nhưng không bằng.

Nhà sản xuất cũng khuyến cáo bạn nên sao lưu lại dữ liệu trước khi sử dụng Hutil vì Hutil là tiện ích với tính năng "chép" và có thể xóa dữ liệu cũ của bạn.

Hutil cũng chỉ hỗ trợ cho những dòng ổ cứng nhất định của SamSung (xem chi tiết tại đây), nên nếu dòng ổ cứng của bạn không được hỗ trợ thì có thể sử dụng SHDIAG.

3. SHDIAG (Diagnostic for Old Drives)

Tiện ích này thường được sử dụng để kiểm tra các ổ cứng Samsung bị nghi ngờ hư hỏng. Nhà sản xuất cũng khuyến cáo bạn nên sao lưu lại toàn bộ dữ liệu trước khi sử dụng SHDIAG và chỉ hoạt động trên môi trường DOS. Nhấn vào đây để xem SHDIAG hỗ trợ các model ổ cứng nào của SamSumg.

4. SUTIL (Utility for Old Drives)

Tiện ích SUTIL này không được sử dụng bừa bãi vì nó có công dụng giúp người dùng xóa những ổ cứng của mình và cấu hình lại mode DMA cho những ổ cứng đó. Nhà sản xuất khuyến cáo người dùng nên sao lưu lại dữ liệu trước khi sử dụng, bạn cũng nên xem chi tiết về các model mà SUTIL hỗ trợ tại đây.

B. Seagate

1. SeaTools Desktop Edition

SeaTools Desktop Edition là tiện ích mà không thể tìm thấy được ở đâu khác được thiết kế bởi Seagate cho các hư hỏng, trục trặc đối với các ổ đĩa cứng Seagate. Không giống như các tiện ích của các hang khác, SeaTools Desktop Edition hoạt động tốt với hầu hết các ổ cứng ATA, SATA và SCSI trong các hệ thống máy tính để bàn với độ chính xác lên đến 98%.

SeaTools Desktop Edition bao gồm 5 thứ tiếng, phiên bản hiện tại là: English, German, Spanish, Chinese, French . Bạn có thể tải đầy đủ cho cả floppy disk hay CD tại đây.

2. SeaTools Enterprise Edition

SeaTools Enterprise Edition cũng như SeaTools Desktop Edition nhưng với những chức năng ưu việt hơn và dành cho việc xử lý đối với các ổ cứng SCSI hay Fibre Channel trong server và workstation. SeaTools Enterprise Edition có thể kiểm tra, xử lý nhiều ổ cứng cùng 1 lúc và liên tục. Phiên bản chưa được thử nghiệm với ổ cứng ATA và SATA.

SeaTools Enterprise Edition hoạt động tốt trên cả Windows và Linux. Bạn có thể tải về:

- SeaTools Enterprise Edition v2.4.29 dành cho Windows.

- SeaTools Enterprise Edition 2.54 dành cho Linux Command Line.

- SeaTools Enterprise Edition 5.2.23-010730 dành cho Linux Graphical

Bộ công cụ chẩn đoán lỗi ổ cứng (Phần cuối)

Trong phần cuối các bạn sẽ làm quen các công cụ tiện ích của Western Digital. Không chỉ là những tiện ích, mà còn những phần trợ giúp từ nhà sản xuất cho người dùng với các sản phẩm Card Reader, Controller Card, Combo/USB/Firewire …

1. Data Lifeguard (dành cho các ổ cứng dung lượng trên 137GB)

Data Lifeguard v11 bao gồm cả 2 phiên bản: dành cho DOS và Windows được thiết kế để cài đặt cho các ổ cứng EIDE của Western Digital. Nếu máy tính của bạn đã cài đặt ổ cứng với hệ điều hành Windows 98 hay cao hơn thì bạn nên sử dụng phiên bản Data LifeGuard dành cho Windows để có hiệu xu¿??t cao hơn. Phiên bản dành cho DOS chỉ sử dụng khi bạn lắp đặt mới máy tính của bạn mà chưa cài đặt hệ điều hành.

2. DLG Diagnostic

DLG Diagnostic cho phép bạn kiểm tra lỗi ổ cứng, in ra kết quả, sửa lỗi nếu có. Để sử dụng tiện ích này, bạn tải về tại đây. Sau khi tải về, bạn chỉ cần thực thi tập tin "DLGDiagv504c.exe" và tiện ích sẽ hướng dẫn bạn tạo đĩa boot kiểm tra cho mình.

DLG Diagnostic 5.04c hoạt động trên hầu hết phiên bản HĐH Windows 98, 98SE, ME, 2000, XP. Người dung có thể tìm hiểu thêm về cách sử dụng DLG Diagnostic tai đây.

3. DLGDIAG cho Windows

Data LifeGuard Diagnostic for Windows 1.02, đây là phiên bản dành cho Windows của Data LifeGuard. Tiện ích có thể giúp xác định ổ cứng, phân tích, sửa lỗi trên một ổ cứng Western Digital FireWire, EIDE, hay ổ USB. Ngoài ra, tiện ích còn có thể cung cấp cho bạn số serial và model của ổ đĩa cho bạn.

Ngoài những công cụ tiện ích cho ổ cứng, Western Digital cũng có một vài bộ công cụ, hỗ trợ cho các Card Reader, Controller Card … mà tôi giới thiệu với bạn bên dưới đây:

Media Center Tools

- Media Center / Dual-Option Backup USB Driver Update for Windows ME

- Media Center Driver Update for Windows XP v11.8

Card Reader Drivers

Card Reader Driver Update for Windows 2000

Controller Card Drivers & Software

- Promise Ultra TX2 Windows Driver 2.0.0210.36

- SIIG Serial ATA Controller Windows Driver

- Serial ATA RAID Controller Drivers

Combo/USB/Firewire

- External Combo FireWire/USB 2.0 Driver for 98SE

- Series II USB 2.0 Hard Drive for 98SE

- Series I USB 2.0 Hard Drive for 98SE

- Essentials USB Driver

- Spindown or Stop Utility for External Drives v1.00

EIDE RAID Utility

- IDE RAID Upgrade - 3Ware v1.07

- IDE RAID Upgrade - non-3Ware v1.07

Terry Trần

Theo dõi đĩa cứng bằng "HDDlife for Notebooks"

Tác giả: HOÀNG HẢI (tuoitre.com.vn)

Đĩa cứng có thể nói là bộ phận quan trọng nhất của máy tính vì nó chức rất nhiều dữ liệu quan trọng. Nắm được tình trạng hoạt động của đĩa cứng để bảo vệ nó một cách tốt nhất cũng chính là biện pháp song hành với các biện pháp bảo vệ dữ liệu khác.

Công cụ mang tên "HDDlife for Notebooks" (HDN) sẽ giúp bạn nắm được tình trạng hoạt động của đĩa cứng theo thời gian thực để có biện pháp sao lưu dữ liệu kịp thời cũng như đem đĩa cứng đi sửa chữa ngay khi có những biểu hiện xấu trong quá trình hoạt động.

Là một phần mềm ngoại 100% nhưng điều khá đặc biệt của HDN là nó có hỗ trợ luôn tiếng Việt trong giao diện sử dụng. Khi kích hoạt lần đầu tiên, bạn nên vào menu "Language" và chọn "Vietnamese" để HDN chuyển sang giao diện tiếng Việt.

HDN đơn thuần chỉ là một công cụ kiểm tra và đưa ra mọi cảnh báo cần thiết về tình trạng hoạt động của đĩa cứng, cho nên người dùng chỉ cần… nhìn là đủ. Trên giao diện của HDN sẽ thể hiện đầy đủ các thông số sau bằng tiếng Việt:

- ***Nhiệt độ:*** Nếu nhiệt độ hoạt động của đĩa cứng là dưới 45^0C thì HDN sẽ thể hiện thang nhiệt bằng màu xanh an toàn, còn nếu nhiệt độ vượt quá 45^0C thì HDN sẽ đưa ra cảnh báo màu đỏ chứng tỏ nhiệt độ đã đạt đến ngưỡng nguy hiểm.

- ***Thời gian làm việc:*** HDN sẽ cho bạn biết tổng số thời gian đã hoạt động của đĩa cứng từ lúc được gắn vào máy tính cho đến nay.

- ***Nếu thanh "Tình trạng" và "Hiệu suất"*** đều ở màu xanh chứng tỏ đĩa cứng đang ở tình trạng hoạt động tốt, dung lượng trống vẫn còn nhiều. Nếu thanh "Tình trạng" chuyển sang màu đỏ với cảnh báo là "Kém" chứng tỏ đĩa cứng đang ở giai đoạn sắp bị hư hỏng vật lý và bạn cần phải cấp tốc sao lưu dữ liệu và thay đĩa cứng mới. Nếu thanh "Hiệu suất" chuyển sang màu đỏ chứng tỏ đĩa cứng đã quá đầy.

Ngoài ra, HDN còn cung cấp đầy đủ các thông tin khác về đĩa cứng như nhãn hiệu, số hiệu, số phân vùng, dung lượng còn trống chi tiết của từng phân vùng. Khi hoạt động, HDN sẽ thể hiện biểu tượng của mình dưới hình thức là chỉ số nhiệt độ hiện hành của đĩa cứng nằm ở khay đồng hồ, và ở mọi biểu tượng đĩa cứng đều được gắn thêm biểu tượng cái khiên màu xanh của HDN. Khi đĩa cứng có biểu hiện hoạt động bất thường, HDN sẽ lập tức đưa ra cảnh báo bằng một hồi còi hú như xe cấp cứu, đồng thời "phun ra" từ biểu tượng hoạt động của mình hàng loạt chỉ số cảnh báo.

Công ty BinarySense đang bán ra bản "HDDlife for Notebooks 2.8.98 " với giá là 29 USD. Người dùng có thể vào đây để tải về bản dùng thử với dung lượng khoảng 4,6 MB.

Thêm bởi NSTPro: đã có HDDLife Pro bản 2.8.99. Bạn nào cần crack liên hệ qua Y!M với mình: nstproduction

Những điều cần biết để không bị mất cắp tiền trong tài khoản ngân hàng trực tuyến!

Bạn nên biết rằng ở đâu có tiền là ở đó có kẻ cắp!

Kẻ cắp thường ăn cắp login và mật khẩu của mọi người sau đó truy cập vào tài khoản để rút tiền của người ta ra.

Thủ đoạn chính của kẻ cắp là **lập trang site giả, giống hệt trang của ngân hàng trực tuyến** sau đó dùng mọi hình thức để dụ mọi người truy cập vào trang site giả

đó, khi bạn login vào trang giả là bạn bị đánh cắp login và mật khẩu. Kẻ cắp sẽ login vào tài khoản của bạn ở trang thật và rút tiền của bạn ra!

Hiện nay tôi được biết những thủ đoạn của kẻ cắp để dụ mọi người truy cập vào trang giả là **Fishing** và **Pharming:**

- **Fishing:** là thủ đoạn giả danh nhân viên của ngân hàng trực tuyến, hoặc ai đó gửi thư cho mọi người yêu câu truy cập vào tài khoản để bổ xung thêm thông tin cá nhân hay lý do gì đó khác. Nếu có ai đó bị mắc lừa truy cập vào tài khoản băng link trong lá mail đó là bị dẫn vào trang giả, và như thế là bị đánh mất mật khẩu.
- Nếu bạn đã từng tham gia đọc email thì chắc chắn là bạn đã nhiều lần nhận được mail của site trả tiền đọc email thông báo là bạn đã được liệt vào danh sách những người được thưởng 100$, để nhận được tiền thưởng thì bạn phải nộp một khoản tiền nhỏ. Thực ra thì đó là thư của kẻ cắp mạo danh site trả tiền đọc email, gửi cho bạn lá mail đó, nếu bạn nộp khoản tiền nho nhỏ đó hy vọng sẽ nhận được 100$ thì bạn sẽ bị đánh cắp mật khẩu, vì khi đó nếu bạn login vào tài khoản thì thực ra là bạn login ở trang giả.
- Bạn nên nhớ rằng tất cả các ngân hàng, các cửa hàng trực tuyến... họ không bao giờ gửi thư cho bạn để yêu cầu bạn login vào tài khoản. Login và mật khẩu của bạn họ có trong vùng trữ liệu (databas) của họ, họ không cần phải yêu cầu bạn cung cấp cho họ những thông tin đó!
- Bạn chỉ login vào tài khoản ngân hàng của bạn khi bạn muốn, **Đừng bao giờ login vào tài khoản khi có ai đó yêu cầu bạn login!**
- **Pharming:** là thủ đoạn còn nguy hiểm hơn là **Fishing!** Kẻ cắp thay đổi địa chỉ IP của trang ngân hàng, khi bạn login vào trang ngân hàng, mặc dù bạn gõ đúng tên trang ngân hàng nhưng bạn bị dẫn vào trang giả!. Mức độ nguy hiểm rất lớn khi kẻ cắp tấn công vào máy chủ DNS và thay đổi địa chỉ IP của trang ngân hàng, trong trường hợp đó thì hàng chục nghìn người hoặc hơn có thể bị dẫn vào trang giả. Nhưng đó là trách nhiệm của các Admin phụ trách các máy chủ DNS. Máy chủ DNS (Domain Name Server) là máy chịu trách nhiệm biên dich tên miền của các trang thành địa chỉ IP. Khi bạn muốn xem một trang web nào đó, bạn gõ tên trang đó vào trình duyệt web, trình duyệt web gửi thông tin đó đến máy chủ DNS, máy chủ biên dich tên trang web thành địa chỉ IP và kết nối với trang có đị chỉ IP đó.
- **Spear Phishing** - Hình thức lừa đảo Phishing kiểu mới. chi tiết

Làm thế nào để phòng chống thủ đoạn Pharming và Fishing?

- Điều đầu tiên là bạn phải có các chương trình **chống virus, tường lửa (Firewall)** để ngăn chặn kẻ cắp, **hacker** đột nhập vào máy bạn và thay đổi trong máy bạn. Ở Hệ Điều Hành Windows có một file, trong đó có nghi danh sách các trang mà bạn đã từng truy cập, trong danh sách đó bên cạnh tên trang web có địa chỉ IP của trang đó. Khi bạn muốn truy cập vào trang nào đó mà địa chỉ IP của trang đó đã trong file đó thì trình duyệt web sẽ nối trục tiếp tới trang đó theo địa chỉ IP mà không cần phải thông qua máy chủ DNS. Nếu kẻ cắp đột nhập vào máy bạn và thay đổi địa chỉ IP trang ngân hàng, thì khi bạn muốn truy cập vào trang ngân hàng là bạn bị dẫn vào trang giả!
- Khi bạn truy cập vào trang ngân hàng thì bạn để ý xem địa chỉ trang đó hiện ở trình duyệt web có đúng không. Tôi ghi ra đây 2 địa chỉ: http://www.e-gold.com và http://www.e-qold.com Bạn có nhận thấy sự khác nhau giữa 2 địa chỉ đó không? Tôi xin nói cho bạn biết là có khác nhau đấy!
- Khi bạn truy cập vào trang ngân hàng bạn phải để ý xem có biểu tượng cái khóa đóng không? biểu tượng cái khóa đóng thông báo cho bạn biết là bạn nối với trang thông qua hệ thông mã hóa (ssl)
- Khi bạn truy cập vào trang ngân hàng và nhận thấy trang có vẻ khác so với moi khi, thì bạn đừng login, Nếu có điều kiện thì liên lạc với ngân hàng băng điên thoại để hỏi xem họ có thay đổi bộ mặt của trang hay không?
- Bạn không nên sử dụng trình **Internet Explorer** để truy cập vào tài khoản ngân hàng! **IE có nhiều lỗi**, và những lỗi được phát hiện thường không được sửa kịp thời. Bạn nên sử dụng **Mozila, FireFox** hoặc **Opera**, những trình đó an toàn hơn **IE** nhiều, và những lỗi được phát hiên cũng được sửa rất nhanh, cả **3 trình này đêu miễn phí**, Ngoài độ **an toàn cao,** các trình đó còn cho phép bạn có thể **surf cho nhiều trang web cùng một lúc** trong cùng một cửa sổ của trình duyệt web (chi tiết), lúc nào bạn cũng có thể tải phiên bản mới nhất về.
- Trình **FireFox** bạn có thể tải về từ đây:

Mật khẩu

- Bạn nên sử dụng mật khẩu dễ nhớ cho bạn, nhưng khó đoán cho kẻ cắp. **Tuyệt đối không dùng mật khẩu có chứa họ, tên, tuổi, ngày tháng năm sinh, địa chỉ, số thẻ, chứng minh thư, Hộ chiếu của bạn hoặc của bất kỳ ai trong gia đình.** Đó là những từ mà kẻ cắp sẽ sử dụng để dò đoán mật khẩu của bạn.
- Nên sử dụng mật khẩu là ký tự viết tắt của một câu ca dao, tục ngữ, hay một câu văn thơ gì đó mà bạn ưa thích. Ví dụ: mật khẩu: Nmadbntegv là ký tự viết tăt của câu: "Ngày mai anh di biển nhớ tên em gọi về"

- Bạn nên thay đổi mật khẩu thường xuyên, khoảng mỗi tháng một lần.
- Bạn **không nên gõ mật khẩu trực tiếp từ bàn phím khi bạn login**, tốt nhất nên ghi mật khẩu vào một file dạng text (*.txt) sau đó dùng phương pháp **Ctrl+C** và **Ctrl+V** để điền thông tin login. Có những **chương trình gián điệp** ghi nhận thông tin bạn gõ những phím nào khi bạn login rồi chuyển thông tin cho kẻ cắp.
- Mật khẩu bạn cũng **không nên** ghi trong file để trên **pulpit, ổ đĩa C:** hoặc trong tệp **My Document**, đó là những nơi mà các chương trình gián điệp hay dò tìm thông tin để chuyển cho kẻ cắp, **file ghi login và mật khẩu bạn nên giữ trong đĩa mềm A:** chỉ khi nào cần đến bạn mới cho đĩa vào ổ và dùng phương pháp **Ctrl+C** và **Ctrl+V** để login.
- Bạn cũng nên ghi **login và mật khẩu vào sổ tay**, nhưng phải ghi theo **cách riêng của bạn** để lỡ có ai đó đọc được **cũng không biết** đó là login và mật khẩu vào tài khoản ngân hàng của bạn.

Ngăn chặn và diệt trừ Spy và Trojan thường xuyên.

Spy và Trojan là những chương trình gián điệp, chúng thu thập thông tin trong máy của bạn rồi chuyển những thông tin đó cho kẻ đã viết ra những chương trình đó (kẻ cắp).

Một số chương trình cần thiết:

- Kerio personal firewall: Firewall (tường lửa) ngăn chặn sự đột nhập của hacker
- AVG antivirus: Chương trình chống virus
- SpywareBlaster: Chống Spy
- Winpatrol: theo dõi sự hoạt động của các chương trình, khi chương trình nào đó muốn thay đổi trong hệ thống thì Winpatrol sẽ thông báo cho bạn.

Những chương trình kể trên đều miễn phí, bạn có thể tải từ Internet, ngoài ra bạn có thể mua các chương trình chuyên nghiệp ví dụ: Norton antivius, Norton Internet Security...

Quy trình bảo dưỡng PC

Thực hiện: Bùi Xuân Toại

'Bạn chăm sóc tốt PC thì nó sẽ cư xử tốt lại bạn'

Đó chỉ là một cách nói hình tượng đẹp, nhưng thực tế xảy ra đúng như thế: 'Chăm sóc tốt PC, máy sẽ không bị sự cố, không làm mất dữ liệu của bạn, và không khiến bạn phải... mất việc'. Thực hiện đúng các bước sau để tránh các trục trặc cho PC, trước khi chúng gây rắc rối cho bạn.

Hai kẻ thù sinh tử đối với PC là nóng và ẩm. Nhiệt độ quá cao sẽ đẩy nhanh tốc độ hư hỏng đối với những mạch điện tinh vi trong hệ thống. Nguyên nhân phổ biến nhất của tình trạng quá nhiệt là bụi và chất bẩn. Chỗ thoát không khí và quạt CPU bị kẹt sẽ không thể thổi khí nóng ra khỏi hộp máy được. Chỉ cần một lớp phủ mỏng bụi và bẩn cũng có thể làm cho nhiệt độ của các linh kiện trong máy tăng lên.

Mọi chất gây bẩn, đặc biệt là cặn khói thuốc lá, đều có thể ăn mòn các tiếp xúc kim loại để hở. Đó là lý do tại sao phải giữ sạch hệ thống máy của bạn, cả trong lẫn ngoài.

Nếu PC được đặt trong một môi trường tương đối sạch và có kiểm soát thì mỗi năm làm vệ sinh một lần là đủ. Nhưng ở hầu hết chỗ đặt máy thực tế, như văn phòng hay cửa hàng bụi bặm, PC của bạn phải được làm vệ sinh vài tháng một lần.

Tất cả dụng cụ cần dùng chỉ là vài chiếc khăn lau sạch không có lông tơ, một bình xịt khí nén nhỏ, ít giọt dung dịch tẩy rửa nhẹ hòa trong một bát nước, và một vòng tay khử tĩnh điện để bảo vệ cho hệ thống khi bạn dọn vệ sinh bên trong hộp máy.

Kiểm tra bên ngoài hộp máy

Bốn thủ thuật kéo dài tuổi thọ PC

1. Đặt PC trong môi trường không thuốc lá. Khói thuốc lá có thể làm hỏng các tiếp xúc và các mạch điện tử tinh vi.

2. Để cho PC chạy. Bật điện PC từ trạng thái nguội là một trong những động tác gây 'stress' nhất cho những linh kiện trong hệ thống. Nếu không muốn để PC chạy suốt, bạn dùng thiết lập Power Management của Windows để đưa máy vào chế độ Hibernate (ngủ đông) thay vì tắt máy hoàn toàn. Trong Windows XP, bạn nhấn phải desktop và chọn Properties. Nhấn nhãn Screen Saver và chọn nút Power. Chọn nhãn Hibernate để bảo đảm chế độ ngủ đông được kích hoạt, và sau đó chọn thời gian dưới mục 'System hibernates' ở bên dưới nhãn Power Schemes (Lưu ý là tùy chọn này không phải bất kỳ PC nào cũng có). Các máy tính dùng những phiên bản Windows cũ hoặc có hoặc không có những tính năng quản lý điện tương tự. Bạn xem bên dưới biểu tượng Power Management (Power Options trong Windows 2000) để xem xét khả năng PC của mình.

Trước khi bắt đầu dọn vệ sinh, bạn kiểm tra xung quanh PC xem có vật gì ở gần có thể làm tăng nhiệt độ PC hay không (như ánh nắng chiếu qua cửa sổ). Đồng thời dọn sạch tất cả mọi thứ có thể rơi bụi hoặc gây bẩn, như kệ sách hay các chậu cây cảnh chẳng hạn.

Luôn nhớ tắt máy và rút phích cắm điện trước khi làm vệ sinh bất kỳ bộ phận nào của PC. Không được bôi bất kỳ chất lỏng nào trực tiếp lên các bộ phận máy. Dùng khăn không có lông để lau PC.

Dọn vệ sinh hộp máy: Lau hộp máy và dọn sạch các chỗ thoát không khí. Khí nén dùng cho công việc này rất phù hợp, nhưng nhớ không thổi bụi vào bên trong PC hoặc vào các ổ đĩa mềm và ổ đĩa quang. Giữ các dây cáp luôn gắn chặt vào các đầu nối trên hộp máy.

3. Tắt màn hình. Cách tốt nhất để kéo dài tuổi thọ màn hình là tắt màn hình khi không dùng đến
4. Tránh gây sốc PC. Bất kỳ khi nào di chuyển hệ thống, kể cả khi chỉ ngang qua mặt bàn, bạn phải bảo đảm đã tắt điện và rút phích cắm điện.

Bảo trì chuột cơ học: Khi chuột không phải loại quang học bị bẩn, con trỏ sẽ di chuyển thất thường. Tháo vít hình xuyến ở đáy chuột và nhấc hòn bi ra ngoài. Sau đó cạo sạch chất bẩn bám trên hai con lăn plastic được đặt vuông góc bên trong hốc chứa bi.

Giữ bàn phím luôn sạch: Lật sấp bàn phím và lắc mạnh để làm rơi hết các rác bẩn kẹt giữa hai phím. Nếu không hiệu quả, phải thổi nó (từng hơi ngắn) bằng khí nén. Nếu các phím bị dính hoặc bàn phím quá bẩn, bạn cậy phím ra để dễ lau sạch. Các cửa hàng máy tính có bán dụng cụ đặc biệt dùng để tháo phím, nhưng bạn cũng có thể cậy chúng ra bằng cách dùng hai chiếc bút chì cặp hai bên như một cái nhíp nhổ râu lớn (sau khi đã lót bằng vải mềm).

Làm cho màn hình sáng bóng: Khi lau vỏ hộp màn hình và thông các khe thông gió không để bụi rơi vào bên trong máy. Lau mặt màn hình bằng dung dịch lau kính đặc biệt thấm vào khăn vải không có lông tơ. Nếu màn hình có nút khử từ (có ghi biểu tượng là một nam châm nhỏ), bạn ấn nó để khử từ tính bị nhiễm. Nhiều màn LCD có thể lau bằng cồn. Lau màn hình LCD phải nhẹ nhàng: lớp kính của nó bên dưới rất dễ vỡ.

Kiểm tra thiết bị bảo vệ nguồn điện: cắm lại điện cho thiết bị chống đột biến điện. Kiểm tra đèn báo nguy hiểm của thiết bị. Nếu thiết bị chống đột biến điện không

có đèn báo nguy hiểm mà vùng của bạn thường xuyên bị xung quá áp, bạn phải thay ngay bằng loại có đèn báo và được chứng nhận UL 1449.

Lau sạch đĩa CD và DVD: Lau nhẹ nhàng từng đĩa bằng khăn vải ẩm và mềm. Lau theo hướng thẳng từ tâm ra ngoài, không lau cho vòng tròn quanh tâm đĩa.

Bên trong hộp máy

Trước khi tháo hộp máy, bạn nhớ tắt điện và rút phích cắm ra khỏi ổ điện cho PC. Tiếp đất thân thể mình trước khi chạm vào bất kỳ cái gì bên trong máy để tránh làm hỏng các mạch điện do điện tích tĩnh điện. Nếu không tiếp đất thân thể bằng vòng đeo tay, bạn có thể tự tiếp đất mình bằng cách chạm tay vào các vật dụng trong nhà như ống nước kim loại hoặc các dụng cụ điện có nối đất như tủ lạnh, máy giặt, lò nướng v.v... Kiểm tra lại để bảo đảm đã rút phích cắm điện cho PC trước khi mở hộp máy.

Dùng khăn đã khử tĩnh điện để lau sạch bụi bên trong hộp máy. Tránh chạm tay vào bề mặt các bo mạch. Hết sức chú ý đến bộ phận quạt ở nguồn điện, ở hộp máy cũng như ở CPU nếu PC của bạn có trang bị. Thổi sạch bụi ở bộ phận này bằng luồng khí nén; nhưng để tránh thổi bụi từ chỗ này sang chỗ kia, bạn nên dùng một máy hút bụi nhỏ loại cầm tay chạy pin.

Hình 1: Có thể phải thay pin CMOS trên bo mạch chủ sau 4 hoặc 5 năm sử dụng

Nếu PC của bạn đã hơn bốn tuổi, hoặc nếu các card mở rộng cắm trên bo mạch chủ đã quá bẩn, bạn tháo từng card ra ngoài, lau sạch các chân tiếp xúc bằng cồn, rồi lắp lại. Nhưng nếu PC còn mới, bạn chỉ cần ấn nhẹ lên cạnh trên của card, và không chạm vào bề mặt, để bảo đảm cho card được cắm chắc hơn. Tương tự, bạn cũng cần kiểm tra các đầu nối điện, các đầu nối EIDE, và các dây cáp bên trong khác để đảm bảo chúng đấu nối tốt.

Nhân dịp mở vỏ hộp máy, bạn hãy làm quen với pin CMOS trên bo mạch chủ (hình 1). Để biết vị trí của nó, bạn xem lại tài liệu hướng dẫn sử dụng. Nếu PC của bạn đã dùng hơn 5 năm, có thể phải thay pin CMOS này. (Đồng hồ hệ thống chạy sai là một triệu chứng cho biết pin CMOS yếu)

Tìm hư hỏng

Tiến hành kiểm tra định kỳ PC bằng một tiện ích chẩn đoán bệnh phần cứng. Có hai tiện ích tốt nên chọn dùng là Sandra Standard của SiSoftware và #1 - TuffTest-Lite của #1-PC Diagnostics. Bạn đến www.pcworld.com.vn, mục download (ID: 42168) để tải xuống phiên bản miễn phí của Sandra (phiên bản đầy đủ giá 35USD), và #1 - TuffTest-Lite (ID: 42170) (phiên bản đầy đủ chức năng giá 10USD).

Hình 2: Chạy định kỳ chương trình Disk Defragmenter để tăng tốc độ hoạt đông của đĩa cứng.

Việc bổ sung thêm và loại bỏ bớt các bộ phận của hệ thống sẽ để lại các khoản mục 'mồ côi' (không liên quan đến ứng dụng nào cả) trong Windows Registry. Điều này sẽ kéo dài thời gian khởi động của PC và làm chậm tốc độ hoạt động của hệ thống. Có nhiều tiện ích phần mềm được thiết kế để dọn dẹp Registry như Registry Drill của Easy Desk Software. Chương trình này giá 40USD, cho dùng thử miễn phí. Bạn đến www.pcworld.com.vn, mục download (ID: 42172) để tải xuống bản dùng thử.

Windows lưu giữ các tập tin trên ổ đĩa cứng theo các dòng gồm nhiều segment liên tục. Nhưng trải qua một thời gian, đĩa sẽ đầy và các segment bị phân tán, cho nên truy cập sẽ lâu hơn. Để giữ cho ổ đĩa gọn gàng trật tự, phải cho chạy định kỳ tiện ích Disk Defragmenter của Windows. Nhấn Start.Programs (All Programs trong XP).Accessories.System Tools.Disk Defragmenter. Nếu ổ đĩa của bạn bị phân tán segment nhiều, công việc này có thể giúp cải thiện tốc độ làm việc của hệ thống (xem hình 2). Tuy nhiên, việc dồn đĩa (defragment) có thể mất nhiều thời gian. Hãy cấm chương trình tiết kiệm màn hình và các chương trình tự động để 'dồn sức' cho trình dồn đĩa.

Hình 3: Điều chỉnh tập tin tráo đổi bằng cách tạm bỏ thiết lập của Windows

Công cụ Disk Deframenter sẽ không dồn ghép tập tin mà đĩa cứng dùng để chứa những dữ liệu tràn từ bộ nhớ hệ thống (còn gọi là tập tin tráo đổi - swap). Vì phải truy cập thường xuyên tập tin tráo đổi này nên việc dồn ghép nó sẽ gây khó khăn cho PC. Bạn có thể dồn ghép tập tin này bằng tiện ích như chương trình SpeedDisk kèm trong Norton System Works 2004, nhưng có một cách để cài đặt lại nó trong Windows. Trong Windows XP, bạn nhấn phải My Computer và chọn Properties. Nhấn Advanced, rồi chọn nút Settings bên dưới Performance. Nhấn Advanced lại lần nữa rồi nhấn nút Change bên

dưới Virtual Memory. Chọn ổ đĩa hoặc phân vùng ổ đĩa khác, cài đặt kích thước của tập tin tráo đổi, và nhấn OK. Bạn đến find.pcworld.com/42380 để có các hướng dẫn về việc di chuyển tập tin tráo đổi trong các phiên bản Windows khác. Nếu bạn chỉ có một phân vùng ổ đĩa và không có cách nào để tạo phân vùng thứ hai, đồng thời bạn có trên 256 MB RAM, thì bạn nên hủy bỏ tập tin tráo đổi thay vì di chuyển nó. Chọn No paging file trong các thiết lập Virtual Memory (hình 3). Nếu bị trục trặc trong việc khởi động, bạn cho Windows chạy trong Safe Mode và quay lại với tùy chọn này.

Kiểm tra ổ đĩa cứng

Windows XP có khả năng đánh giá sơ bộ tình trạng 'sức khỏe' đĩa cứng bằng tiện ích kiểm tra lỗi của nó. Bạn nhấn phải biểu tượng của ổ đĩa đó trong Windows Explorer và chọn Properties.Tools.Check Now (Windows có thể sửa chữa các lỗi và phát hiện các sector hỏng một cách tự động nếu bạn muốn). Nếu việc kiểm tra này phát hiện một ít lỗi tập tin thì không can gì, nhưng nếu phát hiện hàng trăm lỗi thì ổ đĩa đó có vấn đề.

Hình 4: HDD Health sẽ báo trước trục trặc sắp xảy ra nhờ công nghệ S.M.A.R.T có sẵn trong ổ đĩa

Để có một cách kiểm tra thấu đáo hơn, bạn đến www.pcworld.com.vn, mục download (ID: 42176) để tải xuống tiện ích HDD Health miễn phí của Panterasoft. Tiện ích này sẽ theo dõi tốc độ làm việc của đĩa cứng và cảnh báo về tai họa sắp xảy đến (hình 4). Chương trình này chỉ hoạt động được với ổ đĩa hỗ trợ công nghệ S.M.A.R.T, hầu như tất cả ổ đĩa xuất xưởng từ năm 2000 về sau đều hỗ trợ công nghệ này.

Nhiều nhà thiết kế phần mềm (và driver phần cứng) chủ quan cho rằng bạn sẽ muốn chương trình của họ luôn chạy trên PC, vì vậy họ thiết lập để Windows tải chương trình ngay lúc khởi động (do vậy số các biểu tượng trong khay hệ thống cứ tăng lên mãi). Các chương trình này ngốn nhiều tài nguyên hệ thống và thường tạo ra các tranh chấp phần cứng cũng như các trục trặc về tính tương thích. Muốn ngăn không cho chúng khởi động, bạn chỉ cần nhấn Start.Run, gõ msconfig, và ấn <Enter>. Các chương trình liệt kê bên dưới nhãn Startup đều được cài đặt để khởi chạy cùng với Windows. Bạn bỏ dấu chọn ở ô bên trái của từng chương trình không mong muốn, để nó khỏi tự động chạy.

Bùi Xuân Toại
PC World Mỹ 8/2004

Các lệnh tìm kiếm thông dụng trong Google

Có lẽ mục đích duy nhất của bạn khi sử dụng công cụ tìm kiếm là muốn thấy kết quả càng chính xác càng tốt, nhưng đôi khi những gì mà bạn có được không đúng như mong muốn vì kết quả chứa quá nhiều thông tin tạp, thậm chí không liên quan gì tới chủ đề bạn cần tìm kiếm. Trong trường hợp này, sử dụng vài thuật toán tìm kiếm có thể giúp ích cho bạn rất nhiều.

*** Lệnh tìm kiếm thông tin phục vụ cho mục đích nhất định**

- Cấu trúc: "mục đích" text "nội dung"

- Ví dụ: vulnerabilities text yahoo (tìm kiếm danh sách, chi tiết về những lỗ hổng bảo mật bằng công cụ tìm kiếm Yahoo).

*** Lệnh tháo gỡ rắc rối về một chủ đề**

- Cấu trúc: "mục đích" help "nội dung"

- Ví dụ: vulnerabilities help yahoo

*** Lệnh tìm kiếm những thông tin mới nhất**

- Cấu trúc: What's news

*** Lệnh tìm kiếm đối với các cụm từ nhất định**

- Cấu trúc: "+" search

- Vì Google có xu hướng bỏ qua một số từ hoặc kí tự thông dụng như: "where" và "how", các con số đơn và chữ cái, nên nếu trong từ khoá của bạn những từ này, bạn cần phải cho thêm dấu "+" vào trước (nhớ là có khoảng trắng trước dấu "+").

- Ví dụ: Bạn cần tìm kiếm bộ film Star Wars tập 1, thay vì bạn gõ cả cụm từ Star Wars Episode I vào ô tìm kiếm, bạn cần chia từ khoá này thành 2 phần vì nó có chứa con số (số 1):

*** Lệnh loại trừ**

- Cấu trúc: "-" search

Trong nhiều trường hợp, từ khoá của bạn có thể khiến công cụ tìm kiếm cho ra nhiều kết quả không mong muốn, chính vì vậy bạn cần phải bổ xung dấu "-" (loại tr&#7915
trước những khái niệm bạn không muốn hiển thị.

- Ví dụ: từ "bass" trong tiếng Anh có 2 nghĩa, vừa chỉ tên một loại cá, vừa có liên quan tới âm nhạc. Nếu bạn chỉ muốn tìm kiếm nghĩa "cá" của từ này mà không quan tâm tới nghĩa "âm nhạc", bạn cần phải cho thêm dấu "-" vào trước từ "music":

*** Tìm từ đồng nghĩa**

- Cấu trúc: " ~" Searches

Bạn không chỉ muốn tìm kiếm một từ khoá đặc biệt mà còn muốn tìm từ đồng nghĩa của nó? Hãy đặt dấu "~" vào trước chúng:

*** Lệnh gộp**

- Cấu trúc: * "OR" Searches

- Google hỗ trợ cả thuật toán "OR", nên bạn muốn hiển thị cả nghĩa A và B, bạn cần bổ sung thêm từ "OR" ở giữa.

*** Tìm kiếm theo cụm từ**

- Bạn hãy đặt cụm từ tìm kiếm trong dấu "" để có được kết quả chính xác hơn. Kỹ thuật này đặc biệt có ích khi bạn tìm kiếm một câu nói hoặc một câu thành ngữ nổi tiếng.

*** Tìm kiếm tên miền (domain) riêng biệt**

Nếu bạn chỉ biết tới tên website truy nhập mà không chắc thông tin cần tìm được đặt ở vị trí nào trong website đó, bạn có thể sử dụng Google để chỉ tìm kiếm tên miền đó.

Chẳng hạn bạn muốn tìm kiếm domain quản trị của website Trường Đại học StanfordUniversity:

Theo VnMedia

Bí quyết tinh chỉnh hệ thống

Thực hiện: Anh Khoa

Bạn có thể nhanh chóng nâng cấp máy ảnh số, máy nghe nhạc MP3, mạng máy tính và máy tính cá nhân nhằm cải thiện tốc độ, bổ sung những tính năng mới và nâng cấp dung lượng lưu trữ. Việc nâng cấp ở đây chỉ đơn giản là tải về phần mềm, thay đổi phụ kiện và chỉnh lại vài cấu hình cần thiết.

Đôi điều lưu ý

Bạn cần biết rằng một số việc nâng cấp hay tinh chỉnh thiết bị có thể vi phạm các qui định bảo hành của nhà sản xuất. Cũng lưu ý có một số nhà sản xuất khá dễ dãi, cho phép tinh chỉnh - như Intel và NVidia, thậm chí còn cung cấp cho người dùng các công cụ tinh chỉnh cần thiết, nhưng nhiều hãng khác rất khắt khe và cố tình "làm khó" người dùng. Dù trong bất kỳ trường hợp nào, bạn cần phải nhớ các lưu ý sau:

- Trước hết hãy sao lưu tất cả dữ liệu hoặc bắt đầu công việc từ một thiết bị hoàn toàn "trống". Việc nâng cấp có thể tiến hành rất nhanh, tuy nhiên việc khôi phục dữ liệu mất khá nhiều thời gian.

- Lưu lại các trình điều khiển gốc, trong trường hợp xấu xảy ra thì bạn vẫn có thể khôi phục lại trình trạng làm việc cũ.

- Trước và sau tiến hành nâng cấp, hãy dùng một phần mềm kiểm tra hệ thống chuyên dụng để đánh giá mức độ cải thiện hiệu năng máy tính.

- Ngắt điện khi tiến hành thao tác với thiết bị trong thùng máy. Hãy cẩn thận và đừng làm rơi bất kì dụng cụ, ốc vít hay vật dụng gì bằng kim loại vì chúng có thể gây chạm điện và làm hỏng thiết bị.

PHẦN CỨNG

ÉP XUNG MÁY TÍNH

Những biện pháp cơ bản

Liệu có biện pháp nào cải thiện tốc độ máy tính mà không cần nâng cấp phần cứng? Câu trả lời rất đơn giản, hãy sử dụng một thủ thuật thông dụng: ép xung máy tính (overclocking). Các CPU hiện nay có thể xử lý các tác vụ nhanh và hiệu quả hơn nếu chúng ta tinh chỉnh cẩn thận vài thông số cần thiết. Ép xung không phải là một phép mầu để hóa cỗ máy cũ thành một siêu máy tính nhưng sẽ phần nào giúp bạn vắt kiệt hiệu năng hệ thống sẵn có.

Hai thông số chính ảnh hưởng đến tốc độ làm việc CPU là tốc độ bus và hệ số nhân. Để xác định tốc độ làm việc thật của CPU, bạn hãy nhân hai thông số trên. Ví dụ với tốc độ bus 100MHz và hệ số nhân 5,5 sẽ cho tốc độ hoạt động của CPU là 550MHz. Công thức này được áp dụng cho hầu hết các bộ xử lý Intel Celeron, Pentium II, Pentium III, IV và cả bộ xử lý AMD.

Hình 1: Thiết lập ép xung trong tiện ích PC Setup của BIOS.

Một số tổ hợp bo mạch chủ (BMC) và CPU cho phép thay đổi một hoặc cả hai thông số trên để thiết lập một tốc độ mới cho hệ thống. Thường thì các BMC và CPU vẫn làm việc tốt khi ép xung CPU lên 10-20% so với tốc độ chuẩn. Việc chỉnh tốc độ bus cũng có thể ảnh hưởng đến tốc độ bus PCI và AGP, điều này phụ thuộc vào chipset được tích hợp trên BMC và cách thức mà chipset đó kết nối với các thành phần khác.

Một kinh nghiệm khi tiến hành ép xung là biết dừng ở giới hạn cho phép của CPU, bus hệ thống và bộ nhớ RAM. Nếu thiết lập xung nhịp quá cao trong BIOS, máy tính có thể không hoạt động. Khi ấy, bạn cần dùng trình cài đặt PC Setup để cấu hình lại các thông số trong CMOS RAM. Trong vài trường hợp, bạn phải khôi phục CMOS RAM hoàn toàn bằng cách tháo nguồn pin nuôi CMOS hoặc dùng jumper có kí hiệu “Clear CMOS” trên BMC. Nếu máy tính dùng switch (nút gạt) hay jumper để thiết lập xung nhịp và hệ số nhân thì bạn cần đặt chúng lại ở tốc độ thấp hơn.

Một vài tiện ích như NTune của NVIDIA (tải về tại www.pcworld.com.vn, Download, ID:46554) có thể giúp bạn dễ dàng thực hiện thay đổi các thiết lập. Tuy nhiên, một vài hệ thống của Dell, Gateway, HP, IBM và nhiều máy Pentium I, II,

III không cho phép bạn thực hiện ép xung hệ thống.

Ép xung CPU bằng tiện ích BIOS

Hầu hết các BMC được sản xuất trong 3-4 năm trở lại đây như Asus, Abit, MSI và Tyan đều được cài sẵn chương trình thay đổi xung nhịp CPU trong BIOS. Khi máy tính khởi động, bạn sẽ thấy xuất hiện thông báo chỉ định một phím để kích hoạt trình PC Setup. Tài liệu của BMC sẽ hướng dẫn bạn xác định các thông số liên quan đến việc điều khiển tốc độ CPU.

10 PHÚT

Nâng cấp lên Radeon XT Platinum

Đôi lúc chỉ cần vài thủ thuật nhỏ, bạn hoàn toàn có thể nâng cấp sức mạnh cho thiết bị sẵn có mà không tốn một khoản chi phí nào. Với các tài liệu tham khảo được công bố tại I-hack.com (find.pcworld.com/46432), bạn có thể nâng cấp "firmware" cho card đồ họa ATI Radeon X800Pro hiện hữu lên thành Radeon XT Platium.

Tiện ích PC Setup (hình 1) của bo mạch Abit KA7 đưa ra nhiều thông số cho việc ép xung khi tùy chọn CPU Operating Speed được thiết lập ở chế độ "User Define". Thông số CPU FSB/PCI Clock cũng ảnh hưởng đến tốc độ của bus PCI. Thực tế cho thấy hầu hết các card PCI có thể được ép xung như CPU.

Người dùng có thể ép xung CPU AMD Athlon XP+ 2600 trên bo mạch ECS KT-600A chỉ qua một thao tác cài đặt. Hệ số nhân xung nhịp của CPU Althon XP+ 600A là 11,5, cho tốc độ CPU đạt từ 1910MHz (166x11,5) đến 2288MHz (199x11,5). Qua thử nghiệm thực tế của PC World Mỹ, chipset này có thể hoạt động hiệu quả khi được ép xung đến 2200MHz.

Cấu hình trên bo mạch chủ

Hình 3: (dưới)
Hình 4: (trái)

Trước khi các nhà thiết kế cho phép thay đổi tốc độ CPU bằng phần mềm, các switch và jumper trên BMC đảm nhận công việc này. Việc tiến hành ép xung CPU bằng cách thiết lập jumper cũng tựa như trình PC Setup: bạn chỉ việc tăng tốc độ bus và hệ số nhân để tăng tốc độ làm việc của CPU cho đến khi tìm được tốc độ giới hạn làm việc ổn định. Hình 3 và 4 chỉ ra vị trí các jumper xác lập tốc độ FSB của CPU (từ 100MHz đến 110MHz). Bạn có thể thấy bảng hướng dẫn thiết lập các jumper/switch được khắc trên BMC (tuy nhiên đừng quá tin vào chúng, hãy tham khảo tài liệu hướng dẫn đi kèm của BMC để có thông tin cấu hình chính xác nhất).

Tăng tốc độ xử lý đồ họa

Đa phần việc ép xung không nhằm làm cho PC chạy nhanh hơn mà nhằm làm cho việc chơi game "trơn tru" hơn. Bạn có thể ép xung bộ xử lý của chip đồ họa theo cách giống như CPU. Nâng tốc độ đồ họa không đòi hỏi người dùng phải thao tác với các thiết bị bên trong thùng máy, đơn giản bạn chỉ cần tải về tiện ích nâng cấp. Thậm chí, hãng NVIDIA đưa luôn thiết lập ép xung vào trình điều khiển (phiên bản mới nhất). Để kích hoạt, bạn hãy chạy trình Windows Registry bằng cách nhấn Start.Run, gõ vào regedit và nhấn Enter. Tìm mục HKEY_LOCAL_MACHINE/SOFTWARE/NVIDIA Corporation/Global/NVTweak/, nhấn phải chuột vào cửa sổ bên trái và chọn New.Dword value, đặt tên coolbits và gán giá trị là 3 (hệ Hex). Ở tab NVIDIA (hình 5) trong cửa sổ cấu hình thiết bị đồ họa, cửa sổ "Clock Frequency Settings" cho phép bạn chỉnh dung lượng bộ nhớ và tốc độ xung của chip đồ họa. Chọn nút "Detect Optimal Frequencies" nếu bạn muốn tiện ích tự động đưa ra một con số an toàn cho việc ép xung card đồ họa.

Hình 5: Ép xung chip đồ họa NVIDIA

ATI thì đưa vào tab "Overdrive" trong cửa sổ Display Properties/Settings/Advanced, bạn có thể thay đổi các thông số cho card Radeon trên hệ thống của mình. Để tinh chỉnh tốt hơn, hãy tải về tiện ích ATITool

(www.pcworld.com.vn, Download, ID:46428), chương trình sẽ tự động xác lập tốc độ nhanh nhất cho card đồ họa của bạn.

NHỮNG TIỆN ÍCH ĐÁNH GIÁ HỆ THỐNG

Hình 2: Kiểm tra hệ thống với tiện ích Sandra.

Hiệu quả của việc nâng cấp thường rất rõ rệt, tuy nhiên để biết chính xác những gì đã đạt được, bạn hãy tiến hành chạy các phần mềm benchmark để đánh giá bộ vi xử lý, bộ nhớ và tốc độ ổ đĩa cứng.

Các kỹ thuật viên chuyên nghiệp thường sử dụng các phần mềm đánh giá hệ thống toàn diện có tên tuổi như WorldBench 5 (249USD, www.worldbench.com) và VeriTest (find.pcworld.com/46430). Người dùng phổ thông thường chọn tiện ích Sandra của SiSoftware (40USD, www.sisoftware.net) hay 3Dmark và PCMark của Futuremark (20USD, www.futuremark.com).

Tiện ích Sandra của SiSoftware (hình 2) nhanh chóng đưa ra kết quả đánh giá CPU, bộ nhớ, thiết bị I/O.

Để đánh giá các thiết bị đồ họa, tiện ích 3DMark thực hiện chạy để lấy điểm nhiều lần, bằng nhiều phương pháp khác nhau. Khi chạy 3DMark, bạn sẽ thấy trên màn hình nhiều đoạn video được trích ra từ các game và những hình ảnh đồ họa phức tạp.

Bằng cách sử dụng cả Sandra và 3Dmark, bạn có thể đánh giá được chính xác mức độ cải thiện của hệ thống sau khi tiến hành nâng cấp.

HỆ ĐIỀU HÀNH ĐỂ WINDOWS HIỆU QUẢ HƠN

Tinh chỉnh Windows

Hình 6: Thiết lập kích thước tập tin nhớ tạm (swap).

Quá trình thay đổi các thông số trong Windows đòi hỏi người dùng phải nhớ chi tiết từng bước thực hiện, chính xác tính năng từng thông số. Thật là phức tạp! X-Setup Pro (www.x-setup.net) của XQDC có thể giúp cho việc này trở nên đơn giản. Phần mềm cho phép truy cập đến hàng trăm thông số quan trọng điều khiển hoạt động của Windows hoặc các ứng dụng. Hơn thế nữa, X-Setup Pro còn cho bạn biết ý nghĩa của từng tham số và tác động của chúng đến hệ thống.

Tuy vậy, trước khi tiến hành cấu hình lại Windows, bạn hãy dùng vài biện pháp đơn giản hơn được đề cập trong bài "Trẻ hóa Windows" trong số báo này, trang 103. Với những yêu cầu cao hơn, bạn có thể điều chỉnh vài tham số để cải thiện tốc độ làm việc của Windows. Hệ thống sẽ hoạt động hiệu quả hơn nếu bạn thay đổi dung lượng và đĩa cứng mà Windows sử dụng để lưu các tập tin tạm và dùng làm bộ nhớ ảo (hình 6).

Thay đổi hai thông số chính

10 PHÚT

Tận dụng bộ nhớ

Windows cung cấp nhiều tùy chọn và các hiệu ứng để tuỳ biến giao diện hệ thống. Giao diện càng đặc sắc thì tài nguyên hệ thống càng bị chiếm dụng nhiều. Bạn có thể phần nào tiết kiệm bộ nhớ bằng cách tắt đi hình nền, trình bảo vệ màn hình hay các hiệu ứng đặc biệt khác. Các bước thực hiện như sau:

1. Nhấn phải chuột lên màn hình và chọn Properties.

2. Ở tab Desktop, chọn (None) cho mục Background.

3. Ở tab Appearance, nhấn nút Advanced. Tiếp đến chọn Desktop ở trình đơn thả xuống và chọn màu nền màn hình ở trình đơn Color 1.

Trước khi tiến hành thay đổi các thông số trên, bạn hãy dọn dẹp ổ cứng theo các bước sau:

1. Mở cửa sổ My Computer, nhấn phải chuột lên ổ C: và chọn Properties.

2. Nhấn Disk Cleanup và chờ công cụ này thực hiện xong công việc, sau đó nhấn OK và Yes để xóa các tập tin rác.

3. Nhấn OK để đóng cửa sổ Properties.

Tiếp đến, tiến hành tinh chỉnh Windows lần lượt theo các bước sau:

1. Nhấn phải chuột lên My Computer và chọn Properties.

2. Chọn tab Advanced và nhấn Environment Variables.

3. Trong hộp thoại Environment Variables, chọn TEMP và TMP, thay đổi đường dẫn để bạn dễ dàng nhận biết vị trí của chúng. Sau đó nhấn OK.

4. Ở tab Advanced, trong phần Performance chọn nút Settings.

5. Trong cửa sổ Performance Options, chọn tab Advanced.

6. Trong phần " Virtual memory" nhấn nút Change.

7. Chọn Custom size, điền vào cùng giá trị cho Initial và Maximum sizes, sau cùng nhấn nút Set (hình 6). Bạn nên thiết lập kích thước tập tin tạm (swap file) tối thiểu bằng 1,5 lần kích thước bộ nhớ RAM hệ thống. Ví dụ ở hệ thống 256MB RAM, kích thước tập tin tạm có thể là 384MB. Tuy nhiên qua thực tế, ở những hệ thống được trang bị nhiều RAM như 512MB hay 1GB RAM, bạn chỉ cần đặt các kích thước tập tin tạm này là 512MB và 768MB.

8. Nhấn OK để đóng hộp thoại và khởi động lại Windows.

4. Nhấn OK hai lần để đóng tất cả các hộp thoại.
5. Nhấn phải chuột lên biểu tượng My Computer và chọn Properties.
6. Ở tab Advanced, chọn nút Settings trong mục Performance.
7. Trong hộp thoại Performance Options, đánh dấu tùy chọn Custom và bỏ tất cả các chọn lựa bên trong.
8. Nhấn OK hai lần để đóng tất cả các hộp thoại.

TÙY BIẾN GIAO DIÊN WINDOWS

Không còn mấy hứng thú với giao diện Windows thân thuộc, hãy thử biến hóa một màn hình mới bằng bộ phần mềm Object Desktop giá 40USD của hãng Stardock (www.stardock.com) bao gồm các ứng dụng nhỏ có khả năng chỉnh sửa hầu hết các giao diện của Windows.

Một tiện ích đơn của StartDock là WindowBlinds (20USD) cho phép bạn thay đổi các chi tiết như hình nền, thanh tác vụ, kiểu dáng thanh cuộn, màu sắc, font chữ, các hiệu ứng đặc biệt và hơn thế nữa.

Bạn không thích trình đơn Start trong Windows XP? Tiện ích bổ sung ObjectBar (20USD) cho phép bạn tự tạo một thanh công cụ mới và thanh duyệt chương trình riêng.

Và nếu thích tính năng chuyển đổi tác vụ dạng thumbnail tuyệt vời của Mac OS X, tiện ích WinPlosion (www.winplosion.com) sẽ trang bị tính năng này cho hệ thống Windows của bạn. Một tiện ích khác của StarDock là Bootskin (miễn phí) sẽ nhanh chóng thay đổi logo khởi động của Windows.

Tiện ích WindowBlinds cung cấp nhiều giao diện mới.

Chọn đúng cửa sổ cần thiết trên desktop rồi rắm... bằng cách nhấn vào một trong các hình thu nhỏ của WinPlosion.

MẠNG MÁY TÍNH
TÙY CHỈNH CÁC THÔNG SỐ KẾT NỐI

Hình 7: Thiết lập các thông số lưu trữ tạm thời

Sự an toàn và tốc độ của mạng phụ thuộc vào việc cấu hình hai thông số là RWIN (Receive Windows) và MTU (Maximum Transmission Unit) trong Windows. Bạn có thể dùng Windows Registry để thay đổi chúng theo hướng dẫn tại find.pcworld.com/46436 hay sử dụng tiện ích miễn phí DrTCP (tải về tại www.pcworld.com.vn, Download, ID:46436).

Tham số RWIN thay đổi dung lượng bộ đệm dữ liệu nhận trong giao thức TCP/IP. Giá trị càng cao, tốc độ tải càng nhanh và con số này không có giới hạn. Theo kinh

nghiệm của đa số người dùng, giá trị RWIN trong khoảng 32768 và 65536 sẽ cho tốc độ tốt nhất (nếu bạn không thiết lập, giá trị mặc định của RWIN sẽ gấp 4 lần giá trị MTU). Tham số MTU sẽ thiết lập dung lượng lớn nhất của gói dữ liệu gửi/nhận, và con số này phụ thuộc vào loại kết
nối (dial-up, LAN hay ADSL). Giá

trị mặc định cho giao thức TCP/IP là 1500; nhưng ở kết nối dial-up (quay số), giá trị này là 576; với giao thức PPPoE (cáp hay DSL), giá trị này phải nhỏ hơn 1492. Một vài ISP và mạng riêng ảo (VPN) yêu cầu giá trị thấp 1300 để kết nối các hệ thống với nhau và mã hóa dữ liệu.

Hình 8: Sử dụng DrTCP để cấu hình thông số mạng

Để tăng thêm tốc độ, bạn có thể chỉnh số lượng kết nối cùng lúc đến máy chủ. Nếu đang sử dụng đường truyền tốc độ cao (cáp hay DSL) thì thay đổi các thông số này làm cho việc tải trang web đáp ứng nhanh hơn. Một vài máy chủ dịch vụ web giới hạn hai kết nối cùng lúc vì vậy bạn sẽ không thấy tăng tốc ở tất cả các site.

TĂNG PHẠM VI HOẠT ĐỘNG MẠNG KHÔNG DÂY

Mạng không dây ngày càng được sử dụng rộng rãi dù chưa thật hoàn hảo. Để mở rộng phạm vi hoạt động mạng và ít nhiễu sóng hơn, bạn không thể đơn giản trang bị thiết bị Wi-Fi (adapter, access point) có công suất mạnh hơn do qui định của tổ chức FCC (Federal Communications Commission). Thay vào đó, bạn cần anten phát và thu sóng tốt hơn ở cả đầu phát và đầu thu để gia tăng cường độ tín hiệu và giảm nhiễu.
Hầu hết các access point không dây đều sử dụng anten có thể tháo rời, nhưng chỉ có vài sản phẩm Wi-Fi adapter được trang bị đầu nối anten ngoài như các model Orinoco/Avaya (giá 30 - 80USD). Với các thiết bị loại này, người dùng có thể trang bị đầu nối (giá khoảng 20USD) và cáp xoắn để nối với anten gắn ngoài. Bằng cách này, bạn có thể mở rộng phạm vi hoạt động mạng không dây của mình. Tham khảo tài liệu tại www.hyperlinktech.com hay www.antenna.com.

MÁY TÍNH ÊM VÀ MÁT HƠN

Làm mát CPU

Hình 9: Quạt làm mát CNPS7000B của Zalman.

Khi máy tính hoạt động, nhiệt độ trong thùng máy sẽ nóng lên, tốc độ xử lý càng cao thì nhiệt độ cũng không ngừng tăng theo. Hầu hết các máy tính đều được trang bị hệ thống tản nhiệt và quạt làm mát, tuy nhiên các thiết bị này tỏ ra "bất lực" với các hệ thống máy tính được thực hiện ép xung. Một vài thiết bị tản nhiệt và quạt làm mát mới có thể làm giảm nhiệt độ CPU và tạo ra ít tiếng ồn hơn. Ví dụ như quạt làm mát CNPS7000B giá 50USD của hãng Zalman dùng cho các CPU Athlon và Pentium 4 hay hệ thống tản nhiệt CL-P0092 giá 40USD của Thermaltake dùng cho hệ thống Pentium 4.

Các hệ thống tản nhiệt và quạt làm mát có thể là chọn lựa tốt cho người dùng thông thường. Hiện nay, nhiều hệ thống máy tính ép xung được trang bị hệ thống tản nhiệt bằng nước (giá dao động từ 100 đến 180USD) thường được sử dụng trong các siêu máy tính. Nguyên lý hoạt động của các hệ thống này là luân chuyển nước qua một miếng tản nhiệt đặt trên mặt CPU, bơm lên và sau đó dùng quạt thổi hơi nóng ra. Phương pháp này rất hiệu quả cho việc ép xung trên CPU, chipset và card đồ họa. Tuy nhiên, bạn cần phải có đủ không gian trong thùng máy và xung quanh CPU để trang bị hệ thống làm mát như vậy.

Tăng công suất và giảm tiếng ồn

Việc ép xung CPU và tinh chỉnh máy tính có thể dẫn đến tình trạng thiếu nguồn điện. Khi ấy, bạn cần nâng cấp nguồn công suất lớn hơn. Antec Phantom giới thiệu bộ nguồn rời 350 watt không có quạt giá 170USD (hình 10). Bộ nguồn này có trang bị phiến tản nhiệt bên trong đủ làm mát mà không cần dùng quạt và do vậy giảm thiểu tiếng ồn.

Để PC hoạt động êm hơn

Hình 10: Bộ nguồn rời Antec Phantom

Bộ nguồn đã hoạt động êm hơn, giờ đến lúc xử lý cho máy tính. Bạn không thể bỏ qua tiếng ồn do quạt. Một biện pháp để giải quyết vấn đề là dùng quạt làm mát tự động điều chỉnh tốc độ theo nhiệt độ của Thermaltake A1214 giá 6USD. Dù vậy, những rung động từ quạt và ổ đĩa cứng có thể vẫn làm bạn khó chịu. Các nắp đậy phẳng hai bên thùng máy cũng có thể gây ra tiếng ồn cho máy tính. Bạn có thể khắc phục phần nào tiếng ồn này nếu sử dụng các miếng dán chống rung của DampTek (hình 11) giá 50USD/hộp 3 miếng.

MÁY ẢNH SỐ
CHỈNH SỬA HÌNH ẢNH

Biến Canon EOS 300D thành Canon 10D

Chỉ đơn giản bằng cách tải về một tập tin và nâng cấp "firmware", chiếc Canon EOS300D của bạn sẽ nhanh chóng có được những tính năng tương tự dòng máy cao cấp Canon 10D, bao gồm chỉnh độ nhạy ASA/ISO 3200, menu tính năng tùy chọn, chụp không dùng thẻ nhớ Compact Flash. Bạn có thể tham khảo tại find.pcworld.com/46442 để biết thêm thông tin về cách nâng cấp này.

Tuy nhiên trước khi tiến hành, hãy tải về bản nâng cấp "firmware" mới nhất (của EOS 300D) từ website của Canon, phòng trường hợp quá trình nâng cấp gặp trục trặc bạn có thể cài đặt lại từ "firmware" này. Sau đó, bạn tuần tự làm theo các bước sau:

1. Tải về "firmware" máy Canon 10D tại find.pcworld.com/46444.

2. Dùng máy ảnh để "format" lại thẻ CF (dung lượng ít nhất là 8MB) và chép "firmware" vừa tải về lên thẻ nhớ này.

3. Cho thẻ CF vào máy.

4. Mở máy, và thiết bị sẽ tự động nhận biết "firmware" mới và hướng dẫn bạn cách thực hiện ngay trên màn hình LCD (đơn giản chỉ là chấp nhận cấu hình mới và khởi động lại thiết bị).

10 PHÚT

Điều khiển từ xa máy ảnh số

Nếu đang sở hữu một máy Canon EOS Digital Rebel và thiết bị PDA dùng phần mềm Nevo (thường là máy IPaq), bạn có thể tải về tiện ích ở site CameraHacker (find.pcworld.com/46450) để điều khiển chụp Rebel từ xa

Lấy ảnh từ máy Dakota

Bạn mua máy ảnh dùng một lần Dakota và bây giờ cần đem đến tiệm để rửa ảnh. Không cần thiết, chỉ với vài thao tác bạn hoàn toàn tự làm được chuyện ấy bằng cách tham khảo tài liệu hướng dẫn cách kết nối USB thiết bị này tại find.pcworld.com/46446, hoặc cách chép 25 bức ảnh trong máy ra theo các hướng dẫn tại find.pcworld.com/46448.

bằng PDA. Ngoài ra, website cũng giới thiệu nhiều thủ thuật hữu ích khác mà có thể bạn chưa từng biết đến.

MÁY NGHE NHẠC SỐ LƯU TRỮ NHIỀU HƠN

Nâng cấp ổ cứng cho máy nghe nhạc Nomad Zen

Hình 11: Miếng dán chống ồn DampTek

Một khi dung lượng 20GB của chiếc máy nghe nhạc số Nomad Zen không đáp ứng yêu cầu lưu trữ hay đơn giản bạn muốn tăng dung lượng thì nên nâng cấp ổ đĩa cho máy. Việc nâng cấp chỉ mất chừng 30 phút với vài thao tác rất đơn giản. Mọi hoạt động của máy Zen đều nằm trong "firmware", do vậy bạn có thể thay đổi ổ cứng dễ dàng mà không phải lo ngại bất cứ chuyện gì ngoài tem bảo hành bị rách.

Bước thứ nhất, bạn phải có sẵn một ổ cứng thay thế. Theo Creative, máy Nomad Zen sử dụng ổ cứng dành cho máy tính xách tay của Fujitsu và bạn không quá khó để tìm một ổ đĩa dung lượng 20GB, 40GB hay thậm chí 60GB.

Bạn nhớ cài phần mềm của Nomad Zen vào máy tính trước và sao lưu lại tất cả các tập tin nhạc hiện có.

Tiến hành tháo ổ cứng cũ khỏi máy theo các bước sau:

1. Tháo 4 con vít ở mặt sau máy

2. Tách nắp đậy khỏi thân máy, bạn sẽ thấy ổ cứng được gắn với một đai bằng kim loại.

10 PHÚT

3. Tháo đai ra bằng cách nạy các cạnh xung quanh và nhớ giữ lại khung này.

4. Nhẹ nhành nâng ổ cứng lên ở đầu đối diện các đầu nối.

5. Cẩn thận kéo ổ cứng lên bằng cách giữ chặt các mạch điện và đầu nối.

6. Lúc này, bạn sẽ nhận ra một tấm bọt biển mỏng (hình 12) có tác dụng chống va chạm, hãy giữ lại nó.

Lúc này, bạn đã hoàn thành được nửa chặng đường và hãy cố gắng hoàn thành các công đoạn lắp vào và "format" ổ cứng mới:

1. Một lần nữa hãy giữ chặt các mạch điện và đầu nối, cẩn thận cắm ổ cứng mới vào đầu nối đó.

2. Lắp ổ vào thân máy.

3. Đặt lại đai kim loại xung quanh ổ đĩa mới và cẩn thận gài chúng vào thân máy (hình 13).

4. Gắn lại mặt sau máy và siết chặt 4 con vít đã gỡ trước đó.

Những tiện ích tốt hơn cho máy nghe MP3

Nếu bạn thất vọng với các phần mềm đồng bộ dữ liệu đi kèm với máy nghe nhạc MP3, đừng lo vì giờ đây có rất nhiều phần mềm khác cũng có tính năng tương tự. Hãng phần mềm Red Chair (www.redchairsoftware.com) giới thiệu nhiều phần mềm quản lý máy nghe nhạc số hiệu quả như Notmad Explorer (35USD) dành cho máy MP3 Creative, Anapod Explorer dành cho máy Ipod và Ipod Mini của Apple. Ngoài ra, bạn có thể dùng phần mềm Riorad Explorer (tương thích với máy nghe nhạc Rio) và Dudebox Explorer (dùng cho máy Dell).

BẢO QUẢN MÁY IPOD

Trong trường hợp chiếc IPod bị ướt, Apple khuyến cáo người dùng đừng cố nhấn các nút trên máy vì như thế có thể làm chất lỏng thấm sâu vào bên trong. Thường người ta tắt máy khoảng 24 giờ, sạc lại pin và sử dụng lại. Tuy nhiên, bằng cách mở nắp máy ra bạn có thể nhanh chóng làm khô các chất lỏng dính bên trong và máy sẽ an toàn hơn.
Biện pháp đơn giản nhất là sử dụng một vật mỏng để tách mặt đáy kim loại và phần khung nhựa plastic bên trên. Tuy nhiên bạn phải cẩn thận để không làm hỏng các đầu nối bên trong.

Các bước tiếp theo để hoàn tất quá trình:

Hình 12

1. Kết nối bộ chuyển đổi nguồn AC với thiết bị và đừng kết nối thiết bị với máy tính.

2. Bật máy Zen, trên màn hình sẽ hiển thị menu "rescure mode". Nếu không thấy gì, bạn hãy nhấn và giữ nút Play/Pause và khởi động lại máy.

3. Chọn tùy chọn Format All, quá trình sẽ kéo dài khoảng vài giây nhưng không phải là định dạng lại ổ đĩa mới mà là tải lại firmware cho thiết bị.

4. Tiếp đến, hãy kết nối Zen với máy tính. Nếu bạn đã cài sẵn chương trình Nomad Zen, thiết bị sẽ được tự động nhận dạng và hộp thoại "ZenUniversalUpgrade" sẽ xuất hiện. Nếu không, bạn cần tháo thiết bị ra và cài lại phần mềm trên máy tính.

5. Chọn Yes để tiến hành cập nhật "firmware", sau vài giây bạn sẽ thấy xuất hiện hộp thoại "JukeBox Information" hiển thị thông tin phiên bản firmware và dung lượng ổ đĩa mới.

Hình 13

6. Tải nhạc vào thiết bị và sử dụng thiết bị như bình thường.

Anh Khoa
PC World Mỹ 3/2005

Bí quyết phần cứng

Thực hiện: Hồng Anh

Bạn có ý định đưa các thiết bị đang sử dụng vào "viện dưỡng lão"? Đừng vội. Bài viết này sẽ giới thiệu hơn 50 thủ thuật nâng cấp và giải pháp tiết kiệm hiệu quả giúp bạn khai thác triệt để máy tính, máy in, máy ảnh số và các thiết bị khác.

MÁY TÍNH ĐỂ BÀN

Bổ sung bộ nhớ

Microsoft cho biết Windows XP đòi hỏi 64MB bộ nhớ RAM nếu bạn chạy các ứng dụng đơn giản, chẳng hạn Notepad. Để thực thi các ứng dụng lớn, Microsoft khuyến cáo RAM cần đạt 128MB nhưng thực tế cho thấy hệ thống sẽ "ngã gục" nếu không có tối thiểu 256MB RAM. Đa phần các máy tính được sản xuất trong vòng 2 năm trở lại đây đều được trang bị RAM 512MB (hệ điều hành Microsoft Windows Vista Premium đòi hỏi bộ nhớ tối thiểu ở mức này) nhưng xem ra con số 1GB sẽ giúp máy tính của bạn vận hành "trơn tru" hơn. Để xem hướng dẫn về cách bổ sung RAM, tham khảo find.pcworld.com/55230.

Hình 1: Mở rộng bộ nhớ bằng cách gắn thêm đầu đọc thẻ nhớ.

Ngoài ra, để tiết kiệm chi phí trong việc nâng cấp RAM, bạn cần hỏi xem cửa hàng bán linh kiện có thực hiện việc "đổi cũ lấy mới" không? Một vài cửa hàng nhận mua lại RAM cũ hoặc giảm giá RAM mới khi đổi RAM cũ.

Gắn thêm đầu đọc thẻ nhớ

Việc lấy dữ liệu từ thẻ nhớ sẽ dễ dàng hơn mà bạn không cần phải kết nối máy ảnh số hay thiết bị khác với máy tính bằng cáp USB. Hãy lấp khoảng trống của khoang gắn ổ đĩa 5,25" hay 3,5" bằng một đầu đọc thẻ nhớ gắn trong, chẳng hạn như loại CompUSA Removeable 9-in-1 Flash Media Reader/Writer (find.pcworld.com/55367, Hình 1), giá 25 USD. Nếu tất cả khoang gắn ổ đĩa đều được sử dụng (và bạn không thích đặt thêm một thiết bị gắn ngoài lên bàn làm việc), hãy chuyển đổi (hay bỏ hẳn) ổ đọc đĩa mềm. Còn nếu không ngại sự vướng víu, bạn có thể trang bị một đầu đọc thẻ nhớ gắn ngoài kết nối với máy tính qua cổng USB (hầu hết thiết bị loại này hiện có trên thị trường đều hỗ trợ mọi loại thẻ nhớ thông dụng).

Một số nhà sản xuất còn bổ sung một cổng USB 2.0 hay cổng FireWire vào đầu đọc thẻ nhớ để người dùng có thể dễ dàng truy xuất từ phía trước. Không những thế, vài loại đầu đọc thẻ nhớ đắt tiền (có thể trên 100 USD) được trang bị thêm cổng SATA, jack cắm loa và micro, hay thậm chí màn hình LCD bé xíu hiển thị nhiệt độ của CPU.

Mở rộng với SATA

Nếu đầu đọc thẻ nhớ vừa trang bị không đi kèm cổng kết nối với đĩa cứng SATA gắn ngoài, bạn hãy bổ sung một card cung cấp vài kết nối SATA gắn ngoài. Ví dụ, bộ chuyển đổi 2-Port eSATA PCI của hãng Addonics (find.pcworld.com/55227), giá 29 USD, có thể được sử dụng để cấp nguồn cho bất kỳ đĩa cứng SATA chuẩn 3,5" nào. Nếu muốn chuyển đổi một đĩa cứng gắn trong thành dạng gắn ngoài, bạn cần mua thêm hộp chuyển đổi (hay còn gọi là HDD Box) để nối đĩa cứng IDE/SATA với máy tính thông qua cổng USB 2.0. Bạn có thể dễ dàng tìm mua thiết bị này tại các cửa hàng tin học với giá trong khoảng 10 - 30 USD.

Sao lưu gắn ngoài

Đĩa cứng gắn ngoài thường đắt tiền hơn loại đĩa cứng gắn trong có cùng dung lượng, nhưng bù lại chúng đem đến sự thuận tiện để sao lưu dữ liệu. Với một đĩa cứng gắn ngoài, bạn có thể sử dụng tiện ích Backup và Task Scheduler của Windows XP để tự động thực hiện công việc sao lưu (xem thêm hướng dẫn tại find.pcworld.com/55228). Một đĩa cứng gắn ngoài cũng giúp thuận tiện hơn trong việc truyền nhận tập tin dung lượng lớn giữa các máy tính, nếu bạn thiết lập thiết bị này làm ổ đĩa chia sẻ trên mạng (hướng dẫn chi tiết tại find.pcworld.com/55326). Hoặc bạn có thể trang bị một đĩa cứng mạng (NAS) để phục vụ cho nhu cầu sao lưu tự do của tất cả các máy tính. Để khôi phục dữ liệu, bạn chỉ cần đơn giản kết nối trực tiếp đến đĩa cứng này và tải các tập tin cần thiết về máy tính.

Nâng cấp ổ ghi DVD

Nếu máy tính bạn đang sử dụng chỉ được trang bị ổ ghi CD, hãy nghĩ đến việc bổ sung một ổ ghi DVD. Các thế hệ ổ ghi DVD mới nhất đều hỗ trợ các định dạng đĩa DVD thông dụng như DVD+R/RW và DVD-R/RW, kể cả đĩa một lớp hay hai lớp (8,5GB). Vài model ổ ghi còn có khả năng hỗ trợ định dạng đĩa ít thông dụng là DVD-RAM. Do các ổ ghi này cũng có khả năng ghi đĩa CD nên việc bổ sung một ổ quang thứ 2 vào máy tính sẽ giúp bạn đơn giản hóa công việc sao chép. Hiện nay, giá ổ ghi DVD đã giảm đáng kể, có vài model được bán dưới 50 USD.

Còn nếu "rủng rỉnh" tiền bạc và cần dung lượng lưu trữ nhiều hơn thì tốt nhất là bạn nên trang bị ổ ghi đĩa DVD Blu-ray, ổ ghi HD-DVD hiện vẫn chưa có mặt trên thị trường.

Ép xung hệ thống

Khi các hãng sản xuất CPU thiết lập tốc độ cho sản phẩm của mình, họ chọn điểm

giao giữa độ tin cậy và hiệu suất hoạt động. Tuy nhiên, bạn vẫn có thể buộc CPU làm việc "sung" hơn chút ít bằng cách thực hiện ép xung (overclock).

Hình 2: Bộ thu phát sóng Bluetooth gắn ngoài mở rộng khả năng kết nối cho hệ thống.

Vài card đồ họa cũng có thể được ép xung (tham khảo bài "Bí quyết tinh chỉnh hệ thống", ID: A0503_78). Bạn có thể cải thiện hiệu suất hoạt động của hệ thống bằng cách thay đổi các cài đặt về tốc độ xung nhịp và mức điện áp trong chương trình cài đặt cấu hình của máy tính hoặc điều chỉnh trực tiếp trên bo mạch chủ. Hầu hết dân ép xung chuyên nghiệp thường bắt đầu bằng cách tăng từ từ tốc độ hay mức điện áp trong BIOS, và giảm xuống ngay khi nhận thấy hiện tượng hệ thống vận hành không ổn định hoặc các dấu hiệu bất ổn khác.

Để có thêm thông tin về vấn đề ép xung, bạn có thể tham khảo các website như Overclokers.com, Extreme Overcloking (www.extremeovercloking.com) và Overclock.net. Hãy nhớ đọc kỹ mục hướng dẫn cách làm mát (giải nhiệt) vì nhiệt độ trên các chip được ép xung sẽ nóng lên rất nhiều so với bình thường. Tuy nhiên, nếu mua máy tính nguyên bộ từ Dell, Gateway, HP hay của những hãng tên tuổi khác, bạn không thể thực hiện điều này do họ thường "khóa chết" tốc độ của CPU để hạn chế hiện tượng cháy chip.

Thay mới CPU

Nếu việc ép xung vẫn chưa cung cấp được sự cải thiện tốc độ mà bạn mong muốn thì câu trả lời là cần thay CPU mới. Hãy đọc tài liệu hướng dẫn đi kèm bo mạch chủ (hay tham khảo trên website của hãng sản xuất) để biết được tốc độ CPU mà bo mạch chủ này hỗ trợ. Bạn nên xem hướng dẫn thay CPU tại find.pcworld.com/55235.

Làm sạch để tăng tốc

Một máy tính không thể đạt đến "đỉnh cao" phong độ nếu như nhiệt độ bên trong thùng máy quá nóng, vì thế hãy thường xuyên làm vệ sinh các lỗ thông gió và bộ

phận tản nhiệt. Trước hết, hãy hút bụi (sợi vải, tóc, giấy...) đang che kín các lỗ thông gió phía trước và sau thùng máy. Sau đó, mở thùng máy và cẩn thận thổi sạch các lỗ thông gió, quạt làm mát, bộ phận tản nhiệt bằng 1 bình xịt không khí nén (thường được bán ở các cửa hàng với giá khoảng 7 USD). Các khe, rãnh nhỏ của bộ phận tản nhiệt thường là nơi "hấp dẫn" bụi và các thành phần đầy bụi này có thể dẫn đến tình trạng treo máy, đột ngột tắt máy mà không rõ nguyên nhân hoặc những trục trặc khó hiểu khác. Ngoài ra, bạn cũng cần vệ sinh card đồ họa.

Bên trong thùng máy, bạn nên sắp xếp cáp nối gọn gàng, tốt nhất là bố trí chúng dọc theo cạnh của thùng máy để tối ưu sự đối lưu không khí. Hãy đảm bảo các lỗ thông gió không bị che chắn hay quá sát tường hay vách ngăn.

Tăng chất lượng âm thanh

Trừ khi đang sở hữu một dàn máy giải trí gia đình (home theatre) với hệ thống âm thanh 5.1 kênh hay một máy tính chơi game loại xịn, thì nhiều khả năng là bạn đang thưởng thức âm nhạc trên máy tính thông qua một card âm thanh bình thường (hay chip âm thanh tích hợp trên bo mạch chủ) và 1 cặp loa không có khả năng giả lập các kênh riêng biệt. Để tăng công suất cho dàn âm thanh của máy tính, bạn hãy gắn thêm một bộ khuyếch đại ở ngõ ra tín hiệu âm thanh của card âm thanh.

Mở rộng Bluetooth

Bluetooth là công nghệ tuyệt vời để kết nối tai nghe không dây và truyền nhận dữ liệu. Tuy nhiên, trong khi nhiều loại điện thoại di động và thiết bị cầm tay được tích hợp khả năng kết nối Bluetooth, hầu hết máy tính để bàn và nhiều model máy tính xách tay lại thiếu tính năng này. Giải pháp được đề ra là gắn thêm một bộ thu phát sóng Bluetooth (Bluetooth dongle) kết nối với máy tính qua cổng USB khi cần thiết (Hình 2). Tại Việt Nam, bạn có thể mua thiết bị này tại các cửa hàng tin học với giá dao động trong khoảng 25 - 50 USD. Ngoài ra, bạn có thể ghé qua địa chỉ find.pcworld.com/55536 để biết thêm thông tin về công nghệ Wibree của Nokia, được cho rằng có khả năng cải thiện khả năng kết nối Bluetooth.

MÁY TÍNH XÁCH TAY

Thưởng thức âm nhạc và thực hiện cuộc gọi

Sử dụng máy tính xách tay để nghe nhạc và xem phim ở những nơi công cộng có thể đem đến cho bạn sự vướng víu do dây cáp của tai nghe. Và khi điện thoại di động đổ chuông, bạn phải gỡ tai nghe khỏi đầu để trả lời cuộc gọi. Khi ấy, bạn cần sử dụng một headset (tai nghe kèm micro) không dây hai chức năng, có thể khai thác tính năng "đa kết nối" (multiple-connection) của sóng Bluetooth. Ví dụ, Jabra BT620s (find.pcworld.com/55245), 83 USD, kết hợp một micro vào tai nghe stereo, vì thế bạn chỉ cần ấn một nút để chuyển đổi giữa nghe nhạc đang phát trên

máy tính xách tay hay trả lời cuộc gọi từ điện thoại di động có tính năng Bluetooth của mình. Với tai nghe dạng này, khi có một cuộc gọi đến, nhạc sẽ tự động được tạm ngưng, người dùng ấn vào nút ở bên hông tai nghe để chấp nhận hay từ chối cuộc gọi; khi trả lời điện thoại xong, nhạc sẽ được phát trở lại. Thông thường, pin sạc đi kèm trong tai nghe loại này cho phép đàm thoại liên tục 14 giờ cho mỗi lần sạc.

In không cần máy in

Máy tính xách tay giúp người dùng tự do làm việc bên ngoài văn phòng nhưng điều này cũng đồng nghĩa với việc bạn sẽ không dễ dàng thực hiện các tác vụ in ấn. Trong tình huống này, bạn cần trang bị một chiếc máy in xách tay hoặc sử dụng dịch vụ in ấn của khách sạn để in tài liệu được lưu trong bút USB, thẻ nhớ hay đĩa cứng di động.

Hình 3: Bạn vẫn có thể sử dụng cổng USB ngay khi tắt máy tính với bộ đế Targus.

Hiện nay, tại Mỹ đã xuất hiện vài dịch vụ trực tuyến giúp giải phóng sự vất vả này. Ví dụ, PrinterOn (www.printeron.net) hướng dẫn bạn đến một máy in mạng gần đó và cho phép bạn in các tập tin của mình ở 100 định dạng khác nhau, bao gồm tập tin Office, PDF và JPEG. Dịch vụ này liên kết với nhiều chuỗi khách sạn lớn như Doubletree, Embassy Suites và Hilton, cho phép khách hàng gửi lệnh in (miễn phí) đến Business Center của khách sạn nơi họ đang cư trú.

Ngoài ra, phần mềm miễn phí FedEx Kinho (www.fedexkinkis.com/fpfk) cho phép bạn gửi lệnh in đến một máy in ảo (virtual printer) trên máy tính của mình, rồi chuyển lệnh in này đến một địa điểm thuộc hệ thống FedEx Kinko mà bạn chọn hay gửi bản in trực tiếp đến bạn thông qua dịch vụ chuyển phát nhanh FedEx. Bạn có thể xem trước bản in của mình thông qua trình duyệt và trả tiền qua mạng (chi phí phụ thuộc vào kích thước tập tin và loại giấy in mà bạn chọn).

Gắn thêm bộ đế

Máy tính xách tay được thiết kế riêng cho nhu cầu làm việc di động nhưng phần lớn thời gian thiết bị này lại “an cư” trong văn phòng hay gia đình. Một bộ đế (dock hay có người gọi là đế mở rộng) sẽ cung cấp các cổng kết nối cho các thiết

bị ngoại vi như bàn phím, chuột, màn hình, loa và máy in. Bộ đế Targus Universal Notebook Docking Station with Video (find.pcworld.com/55247, Hình 3), giá 120 USD cho phép bạn kết nối tất cả thiết bị thông qua một cổng USB duy nhất trên máy tính xách tay của mình. Hai trong tổng số 4 cổng USB của bộ đế này luôn được cấp nguồn ngay cả khi máy tính tắt hay hoạt động ở chế độ chờ, giúp thuận tiện cho việc sạc pin điện thoại di động, PDA hay chuột không dây.

MÁY IN

Tiết kiệm chi phí

Hầu hết máy in đều cho phép bạn kéo dài thời gian sử dụng một hộp mực bằng cách thiết lập chế độ in draft, tạo ra văn bản ở sắc độ xám nhưng vẫn có thể đọc được. Bạn cũng sẽ tiết kiệm được đáng kể lượng mực in bằng cách tắt chế độ in màu, giá mực đen luôn rẻ hơn mực màu. Ngoài ra, bạn có thể in 2 mặt trên cùng 1 tờ giấy. Nếu máy in có bộ đảo giấy (duplexer), hãy thiết lập chế độ mặc định in trên cả 2 mặt giấy.

Tạo máy in ảo

Không phải tất cả bản in đều được tạo ra giống nhau: có lúc bạn cần chất lượng, có lúc cần tốc độ, có lúc màu sắc... Với mỗi loại bản in, bạn phải thay đổi các cài đặt trong hộp thoại Print Properties của Windows. Tuy có vài máy in cho phép người dùng thiết lập các chế độ sử dụng (profile), nhưng thường thì bạn phải "lục tung" hộp thoại Print Properties để tìm những thông số cần tinh chỉnh. Để đạt được cùng kết quả này nhưng dễ dàng hơn, hãy tạo ra các profile máy in riêng biệt cho mỗi nhu cầu in ấn cụ thể. Mở cửa sổ Printer and Fax trong Control Panel, chọn Add a printer và thực hiện theo các hướng dẫn của Add Printer Wizard. Kế đến, chọn máy in và nhấn Set printer properties trong khung cửa sổ bên phải (hay nhấn phải chuột lên máy in đó và chọn Properties). Đặt tên cho máy in (chẳng hạn như Injet Draft hay Laser Letterhead Paper) và nhấn Printing Preferences.Advanced. Sau đó, thiết lập các thông số theo ý riêng của bạn (tùy chọn trên từng máy in thường khác nhau nhưng hầu hết đều cho phép bạn chỉnh độ phân giải tương ứng với bản in chất lượng cao hay thấp). Trong lần in kế tiếp, chọn biểu tượng tương ứng với máy in cần sử dụng từ trình đơn thả xuống trong hộp thoại Print (Hình 4).

Chọn đúng loại giấy

Hình 4: Chọn máy in được thiết lập sẵn cho từng nhu cầu in ấn cụ thể.

Nếu máy in của bạn có nhiều khay nạp giấy, hãy để một khay chứa loại giấy in thông thường, thiết lập profile in mặc định sử dụng khay giấy này và đặt loại giấy chất lượng cao vào những khay còn lại. Khi bạn cần in với chất lượng cao, chọn đúng khay giấy cần thiết trong hộp thoại Print Properties. Để có được văn bản sắc nét khi sử dụng máy in phun, hãy sử dụng loại giấy được sản xuất đặc biệt cho loại máy này - giấy in dành cho máy in laser và máy photocopy hút mực hết như một tấm bọt biển vì thế văn bản sẽ trông mờ hơn. Để màu sắc được thể hiện chính xác và bản in tồn tại lâu dài, bạn nên sử dụng loại giấy được hãng sản xuất máy in khuyến cáo sử dụng - thường là giấy do chính họ cung cấp. Vài loại máy in, ví dụ như vài model gần đây của Canon, thậm chí không cho phép bạn chọn chế độ in chất lượng cao nếu máy nhận ra bạn không sử dụng đúng loại giấy đặc biệt của hãng này.

Mua giấy và mực in theo gói

Các thử nghiệm trước đây của PC World Mỹ cho thấy, chi phí in một ảnh 4x6 inch dao động trong khoảng 0,23 – 0,97 USD. Nhiều hãng sản xuất máy in hiện có cung cấp nhiều lựa chọn giấy và mực in. Ví dụ, gói vật tư in dành cho máy Photosmart 385 và 375 bao gồm 1 catridge mực (loại 3 màu) và 50 tờ giấy in ảnh với giá 20 USD (rẻ hơn mức giá 25 USD của 1 catridge mực khi mua lẻ).

Chọn catridge theo nhu cầu

Mua mực in dành cho máy in laser với số lượng lớn (hay nói chính xác là loại catridge dung tích lớn) cũng sẽ giúp bạn tiết kiệm được đáng kể chi phí. Brother là một điển hình trong số các hãng sản xuất máy in laser cung cấp catridge mực in với nhiều loại dung tích khác nhau. Loại catridge dùng để in 3.500 tờ giấy dùng cho máy in Brother HL-5250DN được bán ở giá 74 USD. Bạn có thể mua loại có dung tích gấp đôi với giá 100 USD.

Kết nối trực tiếp

Hầu hết các máy in ảnh hiện nay đều cung cấp 1 cổng ở phía trước để in ảnh trực tiếp từ máy ảnh số mà không cần sử dụng đến máy tính. Các máy ảnh số sử dụng

chuẩn PictBridge để liên kết với máy in thông qua cổng USB. Nhiều máy in còn cho phép bạn kết nối với những thiết bị USB khác, thường là đĩa cứng dạng flash hay bút nhớ USB.

Các máy in thường trang bị một màn hình LCD màu, cho phép duyệt và in ảnh được lưu trên đĩa cứng flash. Ví dụ, máy Epson PictureMate Deluxe Viewer Edition cho phép bạn truyền tập tin ảnh từ thẻ nhớ của máy ảnh số sang bút USB, thuận tiện để lưu trữ ảnh khi không có máy tính. Vài máy in HP, ví dụ máy Photosmart A616, có thể in ảnh được lưu trên máy nghe nhạc iPod. Tuy nhiên, bạn đừng mong đợi sẽ đạt được tốc độ truyền nhận như khi sử dụng cổng USB 2.0 trên máy tính: hầu hết cổng PictBridge có tốc độ chậm hơn USB 1.1.

Tất cả máy tính mới hiện nay đều trang bị cổng USB 2.0 nhưng thiết bị kết nối có thể chạy ở chế độ Hi-Speed (có thể đạt đến 480Mbps) hay Full-Speed (đạt tốc độ giới hạn của USB 1.1 là 12Mbps). Nếu thẻ nhớ dung lượng 1GB trong máy ảnh chứa đầy ảnh thì bạn sẽ nhận ra sự khác biệt lớn về thời gian cần để tải toàn bộ số ảnh khi kết nối với máy in dùng chuẩn PictBridge thay vì kết nối trực tiếp đến máy tính. Dĩ nhiên, hầu hết máy ảnh số vẫn sử dụng chuẩn USB 2.0 ở tốc độ chậm hơn.

Hình 5: Thay đổi thiết lập trang in trong trình duyệt IE để in được đầy đủ trang web.

Khả năng in trực tiếp thật sự thuận tiện và hiện nay bạn cũng có thể tận hưởng điều này với điện thoại di động cũng như các thiết bị cầm tay khác. Hãng Canon cung cấp vài loại máy in với giao tiếp hồng ngoại IrDA, cho phép bạn gửi ảnh trực tiếp đến máy in. Không những thế, Canon, Epson và HP còn cung cấp bộ chuyển đổi Bluetooth có thể cắm vào cổng in trực tiếp trên máy in để bạn có thể in ảnh không dây từ thiết bị Bluetooth của mình. Tại Mỹ, giá thiết bị này dao động trong khoảng 39 – 80 USD.

In đầy đủ trang web

Nếu tiện ích Internet Explorer “cắt đi” phần bên phải của trang web mà bạn cần in,

hãy kiểm tra trên website của hãng sản xuất máy in để tải về phần mềm miễn phí cho phép in đầy đủ trang web. Ví dụ, các tiện ích như EasyWebPrint của Canon, Web-To-Page Utility của Epson và Toolbar của Lexmark cung cấp tính năng "in thay thế" (alternative-print), có khả năng "nhét" gọn trang web vào đúng khổ giấy in thông thường. Một số tiện ích đòi hỏi bạn phải sử dụng đúng máy in của hãng này.

Một giải pháp đơn giản hơn là thay đổi các thông số trang in của trình duyệt IE: nhấn File.Page Setup, định giá trị biên trái và biên phải gần mức 0,25" (Hình 5). Khi ấy, bản in trang web của bạn sẽ rộng hơn so với những gì bạn nhìn thấy trên màn hình.

Tận dụng quà tặng

Các cửa hàng tin học thường bán nhiều sản phẩm thiết kế dành cho việc in ấn, chẳng hạn thiệp mời, poster và những tài liệu phục vụ cho công việc kinh doanh khác. Nhưng trước khi bỏ ra 20 – 100 USD mua chúng, hãy kiểm tra xem bạn được miễn phí những gì với chiếc máy in của mình. Nhiều hãng sản xuất máy in cung cấp các công cụ và mẫu tạo sẵn (template) để khuyến khích bạn sử dụng máy in nhiều hơn (và qua đó sẽ mua nhiều giấy và mực in hơn).

Máy in ảnh của Epson và HP thường đi kèm công cụ tạo thiệp và bộ sưu tập ảnh. Tiện ích Creative Park của Canon (find.pcworld.com/55265) và CreativeZone của Epson (find.pcworld.com/55266) cung cấp các template và hướng dẫn cho nhiều nhu cầu in ấn khác nhau. Trong khi đó, dịch vụ Activity Center của HP (find.pcworld.com/552667) và Project Center của Lexmark (find.pcworld.com/55268) hướng dẫn bạn từng bước trong việc thiết kế thiệp, thư mời và nhiều thứ khác; ở hai tiện ích này, bạn có thể chép hình ảnh của mình lên website, sau đó sử dụng các công cụ để chỉnh sửa chúng. Cả website của HP và Lexmark đều cung cấp các bản in cuối cùng ở dạng tập tin PDF, vì thế bạn có thể in chúng với bất kỳ máy in nào. Thậm chí website của HP còn giúp bạn thiết kế các tài liệu phức tạp như bảng phân công, thông tin liên lạc của các thành viên, kế hoạch thi đấu, thư mời tài trợ đồng phục, áo T-shirt... cho một đội bóng.

ĐỒ HỌA

Tăng xung nhịp

Game thủ và người dùng máy tính đam mê tốc độ thường "vắt kiệt" sức mạnh hệ thống bằng cách tăng tần số xung nhịp của CPU vượt qua thiết lập mặc định của hãng sản xuất. Bạn cũng có thể thực hiện điều này với card đồ họa của mình.

Hai hãng sản xuất card đồ họa hàng đầu là ATI và nVidia đều cung cấp các tiện ích giúp tăng tốc bộ xử lý đồ họa (GPU). Tiện ích Overdrive (ATI) và Coolbits (nVidia) đi kèm theo trình điều khiển thiết bị của card đồ họa (có thể bạn cần phải "bẻ khoá" tiện ích Coolbits để tiện ích này hiển thị trong chương trình cấu hình Forceware của nVidia (để thực hiện điều này, tham khảo bài "Bí quyết tinh chỉnh hệ thống", ID: A0503_78).

Cần lưu ý, hiện tượng nhiệt độ tăng quá cao khi thực hiện ép xung có thể gây hỏng các mạch điện vốn rất mỏng manh của card đồ họa. Tiện ích Overdrive giám sát nhiệt độ của card đồ họa để ngăn ngừa hiện tượng quá nóng và việc sử dụng tiện ích này không làm mất hiệu lực bảo hành thiết bị. Tuy nhiên, việc ép xung card đồ họa nVidia bằng tiện ích Coolbits hay tiện ích của một hãng thứ 3 khác, ví dụ RivaTuner (find.pcworld.com/55274), miễn phí, sẽ vi phạm các quy định về bảo hành.

Tùy chỉnh BIOS

Nếu máy tính của bạn sử dụng card đồ họa chuẩn AGP thì những thông số trong BIOS sẽ cung cấp vài khả năng điều chỉnh cấp thấp để cải thiện hiệu quả đồ họa (việc thay đổi các thông số trong BIOS khá rủi ro, do đó bạn nên tham khảo cách thực hiện được trình bày trong bài "Tinh chỉnh BIOS của PC", ID: A0302_77).

AGP Mode: Chỉnh mục này đến giá trị lớn nhất mà card đồ họa của bạn hỗ trợ - 2X, 4X hay 8X (tìm thông số này trong tài liệu đi kèm hay trên website của hãng sản xuất). Việc điều chỉnh này có thể cải thiện hiệu quả hiển thị đồ họa của hệ thống.

AGP Fast Write: Kích hoạt tính năng này thường giúp tăng tốc card đồ họa nhưng không phải là thực hiện ép xung.

AGP Aperture Size: Cài đặt này sẽ điều khiển luồng dữ liệu đồ họa vào/ra trên RAM hệ thống bất cứ khi nào bộ nhớ trên card đồ họa của bạn cạn kiệt. Đối với các card đồ họa có bộ nhớ dưới 32MB, hãy tăng giá trị này đến 128MB hay cao hơn để cải thiện hiệu quả của tính năng đổ bóng khi chơi game.

Tinh chỉnh màn hình

Cách thức nhanh nhất và đơn giản nhất để sử dụng hiệu quả nhất màn hình CRT

hay LCD là điều chỉnh độ sáng, độ tương phản và những thông số khác; vài điều chỉnh đơn giản có thể tạo ra sự khác biệt lớn cho những gì được hiển thị trên màn hình. Để biết các thủ thuật và tiện ích điều chỉnh màn hình CRT và LCD, tham khảo tại find.pcworld.com/55269 và find.pcworld.com/55270.

Giảm chói và chống nhìn trộm

Màn hình hiển thị quá sáng có thể gây ảnh hưởng không tốt đến sự điều tiết đôi mắt của bạn, đặc biệt khi phải làm việc với máy tính trong thời gian dài. Hãy trang bị một tấm kiếng chống chói hay màn lọc chuyên dụng của hãng 3M (find.pcworld.com/55276) hay Fellowes (find.pcworld.com/55277).

Ngoài ra, đôi lúc bạn không muốn người ngồi cạnh bên hay ai đó vô tình đi ngang qua bàn làm việc của mình có thể đọc được nội dung bản hợp đồng hay thư điện tử mà bạn đang soạn thảo, phải làm sao đây? Giải pháp tối ưu là sử dụng một tấm chắn "bảo mật", không những giúp giảm chói mà còn hạn chế góc nhìn từ ngoài vào màn hình. Tại Việt Nam, bạn có thể tìm mua tấm chắn dạng này của hãng 3M tại các cửa hàng tin học, tuy nhiên giá khá cao (40 – 100 USD tùy kích thước).

Hiển thị trung thực màu sắc

Màu sắc được hiển thị khác nhau ở mỗi màn hình. Nếu bạn muốn ảnh từ máy chụp hình kỹ thuật số và hình vẽ đồ họa trông thật hơn, bạn cần cân chỉnh màu sắc cho màn hình của mình. Phần mềm cân chỉnh màu có thể thực hiện điều này nhưng để đạt màu sắc chính xác, bạn cần đến thiết bị được thiết kế đặc biệt để lấy mẫu và phân tích các thông số màu sắc của màn hình.

Thiết bị Spyder2express của Colorvison (find.pcworld.com/55279, Hình 6), giá 70 USD, sử dụng một bộ quét (có hình dáng của đầu gậy đánh hockey, kết nối với máy tính qua cổng USB) được treo phía trước màn hình để lấy mẫu ánh sáng phát ra và tự động cân chỉnh màu sắc. Phần mềm nâng cấp giá 200 USD cũng của hãng này sẽ bổ sung tiện ích PrintFix, giúp đồng nhất màu sắc của bản in và hình ảnh hiển thị trên màn hình.

Đánh thức điểm ảnh

Hình 6: Sử dụng thiết bị cân chỉnh để màu sắc trông thật và chính xác hơn.

Thỉnh thoảng, các điểm ảnh (pixel) trên màn hình LCD trở nên "bất động", bạn cần đánh thức chúng: hãy thử sử dụng đầu ngón tay được quấn một miếng vải mềm và sạch để "mát-xa" điểm ảnh này một cách nhẹ nhàng từ 10 - 15 giây.

Nếu vẫn không khắc phục tình trạng này, bạn tải về tập tin video miễn phí Stuck Pixel (find.pcworld.com/55280) và phát đoạn phim này liên tục trong nửa giờ đồng hồ. Để phát đoạn video được thiết kế dành riêng cho máy chơi game cầm tay PSP, bạn cần có tiện ích QuickTime (www.quicktime.com) hay bất kỳ tiện ích đa phương tiện nào hỗ trợ tập tin MPEG-4. Lưu ý, tiện ích này chỉ làm việc với các điểm ảnh bị "bất động" chứ không phải các điểm ảnh "chết" (thường là màu đen).

Nâng cấp trình điều khiển

Bạn không hài lòng với hiệu quả đồ họa mà card đồ họa đang sử dụng thể hiện, hãy kiểm tra xem bạn đã cài đặt đúng phiên bản mới nhất của trình điều khiển (driver) cho thiết bị này chưa (việc thay đổi trình driver của card đồ họa thường gây rắc rối, do vậy nếu không có gì trục trặc, tốt hơn hết bạn đừng cố sửa chúng). Trong cửa sổ thuộc tính của driver đồ họa, bạn cần biết qua các tính năng và thông số được liệt kê. Tiện ích Catalyst của ATI và Forceware của nVidia cho phép bạn điều chỉnh nhiều thông số về hình ảnh 3D, màu sắc và những cài đặt nâng cao khác. Bạn cần tham khảo hướng dẫn sử dụng tiện ích Catalyst và Forceware tại trang TweakGuides.com.

Ví dụ, việc thay đổi các thông số gamma của card đồ họa có thể tăng đáng kể độ sáng trong game. Nhiều người dùng chuyên nghiệp còn sử dụng tiện ích PowerStrip (find.pcworld.com/55281), giá 30 USD, cung cấp vô số tính năng tinh chỉnh nâng cao dành cho card đồ họa, kể cả nhiều tinh chỉnh không có trong tiện ích của hãng sản xuất. Ví dụ, người dùng có thể tùy biến độ phân giải để xem phim trên HDTV hay màn hình LCD dạng widescreen, chọn tần số làm tươi phù hợp để bỏ qua giới hạn 60Hz thường gây nên hiện tượng "rung rung" màn hình (Hình 7).

Hình 7: Tiện ích PowerStrip cho phép bạn tinh chỉnh độ phân giải và các thông số của card đồ họa.

MẠNG KHÔNG DÂY

Trả tự do cho thiết bị ngoại vi

Bất kỳ thiết bị ngoại vi nào có một cổng mạng (ethernet) đều có thể được "cởi trói" thông qua một cầu nối WiFi-Ethernet đơn giản, cho phép bạn di chuyển thiết bị này vòng quanh căn hộ hay đặt thiết bị ngoại vi chia sẻ này ở giữa văn phòng. Các hãng như D-Link, Netgear, Belkin đều có cung cấp loại cầu nối không dây này ở mức giá khoảng 50 - 100 USD. Chúng được sử dụng chủ yếu trong vai trò bộ chuyển đổi kết nối không dây cho máy chơi game GameCube, PlayStation và Xbox, nhưng cũng có thể làm việc được với các thiết bị có cổng mạng khác như máy in hay đĩa cứng gắn ngoài.

Nếu mạng không dây của bạn được cấu hình ở chế độ cấp địa chỉ IP tự động (DHCP) thì đó là cơ hội tốt để cầu nối không dây này làm việc hiệu quả. Nếu không, bạn sẽ phải kết nối "cầu nối" này với máy tính, rồi gán địa chỉ IP một cách thủ công. Vài máy chơi game hệ console đời cũ cần một bộ chuyển đổi cổng mạng riêng biệt. Tương tự, Xbox 360 có một cổng USB và Microsoft bán rời bộ chuyển đổi kết nối WiFi.

Tìm kiếm dịch vụ lân cận

Ai còn cần đến hệ thống định vị toàu cầu GPS khi đã có Wi-Fi? Dịch vụ miễn phí Loki (www.loki.com) lập bảng đồ các mạng Wi-Fi tại hầu hết các thành phố lớn của nước Mỹ, cho phép bạn sử dụng PDA, smartphone hay máy tính xách tay có

khả năng kết nối Wi-Fi để định ra vị trí (địa lý) mà mình đang đứng. Loki cài đặt như một thanh công cụ trong trình duyệt IE hay Firefox, cho phép bạn tìm kiếm vị trí của các rạp chiếu bóng, nhà hàng, thông tin thời tiết và nhiều thông tin khác. Hai tính năng được yêu thích trong Loki là tính năng hướng dẫn đường đi (Hình 8) và cung cấp các địa điểm hotspot công cộng.

Thật tuyệt, với Loki, chỉ cần ấn một nút nhấn, bạn có thể gửi email hay tin nhắn SMS với nội dung là vị trí của mình cho một người bạn khác. Sau đó, người nhận sẽ nhấn vào một đường link để nhìn thấy một bản đồ và hướng dẫn đường đi đến chỗ của bạn. Một tính năng hấp dẫn khác của Loki là cho phép bạn "đánh dấu vị trí địa lý" để đính kèm tin blog, hình tải lên Flickr và các nội dung trên web khác.

Bảo mật kết nối

Hình 8: Hướng dẫn chỉ đường của dịch vụ Loki.

Thực tế cho thấy, các hotspot công cộng thường không an toàn. Cho dù bạn sử dụng kết nối Wi-Fi miễn phí tại quán cafe, khách sạn hay nơi công cộng nào đó thì mỗi lần đăng nhập, bạn sẽ phải gửi đi ID và mật khẩu qua sóng không dây. Những kẻ xấu có thể thiết lập một trạm phát sóng không dây với mã nhận dạng tương tự như những gì bạn mong đợi nhận được từ một router không dây thực sự (ví dụ "wayport" hay "t-mobile"), rồi sau đó đánh cắp thông tin cá nhân của bạn.

Để ngăn chặn tình trạng này, bạn cần mã hóa dữ liệu, email hoặc sử dụng mạng riêng ảo (VPN). Hiện có khá nhiều doanh nghiệp, tổ chức đang triển khai dịch vụ VPN cho nhân viên có nhu cầu làm việc di động. Người dùng hotspot thông thường có thể sử dụng dịch vụ VPN trả phí, ví dụ Personal VPN của Boingo (find.pcworld.com/55284); miễn phí dùng thử, 30 USD sử dụng chính thức hay WiTopia personalVPN (find.pcworld.com/55286), phí dịch vụ 40 USD/năm; cả 2 đều dễ cài đặt và sử dụng. Ngoài ra, Microsoft đang thử nghiệm dịch vụ Windows Live WiFi Suite mới, trong đó có dịch vụ VPN.

Hãng JiWire (www.jiwire.com) cung cấp tính năng bảo mật Wi-Fi và mã hóa email hiệu quả với phần mềm Hotspot Helper. Phần mềm miễn phí này tự động mã

hóa tất cả luồng dữ liệu vào/ra mạng Internet và bổ sung một tường lửa để ngăn cản sự truy xuất máy tính bất hợp pháp. Hotspot Helper bảo vệ tất cả email mà

không lệ thuộc tiện ích gửi nhận email bạn đang sử dụng. Phần mềm này kết hợp với dịch vụ tìm hotspot theo yêu cầu Hotspot Finder cũng của JiWire và miễn phí sử dụng trong 10 ngày đầu tiên (phí sử dụng 25 USD/năm).

Dùng "chùa" Hotspot

Tuy phí kết nối không dây khoảng 5-10USD cho mỗi lần kết nối nhưng bạn sẽ không tốn xu nào nếu biết tìm những điểm hotsport công cộng miễn phí. Hãy tải về bảng chỉ dẫn hotspot trước khi đi công tác. Những hotspot miễn phí hiện có sẵn tại AnchorFree (www.AnchorFree.com) và JiWire cho cả miễn phí và có phí. AnchorFree còn có bản cho iPod và cả hai công ty này đều cho phép bạn truy cập chỉ dẫn trực tuyến của họ bằng trình duyệt WAP trên điện thoại di động.

MÁY ẢNH SỐ

Chụp ảnh đẹp

Điều kiện tiên quyết để có bức ảnh đẹp là chỉnh đúng thông số chụp. Khi chụp ở định dạng ảnh JPEG, tuy có thể chọn nhiều độ phân giải và mức chất lượng khác nhau nhưng tốt nhất là nên chọn cao nhất. Ngoài việc giá thẻ nhớ hiện nay đã giảm rất nhiều, với ảnh có độ phân giải và mức chất lượng cao nhất bạn sẽ chủ động khi xử lý về kích thước ảnh, giữ được các chi tiết hay phóng to...

Hình 9: Loại trừ nhiễu do ISO cao bằng chế độ tự thiết lập trong Noise Ninja tùy máy ảnh

Nếu muốn tinh chỉnh tối đa ảnh, bạn nên chọn chế độ chụp RAW+JPEG (nếu máy ảnh có hỗ trợ) để có thể chia sẻ ngay ảnh JPEG nhưng vẫn có thể biên tập ảnh RAW ở mức chất lượng cao nhất.

Đừng quên tận dụng tính năng cho phép chỉnh độ nét vì hầu hết máy ảnh số có khuynh hướng cho ảnh hơi "mềm". Nếu tăng vừa phải độ nét bạn còn tiết kiệm

được việc chỉnh ảnh sau khi chụp trên máy tính.

Giảm nhiễu

Nếu chụp trong điều kiện thiếu sáng, có thể bạn cũng biết là nên tăng độ nhạy ISO của máy ảnh để "bắt chết" đối tượng chuyển động. Tuy nhiên, ISO càng cao thì nhiễu cũng càng cao nên đây là thông số ít được chuộng nhất.

Tuy nhiên, để giải quyết tình trạng này bạn có thể dùng những phần mềm giảm nhiễu như Noise Ninja của PictureCode, giá 35USD (bản miễn phí ít tính năng hơn có thể tải ở find.pcworld.com/55289) có khả năng chỉnh ảnh trong và mịn như chụp ở thông số mặc định. Noise Ninja có sẵn những chế độ (profile) giảm nhiễu cho nhiều máy ảnh phổ biến và việc tạo chế độ riêng cho máy ảnh của bạn theo từng mức ISO cũng dễ dàng (Hình 9). Bạn chỉ cần nạp ảnh, chọn chế độ xử lý, loại máy ảnh và tất cả sẽ được thực hiện trong nháy mắt. Với những ảnh phức tạp, tính năng Noise Brush tỏ ra rất hiệu quả khi xử lý riêng từng vùng nhiễu trên ảnh.

Che điểm ảnh hư

Hình 10: Tăng khả năng nhiếp ảnh của bạn bằng ống kính tiêu cự chọn Lensbaby

Bất kỳ thiết bị nào cũng có thể đánh dấu những điểm ảnh chết, kể cả bộ cảm biến trong máy ảnh số (xem "Đánh thức điểm ảnh", trang 111). Những điểm chết này thể hiện càng rõ khi máy ảnh của bạn càng cũ. Trong hầu hết điều kiện chụp, có thể bạn sẽ không để ý đến chúng nhưng trong một số loại ảnh, nhất là chụp với tốc độ chậm để có ảnh pháo hoa, thành phố đêm, vệt đèn xe... thì những điểm chết này có thể lộ rõ. Khi bạn để màn trập mở trong một khoảng thời gian dài, tác động tích tụ của những điểm chết này sẽ "phá" ảnh của bạn bằng những điểm sáng bất thường.

Để che những điểm ảnh xấu, bạn có thể dùng phần mềm như PixelZap của TawbaWare, giá 15USD. Tiện ích này đủ thông minh để "điền" thông tin bị mất của các điểm chết, loại trừ những điểm sáng hay tối bất thường trên ảnh.

Uốn cong ống kính

Bạn đang tìm cách để chụp được những bức ảnh phi thường? Nếu máy của bạn thuộc loại SLR với khả năng thay ống kính, Lensbaby (Hình 10), 150USD (www.Lensbabies.com) có thể là lời giải. Gắn Lensbaby vào Canon 350D, Nikon D50 hay bất kỳ máy SLR nào để mở rộng "ngôn ngữ" nhiếp ảnh của bạn.

Ống kính chọn tiêu cự này là một chiếc ống có thể uốn bằng tay khi chụp. Kết quả? Một phần của ảnh rất nét trong khi những phần còn lại của ảnh bị mờ. Thử nghiệm với Lensbaby mang lại nhiều điều thú vị.

ĐIỆN THOẠI DI ĐỘNG

Duyệt nhanh hơn trên Treo

Nếu kết nối web trên Treo của bạn chậm, đây là cách tăng tốc: dùng chế độ tốc độ cao của trình duyệt để chặn việc tải xuống ĐTDĐ hình ảnh web để nạp trang nhanh hơn. Trình duyệt đưa tùy chọn "don't load images" ở các vị trí khác nhau. Ví dụ, trong Windows Mobile Treo, mở trình đơn View, chọn Options và bỏ chọn Show Pictures (Hình 11). Tuy ảnh không xuất hiện tự động, nhưng bạn vẫn có thể xem nếu chọn khung chứa ảnh của trang web. Nếu chỉ cần sự đơn giản, hãy đăng ký dịch vụ thông tin miễn phí Mdog.com cho trình duyệt ĐTDĐ. Đăng nhập site này để xem các phiên bản tối ưu cho di động như site về tin tức và thông tin dạng New York Times hay dữ liệu phim (imdb.com).

Hình 11: Nạp trang web nhanh hơn trên Treo bằng cách cấm tải hình tự động

Tuỳ biến phím mềm

Bạn có thể thay đổi phím mềm và phím 4 chiều trên nhiều loại ĐTDĐ để phục vụ những tính năng hay dùng nhất. Trong hầu hết ĐTDĐ, bạn truy cập trình đơn chính để thay đổi thông số. Ví dụ, Motorola Razr, nhấn nút Menu, chọn Settings, nhấn Personalize rồi chọn Home Keys. Cuộn đến phím muốn thay đổi – Up, Down, Left Soft Key hay Right Soft Key – rồi chọn ứng dụng mong muốn.

Sao lưu sổ địa chỉ

Hầu hết những hãng lớn cung cấp dịch vụ không dây đều có ứng dụng sao lưu sổ địa chỉ của ĐTDĐ. Tuy nhiên bạn có thể tìm được dịch vụ sao lưu miễn phí trên web có tên là Zyb hỗ trợ nhiều loại điện thoại và có kết nối Net.

Hình 12: Tự động sao lưu sổ địa chỉ của ĐTDĐ miễn phí tại Zyb.com

Bạn chỉ cần tạo một tài khoản tại zyb.com (Hình 12). Một số điện thoại tự động đồng bộ thông tin (contact) với máy chủ bảo mật của Zyb, nhưng với một số điện thoại khác, bạn phải tải bằng tay sổ địa chỉ lên máy chủ. Website cũng cung cấp hướng dẫn từng bước tùy loại điện thoại.

Nếu điện thoại của bạn tương thích tính năng đồng bộ của Zyb, dịch vụ này sẽ gửi thông tin cấu hình tới điện thoại của bạn. Khi chọn tính năng này, hãng sẽ bật cảnh báo màn hình yêu cầu bạn xác nhận số điện thoại đã nhập (đừng nhập sai). Quá trình đồng bộ có thể mất một lúc, tùy tốc độ kết nối và số đầu mối liên lạc trong sổ địa chỉ. Sau đó bạn có thể cập nhật thông tin liên lạc trên site của Zyb và đồng bộ với ĐTDĐ. Nếu điện thoại của bạn không được Zyb hỗ trợ bạn có thể thử trình sao lưu miễn phí BitPim (www. BitPim.com).

Tạo shotcut cho ứng dụng

Ứng dụng và tính năng của ĐTDĐ thường nằm "sâu" trong trình đơn nên khó tìm và mất thời gian. Bạn có thể truy cập nhanh chúng bằng phím tắt tương tự trên PC. Hầu hết ĐTDĐ cách đây 1-2 năm hỗ trợ vài kiểu tạo phím tắt dù chỉ với những phím điều hướng (tùy chọn này thường nằm trong trình đơn thiết lập thông số điện thoại). Một số điện thoại cho phép gán phím tắt cho từng phím số để khởi động nhanh ứng dụng ưa thích hay tính năng thường dùng nhất.

MÁY NGHE NHẠC

Nâng cấp âm thanh

Nếu tai nghe kèm theo máy nghe nhạc không làm bạn hài lòng, hãy chi thêm một ít tiền để mua cặp tai nghe cao cấp hơn để có âm thanh trong hơn, chi tiết hơn và phổ rộng hơn.

Hình 13: Thay tai nghe kèm máy bằng tai nghe cao cấp hơn Bass Freq của V-Moda

Với những người thích âm trầm (bass) với chi phí tối thiểu thì không thể tìm đâu hơn tai nghe Bass Fréq của V-Moda (find.pcworld.com/55291, Hình13). Những chiếc tai nghe 50USD này cho âm thanh tách biệt và như tên gọi âm trầm được tăng cường.

Tai nghe Super.fi 3 Studio 100USD của Ultimate Ears (find.pcworld.com/55292) cho âm thanh trong hơn và chi tiết hơn của V-Moda. Nó còn kèm theo nhiều phụ kiện như hộp đựng bằng kim loại, 5 cỡ vòng đệm cho tai. Nếu yêu cầu âm thanh cao hơn bạn có thể thử Super.fi 5 Pro, 249USD hay Super.fi 5 EB, 200USD (find.pcworld.com/55542).

Tìm giai điệu "tự do"

Dù có những hạn chế của giới công nghiệp âm nhạc, bạn vẫn có thể tải về những bản nhạc có bản quyền mà không phạm luật. Một số site cung cấp những bản nhạc không quản lý bản quyền số để bạn có thể nghe trên bất lỳ thiết bị nào.

Tại eMusic (www.emusic.com), bạn có thể tải về 40 bản nhạc/tháng với phí 10USD nhưng đừng hy vọng tìm được những bản nhạc đang hot hay phổ biến nhất. Site này hợp tác với những nhạc sỹ độc lập nhưng bạn vẫn có thể tìm được những album từ các nghệ sỹ tên tuổi như Barenaked Ladies, Santana và Van Morrison. Chọn lựa khác là Audio Lunchbox (AudioLunchbox.com) có phần nào nhiều chọn lựa hơn eMusic với cùng mức phí.

Internet Archive (www.archive.org) có nhạc không tính phí của những nghệ sỹ đồng ý phân phối phi thương mại giai điệu của họ (kể cả những ban nhạc như Grateful Dead và Blues Traveler). Để tải về, bạn nhấn phải chuột vào liên kết của bản nhạc và chọn Save Target As.

Người dùng iPod cũng không cần phải vào iTunes. Rhapsody (www.Rhapsody.com) cho phép bạn tự do chuyển những bản nhạc đã mua vào một số thiết bị, kể cả những máy chơi nhạc phổ biến của Apple. Dùng phần mềm Rhapsody để mua nhạc, kết nối với bất kỳ thiết bị được hỗ trợ (www.Rhapsody.com/devices) và kéo bản nhạc vào cửa sổ Transfer (Hình 14).

Hình 14: Kết nối iPod hay bất kỳ máy nghe nhạc nào với dịch vụ tải nhạc của Rhapsody

Hỗ trợ danh mục nhạc

Nếu không muốn tạo danh mục nhạc (playlist) riêng, ứng dụng miễn phí MusicIP Mixer (www.musicip.com/listener) giúp phân tích thư viện và tạo playlist cho bạn bằng cách chọn những bản nhạc có cùng đặc tính nhạc. Nhập nhạc (nhấn Library. Add Songs hay chọn Sync With iTunes), rồi chọn Library.Start Analysis. Khi chương trình hoàn tất, chọn bản nhạc muốn đưa vào playlist và nhấn Mix.

Để tinh chỉnh chương trình tạo playlist, chọn File.Preferences và chỉnh các thông số Mix. Nếu bạn không thích bản nhạc nào thì chỉ cần nhấn phải chuột lên nó và chọn Replace This Song. Một khi đã hài lòng, hãy chuyển sang iTunes hay Windows Media Player bằng cách nhấn vào nút Send To.

Mang YouTube theo

Hàng ngàn đoạn phim giải trí, miễn phí được đưa lên dịch vụ YouTube phổ biến của Google (www.youtube.com). Tinh chỉnh chúng để xem trên máy xem video di động chỉ mất vài phút.

Đầu tiên, tải video vào đĩa cứng máy tính. Để dễ dàng, bạn có thể dùng YouTubeX (www.youtubex.com): gán URL củavideo vào trang YouTubeX và nhấn nút

download để định vị video. Khi nó xuất hiện, nhấn liên kết download ngay bên dưới và chọn thư mục để lưu. Bạn cần bổ sung phần mở rộng .flv vào tên tập tin (Flash Video Format). Tuy nhiên, bạn phải chuyển đổi tập tin .flv sang định dạng mà thiết bị của bạn hiểu được. Một tiện ích miễn phí của eRightSoft có tên Super (find.pcworld.com/55293) chuyển đổi tập tin .flv sang định dạng như .avi, .mp4 và .wmv. Chương trình này thậm chí có cả các thông số dành riêng cho iPod và PSP.

Để chuyển đổi tập tin flv, bạn chỉ cần kéo nó vào cửa sổ của Super và từ trình đơn Select the Output Container, chọn định dạng muốn chuyển sang. Đối với iPod, chọn Apple – iPod; với Creative Zen Vision:M, chọn WMV, định dạng tương thích Windows Media Player mà ứng dụng Zen đồng bộ. Tiếp theo, nhấn nút Encode (Active Job-List Files) và tìm những tập tin đã chuyển đổi trong Program Files/eRightSoft/SUPER/OutPut. Cuối cùng, chuyển các tập tin sang máy của bạn. Lưu ý là cách này làm việc với bất kỳ tập tin flv nào mà bạn tải về từ bất kỳ dịch vụ chia sẻ video nào chứ không chỉ YouTube.

Hồng Anh
PC World Mỹ 12/2006

Làm vệ sinh cho các thanh RAM và Card

(Dân trí) - Các thanh RAM và card chức năng (card màn hình, card sound, modem…) lâu ngày sử dụng sẽ bám bụi, nhất là những khe cắm AGP hay PCI trên mainboard. Bài viết sẽ hướng dẫn cách làm vệ sinh cho chúng.

Có thể dùng cọ quét sơn loại nhỏ hay ống xịt bụi làm sạch bụi bẩn, nhưng riêng đầu cắm (có những chân cắm màu vàng) thì có thể xảy ra hiện tượng hoen ố do bụi bám lâu ngày gây nên.
Để làm được việc này thật đơn giản và hiệu quả giúp cho những card của chúng ta luôn mạnh khỏe và bền bạn chỉ cần làm các bước sau:

- Một cục tẩy bút chì (không dùng tẩy bút mực), khăn giấy.
- Tắt nguồn, chờ 15 phút và tháo các card chức năng.
- Lấy cục tẩy chà đi chà lại 4-5 lần theo chiều dọc vào các chân cắm màu vàng, dùng khăn giấy phủi nhẹ, rồi tiếp tục chà, đến khi nào bạn cảm thấy sáng sủa, hết bụi, vết hoen ố mờ hẳn thì thôi.
- Dùng ống xịt bụi hay cọ quét sơn quét lại bụi, làm sạch bụi ở các khe cắm card trên mainboard. Xong việc bạn có thể cắm lại vào máy và vận hành tiếp.

Hoa Đào

Computer system

Computer System

Book I: computer system fundamentals.

Chapter 1: INTRODUCTION TO COMPUTER.

Question 1. *What is a computer?*

A computer may be defined as a machine which accepts data from an input device, processes it by performing arithmetical and logic operations in accordance with a program of instructions and returns the results through an output unit.

A computer is basically an electronic machine operating on current.

Question 2. *Components of a Computer system?*

A computer system comprises of the following components:

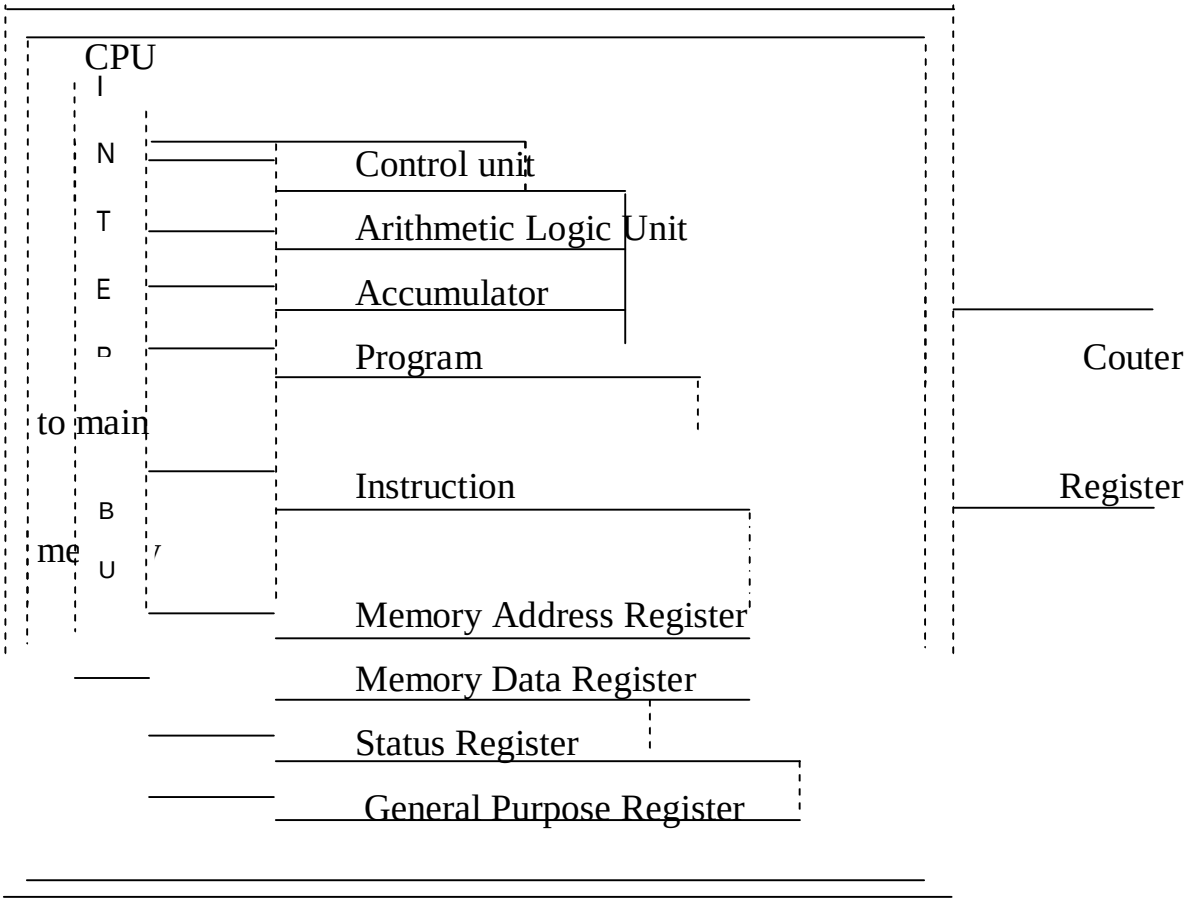
1. Central Processing Unit (CPU).
    - CPU is the heart of the whole sys
    - CPU consists of the :
        - control unit (CU)
        - arithmetic logic unit (ALU)
        - accumulator (ACC)
        - program counter (PC)
        - instruction register (IR)
        - memory address register (MAR)
        - memory data register (MDR)
        - status register (SR)
        - general purpose register
    - The function of each components of CPU:
        - Control unit:
            - control and co_ordinate all hardware functions of the CS.
            - examine and decode all program instructions to the computer and initiate their execution by sending the appropriate signals.
        - ALU:
            - performs all arithmetic <addition, subtraction, multiplication, division & exponentiation> and logic comparision two values functions required by computer.

- ACC:
  - holds the first operand of the temporary result of the ALU.
- PC:
  - contains the add of the next instruction to be excuted.
- IR:
  - contains the current instruction to be executed.

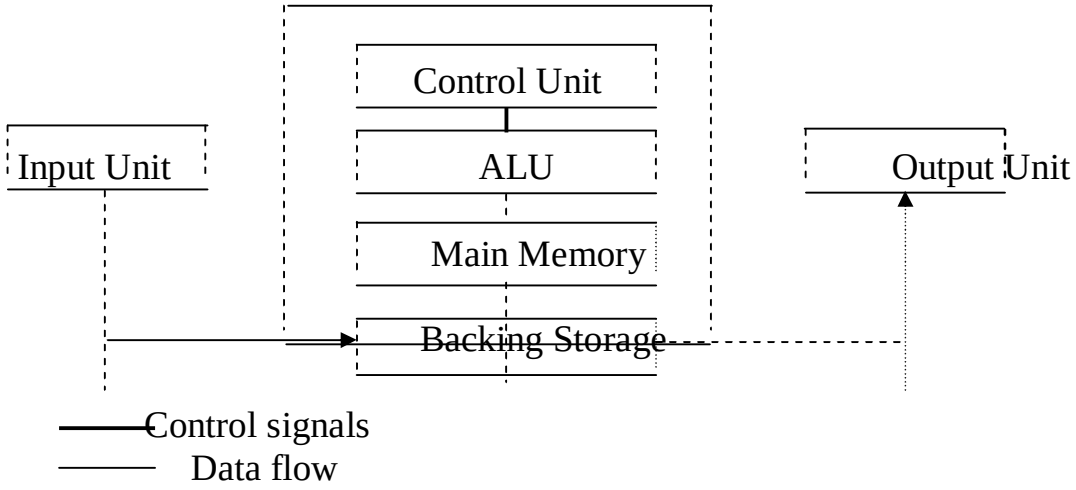
Main memory

- MAR:
  - holds the address location to or from which data is to be transferred
- MDR:
  - contains the data to be written to or read out of the addressed location.
- SR:
  - keeps track of the status of the accumalator.
- General Purpose Register:
  - for general purpose procedures.

Please refer to diagram for an illustratin of the basic components of the CPU.



Basic components of a CPU.



Components of a CS.

2. Input units
   - Used to enter data(raw unprocessed facts) and instructions to the computer.
3. Output units
   - Used for delevering the processed result from the computer in useful form.
4. Backing storage units
   - Backing storage units need for high capacity data storage devices that can store data in a more permanent form for later retrieral, updating and referencing.

Backing storage is also called secondary storage external storage and auxiliary storage.

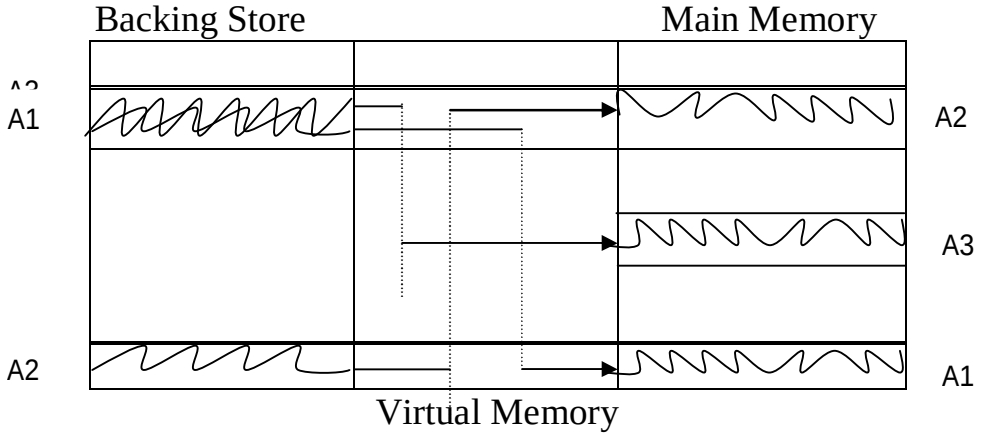
Chapter 2: MICOPROCESSOR.

Question 1. *Cache Memory?*

- Cache memory is a small amount of very fast store with faster access time than the main memory.
- Cache memory is used to temporaryty store data instructions that are likely to be retrieved many times, thus speeds up the processing of data.
- Sits between main storage and the processor acting as holding area through which all data and instructions pass.
- Old data in the cache memory is over written by new then cache is full.

Question 2. *Virtual Memory?*

- Virtual memory makes use of both the main memory and backing store.
- In a virtual memory sys, each user has the illusion that his program is in the main memory all the time.
- The sys maintains this illusion by keeping some of the "unused" portion of the program's code and data on a backing store device which is usually magnetic disk
- The movement of the unused portion from the backing store to the mian memory is transparent to the users.
- Please refer to diagram for virtual memory.



Chapter 3: BATCH/ ONLINE AND REAL TIME PROCESSING SYSTEM.

Question 1. *Batch Processing System?*

- Def: Computer processing does not begin until all the input data has been collected and grouped together called Batched Generally data is accumulated for a certain period of time or unitl a certain quantity.
- Ads:
    - Response time is not critical.
    - Need to process large volumn of data.
    - Computer efficiency is more important than response time.
- Dis:
    - Time between recording and processing of source document is long
    - Rereen normally required if errors are encountered.
    - Data is not current.
    - Error correction is more difficult.

Question 2. *Online Processing System?*

- Def: Inputs data enters the computer directly as soon as it is being transacted. There information will be processed immediately and updated into the master file.
- Ads:
    - Enter availability of information for decision making.
    - More accurate data capture.
    - Schedules suits user.
- Dis:
    - CPU time is used less efficiently.
    - Random arrival of transactions, terminal operator process each transaction separately.
    - More expensive than batch processing.

Question 3. *Real Time Processing System?*

- Def: One which controls the environment by receiving data processing them and returning results sufficiently quickly to affect the functioning of the environment at that time.
- Ads:
    - Response time is very critical and sufficient quick.
- Dis:
    - Expensive hardware & software.
    - Very complex in terms of hardware & software.

Chapter 4: PRINTERS AND TERMINALS.

Question 1. *Classification of printers?*

1. Classifying printers according to speed.
    a. Serial printers

Slow printers that print one character at a time.
Eg: Dot matrix printers
Daisywheel printers

b. Line printers

Medium to high speed printers that can print in excess of 2000 lines per minute.
Eg: Chain Printers
Band Printers
Drum Printers

2. Calssifying printers according to method of printing
   a. Impact printers

   Use hammers or prints to strike a print rebbon in order to form the character on the paper.

   b. Non impact printers

   Use more silent methods of printing.
   Eg: Thermal printers
   Ink Jet printers
   Lazers printers
3. Classifying printers according to print quality
   Kinds of quality printers
   Draft quality
   Near letter quality(NLQ)
   Letter quality
   Graphic quality

Question 2. *Describe some types of printer?*

1. According to speed:
   a. Dot matrix printer
   - Serial impact printers that can print draft, near letter quality and a limited amount of graphics.
   - The print resolution is generally lower than lazer printers.

   b. Daisywheel printers
   - Are serial impact printers, the speed of a daisywheel printer is slow(20-55 characters per second), noisy in operation.
   - The print head has the letters arranged at the end of spokes round a central hub.

   c. Chain printers
   - The chains printers has its characters set rapidly rotating on a print chain.

   d. Band printers
   - The band printer has rotating scalloped steel band.

e. Drum printers
- Are line printers, the print character are raised in bands around a heavy metal drum which rotates at very high speed.
- The print hammers strike the paper and a print ribbon against an apropriate character on the line. An entire line of the same character is printed on one rotation of the drum.

f. Thermal printers
- Uses special heat sensitive paper and a matrix of print wires that become hot when exposed to an electric current. The heated wires come into close contact with the paper, burning the image of the character onto it.
- The more advanced thermal printers are using thermal transfer printing.
- They have a special heat sensitive ribbon and a print head with wires that become hot when a currents is applied.
- The heat from the print wires causes the ink from the ribbon to fuse to a piece of regular paper.

g. Inl Jet Printers
- The ink jet prints by using a small droplet generator to break special inks into tiny drops, which are then forced towards a paper supply.

h. Lazer printers
- Using a photoconductive drum.
- A lazer is then used to write the image of the character onto the drum.
- After exposure to the lazer, the drum rotates through a developing station, picks up toner and transfers it to the paper.
- The character is fused onto the paper by heat.

i. Ion deposition printers
- Ions are created in a cavity, and directed electrically through an orifice onto the dielectric surface of a rotating cylinder.
- The required characters are formed as an electric charge image on the cylinders surface.
- Toner is the applied to the charged image and transferred to the paper on which it is transfixed by pressure(cold fusion).

j. Electrostatic printers
- Letterheads and logos are created electrostatically from a changeable metal cylinder.

k. Magnetic printers
- A drum in the printer has a surface that can be coated with sows of tiny spots of magnetion by means of thousands of minute recording heads.

- As the drum rotates it becomes covered with these magnetic spots so as to from a latent image of the page to be printed.
- Dry ink particles are brought into contact with the drum's surface and these adthere to the magnetised spots. The ink was then pressunal on to the surface and subsequently transferred onto the paper.

Question 3. *Characteristics of a page printers?*

- Speed
- Characters sets
- Copies
- Intelligence
- Output

Chapter 5: DATA STORAGE MEDIA.

Question 1. *Data storage Requirements Characteristics?*

- Low access time: fast speed
- Storage capacity: much enough
- Interchangeability: can be change easily
- Security: safe enough
- Transfer rate: fast enough
- Cost: economic

Question 2. *Magnetic disks?*

- This comprises a drive unit onto which one or perhaps two magnetic disk cartridges are loaded.
- The drive consists of a control unit and a spindle housing that rotates continuously when switch on.
- The cartridge are loaded by the operator so as to provide the data currently needed for the job in hand.
- Bach tracks is devided up into sectors(often 4 or 8), sectors are read or written or more at a time as blocks by means of a read.
- There are usually one head for each surface, all the heads are moved.
- Sunchronously across the tracks.
- Once in position all the data on the equiradial tracks can be read or written without further movement of the heads.
- Cylinder is a set of equiradial tracks.
- A cartridge comprises several flat disks mounted on a central sprindle. When mounted it rotates at a high speed enabling data to be read from or written to it. The data is recorded magnetically on both surfaces of each disk in the form of concertric tracks.
    - Certain models of disk units also have a number of fixed read/write heads in addition to the movable heads.

The fixed head are positioned permanently over certain of the outer tracks, there being one head per track, so climimating the need for head movement.

- The heads are very close disk surface.
- Curshion of air carried by the rotating disk.

Question 3. *Winchester disks(hard disks)?*

- Comprises a number of platters(disks) permanently into an airtight enclosure.
- All dust is excluded thus perimiting the read/write heads to be positioned even closer to the surfaces and so enabling greater recording densities to be employed.
- The disks have greater storage capacity and a higher rate of data transger.
- It has the lubricated surfaces allowing the heads "land" when the platters cease to rotate, so eliminating head crashes.
- Winchester platters are either 14 in, 8 in, 5¼ in or 3½ in diameter.

Question 4. *Floppy disks?*

- Diskettes, generally called floppy disks, are single disks made of flexible plastic and permanently housed is an envelope.
- The data on floppy disks is in concentric tracks on the outer part of the surfaces and access to it is via slot in the envelope.
- The most common size are 3½ in, 5¼in, and 8 in diameter disks, the 3½ in disks have the advantages of a shutter.
- Floppy disks may be either single or double sided and of course the drive needs to be correspondingly equipped.
- Both the drives and the floppy disks themselves are inexpensive with the result that they have come into extensive used by small business and home computer buffs.
- The range of capacities is from 1/4 to 2 megabytes and transfer rates around 125 to 250 kilobytes per seconds.

Question 5. *Optical disks?*

- Optical disk are comparatively new development for data storage.
- Optical disks consist of a single removable glass, plastic or metal disk coated on one side with tellurium and protected by a 1 mm layer or transpacent plastic.
- The disk diameters are mostly between 8 in and 14 in they rotate on a spindle in a similar fashion to magnetic disks.
- The data is recorded in the form of minute pits burned into the telliurium coating by a finely-focused lazer beam.

- Optical disks hold between 0.7 and GBs, this is about 20 times greater than magnetic dis cartridges.
- The data is read by a low power laser beam which moved across the surface and is reflected into a photo cell.
- Optical disks rotate mostly at 1500 r.p.m which, allowing for the movement of the laser unti, given access time of between 16 & 500 ms and data transfer rates of 0.6 to 3 MVs per second.
- The draw back of optical disks is that the data cannot be erased so making them non-rewriteable.

Question 6. *Mass storage media?*

- Mass storage media is a high capacity disk system as when necessary by transferring data from a number of "data cartridges" house in cells.
- Each cartridge consists of a 3 in wide magnetic modium inside a protective cover
- In order to load the disk system, the data cartridges are moved automatically from the cells.
- A typical system consists of 9440 cartridges giving a storage capacity of 472000 million bytes.

Question 7. *Magnetic drums?*

- A magnetic drum consists of a cylinder upon the surface of which data is stored in magnetic form in tracks running around its circumference, each track has its own read/write head.
- A typical magnetic drum has 800 tracks each capable of holding 5000 bytes.

Question 8. *Charge_coupled Device Memory (CCD)?*

- CCD consists of thousands tiny metal squares each capable of holding an electric charge, thus representing a bit.
- The squares are in the form of an array 64 x 64 holding 4096 bits.
- It is very impact.
- CCD is volate lity storage.

Question 9. *Magnetic Bubble Memory?*

- A thin wayer of magnetic garnet is capable of containing tiny domains or cylinders of magnetism, called bubbles.
- By erasing unwanted bubbles, the resultant presence of a bubbles represent a 1 or a 0 bit.
- The main ads are low power consumption, compactness, robustness reliability and non-volitility.

Question 10. *Megnetic tape?*

- The magnetic tape usage is now more as a backup medium rather than a primary method of backing storage.

- It is often used as a depositony for disk dumped from fixed data storage.
- It is in reells of up 3600 feet and is made of Mylar plastic tape, 1/2 in wide and coated with a magnetic material on one side.
- The data is read from one read and written to another.
- A reel of tape is loaded on a magnetic tape drive, and so as many drives are needed as reels during a processing run.
- It is used as a backing medium than a primary method of backing storage.
- The seconds usually have to be sequence where store in magnetic tape.

Chapter 7: COMPUTER FILES.

Question 1. *File Processes?*

1. Sorting
    a. The records in logical file are brought into some sequence as determined by key in the records.
    b. A computer is capable of sorting record into a "nested" sequence.
    c. Sorting is done by a "sorting generator". This is part of the computer's software and comprises several sophisticated sorting techniques that are called into use according to the file and the sort requirements.
    d. The need of sorting has dimished in line with the demise of magnetic tape as backing storage.
2. Merging
    - Merging implies that two or more files in the same sequence are combined into one file.
    a. File merging
        - Two or more separate files of similar seconds and in the same sequence are marged together so as to form one file.
    b. Record merging
        - The records from two or more "input" files, usually in the same sequence, are combined one record in the output file.
3. Matching
    a. Two or more input files (generally in the same sequence) are compared records against record in order to ensure that there is a complete set of records for each key.
    b. Masmatched records are highlighted for subsequent action
4. Summanizing

a. Records with the same key in one file are accumulated together to form one record in the output file.
b. Summanizing usually applies to a file presorted into a certain sequence and the resultant file is in the same sequence.
c. Records to be summarized are generally of a similar type.

5. Searching
    a. Searching is looking for records with certain keys or holding certain data and in some way making a note of these.
    b. An instance is a search for and count of all records with a debt balance of above a certain amount.
6. Information retrieval
    a. Information retrieval is the process that involves the bringing together of data from several files.
    b. Data may also be extracted from several files and combined before being presented as information.

Chapter 8: DIRECT ACCESS FILE ORGANIZATION AND STRUCTURES.

Question 1. *Storage and Access Modes?*

There are 3 principal modes for storing and accessing accords on a disk or drum:

1. Serial mode:
    - The record are stored contigously regardless of their keys
    - The sole way of accessing serial seconds is to search through the complete file starting with the first record.
    - It is sometimes possible to partition a serial files thus reducing the search time by starting the search at the beginning of a known partition.
    - A serial file is normally of a temporary nature awaiting sorting into a useful sequence.
2. Sequential mode:
    - direct access sequential mode normally involves accessing sequential a file that is stored sequentially.
    - sequential mode is often associated with a master file held in a certain sequence and updated by a transaction file sorted into the same sequence.
3. Indexed_sequential/ selective_sequential mode
    - Indexed_sequential is a mode of storage where by records are held sequentially and accessed selectively.
    - Groups of unrequired records are skipped past.
    - Indexed sequential files may also be accessed haphazandly.
4. Random modes:

- Each record is stored in a location determind from the second's key by means of an add generation algorithm.
- The only erricient way to find a record is to use the algorithm
- Random mode is applicable to master files
    - Ads of random modes
        - No index is required thus saving storage space
        - It is a fast access method because little or no searching is involved
        - Transaction do not need storing, thus saving time
        - New records are easily insertly into the random file provided they are not excessive in number
    - Dis
        - The main problem with the random mode is in achieving a uniform spread of records over the storage are allocated to the file

Question 2. *Direct Access Addressing?*

- The key of record is used to identify by record
- The key of record also is used to decide its storage location(or address)

1. Self addressing:
    - Self addressing is a straight forwards method because a record's address is equal to its key's value
    - The file is inevitably stored in key sequence
        - Ads of self addressing
            - It leads directly to the wanted record
            - No indexing or searching is required
            - The key itself need not necessarily be held within the stored record- although it generally is
        - Dis
            - The storage space per second has to be the same
            - When records one missing, storage locations related to its must be left empty
2. Self addressing with key conversion
    - This method a basically similar to self addressing except that the key required a little processing to turn it into the record's address
    - This leads to either a pricise address
3. Matrix addressing
    - In somes case, it is necessary to find the add of a record held within a multi dimensional matrix of record it's called matrix addressing.

Question 3. *Direct Access Searching?*

Where as addressing determines the location of a record by using algorithmic methods, searching finds the record by scanning groups of records, and index, or both.

-]The simplest method is to examine every record a file until the required record is found a shortcut is generally desiable.

1. Indexed sequential searching
   - A cylinder index is created to hold the highest cylinder's key
   - Associated with each cylinder is a block index holding the highest key in each block within that cylinder
   - When searching for a record's key in the index
     - The cylinder index is examined key_by_key until one is found that is larger than or equal to the wanted key this directs the search to the appropriate block index
     - The block index a similarly examined and the search
     - The block is searched record by record until the wanted record is found

1. Binary searching(binary chopping)
   - The key in the index to be binary search must be in sequence and form a complete set
   - The search starts at the midpoint of the index and then moves half way to the left or right(down or up) depending upon whether are wanted key is less than or greater than the midpoint key
   - In pracice, the index is unlikely to as convenient as this example because it is not always possible to exactly halve each sucessive move(complete exact holvingis possible only when the total number of keys in the index is 2^0-1)
   - The average number of examinations comparisons is $(\log_2 k)^{-1}$ (k is the number of keys in the index)
2. Block searching
   - A block is a subdivision of an index. A block is devised to contain, roughly the square root of the number of keys in the whole index
   - The search is first through the block index to find the appropriate block and then through this to find the wanted key
   - The average number of examinations is square – root – ^{k} (k is the total number of keys)
3. Balanced binary tree searching
   - A binary tree is a relationship of keys such that the examination of any key leads to one of two other keys

- The binary tree is actually in the form of an index containing all the keys together with a directory showing the braches stemming left and right from each key
- Binary tree searching is suitable for an unsequenced file
- The search is similar to binary searching in that each key examination holves the rinaining keys, on average

Chapter 11: INTRODUCTION TO ARTIFICAL INTELLIGENCE.

Question 1. *AI?*

Atificial Intelligence

It has three braches

1. Expert systems (or knowledge- base system)
    - ESs are programs that contain the knowledge of human expert, encoded so a computer can understand it with encated- knowledge seasoning machinism, ES can tackle problem that are beyond the seach of conventionally programmed computers.
2. Natural language systems (everyday native language)
    - Natural language systems are programs that understand the native language of the user, such as E
    - The most popular natural language systems are those that act as interfaces to data bases
3. Simple perception systems (for vision, speed and touch)
    - They can interpret visual scenes and decide if object meet inspection standards and quality control criteria, or move a robot to the proper location ot grasp a part for manufacturing

Question 2. *Who does the updates?*

- Updating the knowledge bases is very diffirent when with updating databases because of the difference in the type of information and in the cause and effect relationship contained in knowledge bases
- A knowledge in the area, when databases may be modified by a normal users

Chapter 12: EXPERT SYSTEMS.

Question 1. *What is an ES(Expert system)?*

An ES is a knowledge-intersive program that solves a problem that normally requires human expertise

- Characteristics of ESs
- They solve problems as well as or better than human experts
- They use knowledge in the form of rules or frames
- They can consider multiple hypotheses simultaneouly
- Types of ES
- An assistant

- Is the leasts expert or lowest level ESs
- It helps a decision maker by doing routine analysis and porting out those portion of the work where human expertise is required

- A colleage
  - The new discusses the problem until a joint decission is reached
  - When system is going wrong, the user adds more information to get it back on track
- True ES
  - Is a system that advises the user without question
  - There are no practical areas today in which decission

Question 2. *A ES Life Cycle (ESLC)?*

- An accepted SDLC for expert systems has yet to be developed

There are 6 phases life cycle in an ES

1. Phase1 – Selection of an Appropriate Problem
   - Phase 1 involves finding an appropriate problem for an ES, indentifying an expert to contribute the expertise
   - Establishing a preliminary approach
   - Analysing the cost and benefitsPreparing a development plan
2. Phase 2 – Development of a prototype system
   - A prototype sys is a small version of an ES designed to test assumptions about how to encode the facts, the relationships and the knowledge of experts
   - The prototype permits the knowledge engineer to gain the expert's commitment and to develop a deeper understanding of the field of expertise
   - Other subtasks in this phase:
     - Learning about the domain and the task
     - Specifying performance criteria
     - Selecting an ES building tool
     - Developing an implementation plan
     - Developing a detailed design for a complete system
3. Phase 3 – Development of a Complete System
   - The main work in this phase is the addition of a very large number of rules
   - The knowledge base has to be expanded to full knowledge base appropriate to the real world and the user interface has to be developed
2. Phase 4 – Evaluation of the system

- This phase involves testing the system against the performance establised in earlier stages

2. Phase 5 – Intergration of the system
   - The ES has to be intergrated into the data flow and work patterns of the organization
   - In this stage, the expert system has to be interfaced with other databases, instruments and hardware.
3. Phase 6 – Maintenance of the system
   - The maintenance of the ES involves is updating, charging in the system when operating. When operating, more problems occur in the system, so it is necessary to continue take care the system by expert in a fix period of time
   - So expert system, are so complex that in a few year the maintenance costs will equal the development costs.

BOOK II: Computer systems architecture.

Chapter 1 – 2: NUMBER BASES.

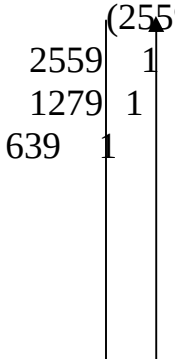
Question 1. *Common number bases used in computer hardware operation?*

- Decimal(denary) system:
- The base is ten – there are 10 different symbols, the digits 0, 1, 2, etc...upto 9
- To represent value less than ten involves only one digit larger values need two or more digits
- Binary system
- The base must be two, with only the digits 0 and 1 available
- To show values of two or ever require two or more binary digits
- Octal system
- Octal system has eight as its base, it uses the symbol 0, 1, 2 up to 7 only
- Two or more digits are needed for values of eight and above
- Hexadecimal system(hex)
- Hexadecimal system has sixteen as its base, it use the symbols 0, 1, 2...,9 & A, B, C, D, E, F, to stand for the "digits" ten, eleven, twelve, thirteen, fourteen, fifteen.

Question 2. *Converting from Bases To Bases?*

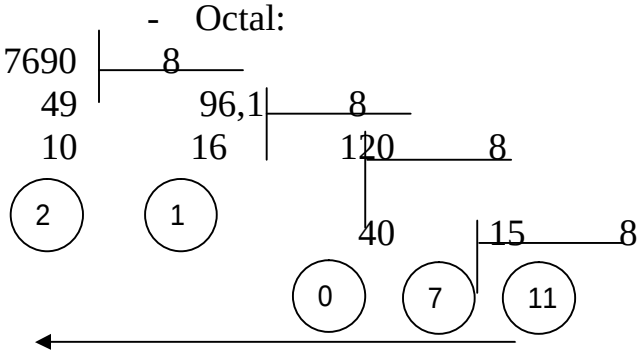
1. Change the decimal
   - Binary:

Eg. (2559) 10



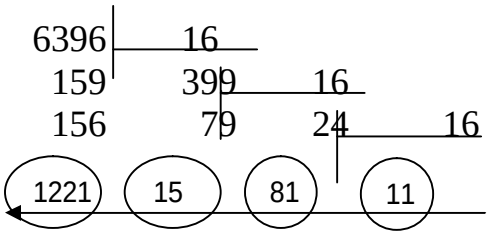
319 1
159 1
79 1 ⟹ $(2559)_{10} = (10111111111)_2$
39 1
19 1
9 1
4 0
2 1
0 0

- Octal:



⟹ $(7690)_{10} = (17012)_8$

- Hexadecimal:



C F

⟹ $(6369)_{10} = (CF81)_{16}$

2. Convert to others from binary
   - To decimal

   $(101010)_2 \longrightarrow (?)_{10}$

$1.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 1.2^1 + 0.2^0 = 42$

⟹ $(101010)_2 = (42)_{10}$

   - To octal

100101101

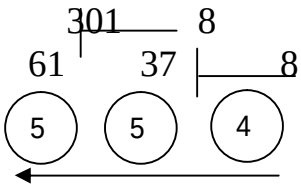
➢ 1st step change into denary

$= 1.2^8 + 1.2^5 + 1.2^3 + 1.2^2 + 1.2^0$

= 256 + 32 + 8 + 4 + 1

$=(301)_{10}$

- 2^{nd} step: convert to octal



$(301)_{10} = (455)_8$ ⟹ $(100101101)_2 = (455)_8$

- To hexadecimal

110111011011

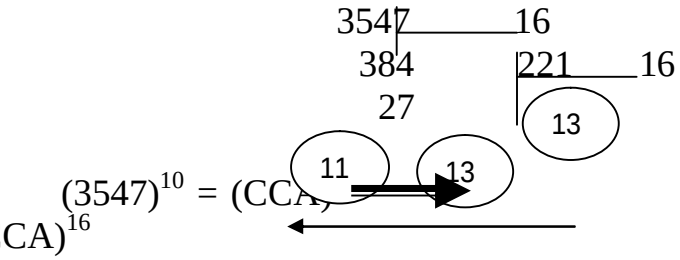
1^{st} step

$= 1.2^{11} + 1.2^{10} + 1.2^8 + 1.2^7 + 1.2^6 + 1.2^4 + 1.2^3 + 1.2^1 + 1.2^0$

$= 2048 + 1024 + 256 + 158 + 64 + 16 + 8 + 2 + 1$

$= (3547)^{10}$

2^{nd} step



$(3547)^{10} = (CCA)$ $(110111011011)^2 = (CCA)^{16}$

1. Convert into binary and display the answer in normalized exponential form

247	1
123	1
61	1
30	1
15	1
7	1
3	1
1	1
0	1

$(247)^{10} = (11110111)^2$

$= 0.1111011 \times 2$

normalized exponential form

Question 3. *Integer and Floating – point arithmetic?*

1. Floating – point Addition
    a. $(0.1011 \times 2^5) + (0.1001 \times 2^5)$
    $= (0.1011 + 0.1001) \times 2^5$
    $= 1.0100 \times 2^5$
    $= 0.10100 \times 2^6$
    b. $(0.1001 \times 2^3) + (0.1110 \times 2^5)$
    $= (0.001001 \times 2^5) + (0.1110 \times 2^5)$
    $= (0.001001 + 0.111000) \times 2^5$
    $= 1.000001 \times 2^5$
    $= 0.1000 \times 2^6$ (here have truncation)
    (0.1000001×2^6)
2. Floating – point subtraction
    a. $(0.1110 \times 2^7) - (0.1100 \times 2^7)$
    $= 0.0010 \times 2^7$
    $= 0.10 \times 2^5$
    b. $(0.1001 \times 2^8) - (0.1000 \times 2^5)$
    $= (0.1001 \times 2^8) - (0.0001 \times 2^8)$
    $= 0.1000 \times 2^8$
3. Floating – point multiplication
    a. $(0.1010 \times 2^3) \times (0.1100 \times 2^3)$
    $= (0.1010 \times 0.1100) \times 2^6$
    $= 0.01111 \times 2^6$
    $= 0.1111 \times 2^5$
    b. $(0.11110 \times 2^3) \times ((0.01011) \times 2^4)$
    $= (0.11110 \times 0.01011) \times 2^7$
    $= 0.001111 \times 2^7$
    $= 0.1111 \times 2^5$
4. Floating – point division.
    a. $(0.11010 \times 2^6) : (0.001 \times 2^6)$
    $= (0.11010 \times 2^6) : (1 \times 2^3)$
    $= 0.1101 \times 2^6 : 1 \times 2^3$
    $= 0.1101 \times 2^3$
    b. $(0.110111 \times 2^6) : (0.1001 \times 2^4)$
    $= (0.110111 : 0.1001) \times 2^2$
    $= (1101.11 : 1001) \times 2^2$
    $= 1.100001 \times 2^2$
    $= 0.1100001 \times 2^3$

Chapter 3: TYPES OF INSTRUCTION AND ADDRESSING.

Question 1. *Types of instructions used in CS?*

1. Arithmetic instructions.

Arithmetic instructions include directives to the computers to perform additions, subtraction, multiplications, divisions and exponentiations.

2. Input/ output instructions.

They direct the computer to read data values from the specified input devices into the main store for processing.

They also include instructions to write the contents of memory locations holding the result of processing to a specified output device.

3. Decision or control instructions.

Most data processing application will contain situations where alternative calculations or procedures will have to be executed based on the result of condition tests carried out.

4. Data handling instructions

They include the copying of the content of one memory location to another or setting a memory locations to an initial value.

Also include the management or insertion of characters into data items

Examples of such instructions include branch instructions, jump instruction & stop instruction.

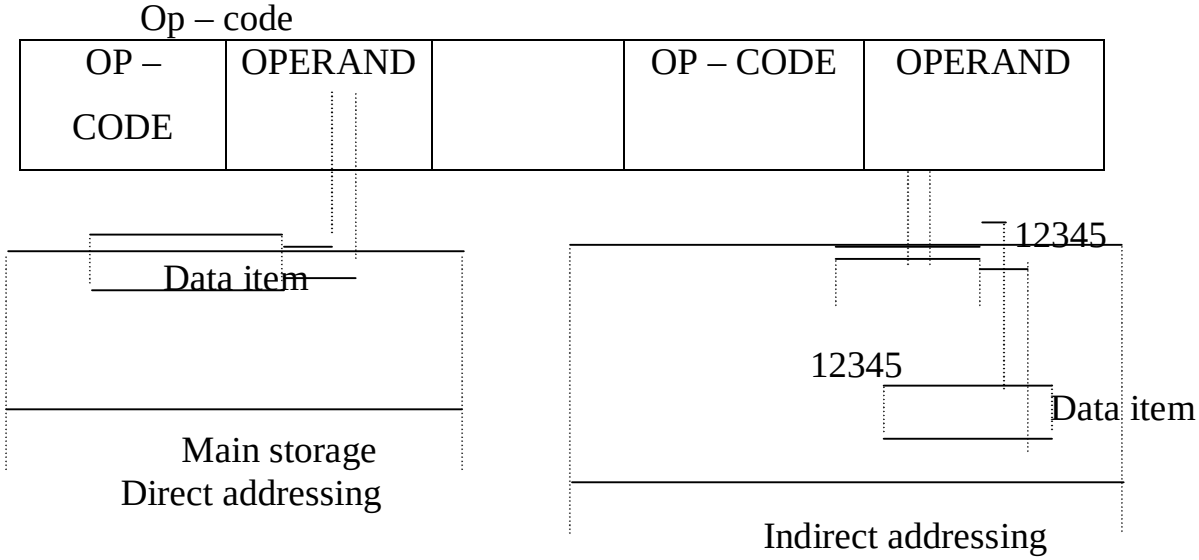
Question 2. *Types of addressing?*

1. Direct addressing

The operands of each machine instructions is used to retrieve the data

2. Indirect addressing

The operands is used to specify the memory address which contains the address of the data to be processed

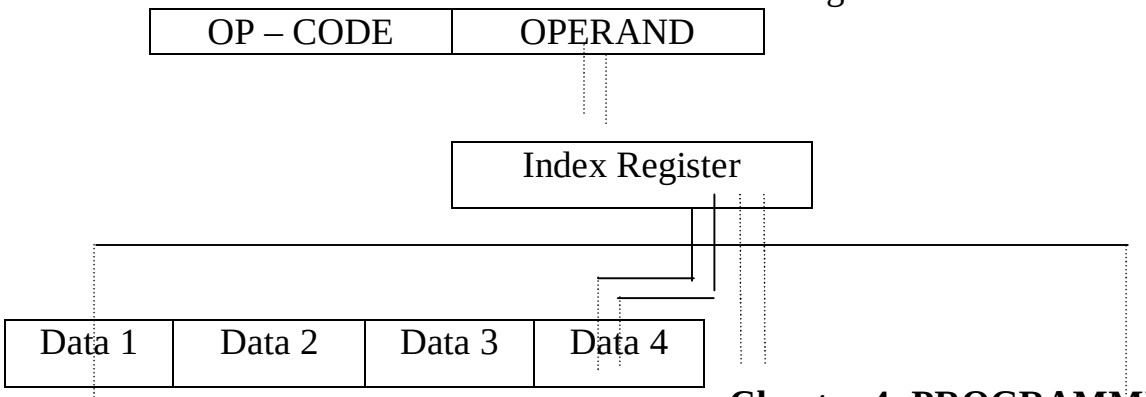


3. Indexed addressing

- The main applications of this type of addressing technique is to enable to access of sequential locations in memory that are adjacent to each other

- Each adjcent memory address has value n+1, where n is the address of the previous location
- When the first of the location have been accessed, the next memory location in sequence is accessed by simply increasing the add of the present location by 1 & using accessing it
- The starting address of the series of locations is specified in the operand of the instruction
- In order to access the next location in sequence, the content of the index register is increased by 1 a added to the opreand address
- This is done repeatedly until the last memory location in the series is processed

Indexed addressing.



Chapter 4: PROGRAMMING LANGUAGES.

Question 1. *Program and level of language?*

Program is group of constructions that is linked together to perform specific task. It's necessary for a computer program to be written in a "PL" because at a computer program is created by a programing using a sys analyst's specification of the job in the hand.

1. Machine language
   - ML is the set of bit(0,1) that can performed considered by CPU
   - Ads
     - fast
     - short prog
     - store in small memory
   - Dis
     - difficult to understand & remember its code
     - takes a lot of time to programming
     - difficult to use
2. Low level language

- LLL is used to dercribe exactly procedure of performance of CPU at certain time
- Features:
    - Instruction is written by natrural English or natural language
    - More powerful and so the prog is shortest
    - Need less instruction
    - Is a one to one relationship between the written instruction and the machine instructions
    - It's instruction tend to be machine. It runs in OS
- Ads:
    - Easy to write
    - Easy to understand
    - Known the processing data in CPU
    - Prog writing is shortset
- Dis:
    - Must be complier
    - The time of running prog is longer than machine language

3. High level language
    - HLL was developed in order to further easy the work of programmers by making the programming language more procedure oriented
    - Features:
        - The statements of HLL are closer to natural english or other natural language
        - A HLL source program must be translated into machine code by means of a compiler or an interpreter
    - Ads:
        - Easy to wirte
        - Easy to understand
        - May be used for everybody
        - Closed to natural languages english language
    - Dis:
        - Must be interpreter by compiler or an interpreter before processing by the computer
        - The prog is long
        - The time to run the prog is longer than low level language

Question 2. *Some High Level Languages (HLL)?*

1. COBOL: Common Business Oriented Language
    - COBOL is an exetensively used HLL and since around 1960 several versions have appeared
    - The original intention was that COBOL should be capable of being compiled and run on any model of computer
    - COBOL is now employed for many business data processing applications, and so a brief explaination of its structure follows
    - A COBOL program consists of 4 divisions:
        - Identifycation division this identifies the prog
        - Enviroment division specifies the computer to be used for compiling and processing
        - Data division specifies the format and relates to these to the names used in the procedure division
        - Procedure division comprises the statements in the source program, this is the main part of a COBOL program
2. BASIC: Beginners ALL purpose Symbolic Instruction Code
    - BASIC is a straightforward HLL intended for use in a time-sharing environment in this respect it is particularly beneficial in educational institutions
    - One of the difficulties with BASIC is the welter of dialects currently in use
    - Essentially BASIC consists of statements made up of verbs & variables. The verbs are similar to those in COBOL but there is a large to them that in effect become the addresses of their locations in the main store
    - A variable name must be unique and generally consists of one or a few alphabetic characters, purhaps followed by a digit
3. PASCAL: named after the famous 17^{th} century French mathematician
    - It was expressly designed as a language to make programming more systematic and discriplired and in these respects lends itself to structured programming
    - It is however more difficult to learn than are COBOLS BASIC and so is unliked to be accepted as a language for microcomputers are geared to BASIC only

Question 3. *Operating Systeim?*

- Concept of OS:

- An OS consists of a suite of programs, one of which, the master, kernel or exeactive program, remains resident in the main store. This program controls the other OS programs in th suites and between them they controls the application programs
- Often the operating system includes various application packages among its suit of programs. Ex of such software include: word processing, electronic mail, networking, speadsheet, graphics and file handling

- Function of OS
  - Pricrity assignment:

Jobs waiting execution are scheduled according to either a predetermined or a dynamic assignments plan

- Control of multiprogramming

Control of accomplish multiprogramming an “executive” or “supervisor” program is employed to control the application programs

- Communication

Control of data transmission between terminals and the computer, and computer to computer

- Database

Control of DBMS

- Software control

Control of assemblers, compilers, utility software, and subroutines so that these are imediately available when required

- Spooling

The control of input/output peripherals in order to achieve their best utilisation

- Dynamic allocation

Of main and backing storage, including virtual storage

- Operating allocation

Via the console printer or VDU

- Debugging and editing new programs

In confunction with the compiler, and passing error msgs to the user

- Operation log

Maintaince of details of all jobs carried out by the computer

- Application package control

Especially with microcomputers, as describe above

Chapter 6: TRANSLATORS.

Question 1. *Translators?*

1. Assemblers

- Def: A program that translates assembly language into machine code.

Dos machine instruction is generated for each source instruction

- The resulting program ran only be executed when the assembly process is completed

- Operation:
  - Translates mnemonic operation codes into machine code & symbolic address into machine address
  - Includes the neressary linkages for closed subroutines and inserts appropriate machine code for macros
  - Allocates area of storage
  - Detects and indicates valid source language instruction
  - Procedures the object program on tape or disk required
  - The lesting may also include error codes if appropriate. To illustrate the methods used just think about an assembly program. We must first look at the directives
    - A directive is used to control the assembly process, it is not asembled but is obeyed by the assembler when it is encouteded, e.g ”END”, is sometimes called a pseudo-operation code on pseudo-opcode

2. Interpreter

A program which translates and executes each source statement in logical sequence as the program one instruction at a time, completely translating and executing each instruction before it goes onto the next

- Interpreter, which deals with the source program one instruction at a time, completely translating and executing each instruction before it goes onto the next
- Interpreter seldom produce object code but call upon inbuilt routines instead
- Some intermediate code is usually produced temporority
- If an interpreter is used, the source program will be translated every time the program is executed
- Interpreters are widely used, particular for the programming language Basic on small computers
- Interpriter are used for such things as:
- Handling user commands in an interactive sys
- Debugging programs as they run
- Handling software produced for or by a different computer

3. Compilers:

A program that translates HLL into a machine orientated language, often the machine code. Many machine instructions are generated for each source statement

- The compiler:
    - Translates the source program statements into machine code
    - Includes linkage for closed subroutines
    - Allcocates areas of main storage
    - Generates the object program on cards, tape and disc as required
    - Produces a printed listing of the source and objected programs when required
    - Tabulates a lish of errors found during compilation
- Compilers are commonly used for the translation of HLL program
- Compiler translates the whole of the HLL source program into a machine code object program prior to the program being loaded into main memory and executed
- If a compiler is used, the same program need only be translated once

• Stages of compilation
    - lexical analysis
    - systatical analysis
    - code generation

Chapter 7: SOFTWARE.

Question 1. *Application software?*

- Application software comprises the programs that are written specifically to achieve resulting appertaining to the company's activities
- Application software comes from two source
    - They produce by themselves
    - Buy from an external agency

1. Ads and dis of using application packages in house

• Ads
- The requirements of the application are more easily met
- There is more control in testing and debugging
- The more control over the usage and support obtained

• Dis
- There is a waiting period before the application can be implemented
- Development cost is higher than buying a package

2. Ads and dis of using application package

• Ads:
- The packages can be used immediately
- Documentation is generally good
- It can be used on a varisty of machines

- It is cheaper as the costs of the packages are shared between many users
- Comprehensive on line help information and guided tutorials available
- Easily remembered command syntax
- Can be used in confunction with other software in an integrated fashion

- Dis:
  - Modifications may be difficult for some applications
  - Package may be two generalized to suit user needs
  - Some features purchased may not be required
  - Support given depends on stability and professionalison of the vendor
  - User are required to comply with the owner's regulations

Question 2. *Utility software?*

- Certain processing is common to a high proportion of computer users, and so utility software has been created to cater for this need
- Utility software is intended to be sufficiently flexible to meet most user's requirements and is tailored to meet their precise needs by means of parameter entered prior to use
- Some of the utility programs described below may be incorporated into the OS that is used with a particular computer
  - File conversion: this convers the transference of data from any medium to any other
  - File copying: an exact copy of a data set is made on to another lot for the same type of storage medium
  - File reorganisation: direct access, files over flow records are stored in designed blocked, this is acceptable up to a point but from time it si necessary to reorganise the file so as to remove the overflow
  - File maintenance(amendment): this procedure involves the straightforward insertion and deletion of records into or form sequential files
  - Sorting: is frequently necessary in order to arrange a set of records into a certain sequence based on their key values
  - Dumping routines: a dump routine is used in confunction with a restfirt program ...
  - House keeping operations: there are programs or parts of a programs not directly concerned with the solution of the problem in hand

Trace routines: these entails, the dumping, display or printing of th program or other contents of the main store during program testing to facilitate error detection

- Utilitys are commonly used to perform these functions:
    - Copying of files
    - Sorting of data
    - Merging of files
    - Data recovery
    - Reformating of records by reamanging their fields
    - File reorganization
    - Reporting of sys status and usages

Question 3. *System software?*

There are three main types of memory placement policy:

- First fit
- Best fit
- Worst fit

1. First fit policy, an incoming job is placed in the first available free space large enough to fit it. This allows the placement decision to be made quickly
2. Best fit policy, an incoming job is placed in the free space in which it fits most tightly
3. Worst fit policy, an incoming job is placed in the largest possible hole of free space

Question 4. *Types of scheduling?*

- Scheduling of job is also an important part of any OS. It involves keeping track of and deciding which job is to be executed
- Types of scheduling
    - Deadline scheduling
    - First in first out scheduling(FIFO)
    - Round robin scheduling
    - Shortest job first(STF) scheduling
    - Shortest remaining time scheduling(SRT)
- More details about types of scheduling
    - In deadline scheduling certains are scheduled to be completed by a specifir time or deadline. Deadline scheduling can be very complex requiring substantial overhead in resource management
    - FIFO scheduling: processes are dispatched according to their arrival time in the ready queue. This type of

- Round robin scheduling is similar to FIFO scheduling but the difference lies in that each job is given a slice of CPU time
- SJF scheduling: shorter jobs are more favoured than longer one. SJF selects job that ensures the next jobs will complete & leave the sys as soon as possible
- SRT scheduling: the job will the smallest estimated remaining run time is executed first. In SRT, a running job may be replaced by a new job with a shorter estimated run time

Chapter 8: MEMORY MANAGEMENT.

Question 1. *Virtual Storage System?*

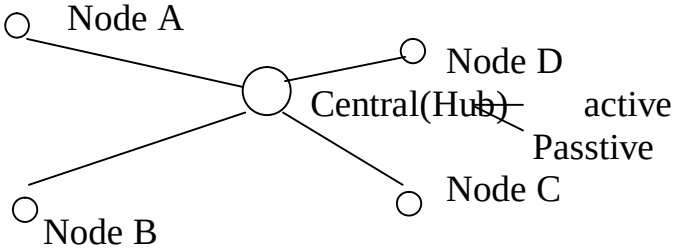
- Instructions and data not currently needed might even be stored on the disk and thus free up a portion memory
- Virtual storage systems have evolved to meet these needs. Virtual storage systems allow programs to be as large as necessary, even larger that the physical storage capacity of the computer
- Translating the user's view of the program into the physical reality of computer storage is one of the major task performed by virtual memory OS like IBM's MVS and digital VMS
- Virtual storage system included ~~non paged systems~~ Paged systems

Chapter 9: NETWORKING.

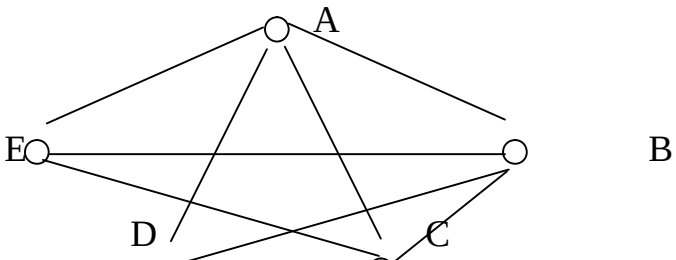
Question 1. *Types of network layout?*

Network topology is the name given to the various types of network layout

1. Start network(or centralised network)
    - This network all communications go through a central node

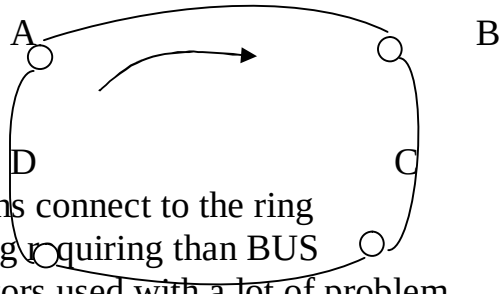


    - The centra of star network is the hub which performs the function of routing msgs and data within the network
    - The hub manages & senvices all incoming and outgoing communication traffic. It's also provide info services from a large central data bases
2. Mesh network (or distributed network)
    - This network may be fully connected or partially connected



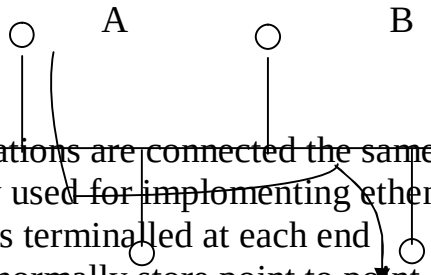
- Data can get from one node to another node via different route
- Multi point to point

3. Ring network(or loop network)



- Work stations connect to the ring
- More cabling r quiring than BUS
- The connectors used with a lot of problem
- Cable is used UTP, STP

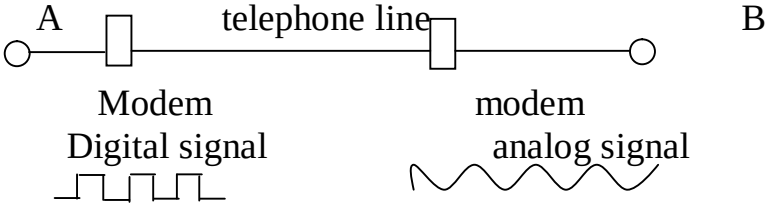
4. Bus network(or multidrop network)



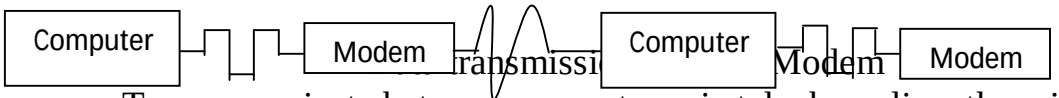
- All workstations are connected the same cable segment
- Commonly used for implomenting ethenet at 10 mbps(Mb/s)
- The cable is terminalled at each end
- Writing is normally store point to point
- A faulty cable or work station will take the entire LAN down

Question 2. *Network control?*

1. Modems(modulation demodulation)



OR



- To communicate between computers via telephone line, there is a need to convert signals from the computer into a form suitable for transmission over the telephone line or convert from digital signals

into analogue signals, and convert back from analogue signals to digital signals

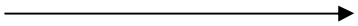
- From source: digitals signals are converted into analogue signals(modulation)
- At the received end analogue signals are converted back into digital signals (demodulation)
- A device to handle modulation, demodulation process is called Modem

2. Bandwidth and Fibre Opties

The major benefits of fibre opties are:

- Fibre optic cables are much lighter and smaller in size
- Greatly increased speed in data transmission
- Greatly reliability
- Greater secerity as lines can not be tapped

3. Transmission
    a. Simplex transmission

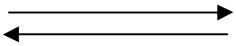


This method allows for transmission in one direction only

    b. Half duplex transmission

This method means that's data can be transmitted in both directions, but is only on direction at a time

    c. Full duplex trasmission



This method of transimission allows for transmission in both directions simultaneously

* Two modes of transmission are used when transmitting data over communication lines. They are
    - asynchrorous
    - synchronous

Asynchronous:

- One character at a time is transmitted or received
- Each character is preceded by a start bit and a stop bit
    - The start bit is used to indicate or character is being sent
    - The stop bit is used to indicate the end of the character
- Asynchronous transmission is used for low speed devices

Direction of transmission

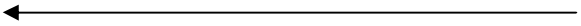
S T S T S T S T

A R T	11000001	O P	1111111	A R T	11000010	O P

Synchronous:

- The speed of transmission is much faster
- Transmission groups of character can be send down the line without the start and stop bits

Direction of transmission



000111000001011100000011

Question 3. *LAN_Local Area Networks?*

- Def: A LAN is a communication network in that connects office equipment to provide a variety of data communication service which features high transmission rates and low error rates
- Characteristics:

- Utilisation of some type of switching topology
- Locality restricted to a few miles or in the same bulding
- Proprietorship by a single organisation

- Features:

- LAN is after used in offices & it connects of fire equipment to provide a variety of data communication. Service with light transmission rate and low errors rate
- The majorities of LANs are connected by coxial cable, and the protocol(rule for communication) is very simple

- Three other important aspects of LANs:

- Acess method (protocol)

Central control
CSMA_CD
Empty slot access
Token access/token passing

- LAN transmission modes:

There are 2 main types of LAN transmission modes

a. Baseband transmission: is essentially & binary method, each bit being represented by one of two states of an electric pulse passing through the network.
   Baseband is nevertheless suitable for most LANs, and is the mode employed by Ethernet and Cambridge Ring network

Broadband transmission: the data is modulates into a carrier wave. Broadband transmission has a much greater band width than baseband, it can transmit sth like ten times as much in a given time

- LAN is one of the distributed processing designs
- LAN are considered loosely coupled system processors are located in separate machines and communicate at relatively low speeds
- LAN is the means by which distribution takes places, regardless of what are distributed

Chapter 10: DATA COMMUNICATIONS.

Question 1. *Write a short note of?*

1. Communication is an extensive subject in its own right, encompassing not only data transmission but also sound and video transmission via telephone lines, radio links and satellite links.
2. Multiplexing is a means of combining together data from several sources so that it can be transmitted along one comminication line
3. Front – end processing: A front – end processor is usually a minicomputer or a microcomputer interposed between the main computer and the multiplexor

Its purpose is to relieve the host computer from the bunden of communications housekeeping

4. Concentrators are device used to gather the bit from each terminal or group of terminal and hold them on buffer store unit until there are sufficient to justify forward transmission
5. Protocol is an "agreement" where by devices can communicate is a fully understand manner
6. Multidrop line<multipoint line> has several terminals on concentrator attached to it
7. Distributed data processing sys is one of which interconnected points at which processing power and storage capacity are availble

Question 2. *Fibre Optics?*

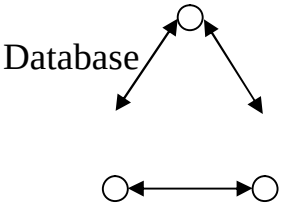
- Fibre optics is that data and other information is transmitted in the form of light through very fine glass fibres
- Ads:
  - High bandwidth eg data transmission capacity
  - Low cross – talk eg interference between adjacent fibres
  - Low attenuation eg loss of signal strength
  - Freedom from interference from external electrical and electromagnetic equipment
  - High reliability
  - Safe because no heat, sparks or electrical voltages are created

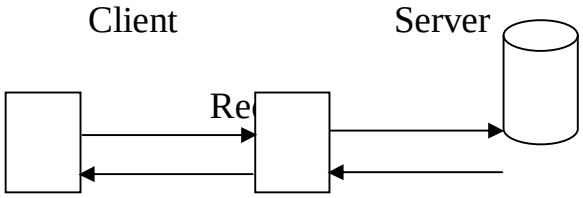
- Economic because glass is loss expensive than copper

Chapter 11: DISTRIBUTED PROCESSING.

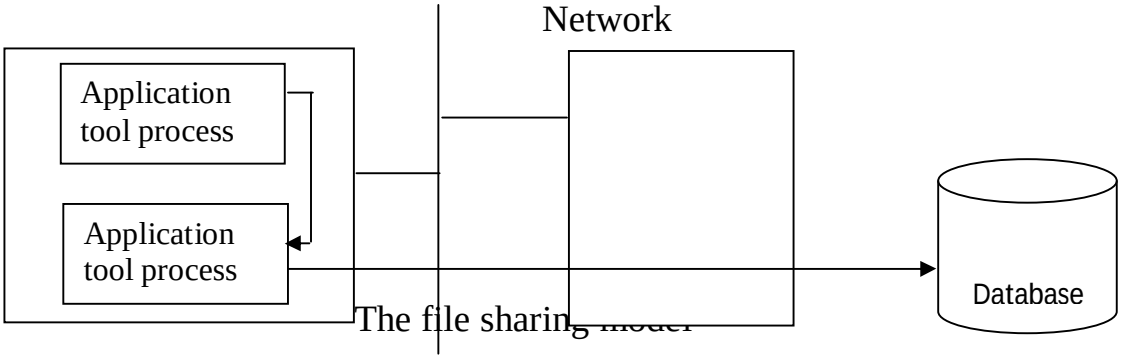
Question 1. *Client/ Server Model?*

- It's common way to employ distributed processing that is client/server architecture which splits into components
- Server store & main palates the actual data & provide secenity, losting function transaction logging recovery capabilities
- Client/ server model seems like PC lan each server support more users
- Data request in form of SQL(structure quenf language) command travel across the network from client to server

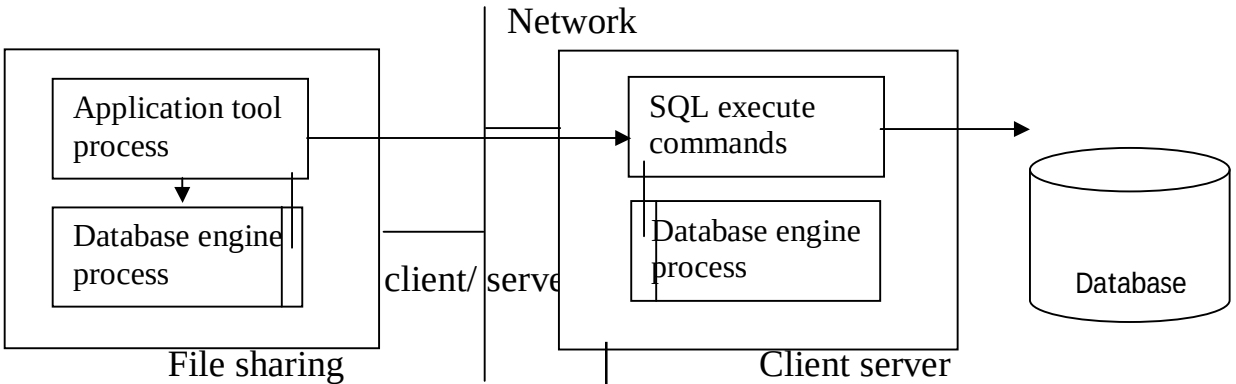




Question 2. *File sharing VS client server?*



<< Continuousting to page 28>>



File sharing

- File are shared for a lot of machines in the network(each

Client server

- Database are stored in the server machines and client

machine can access to the shared files)
- It can create heavy network traffic(each access to a large file can potentially block of the file, showing the system amount of information temporarily unavailable to other user)

machines can send request for appropriate data
- Only the records matching the request criteria raresent back to client machines so the sys never has heavy traffic

Question 3. *Distributed Database Topology?*

- With distributed processing system, user can access data, that is located among a number of physically separate servers. It provides user with a globol view of the data.
- With distributed database, the problems with implementing still exists.
- Developing distributed database application requires extensive planning to anticipate the many complex possibilities.
- For a large number of transactions travelling across the network the capacity of communication lines and the possible impact a system must be carefully considered.

Chapter 12: THE TCP/IP PROTOCOL SUITE.

Question 1. *The OSI model? <Open System Interconnection>*

- OSI model, adopted in 1983 by IOS <International Organization Standardization>, which is a framework for defining standards for linking hetenogenerous computer
- The communication function are pastitioned into a vertical set of layers. Each layer performs are lated subset of the functions required to communicate with other sys
- The OSI layers
    - Physical: concerned with transmission of unstructured bit stream over physical medium, deals with the mechinical, electrical, functional, and procedual characteristrics to access the physical medium
    - Data link: provides for the reliable transfer of information across the physical link, send blocks of data with the necessary synchronization, error control, and flow control.
    - Network: provides upper layers with independence from the data transmission and switching technologies used to connect systems, responsible for establishing, maintaining and terminating connections

- Transport: provides rediable, transparent transfer of data between end points, provide end_to_end error recovery and flow control.
- Session: provides the control structure for communicaton between applications, establishes, manages, and terminates connections between cooperating applications.
- Presentation: provide independence to the application processes from difference in data representation(syntax)
- Application: provide access to the OSI environment for users and also propvides distributed information services

<table>
<tr><td rowspan="2">User oriented</td><td>Application</td><td rowspan="3">Users of transport service</td></tr>
<tr><td>Presentation</td></tr>
<tr><td rowspan="3">End to end connection oriented</td><td>Session</td></tr>
<tr><td>Transport</td><td></td></tr>
<tr><td rowspan="3">Point to point link oriented</td><td>Network</td><td rowspan="3">Network service</td></tr>
<tr><td>Data link</td></tr>
<tr><td>Physical</td></tr>
</table>

Perspectives on the OSI architecture

Question 2. *Protocols?*

Both OSI and the TCP/IP protocol suite deal with communications among hetrnogenerous computers

Both are based on the concept of protocol and have many similarities

a. TCP/IP protocol architecture

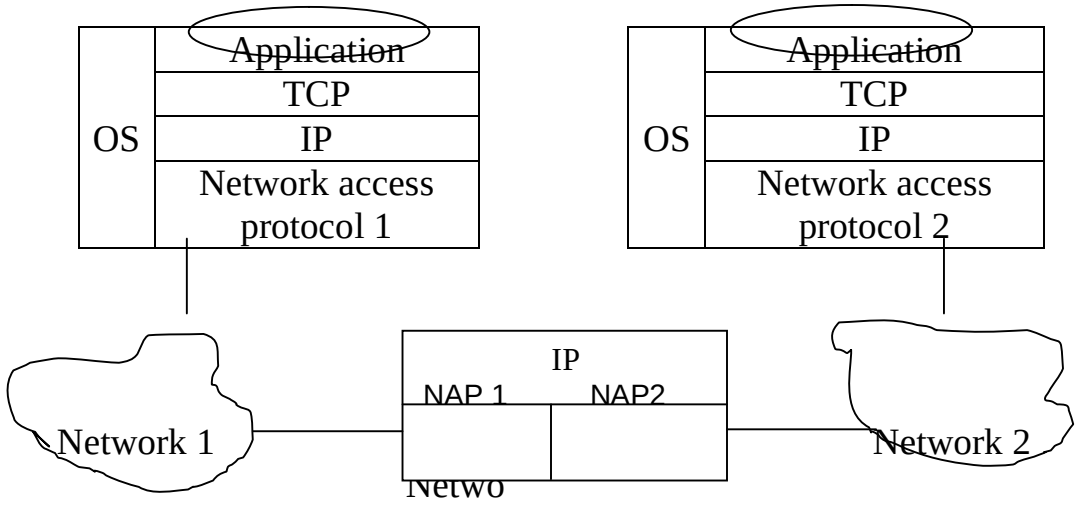
TCP: Transmission Control Protocol

IP: Internet Protocol

- The TCP/IP protocol architecture is based on a view of communication that involves three agents: processes, hosts, and networks
- Communication between processes takes place across networks to which the hosts are attached
- A network need only be concerned with routing data between hosts, as long as the hosts agree how to direct data to processes
- It is natural to organize protocols into four layer

i. Network access layer: contains those protocols that provide access to a communication network
ii. Internet layer consists of the procedures required to allow data to traverse multiple networks between hosts
iii. Host_host layer: containts protocol entities with the ability to deliver data between two processes on different host computers
iv. Process/ application layer: contains protocols for resource sharing and remote access

b. Operation of TCP/IP



Communications using the TCP/ IP protocol architecture

NAP: Network Access Points

- IP is implemented in all of the end systems it keeps track of blocks of data to ansure that all are dilivered veliably to the appropriate application
- For successful communication, every entity in the over all sys must have a unique address, two level of addressing are needed
  - Global Internet Address(for communication)
  - Ports(for service)

Try your best, you will get the best!

Contents

BOOK I: Computer system fundamentals.

BOOK II: Computer systems architecture.

Cách xóa Windows Media Player 11

1a. Cho ai cài wmp11 đàng hoàng:

Code:
"C:\Program Files\Windows Media Player\Setup_wm.exe" /Uninstall

1b. Cho ai cài wmp11 lậu, đổi **C:\Program Files\Windows Media Player** thành link đường dẫn đến folder chứa wmp11 (đã giải nén khi cài lậu).... copy thế vô đoạn trên

2. Vào Start - Run, nhập từ **"** đến **uninstall** -----> enter.. nó sẻ xuất hiện popup nói là sau khi uninstall wmp11, nó sẻ trở về version trước khi install wmp11 (có thể là wmp9 hoặc 10)... click YES - DONE

Làm gì khi máy tính bỗng nhiên chậm chạp? - 19/10/2006 11h:21

1, Virus và Spyware: Ngoài một số tác hại tiêu cực, khi hoạt động virus thường chiếm một lượng tài nguyên nhất định trong máy tính và làm máy chậm chạp.

Hãy "sơ cứu" bằng cách chấm dứt các process khả nghi bằng *Task Manager*, dừng thực thi một số dịch vụ (service) bằng *Management Console*, gỡ bỏ các chương trình tự động khởi động *System Configuration Utility*… và cập nhật ngay các chương trình chống virus, chống spy để rà soát virus trên máy. Một số loại virus phải cần một số công cụ đặc biệt để phát hiện, nếu bạn nghi máy mình bị nhiễm, hãy dò tìm trên website của các hãng bảo mật như Symantec, Mcafee, BitDefender…

2, Quá "nhiệt" vi xử lý: Đôi khi vì một lý do nào đó, quạt CPU của bạn không chạy, gây ra quá nhiệt ở CPU. Vậy thì bạn nên mở thùng máy và kiểm tra lại hệ thống tản nhiệt. Chương trình theo dõi nhiệt độ cũng có thể giúp bạn phần nào, tuy nhiên đó là những công cụ phiền phức.

3, RAM không tốt: Nếu bạn thấy quạt vẫn chạy đều, CPU vẫn mát thì hãy kiểm tra RAM. RAM bị lỗi nhẹ, máy tính sẽ không biết rằng đó là lỗi, nhưng quá trình hoạt động về lâu dài vẫn xảy ra trì trệ. Bởi thế, thử dùng các công cụ kiểm tra RAM, có sẵn trong CD Hiren để kiểm tra. Bạn cũng có thể kiểm tra thủ công bằng cách thay thế bằng một thanh RAM khác (được chắc chắn là tốt xem có cải thiện tình hình hơn không).

4, Đĩa cứng bị lỗi: Đôi khi vì một sự cố nhỏ về điện, đĩa cứng máy tính của bạn sẽ bị một vài lỗi nhỏ trên bề mặt hoặc trong hệ thống mạch điện. Thế là thay vì chỉ mất vài phần ngàn giây để đọc dữ liệu, nó phải tốn hàng giây, thậm chí hàng phút đồng hồ để đọc một lượng dữ liệu tương tự.

Trước hết, để phòng tránh tình trạng trên, bạn hãy dùng máy tính có ổn áp, hay nhất là UPS. Nếu bạn nghi ngờ đĩa cứng bị lỗi, hãy sao lưu dữ liệu dự phòng ngay lập tức và đem bảo hành. Nếu không còn bảo hành, hãy mua đĩa cứng mới, không nên tiết kiệm vài chục USD để khi hư đĩa cứng thì mất toàn bộ dữ liệu.

5, BIOS không tương thích: Đây là lỗi ít gặp, thế nhưng cũng cần phải xem xét. Một khi phần mềm BIOS không tương thích có thể dẫn tới máy tính hoạt động ì ạch hơn mong đợi. Giải pháp là cập nhật BIOS mới nhất cho bo mạch chủ, hay hơn, bạn hãy lùng trên mạng hoặc tham vấn các chuyên gia về cách tinh chỉnh các giá trị của BIOS.

6, Rà soát lại các dịch vụ đang hoạt động để xem có dịch vụ nào dư thừa không. Việc này đòi hỏi bạn có một số kinh nghiệm và kiến thức nhất định.

7, Đĩa cứng bị phân mảnh: Dùng *Windows Defragment* hoặc các công cụ dồn đĩa để xử lý tình huống này.

8, Quá nhiều trình ứng dụng: Một số người có thói quen thử sử dụng rất nhiều chương trình. Thế nhưng, họ lại không biết cách xử lý để loại bỏ hoàn toàn các chương trình đã Uninstall. Hãy dùng các công cụ quét Registry để làm máy tính sạch sẽ và khỏe mạnh hơn. Và tốt nhất là không nên cài quá nhiều chương trình ứng dụng trên một máy tính.

Trần Huy

10 cách tự động thực thi file

Tất cả các loại virus, trojan và những trình hack đều có thể tự động thực thi bất cứ khi nào máy của bạn khởi động. Những file hay folder sau đều có điều kiện thuận lợi để tự thực thi khi hệ thống khởi động.

1. C:\autoexec.bat

Nếu bạn mở file này bằng notepad thì sẽ thấy có vài lệnh dos mà phải được thi hành lúc khởi động. Vì thế nếu có mục "C:\virus_folder\virus.exe" thì virus.exe sẽ luôn luôn chạy khi bạn khởi động PC.

2. C:\windows\Start Menu\programs\startup

Bất kỳ file nào ở trong thư mục này sẽ tự động thực thi khi khởi động PC.

3. C:\windows\win.ini

Ở file này dưới phần windows nếu có mục 'run=something.exe' hoặc

'load=something.exe' thì chắc chắn something.exe đó là virus hay trojan.

4. C:\windows\system.ini

Dưới phần boot theo mặc định thì có đoạn "shell=explorer.exe". Nhưng nếu là "shell=virus.exe,explorer.exe" thì máy của bạn đã bị dính virus.

5. C:\config.sys

File này chủ yếu là chứa những mục nhập của driver. Nhưng cũng cần theo dõi đề phòng.

6. C:\explorer.exe

nếu nó tồn tại thì sẽ thực thi đầu tiên ngoại trừ trường hợp thông thường là C:\windows\explorer.exe. Có tác dụng với Windows95, 98, ME. Nên cẩn thận!
****
Tip: Tất cả những file trên có thể được mở cùng lúc bằng cách vào Start -->> Run, gõ "sysedit" (không có dấu ").
****

7. Ở Registry có thể là

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"Something"="c:\directory\Trojan.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
"Something"="c:\directory\virus.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
"Something"="c:\directory\Trojan.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
"Something"="c:\directory\Virus.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Something"="c:\directory\Trojan.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
"Something"="c:\directory\virus.exe"
****
Lưu ý: -- Chỉnh sửa registry rất là nguy hiểm. Nếu bạn không biết đó là cái gì thì đừng mở ra hay xóa nó. Chỉ cần sai một tí là phải cài lại win đó!

****

8. Registry Shell Open

[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]

Một key với giá trị "%1 %*" có đặt ở đây và đôi khi là những file thực thi nằm ở đây. Nó được sử dụng như: virus.exe "%1 %*"; và nhớ xem kỹ qua.

9. ICQ Net Detect

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]

Key này bao gồm tất cả những file được thực thi nếu ICQ phát hiện bạn đã kết nối Internet. Bạn có thể hiểu rằng chức năng này của ICQ rất thuận tiện cho attacker.

10. ActiveX Component

[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName]
StubPath=C:\directory\virus.exe

VÌ vậy nếu chương trình antivirus không phát hiện được virus hay trojan nhưng bạn vẫn còn nghi ngờ thì nên kiểm tra qua bằng những cách ở trên để chắc ràng mình đã an toàn hơn :)).
Tác giả: sưu tầm

Để có một máy tính hoàn hảo hơn

Lâu nay thấy một số bạn phàn nàn về máy tính shutdown chậm và boot chậm, nên mình viết một số hướng dẫn để các bạn có thể giúp máy chạy nhanh hơn và dễ sửa hơn khi bị hư hỏng do xung đột phần mềm.

Để máy chạy tốt, máy vi tính cần tối thiểu phải có Ram 512, 2.0Ghz, 80Gb ổ cứng, 1 software để back up ổ cứng là Ghost hay True image 9, Software chia ổ cứng và

một phương pháp sử dụng máy tính có tổ chức.

A. Ram 512, 2.0 Ghz

B. Software back up (Ghost hay True image 9), software chia ổ cứng là norton Partition magic 8.05

C. Phần này mình sẽ trình bày chi tiết như sau.

Chúng ta bắt đầu khi máy mới mua hoặc mới cài Win XP nhé.

1. Với máy mới cài Win XP, mọi việc coi như xong ở bước 1, vì các bạn chỉ mới có WinXP trong máy thôi.

Với máy mới mua về, cần phải có thời gian và kinh nghiệm bạn mới biết những software nào trong máy là cần thiết (**để giữ lại dùng**) và software nào ko cần thiết (**để uninstall đi**). Tuy nhiên mình sẽ cho bạn một số gới ý.

Tất cả các game trong máy, nếu bạn thích, thì ghi lại tên và vào các diễn đàn tin học để tìm bản đã đăng ký mà dùng, những bản kèm theo trong máy, bạn nên uninstall toàn bộ (**vì tất cả những game đó đều là bản Trial**). Riêng với bộ anti-virus và Office thì uninstall đi vì chắc chắc đó là **bản Trial** ít chức năng. Tìm bản full trên các diễn đàn và install vào mà dùng khỏe hơn.

Còn lại những software khác, bạn phải có thời gian sử dụng hoặc kinh nghiệm thì mới biết có nên uninstall ko.

2. Trên màn hình Desktop, bấm chuột phải vào **My computer**, chọn **Properties**. Một số máy mới do để style theo kiểu XP nên ko thấy thì có thể vào **Start** rồi tbấm chuột phải vào dòng chữ **My Computer**, chọn **Properties.**.

sau khi bấm sẽ hiện lên một bảng, chọn **Sytem Restore** và chọn turn off all drivers.

3. vào Star- Programs- Accessories- Sytem tools- Disk Cleanup

chọn từng ổ đĩa có trong máy, chắc chắn là ổ C trước, và đánh dấu toàn bộ các mục trong đó, sau đó chọn OK để máy tự xóa hết những cái không cần thiết.

Với máy vừa mới cài Win XP, bước này nhanh, với máy mới mua, bước này lâu

hơn một chút.

4. Vào Start- Run- gõ **msconfig**, sẽ hiện lên một bảng.
Chọn **Startup**, **bỏ trống** hết những ô trong đó ngoại trừ Sound hoặc những software bạn thấy cần thiết thôi. (bước này cần bạn phải có kinh nghiệm sử dụng qua, nhưng nếu bạn chưa sử dụng chức năng này, cứ làm thử).

Tiếp đó, chọn **Services**, trong Services đánh dâu vào ô **Hide all microsoft services**. Bỏ trống toàn bộ những ô trong đó (nhớ chỉ làm việc này sau khi ô Hide all micorsoft service đả được đánh dấu). Nếu mày của bạn có xài bluetooth thì bạn chỉ để lại mình nó thôi.

Công dụng của bước 4 là để hạn chế việc máy chạy những software ko cần thiết khi boot máy lên.

5. Thiết lập kết nối internet, download sofwares mới và Install softwares mới đó (tối cần thiết), những software khác bạn có thể cài vào khi khác.

Netscape 7.0 (một số trang web về chemistry đòi phải có Netscape và MDLChime SP6, dành cho ai học Chemistry)
Mcafee (bộ này nhẹ, dễ sử dụng, và chức năng mạnh)
Norton Partition Magic 8.05
Real Player
Acrobat Reader
Flash player
Shockwave player
Microsoft Office 2003 (bộ này chạy tốt và ổn định hơn 2007, vì 200& chỉ là beta và đòi hỏi cấu hình cao, và rất nhiều ch7úc năng vô ích mà có thể cả đời bạn ko dùng tới
Adware
Super Cleaner
Tuneup Utilities 2006
True Image 9 (hoặc Norton Ghost , mình chưa bao giờ xài Ghost nên chỉ dám giới thiệu True Image 9)
Nếu máy có DVD R/W thì nên cái thêm:
PowerDVD
CloneDVD2, phải có AnyDVD mới phá code được.
CloneCD2
Nero Burn DVD/CD

tất cả software trên tìm bảng mới nhất mà install, bạn có thể tìm trên các diễn diễn tin học. Khi install xong toàn bộ software, bạn mới nên restart lại một lần. Nếu install Mcafee hay bất cứ anti virus soft nào, bạn có thể thực hiện step 4 lần nữa, nếu bạn thích (nên làm)

6. Sau khi hoàn tất việc Install những software cơ bản trên, bạn có thể bắt đầu sử dụng chức năng **Disk defragmenter** để sắp xếp lại đĩa cho máy chạy nhanh hơn. Việc này nên làm vài lần trước khi tiếp tục step 6.

Sử dụng Partition magic 8.05 để chia ổ đĩa ra. Thông thường máy tính 80Gb có thể chia làm 3: 40Gb cho C, 20Gb cho chứa dữ liệu, 20Gb cho back up. Nhưng ổ đĩa cứng này ít được sử dụng nhiều vì đa số máy thường có trữ lượng trên 150Gb cho máy mới. Nên chia ổ cứng ra làm 3 là thích hợp nhất. Nếu máy ổ cứng lớn 250Gb thì nên chia ổ C cũng khoảng 100Gb là vừa, 120Gb là dữ liệu và khoảng còn lại là cho back up. Như dzậy cũng có 3 ổ.

Có nhiều bạn thích dùng nhiều bản Windows khác nhau trên một máy, nhưng điều đó chẳng có ích gì. Nên sử dụng một bản WindowXP là được. (tùy ý bạn thôi, nếu bạn thích nghiên cứu)

Việc chia ổ đĩa bằng Partition magic 8.05, nếu trên diễn đàn có bạn hướng dẫn, mình sẽ add link vào để bạn đọc, nếu ko có, mình sẽ viết riêng một bài để bạn dễ làm hơn.

7. Sau khi chi ổ đĩa, máy của bạn bây giờ có 3 ổ C, D, E. Với một số máy mới của hãng, bạn sẽ có 4, vì đĩa **recovery disk D** là mặc định, bạn nên giữ nó lại cho trường hợp bạn muốn máy trở lại ban đầu như mới mua. Nhưng nếu bạn sử dụng rành rẽ rồi thì ổ đĩa này cứ để chơi, vì bạn đã có phần đĩa backup rồi (dùng Ghost hay True iamge 9)

Việc đầu tiên ở step 7 là nên tập save dữ liệu vào ổ D or G (tùy theo máy) không phải ổ C chứa bản Window là được. Rất có nhều bạn sử dụng Microdoft Office (Word, Excel...) để viết bài, và save trong **My Document**. Nhưng lỡ máy hư thì hỡi ôi, công sức bỏ sông bỏ biển.

Tùy theo ý thích, nên đặt tên các folder là a1, a2, a3.... Tromg mỗi a folder, bạn có thể chia nhỏ theo tên của từng folder file mà bạn muốn. Việc chia như dzậy sẽ giúp

bạn dễ phân loại và dễ tìm hơn.

8. Những icon của software nào đã có ở Desktop bạn có thể xóa bớt những link của nó trong Programs. Vd bằng hình cho dễ hiểu.

mình có xài một số softs nhưng cái nào có ngoài desktop thì minh xóa trong Programs, nên nó gọn có chút xíu như dzậy thôi.

9. Sau khi xong step 8, bạn nên chạy T**uneup utilities 2006** vài lần để fix các lỗi. Update Adware, Anti-virus.

Tắt Internet. Chạy Adware, Antivirus, Disk Defragment lần nữa để bảo đảm máy sạch và gọn gàng. Sau khi quét virus xong, bạn có thể thực hiện lại step 4 nếu bạn ko muốn Anti virus chạy boot máy.

10. Sau khi hoàn thành xong step 9. Máy của bạn rất ổn định, hãy tạo **backup** cho ổ C vào lúc này. **Nhớ, muốn back up ổ C**([COLOR=Blue]dùng Norton Ghost hay True Image 9), nên quét virus và Disk defragment trước khi tạo backup[/COLOR], nếu ko, bạn back up cả virus vào thì mất công thêm. Dữ liệu đã nằm ổ D, nếu bạn có dữ liệu quá lớn, nên mua thêm một ổ đĩa để tạo back up dữ liệu đề phòng. Nếu dữ liệu ko đáng kể (chỉ softwares), nên chép nó vào DVD. Khoảng vài cái DVD là bạn có thể copy toàn bộ các dữ liệu thông thường. Nhưng dữ liệu sẽ ko mất vì nằm khác ổ đĩa. Nên bạn có sử dụng chức năng Recovery disk (của **Ghost hay True Image**, **phải sử dụng đúng cách nhé**, **không phải Recovery của máy sẵn có**).

nên để bản backup là bản tối thiểu mà bạn thấy ổn định cho máy. Mình đã gợi ý cho bạn ở step 5. Nếu máy của bạn mạnh, có thể cài thêm Photoshop. Tuyệt đối ko cài backup Games, vì Games chỉ làm nặng máy và install lúc nào cũng được. bản backup là bản đơn giản nhưng đầy đủ chức năng. Một số bạn có thói quen backup hết, cứ sợ sẽ mất hết dữ liệu hằng ngày (thói quen này chỉ cho máy làm việc ở công sở thôi), còn máy ở nhà không cần. Vì dữ liệu đã save ở ổ cứng khác, nên chỉ cần một bản tối thiểu ổn định là được.

nên chạy
Disk Defragment 1lần/ngày
Adware sau khi ko xài internet nữa (nếu quét mà ko hết, nên tắt internet trước khi quét, nhớ update trước khi quét)

Antivirus 1tuần/lần (update trước khi quét)
Super cleaner(tùy thích)

Ở đâu có dữ liệu, ở đó có chuyện

Các dịch vụ trực tuyến mới có thể biến bạn thành "miếng mồi ngon" cho các cuộc tấn công dữ liệu cá nhân.

Việc lưu trữ email, văn bản, hình ảnh và thông tin cá nhân ngày càng nhiều trên mạng có gì nguy hiểm? Các chuyên gia đưa ra nhiều tình huống và miêu tả điều gì có thể xảy ra trong vài năm tới nếu các xu hướng cải tiến công nghệ và chính sách chung trong 3 lĩnh vực nóng - lưu trữ trực tuyến, giám sát vị trí và sinh trắc học - vẫn như hiện nay.

Nguy cơ từ web

Tình huống: Bạn nhận được một loạt email. Cái đầu tiên đính kèm bức ảnh tai tiếng thời trung học. Cái thứ hai trích dẫn một nội dung email chứa thông tin mật về cuộc đàm phán liên doanh của công ty bạn. Cái thứ ba sao chép một bức thư mà bạn mới gửi cho người yêu cũ.

Và email thứ tư yêu cầu bạn gửi 50.000 USD đến một tài khoản ở nước ngoài trong vòng 48 giờ; nếu không, vợ (chồng) của bạn hoặc sếp của bạn sẽ nhận bản sao của 3 email kia. Có ai đó biết được những thông tin quan trọng của bạn trên mạng và đang dùng chúng để tống tiền. Bạn không biết tại sao mình lại trở thành mục tiêu!

Từ năm 2005, Google và bộ ứng dụng nền web Microsoft Windows Live cùng hiện thực một ý tưởng là đưa toàn bộ ứng dụng nghiệp vụ thành trực tuyến; và các máy trạm làm việc sẽ không cần gì khác ngoài trình duyệt web. Tiếp ngay sau đó, một hệ thống hoạt động đa nền tảng xuất hiện để kết nối với TV, xe hơi, điện thoại di động và đầu DVD. Việc truy cập tức thời và dễ sử dụng của nó đưa đẩy bạn lưu những tư liệu quan trọng, hình ảnh... trên các máy chủ ở đâu đó.

Giống như vô số người khác, bạn tin tưởng các nhà phát triển tên tuổi của HĐH mới và các ứng dụng web sẽ bảo mật an toàn cho dữ liệu của bạn. Nhưng khối lượng thông tin giá trị mà họ lưu trữ hấp dẫn các tổ chức tội phạm chuyên ăn cắp dữ liệu trên mạng. Các tổ chức này dường như luôn tìm ra cách để vượt qua các công nghệ bảo mật mới nhất.

Nguyên do: Theo Jon Callas, giám đốc kỹ thuật của PGP Corporation, điều gây lo ngại nhất bao trùm hết mọi thứ, từ web mail đến tìm kiếm, bảng tính và HĐH web... đó là có bao nhiêu thông tin của bạn nằm trong tay người khác và vì vậy không thực sự thuộc về bạn. Tất cả mọi thứ đều diễn ra trên server của họ, làm sao bạn có thể kiểm soát?

Ngay cả khi Google cam đoan không bao giờ dò xét hay bán dữ liệu của bạn, bạn vẫn phải đối mặt với các nguy cơ từ tin tặc, đồng nghiệp láu cá và cả từ luật pháp. Các điều luật về quyền riêng tư của Mỹ ít bảo vệ dữ liệu lưu trên server của bên thứ ba hơn dữ liệu lưu trên đĩa cứng riêng.

Tiện lợi so với giám sát

Tình huống: Cảnh sát xuất hiện tại nhà bạn đồng thời hộp thư của bạn tràn ngập quảng cáo đồi trụy - chỉ vì bạn đã từng lái xe đến siêu thị mua một món quà lưu niệm và bị lọt vào "tầm ngắm" của hệ thống giám sát không dây (viễn cảnh năm 2020).

Vào sáng thứ 7, bạn nhảy lên xe hơi và kết nối mạng bằng điện thoại Internet tốc độ cao mới mua để tải về bản đồ lưu thông theo thời gian thực và hướng dẫn đến siêu thị theo đường ít kẹt xe nhất. Để tìm cửa hàng nữ trang, bạn tải về sơ đồ của siêu thị vào điện thoại. Các hướng dẫn ngoằn ngoèo sẽ "dắt" bạn qua khu bán đồ lót mới mở, loanh quanh vài giây rồi bạn cũng đi đến đúng cửa hàng nữ trang, và trong 15 phút bạn mua sắm xong.

Một lát sau, bạn bắt đầu nhận các tin nhắn chào bán các thứ "đồ chơi người lớn" (đồi trụy). Khi bạn đi lạc ở khu bán đồ lót, thiết bị giám sát của cửa hàng phát hiện điện thoại của bạn qua sóng Bluetooth và tự động mua thông tin về bạn từ các nhà cung cấp dữ liệu. Giờ thì hội viên của nó, những người bán "đồ chơi người lớn", có thể hợp pháp tiếp thị đến bạn qua email hay tin nhắn.

Mặt tối của sinh trắc

Tình huống: Bạn ham một máy ảnh 20 megapixel giá hời và bị lừa vét sạch tài khoản ngân hàng. Thủ phạm chính là thẻ tín dụng sinh trắc, được thiết kế để ngăn tội phạm ăn cắp thông tin nhận dạng nhưng lại để tội phạm giả mạo bạn.

Vào năm 2010, sau những vụ rò rỉ hàng triệu số thẻ tín dụng, các công ty tài chính đã đưa ra loại thẻ tín dụng và ATM sinh trắc, yêu cầu vân tay của người dùng thẻ (được kiểm tra bằng bộ đọc vân tay) phải khớp với vân tay của chủ thẻ (lưu trên thẻ). Công nghệ có vẻ như chống được sự giả mạo này cất cánh, và chỉ trong vài năm các PC mới đều được trang bị bộ đọc vân tay cho phép người dùng thực hiện các giao dịch tài chính qua Internet.

Khi bạn sử dụng thẻ kiểm tra ATM sinh trắc để mua máy ảnh, bạn gửi địa chỉ IP của mình, số thẻ và vân tay số qua Internet đến máy chủ thẻ tín dụng. Nhưng thông tin của bạn bị "xem trộm" trên đường truyền và được rao bán trên mạng. Giờ thì ai đó đã rút hết tiền trong tài khoản của bạn, và bạn không thể chứng minh đó không phải là bạn vì vân tay của bạn hiện diện trong tất cả các giao dịch.

Cuối cùng vấn đề cũng được giải quyết ổn thỏa. Nhưng kể từ đó, bạn lại thích hình thức thanh toán lạc hậu: tiền mặt.

Nguyên do: theo Callas của PGP, cơ hội cho tội phạm là lớn và rủi ro cho người có thẻ là rất cao vì người ta thường tin tưởng vào sinh trắc.

Tiếp nữa, hai viên cảnh sát xuất hiện ở nhà bạn giải thích rằng trên đường đến siêu thị, bạn đã đi qua một cửa hàng bán rượu bị hôi của. Thủ phạm tẩu thoát trong một chiếc xe hơi trắng, và các bộ cảm biến trên đường ghi nhận xe của bạn là một trong 10 xe như vậy trong khu vực.

Mặc dù chuyến viếng thăm của cảnh sát chỉ là vấn đề thủ tục, mặc dù bạn có thể dễ dàng yêu cầu ngưng gửi quảng cáo bậy bạ, nhưng giờ đây bạn đã bớt ngưỡng mộ các thiết bị không dây. Bạn ước gì, khi mua chúng và đăng ký dịch vụ, bạn được quyền chọn không cho chia sẻ thông tin cá nhân.

Nguyên do: Việc đi ngang qua cửa hàng đồ lót có thể cho phép người chủ cửa hiệu gửi email cho bạn. Theo chuyên gia về quyền riêng tư của đại học luật California-Berkeley School of Law: các điều luật chống spam, fax quảng cáo và tiếp thị từ xa, tất cả đều có kẽ hở. Chỉ cần bạn lái xe vào bãi đậu xe của công ty bán đồ thể thao là công ty này có thể xem như bạn muốn mua đồ.

Hệ thống thu cước tự động như E-Zpass gắn thiết bị RFID để thu thập thông tin về xe. Hiện tại, các bộ cảm biến chỉ thu thập dữ liệu vô danh, nhưng điều gì sẽ xảy ra nếu luật pháp cho phép sử dụng dữ liệu này để điều tra tội phạm?

PC World Mỹ 11/2006

Mười cách miễn phí giữ cho máy tính của bạn an toàn - 25/8/2006 6h:44

Bạn không phải vận dụng sự mẩy rủi để bảo vệ máy tính của mình tránh virus, trojan, phisher, scammer hay snoop. Và trong thực tế, bạn cũng chẳng phải mất một đồng xu nào cả.

Từ khi bật cho đến khi tắt, máy tính của bạn luôn nằm trong nguy cơ bị tấn công. Các hacker thì cố gắng phá nó; virus, trojan và các sâu cố gắng thâm nhập vào máy; còn spyware thì lại cố gắng tìm hiểu mọi việc bạn đang làm. Sau đó là những những nguy hiểm của mạng không dây và tệ nhất là sự dòm ngó của đồng nghiệp.

Bạn phải làm gì đây? Bạn có thể tiêu tốn hàng trăm, hàng nghì đô la cho các phần mềm và dịch vụ, thêm vào nữa là vô số thời gian chỉ để giữ cho chiếc máy yêu quý của bạn được an toàn. Chúng tôi sẽ chỉ cho các bạn mười bước đơn giản bảo vệ máy tính mà không mất một xu nào.

10 cách miễn phí giữ cho máy tính của bạn an toàn

1. Sử dụng phần mềm diệt virus và chống spyware miễn phí

Nếu bạn muốn bảo vệ máy tính của mình chống virus, bạn có thể phải trả tiền nhiều lần. Các hãng cung cấp phần mềm diệt virus hiện đang bán với mức phí như hàng năm. Chúng không phải chỉ có một cái giá, vì thế cái giá cuối cùng mà bạn mua được có khi lên đến hàng trăm đô la.

Đó là khi bạn còn biết phải dùng chương trình nào. Các công ty như McAfee và Symantec bán theo kiểu này. Tuy nhiên, thực tế có hai chương trình diệt virus miễn

phí với đầy đủ tính năng cần thiết như của các hãng khổng lồ kia. Chẳng hạn như chức năng luôn tự động ngăn ngừa virus trong mọi thời điểm, quét virus và tự động cập nhật phiên bản mới nhất

Một chương trình là AVG Anti-Virus Free của Grisoft có kèm theo cả chương trình chống spyware. Cả hai đều miễn phí, không mang tính thương mại và dùng cho các máy tính cá nhân gia đình.

Chương trình thứ hai được dùng phổ biến hơn là Avast 4, cũng miễn phí và không mang tính thương mại. Avast thậm chí có thể làm việc được với phiên bản beta của Windows Vista, điều mà không phải chương trình diệt virus nào cũng có thể làm được.

Để chống spyware, có rất nhiều chương trình miễn phí. Trong đó Ad-Aware Personal và Spybot Search & Destroy là những sự lựa chọn xuất sắc. Cả hai đều là chương trình bảo vệ giống như Microsoft's Windows Defender. Các chương trình chống spyware không phải lúc nào cũng bắt được cùng một loại malware. Vì thế các bạn nên quét máy thường xuyên với ít nhất là hai chương trình cũng một lúc.

Chương trình bảo vệ Windows Defender. Phần Software Explorer thể hiện tất cả các chương trình đang chạy trong máy và cho phép bạn loại trừ bất cứ cái gì có thể là mailware.

Kiểm tra bảo mật và trình bảo vệ mạng không dây

2. Kiểm tra độ an toàn trực tuyến

Bạn sẽ an toàn đến mức nào khi lướt web? Để biết điều đó các bạn có thể tìm các chương trình kiểm tra an toàn trực tuyến miễn phí. Shields Up là sự lựa chọn đầu

tiên mà bạn nên vào vì nó giúp bạn biết được khả năng chống lại các hacker, những kẻ tò mò và tội phạm máy tính trên máy của bạn. Chương trình mang lại cho máy tính của bạn những phân tích tỉ mỉ và một loạt các bài kiểm tra. Chẳng hạn kiểm tra các cổng Internet, xem liệu máy của bạn có ở chế độ "stealth" (chế độ an toàn nhất) hay không, và liệu nó có đáp ứng câu lệnh ping hay không (ở chế độ an toàn nhất, nó sẽ không đáp ứng). Nó cũng cung cấp các hướng dẫn tắt máy của bạn nếu máy tính của bạn bị bật bởi những kẻ nguy hiểm.

Thành công! Các ô vuông xanh chỉ rằng bạn đã ngăn chặn thành công hacker, cracker, snooper

Symantec cũng đưa ra một chương trình kiểm tra an toàn trực tuyến, nhưng đừng ngạc nhiên nếu bạn thường xuyên được khuyên là nên mua phần mềm bảo mật của hãng. Tương tự, McAfee cũng có một chương trình quét Wi-Fi miễn phí để kiểm tra độ an toàn trong kết nối không dây. Khi thử dùng chương trình này của McAfee, bạn cũng đừng "shock" nếu được khuyên nên mua McAfree Wireless Home Network Security để giải quyết được nhiều vấn đề hơn. Tuy nhiên, ngoài việc mua các chương trình của các hãng lớn bạn còn có nhiều lựa chọn khác trong việc bảo vệ máy tính của mình.

3. Sử dụng phần mềm bảo vệ mạng không dây miễn phí

Hầu hết các mạng gia đình đều rất dễ bị tấn công bởi các "war drivers", đó là những lỗ hổng giúp cho các hacker thâm nhập, phá hoại mạng không dây của bạn. Có rất nhiều cách bạn có thể thực hiện với những thiết lập của router để tự bảo vệ chính mình.

Nhưng bạn không muốn loanh quanh với bộ lọc địa chỉ MAC , thay đổi SSID (tên mạng) hay vô hiệu hoá tên quảng bá SSID? Vậy bạn nên sử dụng một chương trình bảo mật miễn phí có thể thực hiện những việc đó thay cho bạn. Network Magic là

sự lựa chọn tốt với hai phiên bản, miễn phí và trả tiền. Nếu tất cả việc bạn muốn làm chỉ là cấu hình lại mạng không dây với mức an toàn cao nhất thì phiên bản miễn phí là đủ.

Sau khi cài đặt, nó sẽ kiểm tra router, toàn bộ mạng và xây dựng một bản đồ mạng với tất cả các thiết bị kết nối bên trong. Sau đó nó kiểm tra các thiết lập bảo mật cho router và ghi lại những gì nó tìm thấy. Ví dụ, nếu nó phát hiện ra bạn đang quảng bá SSID của bạn, nó sẽ cảnh báo bạn. Chỉ cần một cú nhấp chuột vào hộp checkbox, Network Magic sẽ ngưng ngay việc quảng bá cho bạn.

Network Magic sẽ giúp bạn cấu hình lại bộ định tuyến không dây với mức an toàn cao nhất.

Phiên bản trả tiền có thêm một số tính năng khác như cấu hình cho thư mục và chia sẻ máy in, nhưng nếu bạn chỉ quan tâm đến vấn đề bảo mật thì bạn không cần dùng đến phiên bản đó.

Firewall miễn phí và mã hoá dữ liệu

4. Dùng tường lửa

Sử dụng tường lửa là tuy rất đơn giản nhưng lại là cách tốt nhất giúp bạn chống lại Trojan, virus, worm. Nó có thể ngăn chặn các cuộc tấn công từ xa của hacker, sự xâm nhập của các sâu máy tính.

Nếu bạn sử dụng Windows XP Service Pack 2 thì bạn đã có một nữa mục đích mà bạn cần. (Còn nếu chưa có, bạn hãy vào Windows Update để cập nhật).

Mặc định sau khi bạn cài SP2, tường lửa sẽ được bật. Nếu bạn nghi ngờ nó đột nhiên tắt, bạn có thể kích vào biểu tượng *Security Center* trên khay hệ thống để kiểm tra, màn hình *Security Center* sẽ hiện ra. (Nếu biểu tượng *Security Center* không xuất hiện thì bạn vào *Control Panel -> Security Center*). Để ý phần trên cùng trong màn hình *Security Center* (phần Firewall) để kiểm tra chắc chắn tường

lửa đang bật. Nếu nó chưa được bật bạn hãy kích vào biểu tượng Windows Firewall ở bên dưới, chọn On -> OK. Tường lửa sẽ được bật.

Ít nhất hãy chắc chắn tường lửa đang được bật trong Windows XP

Nhưng tường lửa được thiết lập sẵn trong Windows XP chỉ thực hiện được các chương trình bảo vệ một chiều, hay nói cách khác nó chỉ block được các kết nối vào mà không kiểm tra các kết nối ra. Spyware và Trojan thường thực hiện các cuộc "phone home" để tạo ra các kết nối ra từ máy tính của bạn mà bạn không biết. Nếu bạn muốn block cả các kết nối ra thì bạn cần tường lửa hai chiều. Phần mềm miễn phí tốt nhất mà bạn cần là ZoneAlarm, có thể tìm nó trên trang web Zone Labs. Nếu bạn chỉ cần tìm tường lửa hai chiều thì không cần phải mua phiên bản phải trả tiền vì phiên bản này chỉ bổ sung thêm một số tính năng thành phần mở rộng.

Với những người dùng hệ điều hành Windows cũ thì không có nhiều chương trình diệt virus và spyware miễn phí tương thích cho họ. ZoneAlarm không hỗ trợ trong Windows 98 hay ME. Vì thế nếu bạn đang dùng các hệ điều hành này bạn cần phải bỏ tiền mua một số Firewall như Norton Personal Firewall của Symantec hay PC-cillin Internet Security của Trend Micro.

5. Mã hoá dữ liệu

Bạn đã thiết lập chế độ cấm người khác truy cập máy tính của bạn nhưng cũng chẳng ngạc nhiên lắm nếu vẫn có kẻ thâm nhập và sử dụng nó được một cách thoải mái. Đó có thể là một hacker, hoặc ai đó đang cùng sử dụng mạng với bạn hay thậm chí là người đồng nghiệp ngồi cạnh khi bạn đi ra ngoài.

Vậy giải pháp nào cho các vấn đề đó? Mã hoá dữ liệu là một phương pháp khá hiệu quả. Hầu hết các chương trình mã hoá dữ liệu đều cần phải trả tiền. Hơn nữa lại không dễ dùng. Nhưng Cryptainer LE của Cypherix vừa đơn giản lại miễn phí. Cài đặt nó và bạn sẽ có một bộ mã hoá mới. Nó sẽ tạo hoặc chuyển các file vào bên trong bộ đĩa và mã hóa chúng trong chớp mắt. Bạn vẫn có thể làm việc với

chúng bình thường như với các file khác mà không cần dùng mật khẩu.

Khi bạn muốn bất kỳ file hay thư mục nào được ẩn đi trước những con mắt tò mò, hãy kích chọn chúng, sau đó bấm nút Unload trong Cryptainer LE. Tự nhiên chúng sẽ biến mất. Muốn chúng xuất hiện lại, kích vào nút Load và gõ mật khẩu. Chỉ những ai có mật khẩu thì mới có thể nhìn thấy chúng.

Bảo vệ dữ liệu
của bạn trước các
conmắt tò mò với
phần mêmf miến
phí Cryptainer LE

Phần mềm này cũng rất hữu ích với những ai dùng ổ cứng di động USB để lưu trữ dữ liệu. Bạn có thể mã hoá toàn bộ ổ. Nếu chẳng may bạn mất ổ thì cũng không ai nhìn thấy file trong đó.

Bảo vệ máy tính trước các phishing và các file bảo mật

6. Bảo vệ chính mình trước các phisher

Phishing là một trong những cách tấn công quỷ quyệt và hiểm ác nhất. Bạn đang xem một email xác nhận từ ngân hàng, eBay, PayPal hay các hãng tài chính khác cảnh báo rằng bạn phải kích vào một liên kết để đăng nhập vào tài khoản của bạn với một số lý do nào đó như cập nhật, kiểm chứng thông tin hay thậm chí với mục đích bảo vệ.

Sau khi kích xong, bạn vào website mà bạn nghĩ là thật nhưng lại không phải (thực ra là chỉ giống về mặt giao diện). Sau khi đăng nhập bạn có thể được yêu cầu cung cấp thêm thông tin cá nhân như mã số phúc lợi xã hội và kết quả là bạn sẽ phải "tạm biệt số tiền của mình". Một kẻ lừa đảo nào đó đã gửi mail và cài website giả, dùng các thông tin cá nhân bạn nhập vào để lấy hết tải khoản và ăn trộm nhận dạng của bạn.

Có một vài cách đơn giản ngăn chặn các cuộc tấn công phishing là: Đừng bao giờ kích vào đường link đăng nhập từ một e-mail do các hãng tài chính, eBay hay PayPal gửi. Đừng quan tâm đến vẻ hợp pháp của nó, thay vào đó bạn hãy vào

website và tự mình đăng nhập.

Thứ hai, dùng một thanh công cụ chống phising. Nó sẽ block các trang có phishing mà bạn vào hoặc sẽ cảnh báo nếu bạn đang ghé thăm một website phishing. Bạn có thể dùng Google Toolbar chẳng hạn. Sau khi bạn cài đặt thanh công cụ, kích vào nút "*Option*". Sau đó, dưới tab "*Browsing*", đánh dấu chọn vào ô ngay cạnh "*Safe Browsing*". Kích vào nút "*Save Browsing Settings*" và cấu hình lại mức bảo vệ bạn muốn. Cuối cùng kích vào nút "*OK*".

Đừng có đi vào đây! Goolgle với thành phần chống phishing để bảo vệ bạn từ những kẻ lừa đảo phishing

Một thanh công cụ chống phishing khác cũng rất tốt là Netcraft Toolbar cũng với các chức năng bảo vệ tương tự.

Nhưng chẳng mấy chốc bạn sẽ không cần bất cứ thanh công cụ nào như thế. Vì cả Internet Exporer 7 và Firefox 2.0 đều sẽ có chức năng chống phishing ngay trong trình duyệt. Trong những thử nghiệm sơ bộ, tùy chọn chống phishing trong IE7 "bắt" được nhiều cuộc tấn công phishing hơn Firefox 2.0. Nhưng cả hai sản phẩm đều mới chỉ là phiên bản beta.

7. Vô hiệu hoá việc chia sẻ file

Có một mối nguy hiểm an ninh lớn nhất là bạn có thể mắc phải nhưng bạn không hề biết, thậm chí có khi bạn còn không biết mối đe doạ đó như thế nào. Đó là việc chia sẻ file và folder. Nếu bạn để chế độ chia sẻ thì người khác sẽ cực kỳ dễ dàng xem qua tất cả các file của bạn, thu thập thông tin và thậm chí xoá các file và folder đó, nhưng có khi bạn đang ở chế độ đó mà không biết mình đang bật nó.

Rất dễ dàng để xác định và sau đó là tắt chế độ chia sẻ đó đi. Mở Windows Explorer, xem tất cả các thư mục của bạn. Bất kỳ folder nào có một bàn tay nhỏ bên dưới nghĩa là nó được chia sẻ. Bất kỳ ai kết nối tới mạng của bạn đều có thể

truy cập vào nó. Để tắt chế độ này, kích phải vào thư mục, chọn "*Sharing and Secur*ity", kích vào tab "*Sharing*", chọn "*Do not share this folder*" và kích "*OK*".

Cách tắt tất cả các
file hay folder
chia sẻ

Khi một thư mục được chia sẻ, tất cả các thư mục con bên dưới của nó cũng tự động được chia sẻ. Nhưng những thư mục con đó không có hình bàn tay thể hiện hay bất cứ dấu hiệu nào chỉ ra rằng nó đang được chia sẻ trong tab "Sharing". Vì thế hãy cẩn thận xem xét các thư mục từ trên xuống xem liệu chúng có bị chia sẻ hay không. Và hãy kiểm tra thường xuyên để chắc chắn rằng ổ gốc của bạn không bị chia sẻ. Nếu không người khác có thể truy cập tất cả các thư mục và file trên máy tính của bạn.

Web nặc danh và những cookie nhàm chán

8. Lướt web nặc danh

Khi bạn lướt web, cuộc sống của bạn như một cuốn sách mở. Các website có thể dò ra những "*chuyến du lịch trực tuyến*" của bạn, biết được hệ điều hành và trình duyệt bạn đang dùng, tìm ra tên máy, phát hiện ra website cuối cùng bạn ghé thăm, kiểm tra History của IE và lấy ra mọi thứ từ trong bộ nhớ cache. Họ cũng có thể kiểm tra địa chỉ IP để biết các thông tin cơ bản về bạn như khu vực địa lý và một thông tin linh tinh khác.

Nhưng nếu thích bạn có thể lướt web một cách nặc danh để các trang web không thể bắt được IP hay bất cứ thứ gì từ bạn. Có rất nhiều phần mềm bạn có thể mua để hỗ trợ vấn đề này. Nhưng bạn tội gì không thực hiện việc đó miễn phí bằng cách đặt proxy nặc danh nằm giữa máy của bạn và Web site bạn đang ghé vào. Khi bạn dùng một dịch vụ proxy nặc danh, trình duyệt của bạn sẽ không liên hệ trực tiếp với website. Proxy server hoạt động như một bộ đệm. Có nghĩa là website sẽ xem địa chỉ IP của proxy chứ không phải của máy bạn. Website không thể đọc được cookie, History hay kiểm tra clipboard và bộ nhớ Cache vì máy tính không trực

tiếp kết nối với nó. Bạn lướt web mà không để lại dấu vết gì.

Bạn có thể thử với website The Cloak. Kích vào liên kết "Surf" bên trái. Từ đó, đánh địa chỉ URL bạn muốn ghé thăm. Website sẽ hoạt động như một proxy và ẩn tất cả thông tin của bạn.

Lướt web nặc
danh mà không
phải trả một đồng
nào bằng cách
dùng The Cloak

Nếu muốn bạn có thể tự thiết lập để trình duyệt của bạn dùng một proxy server nặc danh. Tìm một proxy nặc danh tại AiS Alive Proxy List. Ghi lại địa chỉ IP của server và các cổng mà nó dùng (Ví dụ, trong danh sách 24.236.148.15:80, địa chỉ IP là 24.236.148.15 và số cổng là 80).

Sau đó, trong *Internet Explorer*, chọn *Tool -> Internet Option* kích vào tab *Connections -> LAN Settings*, đánh dấu chọn vào hộp "*Use a proxy server for your LAN*".

Trong *Address*, đánh địa chỉ IP của proxy server, trong *Port* nhập địa chỉ cổng của nó, đánh dấu chọn vào hộp "*Bypass proxy server for local addresses*" (Bạn không cần phải để lại thông tin nặc danh trong mạng cục bộ) -> Kích *OK* hai lần để đóng hộp thoại.

Trong Firefox, chọn *Tool -> Options -> General -> Connection Settings*; kích vào nút "*Manual proxy configuration*", nhập thông tin proxy và kích *OK* hai lần.

9. Nói không với Cookie

Các mạng quảng cáo trực tuyến có khả năng tạo ra các profile khá chi tiết về các trang web bạn hay ghé thăm và sở thích cá nhân của bạn. Họ sử dụng các trò gian trá ư? Không, họ chỉ đặt các cookie trên ổ cứng và theo dõi các website bạn hay vào.

Bạn có thể ngăn chặn bằng cách đặt tuỳ chọn *opt-out* cookie. Tuỳ chọn này do

chính các mạng quảng cáo cung cấp.

Ví dụ như để thoát khỏi mạng quảng cáo trực tuyến khổng lồ DoubleClick, bạn hãy vào trang opt-out của hãng, kích vào nút "*Ad Cookie Opt-Out*" ở cuối màn hình.

Một số mạng quảng cáo khác cũng cho phép bạn loại bỏ các cookie. Để biết thêm chi tiết bạn có thể vào Network Advertising Initiative, đánh dấu chọn vào hộp *Out-box* bên cạnh bất kỳ mạng quảng cáo nào bạn muốn, sau đó kích vào nút Submit.

Loại bỏ coookies
bằng chức năng
opt –out của các
mạng quảng cáo

Những nguy hiểm trên ebay

10. Bảo vệ mình trước nguy cơ "*Nigerian Scams*" trên eBay

Kiểu lừa đảo thư điện tử "*Nigerian scams*" được biết đến nhiều nhất và lâu nhất trên mạng Internet. Khi gửi một e-mail yêu cầu giúp đỡ chuyển hàng triệu đô la ra khỏi Nigerian, không hiểu sao tài khoản ngân hàng của bạn trống rỗng.

Thực ra đã có sự tham gia của những kẻ lừa đảo và hiện nay "*Nigerian scams*" đang phổ biến rộng rãi trên eBay. Chúng đang nhắm tới người bán chứ không phải người mua.

Vậy chúng hoạt động như thế nào? Bạn đặt ra một giá vào hộp đấu giá. Tại cuối phiên đấu giá người đặt ra giá cao nhất sẽ liên hệ với bạn và yêu cầu bạn chuyển hàng hoá tới Nigeria hay bất kỳ nước nào khác. Thông thường một câu chuyện kỳ lạ đi kèm, phổ biến là câu chuyện có một người mua sống ở Mỹ nhưng vừa nhận nuôi một đứa trẻ ở Nigeria và đang cần hàng hóa để gửi trực tiếp cho đứa trẻ.

Người thắng trong cuộc đấu giá sẽ gửi cho bạn thông tin nhận dạng PayPal, nói rằng khoản giá đó đã được trả. Hoặc anh ta gửi cho bạn một thư điện tử nói rằng anh ta sẽ trả tiền nhanh nhất sau khi anh ta nhận được hàng hoá đó. Và anh ta sẽ trả bạn qua PayPal.

Chuyển hàng và kết quả là bạn đã bị lừa. Thông tin nhận dạng trên PayPal thực tế là giả mạo. Và tất nhiên nếu bạn chuyển trước khi nhận tiền thì bạn sẽ không bao giờ được nhận khoản đó nữa.

Ngăn chặn hành vi này như thế nào? Đầu tiên, đừng bao giờ chuyển hàng trừ khi bạn kiểm chứng được là bạn đã được thanh toán. Đừng tin vào e-mail của người mua hay từ chính hãng PayPal nếu như các thư đó nói rằng có một khoản đã thanh toán. Thay vào đó hãy tự đăng nhập vào PayPal và kiểm tra lại xem bạn có thêm khoản nào không.

Thứ hai, chỉ bán hàng hoá cho những người sẵn sàng mua tại các phiên đấu giá khác. Những kẻ lừa đảo thường tạo ra các tài khoản mới và các tài khoản này có con số hoạt động là 0. Nếu bạn nhìn thấy mức khởi xướng cao mà con số hoạt động của tài khoản là 0, hãy vào trang web: http://offer.ebay.com/ws/eBayISAPI.dll?CancelBidShow và loại bỏ kẻ mua giả mạo đó

Nhưng những kẻ lừa đảo cũng nhận ra rằng con số hoạt động trong tài khoản có thể chống lại họ. Vì thế họ mua một số hàng hoá ở mục "*Buy It Now*" với mức 99 cent nhằm xây dựng một chương trình hoạt động hợp lý cho tài khoản. Bạn hãy kiểm tra các chi tiết trong hoạt động của người mua hàng. Nếu hầu hết các khoản mua đều nằm trong mục 99-cent Buy for now thì chắc chắn đó là kẻ lừa đảo.

Nếu biết hoặc nghi ngờ một người nào đó, bạn có thể xoá tên anh ta trong các hoạt động mua bán trong tương lai. Hãy vào http://cgi1.ebay.com/ws/eBayISAPI.dll?bidderblocklogin và block tên kẻ lừa đảo đó.

T.Thu (*Theo Informationweek*)

Kiểm soát hiệu quả tập tin và thư mục

Thực hiện: Minh Xuân

Theo lẽ tự nhiên, tập tin dữ liệu trên máy tính không bao giờ tự thu nhỏ kích thước được. Dù đó là tài liệu Word, ảnh JPEG, nhạc MP3 hay phim AVI thì những tập tin này ngày càng gia tăng kích thước và thư mục chứa chúng sẽ nhanh chóng "chén sạch" đĩa cứng của hệ thống. Để tránh cho Windows rơi vào tình trạng bị tắc nghẽn, bạn cần đến các kỹ thuật và công cụ giúp việc quản lý tập tin và thư mục hiệu quả hơn.

Bất kỳ lúc nào muốn tạo mới một thư mục, bạn có thể chọn một thư mục trong cửa sổ Explorer rồi tiếp đến chọn trình đơn File.New.Folder hoặc nhấn phải chuột lên một cửa sổ thư mục rồi chọn New.Folder. Đó chỉ là cách cơ bản nhất, ngoài ra còn ít nhất 3 phương pháp khác giúp bạn thực hiện công việc này nhanh hơn và hiệu quả hơn.

Sử dụng bàn phím: Với cửa sổ Explorer đang mở, bạn hãy nhấn <Alt>-F, rồi nhấn N và F (với Windows 98) hoặc <Alt>-F, rồi nhấn W và F (với các phiên bản Windows sau). Phím tắt này sẽ hoạt động nếu sự lựa chọn được thực thi trong cửa sổ cây thư mục ở bên trái hoặc trong cửa sổ thư mục bên phải của tiện ích Explorer. Phương pháp được nhiều người ưa thích là nhấn <Alt>-F <Enter><Enter>, mặc dù cách này chỉ hoạt động khi không có một thư mục nào được chọn ở cửa sổ bên phải. Nếu một thư mục đã được chọn thì bạn hãy hủy bỏ chọn lựa đó bằng cách nhấn <Ctrl>-<Space>, rồi nhấn <Alt>-F <Enter><Enter> để tạo một thư mục mới.

Sử dụng hộp thoại: Thanh công cụ của tiện ích Explorer vẫn còn thiếu nút nhấn New Folder (với chức năng tạo mới một thư mục mới) nhưng trong nhiều hộp thoại như Open và Save ở các ứng dụng Windows lại có chức năng đó. Nếu đang làm việc trong như Microsoft Word chẳng hạn, bạn chọn File.Save As hoặc File.Open, rồi nhấn vào nút Create New Folder (biểu tượng thư mục với hình ngôi sao ở đỉnh phía trên bên phải) ngay trên danh sách tập tin.

Tạo một trình đơn: Một cách khác là bổ sung thêm lệnh Make New Folder vào trình đơn nhấn phải hay còn gọi là trình đơn ngữ cảnh. Cách này sẽ giảm bớt phiền phức cho bạn khi phải di chuyển đến trình đơn con File.New thường rất chậm chạp. Để tạo một khoản mục mới trong trình đơn ngữ cảnh, bạn mở cửa sổ Explorer (có thể dùng phím tắt là ÿ-E cũng được) rồi chọn Tools.Folder Options. Tiếp đến, tại nhãn File Types và trong danh sách "Registered file types", bạn chọn File Folder rồi nhấn Edit (với Windows 98) hoặc Advanced (trong các phiên bản sau) để mở hộp thoại Edit File Type và nhấn tiếp New. Trong cửa sổ vừa mở ra, ở phần "Action", gõ vào tên lệnh muốn xuất hiện trên trình đơn ngữ cảnh (như New

Folder chẳng hạn), còn đối với phần "Application used to perform action" thì bạn hãy nhập vào lệnh command.com/cmd"%1\New Folder" với Windows 98/Me hoặc cmd.exe/cmd"%1\New Folder" với Windows 2000/XP (Hình 1).

Sau khi hoàn tất, nhấn OK rồi đóng các hộp thoại còn lại. Từ đây về sau, khi nhấn phải một biểu tượng thư mục nào, lệnh New Folder sẽ có mặt sẵn sàng và bạn không cần phải thao tác qua trình đơn New nữa (Hình 2). Tuy vậy, Windows không cho phép tạo hai thư mục cùng tên "New Folder" trên cùng một thư mục nên bạn phải đổi tên thư mục vừa tạo rồi mới có thể thực hiện lệnh đó một lần nữa.

Nếu gặp lỗi với Windows 98, bạn quay lại hộp thoại Edit File Type, chọn lệnh vừa tạo và nhấn Edit để sửa nội dung hoặc Remove để xóa hẳn lệnh đó. Với Windows 2000 hoặc Windows XP, bạn phải sửa lệnh đó thông qua tiện ích Registry Editor, hoặc xóa hẳn nó rồi bắt đầu lại từ đầu. Để biết thêm thông tin về việc xóa bỏ các lệnh khỏi các trình đơn ngữ cảnh, bạn có thể tham khảo bài viết "Loại bỏ chức năng không cần thiết trong menu ngữ cảnh" trên TGVT A 1/2005, t.126 hoặc tra cứu trực tuyến tại www.pcworld.com.vn với ID bài viết là A0501_126.

Hiển thị nội dung thư mục

Có một bạn đọc hỏi chúng tôi rằng anh ta đã thực hiện chép 15015 tập tin nhạc (với dung lượng khoảng 37,7 GB) vào một thư mục. Tuy nhiên, Windows XP không cho phép anh ta "dồn" thêm bất cứ tập tin nào nữa dù đĩa cứng 160GB (được định dạng theo chuẩn FAT 32) vẫn còn nhiều không gian trống. Vậy lý do là ở đâu?

Về lý thuyết, bất kỳ thư mục nào trên đĩa cứng sử dụng hệ thống tập tin FAT 32 có thể lưu trữ đến 65534 tập tin hoặc thư mục con, tuy nhiên điều đó chỉ đúng khi tên tập tin được đặt chính xác theo qui định của DOS, 8 kí tự cho phần tên và 3 cho phần mở rộng. Tổng số tập tin chứa được trong mỗi thư mục sẽ giảm xuống khá nhanh khi các tập tin đó sử dụng tên dài hơn (hầu như tất cả tập tin hiện nay đều như vậy). Do vậy, Windows sẽ không tìm thấy được tất cả các tập tin nhạc nếu bạn di chuyển chúng vào những thư mục khác nhau hoặc đặt lại cho chúng những cái tên ngắn theo đúng định dạng của DOS.

Có một điều bạn cần phải chấp nhận là nếu cứ khăng khăng muốn "nhồi nhét" càng nhiều tập tin vào trong một thư mục dung lượng lớn thì Windows XP sẽ phải thực hiện một số tính năng để giúp áp đặt thứ tự các tập tin trong đó. Trước hết, mở tiện ích Explorer, chọn thư mục mà bạn muốn sắp xếp lại và nhấn View.Chose Details.

Cuộn qua hết các danh sách thuộc tính và đánh dấu chọn những thuộc tính mà bạn cho rằng có thể dùng làm cơ sở để tổ chức lại các tập tin của mình.

Ví dụ, nếu có một thư mục chứa toàn tập tin nhạc, bạn có thể đánh dấu tùy chọn Album Title để Windows sắp xếp các tập tin đó theo từng album tương ứng. Thuộc tính tương ứng với tùy chọn mà bạn đánh dấu sẽ được nhìn thấy trong phần chi tiết nội dung tập tin khi sử dụng Explorer. Khi thực hiện chọn xong, hãy nhấn OK để kết thúc công việc.

Thủ thuật: Với chế độ hiển thị chi tiết (khi chọn View.Details), bạn có thể nhanh chóng thêm hoặc bớt các thuộc tính được hiển thị: nhấn phải chuột lên tiêu đề cột bên trên danh sách tập tin và chọn một thuộc tính cho hiện hoặc ẩn. Cũng xin lưu ý bạn rằng trình đơn này chỉ hiển thị một phần danh sách các thuộc tính có sẵn, hãy chọn More ở cuối danh sách để mở hộp thoại Choose Details để xem toàn bộ danh sách các thuộc tính.

Khi đã có các chọn lựa thuộc tính ở đúng chỗ, bạn nhấn chuột lên tiêu đề ở cột bất kỳ để sắp xếp lại nội dung trong thư mục theo thuộc tính tương ứng với cột đó. Để sắp xếp các thuộc tính ẩn , bạn chọn View.Arrange Icons by và chọn một thuộc tính trong trình đơn con. Tiếp tục ví dụ trên, bạn sẽ phải nhấn View.Arrange Icons by. Album Title để sắp xếp các tập tin theo từng album.

Để "cắt" danh sách tập tin khổng lồ này thành nhiều phần nhỏ hơn dựa trên cơ sở các thuộc tính đúng yêu cầu của mình, bạn chỉ cần chọn View.Arrange Icons by.Shows in Groups. Thao tác này sẽ phân chia thư mục đó thành nhiều đoạn với đầu đề phù hợp tương ứng các thuộc tính bạn đã chọn trước đây. Tiếp tục ví dụ trên, thư mục đó bây giờ sẽ bao gồm các nhóm có tên chính là tựa album (Hình 3).

Một số thuộc tính được tập hợp theo cách riêng của chúng. Ví dụ, nếu sắp xếp theo thuộc tính tên (Name), các nhóm sẽ được đại diện bởi các chữ cái. Sắp xếp theo kích thước (Size) sẽ tạo các nhóm như Tiny, Small, Medium và Large.

Cách tổ chức theo nhóm cho phép bạn thay đổi tức khắc việc hình thành nhóm bằng cách chọn một đặc trưng khác từ trình đơn con View.Arrange Icons by. Nếu thư mục của bạn đã sẵn sàng trình bày các chi tiết tập tin chẳng hạn thì bạn có thể thay đổi các quá trình hình thành nhóm này bằng cách nhấn chuột lên tiêu đề thuộc tính được yêu cầu đang xuất hiện ở trên đầu danh sách tập tin đó. Việc tổ chức lại các thư mục đã có trật tự nhưng chưa được ghép nhóm sẽ tốn nhiều thời gian cho việc sắp xếp lại các tập tin vào nhiều cấp thư mục mới.

Việc ghép nhóm thường đã có sẵn đối với hầu hết các chế độ hiển thị như Thumbnail, Tile, Icon và Details (ngoại trừ chế độ List) của tiện ích Explorer.

Nhận biết thư mục dễ dàng

Bạn có thể nhận ra thư mục cần thiết một cách dễ dàng hơn bằng cách gán cho biểu tượng của nó một dáng vẻ riêng biệt. Windows XP cho phép tạo riêng một biểu tượng tùy ý nếu quan sát các tập tin của bạn dưới dạng hình thu nhỏ (thumbnail), thậm chí là một hình bất kỳ cho một thư mục bằng cách nhấn phải chuột lên thư mục đó và chọn Properties.Customize. (Lưu ý rằng tùy chọn này không có sẵn đối với tất cả thư mục trong Windows XP). Để thêm vào một biểu tượng tùy ý, bạn nhấn nút Change Icon bên dưới mục "Folder icons". Tiếp đến, chọn một trong các biểu tượng sẵn có hoặc nhấn Browse để xác định một tập tin biểu tượng (.ico) trong một trình ứng dụng (.exe), thư viện (.dll), hoặc trong bất kỳ tập tin nào có thể chứa biểu tượng. Khi đã tìm được biểu tượng mong muốn, hãy chọn nó, nhấn Open (nếu cần thiết) và sau đó là OK khi được yêu cầu để đóng tất cả các hộp thoại lại.

Nếu có một hay nhiều thư mục được hiển thị ở dạng hình thu nhỏ (chọn View.Thumbnails) có thể chúng đã có sẵn một dạng hiển thị có khả năng thay đổi, cung cấp các tập tin trong thư mục ở định dạng web thông dụng như .htm cho văn bản, hay .jpg, .gif, .bmp, và .tif cho hình ảnh (quá trình tùy biến biểu tượng tiền chế này cũng được áp dụng cho các liên kết đến các tập tin cũng theo định dạng này). Windows sẽ tự động tạo các hình nhỏ của bốn khoản mục đầu tiên trong thư mục để xuất hiện trên hình thu nhỏ của thư mục. Tất nhiên, nó sẽ tạo không đủ bốn hình nếu thư mục đó chứa không đủ bốn tập tin hay liên kết đến một trang web nào đó. Nếu thư mục chứa các liên kết đến một website, Windows chỉ có thể tạo hình thu nhỏ cho khoản mục này khi máy tính đang được kết nối Internet.

Để nhận dạng bốn hình nhỏ trên biểu tượng hình thu nhỏ của thư mục đòi hỏi bạn phải có một con mắt thật tinh tường. Để làm nổi bật những thư mục này, bạn chọn một hình độc đáo nhất cho hình thu nhỏ đó: nhấn phải chuột lên thư mục, chọn Properties.Customize, và nhấn Choose Picture trong phần "Folder pictures". Xác định đường dẫn và chọn một tập tin hình ảnh như đã trình bày ở trên rồi nhấn Open rồi đến OK.

Dĩ nhiên, để thực hiện theo các bước này đối với tất cả thư mục mà bạn muốn thay đổi biểu tượng sẽ mất chút ít thời gian. Để đẩy nhanh tốc độ, bạn hãy xác định những hình sẽ dùng cho hình thư nhỏ của thư mục, đặt tên cho tập tin đó là folder

(hoặc folder.jpg, folder.gif, hoặc tên gì đó phù hợp nếu nhìn thấy phần mở rộng tập tin) và kéo chúng vào trong thư mục được yêu cầu. Windows sẽ tự động dùng một tập tin với tên này để làm hình thu nhỏ cho thư mục đó.

Thủ thuật: Nếu không tìm được hình để diễn đạt nội dung của thư mục, hãy đến website Google Images (www.google.com) và nhập từ khóa để thực hiện tìm kiếm. Khi thấy được một hình ưng ý, bạn nhấn phải chuột lên đó và chọn Save Picture As (trong Internet Explorer) hoặc Save Image As (trong Firefox). Tiếp đến là xác định đường dẫn đến thư mục của bạn, và đặt tên là folder.jpg và nhấn Save. Đến đây, hình thu nhỏ của thư mục sẽ xuất hiện hình bạn vừa chọn xong.

Cuối cùng, nếu nhận thấy các hình thu nhỏ quá to và thô, bạn có thể tải về tiện ích miễn phí Tweak UI của Microsoft (find.pcworld.com/47124). Sau khi đã cài đặt xong, chạy Tweak UI, nhấn đúp vào mục Explorer, chọn Thumbnails trong khung cửa sổ bên trái và thay đổi giá trị mục Size trong hộp thoại Thumbnail, chẳng hạn như giảm xuống 64 và sau đó nhấn OK. Bạn có thể phải đóng và mở lại cửa sổ thư mục để thấy được các hình thu nhỏ xuất hiện với kích thước mới.

Minh Xuân
PC World Mỹ 6/2005

Kill Protected Processes

Trong Task Manager nếu bạn dùng chức năng End Process thì bạn chỉ kết thúc được một số Process của các chương trình bình thường. Đối với các Process được bảo vệ như tiến trình của OS hay các trình diệt virus thì bạn không thể kết thúc dễ dàng như thế. Điều này cũng tương tự khi ta dùng hàm API TerminateProcess().

Nguyên lý: Một process có thể Kill một Process khác được bảo vệ nếu như process này có đặc quyền DEBUG các process khác, sau đó process này có thể dùng hàm API TerminateProcess(hProcess,0)!
Đoạn mã sau dùng để gán quyền DEBUG cho một process:

Code:

```
void GetDebugPriv( void )
{
HANDLE hToken;
LUID sedebugnameValue;
TOKEN_PRIVILEGES tkp;
if ( ! OpenProcessToken( GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES |
TOKEN_QUERY, &hToken ) )
return;
if ( !LookupPrivilegeValue( NULL, SE_DEBUG_NAME, &sedebugnameValue )
)
{
CloseHandle( hToken );
return;
}
tkp.PrivilegeCount = 1;
tkp.Privileges[0].Luid = sedebugnameValue;
tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
AdjustTokenPrivileges( hToken, FALSE, &tkp, sizeof tkp, NULL, NULL );
CloseHandle( hToken );
}
```

ngoalong(HVA)

Trong thời gian qua, chuyên mục "Những câu hỏi nhỏ" đã trả lời rất nhiều thắc mắc của bạn đọc xung quanh những sự cố, hỏng hóc thường gặp của máy tính. Trong khuôn khổ bài viết này, một lần nữa chúng tôi sẽ điểm lại một số câu hỏi được đề cập nhiều nhất.

MÁY TÍNH HOẠT ĐỘNG BẤT THƯỜNG

Một câu hỏi thường nhận được có dạng "Làm thế nào mà những thứ gì đó không được tải lên từ lúc tôi nâng cấp trình điều khiển thiết bị đang sử dụng của mình?" hoặc "Tại sao <tên thiết bị> luôn gặp trục trặc mỗi khi tôi khởi chạy <tên chương trình>?". Cho dù triệu chứng ra sao thì những thủ thuật chẩn đoán phù hợp chắc chắn sẽ giúp ích cho bạn.

Hình 1: Công cụ quét hệ thống của Driveragent.com cho biết driver của thiết bị nào cần được cập nhật.

Trước khi thực hiện bất cứ việc gì, bạn cần phải sao lưu Windows Registry. Nếu việc "táy máy" của bạn làm cho mọi thứ trở nên tồi tệ hơn thì bước sao lưu này sẽ giúp ích rất nhiều. Tiện ích System Restore của Windows XP sẽ tự động sao lưu Registry và các tập tin quan trọng khác của Windows, nhưng chưa tạo được sự tin tưởng tuyệt đối (Windows 2000 lại không đi kèm tiện ích này).

Một giải pháp an toàn hơn so với việc dựa vào System Restore là sử dụng tiện ích Emergency Recovery Utility NT (ERUNT) miễn phí của Lars Hederer (find.pcworld.com/52208). Sau khi tải về và cài đặt chương trình này, người dùng Windows XP cần tạo một sao lưu ERUNT khởi đầu khi máy tính đang hoạt động theo đúng ý họ. Trong khi đó, người dùng Windows 2000 phải bổ sung một liên kết đến tiện ích ERUNT vào trình đơn StartUp để tiện ích này được nạp vào mỗi khi khởi động Windows.

Kiểm tra phần mềm nguy hại: Đó luôn là một ý kiến tốt để chắn chắn máy tính của bạn luôn "trong sạch". Về vấn đề này, bạn nên tham khảo lại các bài viết sau: "Hibernate theo lịch định" (ID: A0609_131), "Đĩa cứng bị chậm" (ID: A0604_148), "Chống virus xảo quyệt" (ID: A0509_142).

Cập nhật trình điều khiển thiết bị mới: Về cơ bản, cập nhật các trình điều khiển thiết bị (driver) không phải là một phần của công việc bảo trì định kỳ hệ thống. Nếu không xảy ra hỏng hóc nào, bạn không cần thực hiện điều này. Dù vậy, nếu có

một thiết bị nào đó gặp sự cố thì việc cập nhật driver là một giải pháp miễn phí và tương đối dễ thực hiện.

Bạn có thể ghé qua trang Driver Updates của TouchStone Software ở địa chỉ www.driveragent.com để kiểm tra driver mà máy tính của mình đang sử dụng. Website này (làm việc với trình duyệt Internet Explorer) sẽ tiến hành quét kiểm tra tất cả đĩa cứng và cung cấp cho bạn một danh sách tương đối chính xác những driver đã lỗi thời (Hình 1). Khi biết rõ một driver nào đó cần phải cập nhật, bạn sẽ dễ dàng tìm chúng trên website của hãng sản xuất.

Tắt các ứng dụng tự khởi chạy: Những ứng dụng tự khởi chạy (tự động chạy mỗi khi bạn khởi động Windows) sẽ gây nhiều trục trặc cho máy tính. Sau khi khởi động Windows, bạn hãy quan sát các biểu tượng tí hon xuất hiện trong khay hệ thống (system tray), chúng đại diện cho những ứng dụng tự khởi chạy vốn "bòn rút" tài nguyên hệ thống và thậm chí gây tê liệt các ứng dụng khác.

Để xem danh sách tất cả ứng dụng tự khởi chạy và tắt chúng, bạn chọn Start.Run, gõ vào lệnh msconfig, ấn <Enter>, rồi chọn thẻ StartUp. (Windows 2000 không có lệnh này, bạn cần sử dụng tiện ích Startup Control Panel, tải về miễn phí từ địa chỉ find.pcworld.com /54975).

Hãy nhớ những ứng dụng nào trong danh sách các ứng dụng tự khởi chạy đã được chọn hoặc không chọn (bạn sẽ muốn quay lại các thiết lập này sau khi xảy ra trục trặc). Sau đó, bỏ chọn đối với tất cả, khởi động lại máy tính và theo dõi xem sự cố có còn tiếp diễn hay không. Thay đổi này sẽ làm vô hiệu hóa phần mềm bảo mật của bạn, nên nếu máy tính đang kết nối Internet thì bạn đừng để các ứng dụng này bị loại bỏ quá lâu và phải cẩn thận đối với các website định truy xuất.

Nếu không còn trục trặc gì thì chắc chắn một trong số các ứng dụng tự khởi động chính là thủ phạm. Bạn hãy sử dụng phép loại trừ dần để tìm ra thủ phạm. Nếu thủ phạm là phần mềm tường lửa (firewall), tiện ích phòng chống virus/spyware hay một tiện ích bảo mật nào khác thì bạn cứ đánh dấu chọn đối với tiện ích này rồi sau đó thông báo với hãng sản xuất về sự cố đang gặp phải, hoặc cân nhắc đến việc mua một phần mềm khác. Bạn có thể bỏ đánh dấu chọn đối với những ứng dụng còn lại.

Còn có một cách khác hiệu quả hơn để biết tên các ứng dụng tự khởi chạy là sử dụng tiện ích miễn phí Startup Applications List (find.pcworld.com/54976, hình 2). Ngoài ra, bạn cũng có thể đến bất kỳ trang web tìm kiếm nào và nhập vào từ khóa là tên ứng dụng cộng với từ "msconfig" để tải về những tiện ích có tính năng tương

tự.

Giống như quái vật trong phim kinh dị, một số ứng dụng tự khởi chạy đã bị loại bỏ nhưng vẫn xuất hiện trở lại. Các ứng dụng này đã hiệu chỉnh "lỗi" của bạn là đã tắt module tự động khởi chạy trong ứng dụng. Để không còn gặp phải tình trạng này, bạn hãy tìm và tắt tùy chọn thiết lập tính năng tự khởi chạy trong trình đơn của ứng dụng đó. Nếu không tìm thấy, bạn nên liên hệ với nhà sản xuất để nhận được sự trợ giúp cụ thể.

Có thể không phải do Windows: Sự cố có thể do thiết bị phần cứng gây ra. Một cách đơn giản để giúp Windows thoát khỏi vòng luẩn quẩn này là bạn có thể kiểm tra phần cứng đó bằng cách cho nó khởi động trên một hệ điều hành khác.

Ví dụ, bạn có thể khởi động hệ điều hành miễn phí Puppy Linux từ một đĩa CD (find.pcworld.com/54972). Nếu trục trặc vẫn tồn tại trên hệ điều hành mới thì nguyên nhân gây ra sự cố chính là một món gì đó liên quan đến phần cứng. Để nhanh chóng trị dứt căn bệnh đang gặp phải, bạn tham khảo lại bài viết "5 phút thế là xong" (ID: A0501_84).

BẢO ĐẢM AN TOÀN DỮ LIỆU

Thông thường, có nhiều bạn không hỏi tôi về cách bảo vệ máy tính cho đến khi bị hỏng một cái gì đó. Sau đây là các thủ thuật theo từng bước mà bạn nên tuân thủ để giảm tối đa hư hỏng khi thực hiện các thủ thuật.

Hình 2: Tìm thêm thông tin chi tiết của các ứng dụng tự khởi chạy bằng Startup Application List.

Sao lưu: Khi hệ thống đang vận hành tốt, bạn nên tạo một bản sao lưu đầy đủ, kể cả các thông số cài đặt Windows. Khi Windows trở nên không ổn định, việc phục hồi hệ điều hành từ kết quả sao lưu sẽ dễ dàng hơn rất nhiều so với phải cài đặt mới. Để biết cách bảo quản và sao lưu dữ liệu, bạn tham khảo bài viết "Bảo quản an toàn dữ liệu sao lưu" (ID: A0603_130). Bạn có thể sử dụng các tiện ích sao lưu thông dụng như Dantz Retrospect, NovaStor NovaBackup và Acronis True Image... (xem thêm bài đánh giá 5 công cụ sao lưu hàng đầu hiện nay tại địa chỉ find.pcworld.com/54980).

Hệ thống không thể khởi động: Nếu Windows không khởi động được, một bản sao lưu hệ thống nhiều khả năng có thể khắc phục sự cố nhưng cũng có trường hợp không giúp ích được gì cho bạn. Ngay cả trong hình huống xấu nhất, vẫn còn một giải pháp dễ dàng hơn so với việc phục hồi một bản sao lưu.

Với Windows 9x, bạn chỉ cần tạo một đĩa mềm khẩn cấp để khởi động hệ điều hành DOS và đi kèm theo là tất cả công cụ chẩn đoán. Tuy nhiên, không may mắn như Windows 2000 hoặc Windows XP, DOS không thể thấy được một phân vùng đĩa cứng định dạng NTFS.

Tuy nhiên, bạn có thể tập hợp thêm vài công cụ cho những ngày đen tối như thế này, tham khảo chi tiết tại bài viết "Khi Windows XP hoặc 2000 không khởi động" (ID: A0311_134). Nếu máy tính của bạn không có ổ đĩa mềm, hãy xem hướng dẫn tạo một đĩa CD khởi động được trình bày trong bài viết "Tạo đĩa CD khởi động khẩn cấp" (ID: A0512_146).

Tự phòng thủ: Có lẽ bạn đã sẵn sàng tự bảo vệ máy tính của mình trước spyware, nhưng chúng tôi vẫn muốn giới thiệu một phần mềm an toàn hơn để tăng cường sức mạnh cho những phần mềm khác: Spy Sweeper của Webroot Software (30 USD, find.pcworld.com/54984). Không chỉ là một công cụ "săn" spyware xuất sắc, Spy Sweeper còn có khả năng cảnh báo khi một quá trình cài đặt thiết lập tính năng tự khởi chạy và cho phép bạn ngăn chặn sự bổ sung lén lút này.

SỬA CHỮA REGISTRY

Windows Registry là một cơ sở dữ liệu khổng lồ, đại diện cho cấu hình "độc nhất vô nhị" của mỗi máy tính. Tùy kiến thức của bạn, Registry có thể là công cụ vô giá giúp tăng lực cho các phần mềm trên máy tính nhưng cũng có thể là một "đống hỗn độn" làm mọi thứ trở nên tồi tệ hơn nếu chẳng may bạn thiết lập sai chúng. Trong phần đầu của bài viết này, chúng tôi từng lưu ý bạn có thể sao lưu Registry của hệ thống bằng tiện ích ERUNT miễn phí.

Hình 3: Tự động dọn dẹp Registry hoặc thực hiện thủ công với Reg Organizer.

Dọn dẹp Registry: Một trong số các tiện ích dọn dẹp Registry được nhiều người yêu thích là Reg Organizer của ChemTable (find.pcworld.com/54983, hình 3). Công cụ này giúp bạn kiểm tra tất cả ứng dụng tự khởi chạy, loại tập tin và những trục trặc khác. Tiện ích này cũng có một tính năng tìm kiếm và thay thế rất tốt. Bạn có thể thiết lập tiện ích tự động dọn dẹp Registry hoặc thủ công thực hiện công việc này. Tin xấu: tiện ích có giá 30 USD. Nếu e ngại về tài chính, bạn hãy chọn tiện ích miễn phí EasyCleaner (find.pcworld.com/54985).

Bùi Xuân Toại
PC World Mỹ 12/2006

Bạn cần bộ nhớ bao nhiêu thì đủ? - 9/9/2006 10h:13

Khi có ý định bổ sung thêm bộ nhớ, chúng ta luôn phải đau đầu để cân bằng giữa giá cả và tốc độ. Vậy bạn thực sự cần bộ nhớ dung lượng bao nhiêu, giá cả thế nào? Các cuộc điều tra của chúng tôi mang lại nhiều kết quả đáng ngạc nhiên.

Bộ nhớ bao nhiêu là đủ? Câu hỏi đó vẫn luôn ám ảnh tôi cũng như hàng nghìn người sử dụng máy tính khác trong nhiều năm nay. Đến giờ vẫn chưa có được nhiều câu trả lời thực sự thoả đáng.

Điều này là đặc biệt quan trọng bởi vì kiểu của bộ nhớ (như DDR, DDR2 hay một số kiểu khác) đã bị quy định bắt buộc cùng bảng mạch chính và bộ vi xử lý. Thế nên bạn phải lựa chọn dung lượng bộ nhớ sao cho phù hợp với thiết bị mới (hoặc các thiết bị có thể được bổ sung thêm sau này).

Tuy nhiên, không phải dễ dàng để xác định được dung lượng bao nhiêu là đủ. Dung lượng bộ nhớ máy tính lớn hay nhỏ tuỳ thuộc vào từng hoàn cảnh. Những công việc bạn cần làm, phần mềm bạn đang sử dụng là các yếu tố quyết định để xác định kích thước bộ nhớ phù hợp cho máy tính của bạn. Chúng có thể thay đổi theo từng máy riêng.

Ví dụ, theo Microsoft để chạy được phiên bản Professional của Hệ điều hành Windows XP, bạn cần RAM 128 MB hoặc ít nhất là 64 MB với phần hỗ trợ rất nhỏ và giới hạn khả năng thực thi của nhiều chương trình. Luôn có một bản mô tả chi tiết kỹ thuật tối thiểu tương ứng với một bộ vi xử lý. Nhưng để máy hoạt động tốt nhất, đừng chỉ sử dụng các thiết bị ở phạm vi tối thiểu đó.

Nói như thế tức là cái máy tính IBM ThinkPad 600X với dung lượng bộ nhớ 64MB nhỏ bé và cổ lỗ sĩ của tôi nên chạy Windows XP Pro. Microsoft Word và Lotus Notes đều hoạt động hiệu quả nhưng chỉ đến một chừng mực nhất định nào đấy. Windows có nhiều phương pháp xử lý khá hay: Thay vì chỉ chia nhỏ quá trình tạm ngừng nếu dung lượng bộ nhớ còn lại ít, Windows bắt đầu sử dụng đĩa cứng như là bộ nhớ ngoài, thăm dò dữ liệu và các thiết bị nếu cần thiết. Sự khác nhau về tốc độ (ảnh hưởng lên toàn bộ chương trình thực thi) giống như sự khác nhau giữa đi bộ và chạy thi bằng một con ngựa đua.

Tiến hành kiểm tra

Chúng ta thử tiến hành kiểm tra xem phần bộ nhớ thêm vào tác động lên máy tính ra sao.

Trước hết bạn cần phải có một máy tính với dung lượng bộ nhớ khoảng từ 512MB cho tới 2GB; một DIMM Ballistix 240-pin, modul bộ nhớ DDR2 PC2-6400 (P/N # CT6464AA53E) của Crucial Technology.

Đây là modul thực thi có cấu trúc cao nên thường đắt (khoảng hơn 100$). Bạn cũng có thể sử dụng modul tương đương như tiêu chuẩn PC2-4200 của Crucial (P/N # CT6464AA53E) với giá chỉ khoảng 40$.

Thứ hai bạn cần hai phần mềm là : COSBI- OpenSourceMark (OSMark) và Ulead VideoStudio 10 Plus.

OSMark là chương trình benmark tổng hợp, nghĩa là không có một ứng dụng kinh tế thực nào trong phần mềm này. OSMark được thiết kế để kiểm tra tất cả hệ thống con (CPU, bộ nhớ, các thiết bị đồ hoạ, ổ cứng), sau đó tính toán con số chương trình thực thi đơn bằng cách kết hợp và xử lý các kết quả riêng rẽ.

VideoStudio là chương trình ứng dụng thực. Ví dụ bạn có thể sử dụng chương trình để phân tách 43 phút của một video clip thành một video truyền hình 60 phút. Sau đó lại ghép chúng lại thành một chương trình hoàn chỉnh như ban đầu. Chương trình này nâng cao tính tương đương trong máy tính.

Tiếp theo có một thay đổi bạn sẽ phải thực hiện cùng với việc bổ sung bộ nhớ là lựa chọn sử dụng qua lại kiến trúc bộ nhớ dual-channel.

Dual-channel sử dụng modul bộ nhớ theo cặp chứ không dùng các thiết bị đơn. Như thế tốt hơn bởi thay vì chỉ có một kênh vừa truyền vừa nhận, Dual-channel cho phép quá trình truyền - nhận diễn ra đồng thời, giúp giảm thời gian truyền tải đi một nửa.

Bộ nhớ Benmark

Một máy tính có dung lượng bộ nhớ 512MB tạo ra một OSMark với kết quả là 1053. Đây chưa phải là kết quả tuyệt vời nếu bạn đang tìm kiếm máy tính cá nhân có tốc độ thực thi cao. Máy tính chúng ta đang sử dụng chỉ dùng để thử nghiệm. Bạn có thể nâng cấp nó sau.

Khi bộ nhớ hệ thống vượt quá 1GB, chương trình kiểm tra benmark không thể kiểm tra được sự cải tiến.

Với modul hai thanh Ram 512 (tổng cộng là 1GB), không sử dụng bảng mạch chính kênh kép thì OSMark được kết xuất là 1074. Kết quả cao hơn, nhưng chưa tạo ra sự nâng cấp lớn. Khi sử dụng Dual-channel, con số này lên đến 1111.

Như vậy, việc chuyển từ dung lượng 512MB lên 1GB kênh kép cải tiến tốc độ thực thi chương trình lên khoảng 15%. Nhưng nếu cùng dung lượng bộ nhớ như vậy mà không dùng Dual-channel thì chỉ tăng được khoảng 2%.

Chúng ta thử xem dung lượng bộ nhớ càng lớn thì máy tính có hoạt động tốt hơn không. Thêm một thanh RAM 512MB thứ ba vào máy. Tổng dung lượng bộ nhớ có lúc này là 1,536 MB nhưng quá trình hoạt động của Dual-channel bị rối loạn. Dual-channel đòi hỏi modul bộ nhớ phải là số chẵn. Kết quả của OSMark là 1112. Bổ sung thêm RAM 512MB thứ ba mà chỉ tăng thêm được kết quả trong OSMark. Như vậy dung lượng bộ nhớ càng nhiều thì chưa chắc đã càng tốt.

Bây giờ chúng ta thử với thanh RAM 512MB thứ tư và cũng là cuối cùng. Với con số chẵn bộ nhớ, hoạt động Dual-channel được khôi phục và OSMark có kết quả là… 1112 !

Đó là lý do vì sao ban đừng bao giờ chỉ tin vào benchmark.

Chuyện gì xảy ra khi bộ nhớ hết benchmark? Nó sẽ thông báo OSMark không cần đến 1 GB để chạy. Vì thế chẳng có sự cải thiện nào cho dù bạn bổ sung thêm dung bộ nhớ. Bạn có thể chứng thực trường hợp này bằng chương trình ứng dụng thực: VideoStudio 10 Plus.

Bộ nhớ trong thực tế

Thời gian hoàn trả 43 phút của video clip cũng giải thích cho các vấn đề tương tự.

Chỉ có một chút khác nhau giữa việc thay đổi dung lượng 512MB lên 1 GB, không sử dụng Dual-channel. Thực tế, video clip được hoàn lại trong 35 phút 2 giây (tức là 2 101 giây) khi máy tính sử dụng RAM 512MB và chỉ trong 34 phút 50 giây (tức là 2 090 giây) với máy có RAM 1GB.

Trong các ứng dụng "đời sống thực" càng tăng cường dung lượng bộ nhớ thì thực thì chương trình càng hiệu quả, nhất là khi sử dụng "Dual-channel".

Khi sử dụng bộ nhớ Dual-channel (các khe cắm bộ nhớ được mã hoá màu thành từng cặp để bạn biết được phải cắm ở đâu), thời gian hoàn lại giảm xuống chỉ còn 31 phút 45 giây (tức là 1 905 giây). Tốc độ hoàn lại cao hơn 4 phút. Nếu bạn thực hiện một vài lần hoàn lại trong một ngày, một vài lần trong một tuần, bạn có thể tiết kiệm được lượng thời gian tính theo ngày trong một năm chỉ với việc sử dụng hợp lý modul bộ nhớ bạn cần.

Đối với kích thước bộ nhớ lớn hơn thì sao? Khi bổ sung thêm thanh RAM 512MB thứ 3, thời gian hoàn lại thực tế chậm hơn 17 giây, tức là 32 phút 2 giây (tổng cộng: 1 922 giây). Đó là do thanh RAM thứ 3 làm đảo lộn hoạt động của kênh kép.

Nếu thêm thanh RAM 512MB thứ tư để cân bằng hoạt động cho kênh kép, thời gian hoàn lại chỉ mất 30 phút 31 giây (tức là 1 831 giây). Thời gian hoàn lại giảm nhanh chứng tỏ benmark tổng hợp của OSMark không dùng bộ nhớ 1GB được thêm vào ở trên.

Bạn hoàn toàn có thể bổ sung thêm nhiều thanh ghi bộ nhớ hơn và thời gian hoàn lại sẽ được cải thiện rõ rệt. Nhưng ở đây chúng ta sẽ gặp phải vấn đề nguyên tắc giảm giá trị trả về khi dung lượng bộ nhớ ngày càng lớn.

Chúng ta thử tìm hiểu vấn đề này. Đầu tiên bạn thay thế hai modul bộ nhớ 512MB bằng các modul dung lượng lớn hơn như hai thanh 1GB chẳng hạn. Nhưng tất nhiên tương ứng với thanh ghi bộ nhớ lớn hơn, giá tiền sẽ tăng lên rất nhiều. Trừ khi bạn thực sự quan tâm đến việc dịch lại đoạn video (hay bất kỳ trình ứng dụng quan trọng nào đó) thì việc nâng cấp là cần thiết. Nếu không bạn sẽ chỉ lãng phí tiền bạc. Hiện giờ giá của một RAM 512MB là khoảng 105 $ (giá bộ nhớ biến đổi rất nhanh; hiện giá của loại RAM này có thể rất khác). Sử dụng bộ nhớ 1GB có mã Dual-channel sẽ gấp đôi bộ nhớ ban đầu của bạn và có giá khoảng 210$. Gấp đôi giá ấy lên một lần nữa (420 $) thì bạn có thể mua được bộ nhớ 2GB với tốc độ hoàn lại nhanh hơn rất nhiều.

Nếu bạn muốn mở rộng dung lượng bộ nhớ lên hơn 2GB, bạn cần tăng thêm 2,5 lần số tiền đã mua. Và nhớ răng, để sử dụng bộ nhớ 3GB, bạn cần bỏ đi hai bộ nhớ

ban đầu, tức là bỏ đi 210$ và thêm vào một thanh 1GB với giá 186$. Con số tổng cộng là 1192$ chỉ để cải thiện tốc độ hoàn lại ở mức tốt nhất.
Kết luận

Bộ nhớ Dual-channel thường thích được dùng hơn nhưng dung lượng bộ nhớ sử dụng tuỳ thuộc vào từng máy, phụ thuộc mục đích bạn sử dụng bộ nhớ để làm gì, đang sử dụng các chương trình nào. Nếu dịch lại video là kế sinh nhai của bạn (hoặc đó được coi là một thú vui nghiêm túc), tiết kiệm được chút thời gian sẽ đem lại hiệu quả lớn trong công việc thì bạn nên đầu tư các thiết bị như hướng dẫn ở trên ngay từ ban đầu. Còn nếu không bạn chỉ nên sử dụng bộ nhớ ở mức 2GB, mà thực tế chỉ nên dừng lại ở 1GB.

Việc dịch các video, các bảng tính lớn, các thao tác hình ảnh đồ hoạ và các hog bộ nhớ tương tự cũng khá thú vị. Nhưng cũng với mức tiền tương ứng, bạn có thể trang bị cho mình nhiều thành phần hữu ích và thú vị hơn nhiều. Hãy cân nhắc kỹ trước khi quyết định đầu tư.

T.Thu

Di chuyển dữ liệu sang máy tính mới

Bạn mới "tậu" được chiếc PC mới, bộ xử lý mạnh mẽ, dung lượng RAM lớn, đĩa cứng cũng lớn hơn... nhưng còn dữ liệu trên chiếc máy PC cũ thì sao?

Chuyển đổi sang PC mới và cài đặt hệ điều hành mới cũng giống như chuyển sang ngôi nhà mới, lớn hơn, đẹp hơn. Tất cả những dữ liệu mà bạn có trên PC cũ không thể bỏ đi được, chúng rất quan trọng. Nhưng làm thế nào mà di chuyển được những dữ liệu đó tới PC mới như: sổ địa chỉ, email, các dữ liệu chương trình, thư mục Farvorites, các bản nhạc số, ảnh số, các thư mục đặc biệt...

Về mặt lý thuyết, chúng ta có thể sao chép dữ liệu cũ sang máy tính mới khá đơn giản, nhưng trong thực tế thì không đơn giản như vậy. Trong một số trường hợp có thể dẫn đến hỏng hóc và không thể sửa chữa được. Bạn cho rằng sử dụng các phần mềm sao lưu dữ liệu như Norton Ghost sẽ giải quyết được vấn đề này? Không đơn giản như vậy, Norton Ghost có thể phục hồi phân vùng từ đĩa cứng này sang đĩa cứng khác, nhưng để hoạt động ổn định và hiệu quả trên PC thì lại là vấn đề khác. Hơn nữa, hệ thống Windows cũ sẽ không hoạt động trên PC mới. Tuy nhiên, một số công cụ mới cho phép bạn di dời dữ liệu này sang PC mới đơn giản. Bạn chỉ cần

vài click chuột là mọi dữ liệu từ chiếc PC cũ kĩ sẽ chuyển sang PC mới nhanh chóng. Một số công cụ dưới đây sẽ biến "giấc mơ" của bạn thành hiện thực:

*
Files and Settings Transfer Wizard (FAST) là tiện ích có sẵn trong Windows XP, cho phép chuyển dời các thiết lập Windows, Internet Explorer, Outlook, Outlook Express...
*
Desktop DNA Professional là phần mềm không những cho phép chuyển dời những thiết lập trong các chương trình như FAST mà còn có khả năng di dời các thiết lập từ các phần mềm khác.
*
Alohabob PC Relocator 2005 Ultra Control Edition là phần mềm mạnh nhất. Alohabob cho phép di chuyển cả ứng dụng sang máy tính mới, mặc dù có thể một số ứng dụng sẽ không hoạt động tốt trên PC mới.

Tất cả những công cụ này đều di dời các dữ liệu và các thiết lập trong ứng dụng như: Những tuỳ chọn, thiết lập và cấu hình, vị trí đặt thanh công cụ... Để có thể chuyển đổi một số ứng dụng hoàn hảo, các công cụ này thường được thiết kế đặc biệt hỗ trợ khả năng chuyển đổi. Hầu hết các công cụ đều đều hỗ trợ cho hàng tá những ứng dụng phổ thông từ Microsoft, Intuit tới những phần mềm xuất bản... nhưng bạn cũng nên kiểm tra trước những ứng dụng mà phần mềm di chuyển dữ liệu này hỗ trợ.

Lập kế hoạch chuyển đổi

Trước khi di dời, bạn cần chuẩn bị một số bước sau. Đầu tiên, hãy quyết định lựa chọn sử dụng phương pháp nào để chuyển đổi dữ liệu từ hệ thống này sang hệ thống khác. Lựa chọn này có thể là kết nối mạng chuẩn hoặc các thư mục chia sẻ, kết nối vật lý như: USB, cổng song song, cổng nối tiếp... hoặc qua các thiết bị sao lưu dữ liệu. Di dời dữ liệu sử dụng kết nối mạng là phương pháp nhanh và hiệu quả nhất, nếu chia sẻ tập tin thì hãy chắc chắn rằng các thư mục chia sẻ này đều có thể truy cập tốt.

Thay thế các kết nối mạng bằng phương pháp sử dụng kết nối USB 2.0 có tốc độ cao cũng đem lại hiệu quả tốt. Các phương tiện sao lưu bằng các thiết bị lưu trữ như CD-R chẳng hạn thì cũng không ảnh hưởng lớn. Tuy nhiên, nếu có một kho dữ liệu đồ sộ thì bạn cần phải ngồi đợi, đưa hết đĩa CD này tới đĩa CD khác thì rất mệt mỏi và nhàm chán.

Nếu không thể sử dụng các kết nối mạng, bạn phải sử dụng các kết nối chậm hơn và sử dụng các thiết bị sao lưu thì hãy cân nhắc xoá bớt các tập tin đính kèm lớn trong emails, các bức ảnh cũ, và tiết kiệm được càng nhiều tập tin không cần thiết càng tốt.

Tiếp theo, máy tính cũ sử dụng chế độ đa người dùng, hãy liệt kê danh sách những người sử dụng trên máy tính cũ. Các công cụ này sẽ di dời những tài khoản người dùng sẽ được tạo lại trên máy PC mới hoàn hảo. Bạn thích tính năng di chuyển các thiết lập cũ sang PC mới chứ không phải là toàn bộ ứng dụng (bạn nên sử dụng tuỳ chọn này), hãy cài đặt các ứng dụng trên PC mới trước.

Hãy nán lại vài phút để xem cả 2 PC đều đã hoạt động và thực sự sẵn sàng cho chuyển dời dữ liệu hay chưa. Một ý kiến hay là cập nhật Windows tất cả các bản vá lỗi mới nhất sử dụng Windows Update hoặc truy cập vào trang www.windowsupdate.com. Cập nhật các chương trình chống virus, các phần mềm chống gián điệp và quét toàn bộ cả 2 máy để đảm bảo chúng đều sạch sẽ và không chứa bất cứ mối nguy hiểm nào. Sau khi đã quét xong toàn bộ, hãy tạm thời tắt bỏ các ứng dụng thời gian thực như và cả phần mềm tường lửa, bởi chúng có thể làm gián đoạn tới quá trình chuyển dời dữ liệu. Kết nối Internet cũng nên ngắt tạm thời.

Sử dụng các công cụ di chuyển

Sử dụng FAST

FAST (Windows Files and Settings Transfer Wizard) là chương trình chỉ có khả năng di chuyển các thiết lập người dùng Windows, Internet Explorer, Outlook, Outlook Express... không cho phép chuyển dời các ứng dụng, và có rất ít lựa chọn và không có khả năng undo hoặc khả năng báo cáo chi tiết. Nhưng vì đây là phần mềm đi kèm với Windows XP nên rất tiện lợi và không phải tốn chi phí đầu tư.

FAST có thểchạy bằng 2 cách: Cách thứ nhất bạn chỉ cần đưa đĩa CD Windows XP vào ổ và chọn Perform Additional Tasks, tiếp đó chọn Transfer Files and Settings. Cách thứ hai: Start -> All Programs -> Accessories -> System Tools -> Windows Files and Settings Transfer Wizard.

FAST thực sự là một đồ thuật đơn giản, chỉ với một vài bước lựa chọn thư mục và các tập tin, thiết lập cấu hình... dữ liệu sẽ được di chuyển tới máy PC mới. FAST

đơn giản, không có nhiều tính năng cao cấp, nếu muốn biết thông tin chi tiết, nhiều lựa chọn hơn thì hãy sử dụng công cụ như Desktop DNA, Alohabob

Sử dụng Desktop DNA

Desktop DNA của Computer Associates chỉ cho phép chuyển dời các thiết lập và cấu hình sẵn có chứ không phải là các ứng dụng, Desktop DNA cho phép truyền dữ liệu trực tiếp hoặc gián tiếp. Cũng giống như FAST,Desktop DNA di dời các thiết lập theo thời gian thực, diễn ra khá nhanh chóng và đơn giản.

Desktop DNA có khả năng chuyển dời gián tiếp, đây là sự thay thế tiện lợi nếu bạn không thể sử dụng 2 máy tính đồng thời. Chương trình tạo ra một tập tin thực thi được (.exe) từ hệ thống cũ và bạn có thể sao chép chúng tới hệ thống mới bằng bất cứ phương tiện lưu trữ khác. Khi nào cần thực hiện cài đặt thiết lập, chỉ cần chạy tập tin này là hoàn thành. Desktop DNA cung cấp lựa chọn các thiết lập và khả năng undo mạnh mẽ mà FAST không có.

Sử dụng Alohabob Pc Relocator

Alohabob PC Relocator 2005 Ultra Control Edition làm việc không những "ổn" như Desktop DNA mà còn có thể di chuyển rất nhiều ứng dụng. Hãy cài đặt phần mềm này trên cả máy tính cũ và mới, và thực hiện một số bước hướng dẫn cài đặt đơn giản. Nếu cả 2 máy tính này đều nối mạng thì quá trình di chuyển này thực sự rất đơn giản. Bạn chỉ cần chọn máy nguồn (source) và máy đích (target), lựa chọn chế độ truyền tự động (automatic), hãy xem xét và chấp nhận đề nghị mà chương trình đưa ra, thực hiện những bước mà phần mềm yêu cầu. Là mẫu người thích khám phá, bạn có thể lựa chọn chế độ chuẩn (Standard) hoặc chuyên gia (expert), để lựa chọn bằng tay các kiểu tập tin, thư mục, các thiết lập... hoặc các ứng dụng mà chương trình hỗ trợ. Trong chế độ chuyên gia, bạn có thể chuyển đổi toàn bộ ứng dụng tới đĩa cứng mới. Nếu gặp lỗi, PC Relocator có chức năng undo để có thể quay về các trạng thái ban đầu.

Sau khi di chuyển dữ liệu thành công

Khi hoàn thành quá trình chuyển đổi, hãy kiểm lại PC mới để đảm bảo chắc chắn quá trình di dời diễn ra tốt đẹp, đúng như mong đợi. Mặc dù các công cụ di dời thực sự đem lại khả năng di chuyển dữ liệu, ứng dụng hữu ích và đơn giản, nhưng các chương trình này không phải là những "chiếc đũa thần" hoàn hảo. Một số lỗi nhỏ có thể sẽ xuất hiện, nhưng dẫu sao những phần mềm này cũng là lựa chọn tốt cho nhu cầu của bạn.

Overclock: được, mất và những điều cần biết

Ép xung - overclock (OC) đã xuất hiện từ khá lâu, từ những chiếc máy tính dùng bộ xử lý 286, 386. Có thể bạn không tin nhưng hãy nhớ lại xem có phải trên những chiếc máy đó luôn có nút Turbo hay tương tự không? Mỗi khi ấn nút này là máy được overclock một chút, độ tăng xung nhịp không lớn lắm tùy theo mặc định của nhà sản xuất. Đơn cử như chiếc máy 386 của tôi dùng ngày xưa tốc độ mặc định là 33Mhz, khi chuyển sang chế độ Turbo tốc độ tăng lên 40Mhz. Cùng với tốc độ phát triển chóng mặt của công nghệ sản xuất chip, những khái niệm xoay quanh vấn đề OC cũng có sự thay đổi.

Hiện nay, ngoài OC tăng tốc FSB để đạt được tốc độ chip xử lý cao hơn, còn có OC card màn hình, RAM, gắn thêm tụ để gia tăng độ ổn định của điện nguồn cấp cho chip hay các giải pháp tản nhiệt nhằm đạt được khả năng OC cao hơn. Bài viết này sẽ giới thiệu những vấn đề cơ bản về các giải pháp OC.

Linh kiện hỗ trợ OC

Nếu hỏi bất kỳ một chuyên gia OC (Overclocker hay Ocer): Điều gì quan trọng nhất đối với việc ép xung? Câu trả lời sẽ là tìm mua được linh kiện 'ngon'. Chúng ta hãy cùng nhau điểm qua các linh kiện quan trọng của hệ thống máy tính.

1. Mainboard (MB)

MB là thành phần quan trọng đối với OC vì nó là thứ kết nối tất cả mọi bộ phận với nhau. Nếu hình dung máy tính giống một chiếc xe máy thì MB giống cái khung xe. Nếu xe muốn chạy nhanh thì bộ khung phải tốt và có sức chịu lực cao. Đối với MB cũng vậy. Hiện trên thị trường Việt Nam có nhiều hãng MB tên tuổi như:

- **Albatron:** Đây là gương mặt mới đối với thị trường VN, tuy mới thành lập nhưng Albatron đã nhanh chóng chứng minh được vị thế và khả năng của mình.

MB Albatron nói chung rẻ và khả năng OC trên một số dòng MB gần đây được đánh giá khá cao như: PX845PE Pro II (chipset 845PE), PX865PE Pro (chipset 865PE Springdale).

- Asus: Tuy không quảng cáo rầm rộ về khả năng OC nhưng độ ổn định cũng như khả năng chịu xung nhịp cao của MB Asus tốt nhất. Vào thời điểm bạn đọc bài này thì trong top 10 xếp hạng của các Ocer trên thế giới, Asus chiếm tới 5 vị trí (bao gồm vị trí số 1). Điểm yếu duy nhất của MB Asus là giá cao (đôi khi tới gấp rưỡi) so với các MB cùng loại của các hãng khác.

- Abit: Quảng cáo rất rầm rộ về khả năng OC với công nghệ Softmenu III, tuy khả năng ép xung rất tuyệt vời nhưng thường kém ổn định ở tốc độ cao, những model cho khả năng OC tốt và đầy đủ chức năng lại rất đắt.

Hình 1: Ảnh phía sau hộp CPU nơi có thể tìm thấy MM Code và Product Code.

- Gigabyte: Nói chung đây là hãng sản xuất nhắm vào thị trường phổ thông nên không chú trọng lắm đến OC, tuy nhiên một số model gần đây thuộc dòng XP với Dual Power Supply thì khả năng OC khá cao do nguồn điện cấp cho CPU rất ổn định: 8INXP (chipset Intel E7205), 8KNXP (chipset 875P Canterwood), 8PENXP (chipset 865PE Springdale).

- MSI: Khá giống Gigabyte về mục tiêu thị trường, tuy nhiên những model Neo sử dụng chipset Intel 865, 875 gần đây cũng rất khá và được đánh giá tương đối cao.

- Epox: Gần tương tự với Abit về khả năng, tuy nhiên đôi khi gây cho người dùng ấn tượng là các model của Epox chỉ dùng để OC chứ không phải để sử dụng hàng ngày. Các model cho AMD của Epox xuất sắc hơn nhiều so với những loại cho Intel. Ưu điểm: giá rẻ hơn nhiều so với Asus, Abit.

- ASRock, FIC, ECS, Biostar...: Đây là những MB hướng vào người dùng quan tâm về giá, tuy nhiên chúng lại khá hay đối với một số tay chuyên nghiệp do khả năng chỉnh sửa dễ dàng (ví dụ model K7S5A cho chip AMD của ECS).

Khi mua MB bạn nên chú ý tới các thông số thiết lập trong BIOS qua sách hướng dẫn đi kèm (User Manual), thường thì các MB cao cấp hỗ trợ tốt OC cho chỉnh rất chi tiết những thông số liên quan tới FSB, Vcore, tốc độ RAM,... Một số hãng cung cấp các phần mềm ép xung ở cấp hệ điều hành như Gigabyte hay MSI nhưng theo tôi nó gây rắc rối nhiều hơn là tiện lợi, hơn nữa việc thay đổi tốc độ và điện thế CPU trong khi đang vận hành rất nguy hiểm.

2. CPU: Intel và AMD.

Intel: Có một số điểm cần lưu ý.

- **Số Sspec hay thường gọi là Stepping Mask:** Hiện bán trên thị trường chủ yếu là loại B0, B1 tuy nhiên C1 và D1 mới là siêu sao trong giới OC. Chắc bạn sẽ thắc mắc làm thế nào để phân biệt? Rất đơn giản: Bạn hãy để ý 5 chữ số cuối ở hàng code (ở hình 1 là SL6WF) rồi so sánh với bảng tra cứu CPU stepping.

Hiện trên thị trường xuất hiện loại Pentium 4 tốc độ 2,4Ghz với code SL6RZ, đây là loại có khả năng ép xung siêu hạng. Ví dụ trong điều kiện bình thường P4 2,4Ghz SL6RZ (18x133Mhz) có thể ép xung chạy ổn định ở tốc độ 3,24Ghz (18x180Mhz) mà không cần thêm giải pháp tản nhiệt nào. Còn với giải pháp tản nhiệt bằng LN2 (sử dụng băng khô hay Nitơ lỏng để hạ thấp nhiệt độ chip xuống dưới 0 độ C) thì có thể đẩy tốc độ lên trên 4Ghz. Tất cả các loại Pentium 4 3,06 đều là stepping C1, các loại Pentium 4-C FSB 800Mhz mới đều là stepping D1. Bạn có thể tìm con số này tại: http://support.intel.com/support/processors/

- **Hệ số nhân:** Bạn nên chọn loại có hệ số nhân càng cao càng tốt vì nó sẽ quyết định tốc độ chip tăng thêm khi tăng 1Mhz FSB. Hiện cao nhất có thể là loại 2,4Ghz FSB 400Mhz có hệ số nhân tới 24x, tuy nhiên loại này rất khó mua. Theo tôi, bạn nên chọn loại 2,4B Ghz FSB 533Mhz để đạt được hiệu năng và giá cả hợp lý nhất.

AMD: Hiện có rất ít cửa hàng bán chip AMD, nhưng nếu bạn thực sự muốn mua thì tất nhiên vẫn có chỗ bán. Ưu điểm lớn nhất của AMD là giá rẻ, chip Athlon XP1700+ giá chỉ khoảng 70USD so với 143USD của Pentium4 1,7Ghz. Tuy nhiên, bạn nên lưu ý là trên thị trường có tới 4 loại chip AthlonXP với tên mã (codename) khác nhau:

- **Palomino:** Đây là chip Athlon XP đời đầu tuy hiệu năng cao nhưng chạy rất nóng do vẫn dùng công nghệ 0,18 micron và bị khóa hệ số nhân. Tuy vẫn có cách mở khóa nhưng rất nguy hiểm và có thể gây hỏng chip.

Hình 2: CPU sau khi OC đang trong quá trình khởi động

- **T-bred A:** Athlon XP đời thứ 2, sử dụng công nghệ 0,13 micron chạy mát hơn nhiều, có thể so sánh với Pentium 4 Northwood, đặc biệt là hệ số nhân không bị khóa.

• **T-bred B:** Athlon XP đời thứ 3, cấu trúc tương tự loại A nhưng có một số cải tiến nên có khả năng chạy ở xung nhịp cao hơn nhiều. Ví dụ T-Bred B 1700+ xung thực là 1433Mhz (11x133) có thể chạy ổn định ở tốc độ 2400Mhz (khoảng 3200+) (200x12).

• **Barton:** Athlon XP mới nhất với L2 cache 5120KB và FSB 333/400Mhz, hiện tại loại thông dụng nhất 2500+ với xung thực là 1833Mhz; loại này chưa có bán ở VN. Barton chỉ có thể hoạt động hoàn toàn ổn định với một số loại MB mới như Abit NF7-S hay một số dòng MB dùng chipset NF2 khác, đôi khi bạn cũng cần phải cập nhật BIOS.

Tất nhiên có thể nhận thấy dòng T-bred B là ngôi sao đối với người dùng AMD và rất dễ mua, tuy nhiên cũng giống Intel, bạn cần chọn loại có code là 0308 hay 0307 đối với loại 1700+ thì tốt hơn. Các dòng cao hơn như 2100+ hay 2400+ giá khá cao mà hiệu năng không cải thiện nhiều đồng thời giới hạn ép xung cũng không cao hơn mà lại khó tìm mua.

Mainboard cho AMD tuy khó tìm nhưng hiện bạn có thể mua được những loại tốt nhất ở VN như: Abit NF7-S, Epox 8RDA+, Asus A7N8X, Soltek 75FRN2-S/SL, tất cả đều dùng chipset nForce2 của nVidia. Các MB như Asus K7V8X hay Abit KD7, dùng chipset của VIA Technologies cũng tốt nhưng đã cũ. Theo một số ý kiến thì chipset nForce2 của nVidia với stepping C1 là tốt nhất, tuy nhiên để chọn được đúng loại thì chỉ có thể do may mắn, bạn có thể để mắt đến loại Abit NF7-S phiên bản 2.0 là một trong số ít các MB dùng chipset C1 mà người mua có thể nhận biết.

Hình 3: Chương trình hiển thị thông số CPU - WCPUid

Ngoài thị trường có bán khá nhiều chip T-bred 1700+ mà theo nhà sản xuất là được hạ xuống (downgrade) từ dòng 2700+. Những chip này không đạt các phép kiểm tra đối với chip 2700+ (không chạy ổn định ở 2700+) nên bị giảm tốc độ và bán ra dưới dạng 1700+, trong khi những loại 1700+ bình thường lại dễ dàng chạy ở 2700+ hay thậm chí cao hơn.

3. RAM

Khi FSB tăng thì bus RAM cũng sẽ tăng theo, ví dụ khi FSB là 400Mhz thì RAM cũng chạy ở 400Mhz. Các loại MB mới gần đây cho phép chỉnh hệ số tỉ lệ giữa FSB và RAM, hệ số 1:1 có thể hạ xuống 3:4, 2:3 để bus RAM chạy ở tốc độ thấp

hơn. Ngoài tốc độ RAM bạn còn phải để ý đến độ trễ CAS của RAM, càng thấp càng tốt, thường là 2.0 đối với các loại RAM hàng hiệu và tốt. Đại đa số các loại RAM trên thị trường VN là CAS 2.5 hay tệ hơn là CAS 3.0. Để nhận biết đặc điểm này bạn cũng áp dụng cách tương tự như CPU. Ví dụ thanh Kingston 512MB DDR333 có Serial: KVR333X64C25/512 thì C25 chính là CAS của RAM.

Đối với các hiệu RAM khác thì số hiệu có thể khác nhưng thường số CAS của RAM có dạng Cxx. Một số loại RAM tốt mà bạn có thể mua ở nước ngoài như Corsair XMS, Kingston HyperX... Những chipset mới như nFORCE 2 hay 875P, 865PE hỗ trợ công nghệ Dual Channel DDR, tuy cho băng thông rất lớn nhưng lại hạn chế về khả năng OC.

Hình 4: Chỉnh sửa CAS và các thông số timming của RAM trong BIOS

Một số người không coi trọng RAM lắm và luôn hạ tốc độ RAM xuống thấp trong khi ép xung CPU lên cao. Thực tế, điều này không có lợi chút nào vì dù CPU xử lý nhanh nhưng khi dữ liệu qua RAM bị tắc nghẽn thì cũng không hiệu quả. Đối với AMD, nếu bạn chạy FSB với RAM đồng bộ thì hiệu suất hệ thống sẽ có cải thiện đáng kể.

4. Card màn hình

Khi bạn tăng FSB thì tốc độ bus AGP/PCI cũng tăng theo, các MB mới gần đây đã cho khóa bus AGP và PCI lại nên điều này không quan trọng, tuy nhiên nếu card tốt có thể chịu bus AGP/PCI cao thì dĩ nhiên sẽ tăng tốc độ. Điều quan trọng: card màn hình (vid) chính là cái bạn có thể ép xung rất cao. Card màn hình cũng có thể coi như một máy tính, có bản mạch chính (PCB), bộ xử lý đồ họa GPU (Core), RAM đồ họa (Vidmem), chính vì thế mà việc lựa chọn card tốt là rất quan trọng; bạn không thể mua rời từng bộ phận rồi lắp lại.

Hình 5: Card đồ họa Abit Siluro OTES 4200-8x (GPU Rev Á Ti4800SE)

Bảng mạch (PCB) của card đồ họa cao cấp như GeForce4 Ti hay 9700 Pro thường có từ 8 lớp trở lên nhằm tăng tính ổn định nguồn điện cấp cho các thành phần của vid. Các hãng sản xuất cung cấp card màn hình cũng rất phong phú giúp cho bạn có nhiều chọn lựa. Nói chung hầu hết các hãng sản xuất MB tên tuổi đều cung cấp cả card màn hình như MSI, Asus, Gigabyte, Abit, Albatron... ngoài ra cũng có những hãng chuyên sản xuất card màn hình như Sparkle, Palit,

Hercules, Gainward, Leadtek, HIS, Sapphire... Và tôi có thể cho bạn một vài gợi ý nhỏ:

Nhìn chung, nếu nhằm vào nhu cầu sử dụng bình thường thì hầu như loại nào cũng đáp ứng được, tuy nhiên cần đề phòng một số đồ nhái hàng cao cấp đã bắt đầu xuất hiện trên thị trường. Khi mua card màn hình bạn cần xác định rõ một vài điều. Nếu là dân OC chuyên nghiệp thì đa phần sẽ mua card có tản nhiệt dễ tháo và có bản mạch lớn để có thể tháo lắp và thay đổi các linh kiện dễ dàng. Nếu bạn là 'amateur' hay 'semi-pro' (nghiệp dư) thì sẽ chọn những loại tản nhiệt 'hầm hố' như Abit Siluro OTES hay Albatron Medusa Series với tản nhiệt đồng vì chúng làm mát rất tốt nhưng lại khó tháo lắp. Card được đánh giá cao trên thị trường thế giới hiện tại là Hercules nhưng giá thường rất đắt và hầu như không thể mua tại VN vì không có đại lý chính thức. Cho nên Asus, Abit, Albatron là những lựa chọn sáng giá.

5. Bộ tản nhiệt

Đối với CPU, nếu có điều kiện bạn nên tìm mua một số loại tản nhiệt HSF (HeatShink and Fan - phiến tản nhiệt và quạt) có tên tuổi như Thermaltake, Zalman... Chúng được thiết kế tỉ mỉ theo đúng kĩ thuật và chế tạo hết sức cẩn thận. Đa số đều được làm bằng đồng hay lõi đồng cộng với quạt tốc độ cao cỡ 6000-7000 vòng/phút (rpm) - cao hơn nhiều so với tốc độ từ 2500-3500rpm của quạt bán kèm theo CPU. Hơn nữa, đồ 'xịn' có rất nhiều tính năng phụ như bộ chỉnh tốc độ hay tự báo động khi có trục trặc. Bạn cũng nên để ý xem chip của mình là loại nào để chọn bộ tản nhiệt thích hợp. Với Socket 370 của Pentium III và Socket A (Socket 462) của AMD do dùng chung 1 loại chốt nên chúng cũng có thể dùng cùng loại tản nhiệt. Đối với P4 do cấu trúc socket khác nên tản nhiệt có nhiều điểm đặc biệt. Tất nhiên có một số loại lắp được cả cho 2 dòng nhưng giá thường đắt hơn bình thường như Volcano 7+ của Thermaltake. Bạn cũng nên chú ý chọn loại tản nhiệt được tạo từ 1 khối chứ không phải được hàn từ các lá hợp kim vì sẽ hút nhiệt tốt hơn.

Với thùng máy (case) thì đơn giản hơn, bạn có thể tự mình thiết kế hệ thống làm mát nhưng nói chung đều dựa trên nguyên tắc hút/đẩy. Có thể hút từ mặt trước rồi đẩy ra sau hay hút từ dưới đẩy lên trên hoặc cả hai tùy ý. Tuy nhiên hãy tính toán thật cẩn thận trước khi quyết định. Hãy tìm case loại lớn nhằm tăng sự thoáng mát như loại Professional Workstation Case của Compaq với giá hợp lý rồi cắt, đục theo thiết kế để lắp quạt thông gió. Bạn cũng có thể thay toàn bộ đĩa cứng IDE cũ bằng loại Serial ATA để giảm độ cản gió nhờ dùng dây cáp nhỏ hơn, hay ít ra thay cáp to bản bình thường bằng loại cáp tròn có giá khoảng 10-20USD tùy loại.

Hình 7: Tản nhiệt nước cao cấp

Ngày nay, tản nhiệt bằng nước (watercooling) đã trở nên hiện thực. Tuy nhiên, nên đặc biệt cẩn thận với loại tản nhiệt này vì nếu bị rò rỉ thì hệ thống của bạn sẽ 'tiêu' ngay. Ngay cả với bộ xịn giá vài trăm đô thì bạn cũng nên để chạy thử vài ngày trước khi lắp vào hệ thống. Ngoài ra cũng cần phải đề phòng hiện tượng ngưng tụ nước trên mặt ngoài của bộ tản nhiệt khi nhiệt độ trong và ngoài chênh lệch quá lớn.

Một số người còn mạo hiểm hơn bằng cách sử dụng băng khô hay nitơ lỏng để làm mát. Tuy cách này hiệu quả nhất (nhiệt độ có thể xuống tới -15 độ C) tuy nhiên rất nguy hiểm bởi các bộ phận của máy tính thường chỉ được khuyến cáo sử dụng trong nhiệt độ từ 10-60 độ C.

6. Bộ nguồn:

Hình 6: Quạt EARO Cool Ver: 8 cho CPU Socket 478

Khi các bộ phận của máy tính hoạt động ở tốc độ cao hơn tất nhiên nó sẽ yêu cầu nhiều điện hơn. Nếu không cấp đủ điện cho các linh kiện thì nhẹ là thường xuyên được 'thưởng thức' các thông báo lỗi của hệ điều hành, nặng là máy đang chạy đột nhiên tắt ngóm hoặc bật không lên. Có thể bạn thấy vô lý khi một bộ nguồn đôi khi có giá cao hơn cả những thành phần quan trọng nhất của máy tính nhưng điều đó lại hoàn toàn hợp lý. Bản thân tôi khi sử dụng bộ nguồn thông thường đi kèm các loại case trên thị trường đã thường xuyên gặp các loại lỗi như đã nói, nhưng khi thay bằng một số loại nguồn 'hiệu' như Herolchi, Thermaltake, Antec TrueControl hay Enermax thì không còn thấy chúng xuất hiện. Tiện đây cũng giới thiệu các bạn chương trình Speedfan: Đây là một phần mềm đa năng hiển thị các thông số của hệ thống một cách đầy đủ bao gồm: Nhiệt độ mainboard/chip/ổ cứng, tốc độ quạt

CPU/Case/PSU, mức điện áp của các đường điện chính trong hệ thống (3,3v/5v/12v). Bạn có thể download miễn phí tại http://www.almico.com/speedfan.php. Chương trình có thể sử dụng với hầu hết các loại MB có bán trên thị trường trong cũng như ngoài nước.

Để chọn mua bộ nguồn phù hợp, bạn có thể tham khảo các bài báo hướng dẫn rất chi tiết trên các số PC World trước đây. Bên cạnh đó cũng nên chú ý một vài điểm: Đối với P4 bạn nên chọn loại nguồn có công suất đường 12v thấp nhất cũng phải là 15A, một số loại MB mới của AMD cũng có đường 12v phụ hỗ trợ chip nhưng không ăn điện nhiều như P4 mà chủ yếu vẫn phụ thuộc vào đường 5v nhiều hơn.

Đường 3,3v là nguồn nuôi MB và các card hệ thống nên bộ nguồn có đường 3,3v ổn định sẽ giúp bảo đảm an toàn cho thiết bị.

Tâm tình

Hình 8: Tản nhiệt bằng Nitơ lỏng

Người dùng máy tính 'chuyên nghiệp' không chỉ coi OC là phương pháp để đạt mục đích 'chi ít được nhiều' mà còn bởi đam mê 'đua' Mhz hay điểm benchmark. Một khi đã đạt đến đỉnh cao của tốc độ thì cũng phải có cách nào đó để ghi nhận thành tích. Có 2 cách đánh giá: 'Đạt được' và 'Ổn Định'.

'Đạt được' có nghĩa là bạn vươn tới được tốc độ x nào đó nhưng chỉ có thể làm một vài tác vụ cơ bản, chụp vài bức hình hay lấy điểm benchmark khoe bạn bè. Khi để hệ thống chạy ở tốc độ quá cao như vậy sẽ gây rối loạn, những lỗi kỳ lạ như từ sao hỏa sẽ liên tục xuất hiện khiến bạn không biết đâu mà lần... tóm lại là rất khó chịu.

Bạn chỉ nên OC lên mức này trong các cuộc đua tốc độ hay hiệu năng đồ họa và bạn cần 1 chương trình như CPU-Z , WCPUid hay Sisoft Sandra để lấy thông số.

Trong trường hợp đua sức mạnh đồ họa thì card màn hình đóng vai trò rất quan trọng, bạn cần có hệ thống ổn định hơn để có thể vượt qua mọi thử nghiệm với 2 chương trình được yêu thích nhất là 3Dmark 2001 và 3D Mark 2003 của Futuremark. Sau khi có điểm bạn có thể đăng kí lên bảng xếp hạng trực tuyến (ORB - Online Result Browser) của công ty. Hiện tại cuộc đua trên ORB có trên 1 triệu người trên khắp thế giới tham gia với nhiều giải cho các cấu hình máy khác nhau. Vào thời điểm viết bài này, tôi đang chiếm vị trí thứ 2 với card Ti4200 chạy trên nền tất cả mọi loại CPU. Rất có thể khi bạn đọc bài này thì một ai đó từ nước khác vượt lên nhưng điều đó chỉ làm cho cuộc chơi thêm phần thú vị.

- **Internal Clock Speed:** Tốc độ hoạt động của CPU hệ thống (ví dụ 1.4Ghz hay 2.4Ghz).
- **Front Side Bus (FSB):** Bus truyền dữ liệu của CPU và hệ thống.
- **Multiplier:** Hệ số nhân.
- **Vcore:** Điện thế nhân của CPU.
- **AGP/PCI Clock:** Tốc độ hoạt động của bus PCI và AGP.
- **Vid:** Card màn hình.
- **Overclock(OC):** ép xung.
- **BOSD (Blue Screen of Death):** màn hình báo lỗi với màu xanh rất 'dễ thương' của Windows.

Nếu bạn thuộc 'tip' người 'ăn chắc mặc bền', muốn có một hệ thống nhanh nhưng phải ổn định để làm việc thì hãy thử tính ổn định với 2 chương trình kiểm tra Prime 95 và Super PI. Mỗi chương trình có một nguyên tắc hoạt động khác nhau. Với Prime95, nó sẽ tự động sử dụng những phần CPU rảnh rỗi để thực hiện các chuỗi tính toán nhằm làm cho CPU luôn hoạt động trong trạng thái bận rộn (100% usage) trong khi bạn vẫn có thể thực hiện những công việc thường nhật như xem phim, soạn văn bản thậm chí chơi game. Đối với SuperPI thì ngược lại: Một khi được kích hoạt, chương trình sẽ thực hiện những phép tính rất lớn tới hàng tỉ con số để bắt toàn bộ hệ thống làm việc hết công suất nhằm tìm ra những điểm bất ổn định. Nếu hệ thống của bạn có thể chịu được quá trình này từ 4-8 tiếng thì có thể xem như nó đã ổn định và có thể dùng để chạy hàng ngày còn nếu không may gặp lỗi thì hãy giảm tốc độ xuống một chút hay tăng thêm chút ít Vcore (điện thế nhân CPU) rồi thử lại.

Nhân tiện nói tới Vcore (điện thế nhân CPU) tôi cũng xin nêu một vài điều: Khi bạn tăng tốc độ chip thì nó sẽ yêu cầu thêm điện thế để có thể chạy ổn định. Việc tăng điện thế lên quá cao có thể gây cháy chip nhưng hiện tại việc này rất khó xảy ra do tất cả các loại MB đều có hệ thống an toàn, tuy nhiên nếu để Vcore cao có thể làm chip bị quá nóng dẫn tới mất ổn định. Bạn có thể tìm ra những con số an toàn nhất đối với hệ thống của mình theo quy trình sau:

Hình 9: Một bộ tản nhiệt nước tự chế sau khi đã lắp đặt hoàn thiện

1. Đẩy CPU lên hết mức cho đến khi bắt đầu mất ổn định.

2. Tăng Vcore lên 1 mức (thông qua BIOS hay jumper trên MB).

Lặp lại bước 1 và bước 2 cho đến khi nhiệt độ vượt quá giới hạn cho phép (thường là 68-70 độ C) thì tăng cường giải pháp làm mát rồi tiếp tục lặp lại như trên. Nói chung trong điều kiện khí hậu VN cũng như các giải pháp tản nhiệt hiện có thì bạn không nên đẩy Vcore quá 1,85v đối với P4-Northwood và 2,1v đối với AMD T-Bred.

Đôi khi lỗi không do CPU gây ra mà có thể do RAM kém chất lượng. Những loại RAM tốt có thể để 'timming' ở 2.2.2.5 (con số đầu là CAS của RAM, số cuối là khoảng thời gian giữa các lần nạp điện vào chip nhớ), nếu gặp bất ổn thì hạ xuống 2.2.2.7 hay 2.5.3.3.7. Bạn không nên hạ xuống thấp hơn 3.3.3.8 vì như thế hệ thống của bạn sẽ trở nên tồi tệ. Cũng cần phải lưu ý là đối với Intel thì các thông số này không thực sự quan trọng như AMD. Một hãng RAM có thể có nhiều lô hàng sử dụng các loại chip nhớ khác nhau, tuy nhiên bạn hãy cố gắng chọn lựa những loại RAM dùng chip nhớ Samsung, Hynix, Winbond hay Infineon là tốt nhất. Đối với RAM của card màn hình cũng áp dụng tương tự nhưng với chỉ số khác. Những hãng tên tuổi cũng như dòng sản phẩm cao cấp luôn sử dụng những loại chip RAM tốt như đã liệt kê ở trên.

Đối với card màn hình bạn cần chú ý tới con số 'timming' của RAM, những loại tốt thường là -3,3ns (550Mhz-600Mhz) như GeForce 4 Ti4200-8x, Radeon 9500 Pro, GeForce4 Ti 4800(/SE), dòng sản phẩm cao cấp sử dụng loại RAM nhanh hơn như -2.8ns (600-650Mhz) đối với card Ti4600, Radeon 9700 hay thậm chí là -2ns như Geforce FX 5800/5900 Ultra. Không phải mọi sản phẩm cùng loại đều giống nhau mà phải tùy theo từng lô hàng, đơn cử như card Abit Siluro Ti4200-8x OTES vào lúc tôi mua thì sử dụng chip RAM Samsung -3.3ns và GPU NV28 Stepping A1

của nVidia (tương đương loại dùng cho card Ti4800SE) cho tốc độ rất tốt nhưng khi giới thiệu cho một người bạn mua thì rất tiếc lại không may mắn như vậy. Chẳng công ty nào cho bạn tháo tản nhiệt ra mà xem bên trong khi mua hàng cả. Muốn ép xung card đồ họa bạn có khá nhiều lựa chọn: đối với những card sử dụng GPU của

nVidia thì bạn có thể dùng Rivatuner, Powerstrip, hay đơn thuần là 1 bản patch để kích hoạt tính năng ép xung trong driver của nVidia, đối với card dùng GPU thuộc dòng Radeon của ATI thì bạn cũng có thể dùng Rivatuner hay Powerstrip, ngoài ra còn có Rage3d (www.rage3d.com) hay Radeonator cho riêng GPU ATI. Nếu bạn mới tập tễnh vào nghề thì tốt nhất nên chọn Powerstrip vì giao diện chương trình đơn giản và dễ dùng, còn nếu bạn tự tin mình vào bản lĩnh của mình thì hãy chọn Rivatuner (www.nvworld.ru), theo đánh giá cá nhân tôi thì đây là chương trình rất chuyên nghiệp, nếu chưa từng làm quen, bạn có thể bị choáng ngợp trước số lượng lớn các thiết lập và thông số lạ hoắc như ngôn ngữ 'ngoài hành tinh', ví dụ: 'Enable FOURCC NVHS/NVHU Textures'... Tốc độ của card đồ họa được dựa trên 2 con số viết dưới dạng tốc độ core/mem, ví dụ với card Albatron Medusa GeForce 4 Ti4800SE có tốc độ mặc định là 275/550 có nghĩa tốc độ GPU là 275Mhz còn tốc độ RAM là 550Mhz (DDR). Ảnh hưởng của việc ép xung sẽ được thấy rất rõ qua tốc độ dựng hình trong những game 3D cao cấp. Tốc độ của GPU là quan trọng nhất khi chạy ở chế độ bình thường (không khử răng cưa) còn tốc độ RAM tăng lên sẽ đem lại sự cải thiện đáng kể khi bật chế độ khử răng cưa.

Ngoài ra còn 1 thông số liên quan đến card màn hình mà bạn nên quan tâm đó là điện thế khe AGP (VAGP), thông thường là 1,5v nhưng một số MB cho phép đẩy lên 1,6; 1,7, hay 1,8v, tuy nhiên chỉ khi bạn nâng tốc độ AGP lên cao hơn nhiều so với mặc định thì mới cần quan tâm và việc này sẽ khiến cho Northbridge rất nóng khiến bạn lại mất công nghĩ cách làm mát mà hiệu suất cải thiện lại không cao.

Những bộ phận còn lại tuy không quan trọng nhưng bạn cũng nên chọn mua dòng cao cấp nếu có điều kiện vì khi OC tất cả mọi thành phần hệ thống đều chạy nhanh hơn, nếu thiết bị kém chất lượng sẽ không trụ nổi và hỏng bất cứ lúc nào. Đặc biệt là ổ cứng, nếu có điều kiện hãy mua loại Seagate Barracuda 4/5 hay Maxtor Plus Series, Western Digital 8MB Cache. Dung lượng của chúng không quan trọng, hãy chọn loại có tốc độ quay 7200rpm trở lên để có hiệu năng cao nhất.

Tóm lại, nếu bạn đã chọn được đúng những linh kiện tốt thì việc ép xung hệ thống chạy ở khoảng 150% là nằm trong tầm tay. Hiện những hệ thống chạy ở khoảng 200% không còn là chuyện hiếm. Ví dụ:

Hình 10: Chương trình hiển thị thông số CPU (CPUZ)(máy tác giả đang sử dụng)

• **Intel Pentium 4 1.6A Ghz OC 3.2Ghz (200x16) Vcore:** 2.1v Làm mát: LN2. RD-Ram PC1066.

• **Intel Pentium 4 2.4B Ghz OC 3.6Ghz (200x18) Vcore:** 1.8v Làm mát: Watercooling. DDR RAM Corsair XMS PC3200.

• **Intel Pentium 4 3.06 Ghz (SL6S5) OC 4,45Ghz (Vcore 2.1v) Làm mát:** LN2. DDR RAM JetRam PC3200.

• **Intel Pentium 4 2.4B Ghz (SL6RZ) OC 3.4Ghz (Vcore 1.75v) Làm mát:** HSF. DDR RAM Kingston PC3200.

Bạn có thể xem kết quả cuộc đua tại http://www.vr-zone.com hay tham khảo thông tin (tiếng Việt) tại www.vnoczone.com. Tuy nhiên hãy suy nghĩ cẩn thận trước khi quyết định thử những chiêu như hàn thêm tụ vì như vậy bạn đã phá bỏ chế độ bảo hành hay thậm chí tiêu diệt luôn cả thiết bị của mình. Việc đơn giản nhất bạn có thể làm là mày mò chế tạo các loại tản nhiệt cho thiết bị, bạn có thể tìm mua đồng hay đơn thuần là tận dụng những bộ tản nhiệt không dùng đến để cưa, cắt cho phù hợp với kích thước và diện tích cần làm mát. Dĩ nhiên ở VN hiện nay khó có thể tìm mua được những thiết bị làm mát chuyên nghiệp nhưng việc tự chế tạo cho mình một bộ watercooling hay HSF hiệu quả là hoàn toàn có thể thực hiện được. Xin lấy ví dụ hệ thống tôi đang sử dụng: Intel Pentium 4 2.53Ghz (SL682) OC 3.32Ghz (175x19), RAM 512 MB Kingston DDR 400 CAS 2.0, MB Asus P4PE Deluxe (Chipset 845PE), card màn hình Abit Siluro GF4 Ti 4200-8x OTES chip nVidia GeForce4-8x Series Stepping A1, bộ nguồn Helrolchi 450w. CPU làm mát bằng Aero Cool Fan (giá khoảng 13USD, cho chất lượng rất tốt do làm hoàn toàn bằng đồng, tuy nhiên đây là loại tản nhiệt cho AMD nên muốn sử dụng cho hệ thống P4 bạn cần sửa lại một chút). Hệ thống chạy liên tục ổn định trên Microsoft Windows XP SP1a, nhiệt độ chip dao động trong khoảng 48-57 độ C.

Nếu có thắc mắc bạn có thể nêu câu hỏi trực tiếp với các chuyên gia tại http://forums.vnoczone.com. Chúc bạn thành công!ÿ

Nguyễn Thúc Hoàng Linh - D18, P4, TT Kim Liên, Q.Đống Đa, Hà Nội.
Email: valkyrie.forever@usa.com

Cách đặt pass để chống keylog, magic

sau một thời gian dài chinh chiến ở các hàng nét, em xin đưa ra đây một số phương pháp chống keylog và magic của em , các bác đừng cười em

1. keylog (vd: Perfect Keylogger, Family Key Logger, XPSpy.....)

các chương trình keylog ngoài khả năng ghi lại các phím gõ của bàn phím, còn có nhiều lựa chọn, có thể chụp màn hình, ghi lại
Clipboard (các dòng chữ, số khi ta copy, hoặc cut) , ghi lại các click chuột ....

dưới đây chỉ là phương pháp chống keylog ghi lại các phím ta vừa gõ:

Khi học C, C++ ,muốn gõ các kí tự đặc biệt ta phải giữ phím Alt và gõ các số ở phần NumLock " ở bên tay phải dươi ba cái đèn màu xanh" (các số ở dưới các phím F1, F2.... ko gõ được đâu nhé)

ví dụ các bác gõ phím 9, thay vì gõ bình thường các bạn Giữ Phím Alt sau đó bạn gõ 5 7, vẫn sẽ được số 9
làm như vậy các chương trình keylog sẽ không hiểu ta ấn phím 9 mà nó chỉ ghi lại được phím Alt thôi (em test thì thấy thế, ko biết có đúng ko

Dưới đây là bảng số

alt 98 = a
alt 111 = o

alt 48 (0)
alt 49 (1)
alt 50 (2)
alt 51 (3)
alt 52 (4)
alt 53 (5)
alt 54 (6)
alt 55 (7)
alt 56 (8)
alt 57 (9)

chú ý: phương pháp này gõ các ký tự có thể khác nhau với từng loại font, tốt nhất cứ font arial, tohoma ^^

2. Magic (magic se++, có thể lấy pass của Yahoo hiện nay bằng cách gửi tin nhắn

chứa thông tin về user và pass của bạn qua yahoo messenger)

a. phương pháp dùng nick ảo:
vì trong Yahoo Messenger có thể dùng nick ảo để login
nên các bạn hãy làm một cái nick ảo thật xấu vào vi dụ: emselahoahongnho, nguyenvana_2003, sadsadsss.....

nick xấu quá nản chẳng muốn vào^^

b. Phương pháp đặt pass:
nếu ta đặt pass như bình thường 123456, iloveyou....hay Q~!@#$%^&*A magic vẫn gửi pass của bạn y như vậy về nick của hacker
kể cả dùng phương pháp ấn phím alt như đã nêu trên thì vẫn vậy !

Nhưng nếu chúng ta đặt pass như sau em thì lúc magic gửi pass về nick của hacker sẽ là chữ em in đậm "em" (vì trong yahoo đây là thẻ chữ đậm) các bác có thể biến đổi thanh nhiều dạng như 389 (sau khi gõ thì ấn space rồi mới gõ 28 thì lúc magic gửi về sẽ là 287 in đậm, khó mà phát hiện có dấu cách

a` nếu một máy vừa cài magic vừa cài keylog thì ta áp dụng hai phương pháp:
Alt and

Khi đăng nhập nếu dùng bàn phím thì sẽ bị keylog ghi lại
dùng keyboard in screen thì chậm dễ bị tia từ phía sau.
vậy ta dùng chuột và chức năng chuột phải copy rồi paste

khi tạo một pass ta kiếm chỗ nào mà text có sẵn và ko thay đổi theo năm tháng tất nhiên chỗ nào thỉ chỉ ta biết thôi. rồi kiếm 1 đoạn text copy nó
cùng với password chính của tao tạo ra một password dài dằng dặc và ko bị keylog ghi lại
vì ta copy nó nằm ở trong clipboard.

ví dụ: khi đăng nhập mail của yahoo ta làm pass kiểu này
trên mail yahoo luôn có cái dòng text này "Sign in to Yahoo!"
ta copy nhớ dùng chuột
đến chỗ tạo pass: dùng chuột paste
rồi gõ thêm password riêng
ta có pass kiểu sau

"Sign in to Yahoo!<pass word riêng ở đây>"

vậy là pass của ta vừa dài lại vừa dễ nhớ. ko dính kelog

Giám sát hiệu suất hoạt động của phần cứng

Thực hiện: Minh Xuân

Phần mềm gián điệp, tập tin bị lỗi của Windows và các phần mềm kém chất lượng thường là nguyên nhân làm cho máy tính hoạt động ngày càng chậm. Tuy nhiên, dù đã thực hiện tinh chỉnh hệ thống, gỡ bỏ bớt phần mềm và cài lại Windows bạn vẫn không thể ngăn được sự giảm sút hiệu suất hoạt động do phần cứng gây ra (tham khảo bài "Trẻ hóa Windows", ID: A0503_103). Thật may, Windows XP/2000 cung cấp vài công cụ giúp người dùng kiểm soát hiện tượng "thắt cổ chai" ở phần cứng hệ thống.

Tiện ích System Monitor của Windows có khả năng theo dõi liên tục hàng trăm thông số hoạt động của Windows và ghi lại chúng trong các tập tin nhật ký (log) để dễ tìm kiếm và xử lý. Muốn khởi chạy System Monitor trong Windows XP/2000, bạn nhấn Start.Run, gõ vào lệnh perfmon, và ấn . Chọn System Monitor trong khung cửa sổ bên trái, rồi sau đó nhấn chuột vào dấu cộng + trên thanh công cụ ở cửa sổ bên phải để bổ sung thêm bộ đếm (counter) – hay nói chính xác là cảm biến; kết quả từ các bộ đếm này sẽ cho biết hiệu suất hoạt động của máy tính ở chế độ thời gian thực. Tiếp đến, chọn loại đối tượng cần ghi nhận (như CPU, trình duyệt, kết nối mạng...) từ trình đơn thả xuống Performance object, sau đó chọn loại bộ đếm từ danh sách được liệt kê (nếu đánh dấu vào tùy chọn Select counters from list), và nhấn Add (Hình 1). Ngoài ra, bạn có thể nhấn nút Explain để xem phần giải thích cho từng bộ đếm.

Các đồ thị của System Monitor sẽ giúp bạn phát hiện các khu vực gặp sự cố, nhưng tốt nhất bạn nên đánh giá các chỉ số về hiệu suất hoạt động của máy tính trong nhiều giờ (hay thậm chí vài ngày). Việc ghi lại các số liệu này vào một tập tin (log) có thể được thực hiện dễ dàng nhờ Microsoft cung cấp miễn phí phần mềm Performance Monitor Wizard (find.pcworld.com/53646).

System Monitor giúp bạn theo dõi hiệu suất hoạt động của máy tính.

Nhiều bộ đếm trong System Monitor ghi nhận các thông số kỹ thuật "khá lạ", tuy nhiên cũng có vài thông số giúp bạn xác định có cần nâng cấp RAM, CPU hay đĩa cứng mới không. Để biết thêm thông tin về các bộ đếm của System Monitor, bạn có thể tải về sách điện tử The Art and Science of Performance Monitoring của tác giả Guy Thomas (find.pcworld.com/53648).

Sau đây là vài bộ đếm mà bạn cần quan tâm khi sử dụng System Monitor.

RAM: Hai bộ đếm rất hữu ích có trong nhóm đối tượng Memory là Available Bytes và Pages/sec. Bộ đếm thứ nhất cho biết dung lượng bộ nhớ RAM vật lý (bộ nhớ thực) mà Windows có thể sử dụng, trong khi bộ đếm thứ hai cho biết số lần dữ liệu cần chuyển đổi giữa bộ nhớ ảo (sử dụng dung lượng đĩa cứng) và bộ nhớ thực. Nếu giá trị của Available Bytes giảm xuống xuống dưới 10% của dung lượng RAM và Pages/sec có trị số tăng một cách đáng kể, thì nhiều khả năng máy tính của bạn không đủ bộ nhớ thực để cung cấp cho các chương trình đang xử lý. Tính năng này thường được sử dụng để quyết định xem có nên nâng cấp RAM cho một máy tính hay không.

CPU: Bộ đếm % Processor Time trong nhóm Processor cho biết mức độ sử dụng CPU của máy tính. Quá trình khởi động của các phần mềm cũng như nhiều tác vụ khác có thể đẩy giá trị này lên mức trên 90% đến dưới 100%. Tuy nhiên, trong quá trình làm việc, nếu bộ đếm này vẫn kiên định giữ mức trên 80% thì nhiều khả năng CPU không đủ công suất để gánh vác công việc của hệ thống. Nếu đang sử dụng

loại CPU 2 nhân (hay còn gọi là lõi kép), bạn có thể chọn bộ đếm riêng cho mỗi nhân, hoặc một bộ đếm chung cho cả hai.

Đĩa cứng: Bộ đếm % Disk Time trong nhóm PhysicalDisk sẽ hiển thị thời gian mà

đĩa cứng cần sử dụng để đọc hay ghi dữ liệu. Nếu máy tính được trang bị nhiều đĩa cứng, bạn có thể chọn đĩa cứng cụ thể để theo dõi (ngoài ra, nếu máy tính sử dụng nhiều đĩa cứng ở chế độ RAID, hãy sử dụng bộ đếm % Disk Time trong mục LogicalDisk Performance). Nếu giá trị % Disk Time đạt từ 40 đến 50%, bạn cần thay đĩa cứng mới.

Minh Xuân
PC World Mỹ 9/2006

Tăng tốc toàn diện cho máy vi tính

21:55:56, 02/10/2005

Bạn cảm thấy không hài lòng với hiệu suất làm việc của máy tính, dù trong tay bạn là một hệ thống có cấu hình khá mạnh? Làm cách nào để máy tính hoạt động nhanh hơn? Chương trình AusLogics BoostSpeed có thể sẽ là câu trả lời.

Thực vậy, AusLogics BoostSpeed là một bộ công cụ toàn diện giúp máy tính của bạn hoạt động hết tiềm năng vốn có. Không những gia tăng tốc độ truy xuất của modem đến 300%, tăng tốc khởi động và nâng cao hiệu suất hoạt động của Windows, AusLogics BoostSpeed còn tích hợp thêm các nhóm tính năng tuyệt vời khác giúp hạn chế sự cố cho hệ thống, rút ngắn thời gian khởi động và tăng thêm tốc độ xử lý cho các ứng dụng thứ ba. Phiên bản mới nhất AusLogics BoostSpeed v3.2.1.527 có dung lượng 2,33 MB, tương thích với Windows 9x/ME/2000/XP, tương thích với Windows 9x/ME/2000/XP, có thể tải về bản dùng thử tại địa chỉ http://www.boost-speed.com/ru/download/boostspeed_install_ru.exe (hoặc tìm mua trong các CD phần mềm MPS).

Sau khi cài đặt, chương trình có giao diện như hình bên. Một số tính năng cụ thể như sau:

Welcome
- Find Out How To Optimize Your Computer: Chương trình sẽ tự động phân tích và đưa ra những lời khuyên cần thiết để bạn điều chỉnh một số thiết lập quan trọng của Windows, giúp hệ thống hoạt động nhanh và ổn định hơn.

- Boost Internet Speed: Là phương thức nhanh và dễ dàng nhất để tăng tốc độ kết nối cho modem. Bằng cách thay đổi giá trị của các thiết lập ẩn trong registry, chương trình sẽ tự động xác lập giá trị tối ưu nhất cho các thông số kết nối giúp modem đạt đến tốc độ truy xuất cao nhất có thể. Chương trình hỗ trợ cho hầu hết

thiết bị kết nối như: dial-up modem, IDSL, DSL, cable modem, wireless...

Boost Internet
- Status and Statistics: Theo dõi trạng thái và tốc độ đường truyền của modem.
- Optimize Internet (Wizard): Chế độ thuật sĩ tăng tốc, tương tự tính năng Boost Internet Speed đã nêu ở trên.

- Optimize Internet (Manually): Nếu bạn là người có nhiều kinh nghiệm về mạng thì đây là tính năng cần thiết để bạn khám phá và tự xác lập giá trị tối ưu hơn cho các thông số kết nối quan trọng như: Maximum Transmition Unit (MTU), TCP Receive Windows Size (RWIN), Time to Live (TTL)...

Boost Windows
- Optimize System Settings
* Optimize Windows Core: Tối ưu một số thiết lập quan trọng như: prefetch (thư mục truy xuất nhanh trong WinXP), swap file (tập tin hoán đổi)... giúp tăng thêm tốc độ và hiệu năng làm việc của Windows.

* Optimize File System: Tối ưu một số thiết lập quan trọng khác của hệ thống như: disk cache, memory cache, chỉ định kích thước MFT (master file table) lớn hơn cho phân vùng NTFS... giúp giảm tải cho bộ nhớ RAM, tăng tốc xử lý cho các ứng dụng, hạn chế sự phân mảnh ổ cứng.

* Optimize Windows Services: Tùy chỉnh việc tắt bớt những dịch vụ (service) không cần thiết để tăng thêm "sức mạnh" cho việc chơi game, lướt web hay in ấn... Nếu có sự cố đáng tiếc xảy ra (chẳng hạn không kết nối được internet), bạn bấm vào thẻ Optimize For > Restore default services để khôi phục cấu hình dịch vụ của Windows về tình trạng ban đầu.

- Startup/Shutdown Speed
* Increase Boot Speed: Thay đổi một số thiết lập quan trọng giúp giảm bớt thời gian khởi động Windows như: kích hoạt tính năng boot defragmentation, vô hiệu hóa tính năng user tracking, bỏ logo khởi động của Win9x/ME.

* Increase Shutdown Speed: Hiệu chỉnh một số thiết lập quan trọng trong registry giúp việc tắt máy diễn ra nhanh hơn như: tự động đóng các ứng dụng bị treo, giảm bớt thời gian chờ khi đóng các ứng dụng đang chạy.

* Optimize Other Settings: Tối ưu một số thiết lập khác của Windows như: bỏ tính năng autorun của CD/DVD, bỏ tính năng gửi thông báo đến Microsoft khi có ứng dụng nào đó bị lỗi.

- Optimize System Memory
* Manual Optimization: Giải phóng dung lượng cho bộ nhớ RAM giúp hệ thống có nhiều tài nguyên hơn dành cho các ứng dụng.

* Proccess: Theo dõi các dịch vụ và ứng dụng chạy nền trong Windows.
* Settings: Lựa chọn phương thức tối ưu cho bộ nhớ RAM. Chọn thẻ Enable Auto Optimization để chương trình tự động tối ưu hoặc sử dụng tổ hợp phím tắt Ctrl+Alt+ O.

- Optimize Apperance
* Visual Effect Settings: Bỏ bớt các hiệu ứng hiển thị giúp Windows hoạt động trơn tru hơn .

* Menu Apperance Settings: Tăng độ nhạy cảm của chuột khi di chuyển trong Start menu.

* Font Smoothing Settings: Thay đổi độ tương phản, độ sắc nét của font chữ.

Boost Programs
- Microsoft Office: Rút ngắn thời gian khởi động và tăng thêm tốc độ xử lý cho các chương trình trong bộ Microsoft Office như: Word, Excel, Access, Outlook.

- Internet Browsers: Giảm bớt thời gian khởi động và tăng tốc lướt web cho các trình duyệt Internet Explorer, Opera, Mozilla, Netscape, Firefox.

- Mail Clients, Internet Pagers: Giảm bớt thời gian khởi động cho trình nhắn tin ICQ, chương trình chat MSN Messenger, Outlook Express, The Bat!; tăng tốc gửi thư cho Outlook Express, The Bat!.

- Windows Accessories: Tăng thêm khả năng "trình diễn" cho Windows Media Player, tăng hiệu suất hoạt động cho các thành phần của Microsoft DirectX và bộ công cụ Norton SystemWorks của Symantec.

Optimization Tools
- Registry Cleaner: Sửa chữa, loại bỏ các lỗi phát sinh từ registry giữ cho hệ thống luôn ở trạng thái ổn định.

- Disk Cleaner: Dọn dẹp sạch sẽ tất cả các file "rác" để giải phóng không gian cho ổ cứng.

- Autostart manager: Quản lý các chương trình khởi động chung với Windows.

- Uninstall manager: Trình gỡ bỏ các ứng dụng cài đặt trong máy. Đặc biệt hơn, chương trình sẽ thông báo cho bạn biết một số thông tin thú vị như: những ứng dụng nào có mối liên hệ với Microsoft, ứng dụng nào cài đặt trong máy chiếm dụng nhiều không gian đĩa cứng nhất...

Network Tools
- Stay Connected While Away: Hạn chế tình trạng ngắt kết nối từ ISP (nhà cung cấp dịch vụ) với máy của bạn.

- Keep Your Computer Clock Accurate: Đồng bộ hóa đồng hồ máy tính với đồng hồ nguyên tử của những web server có hiệu lực trên Internet.

- Lookup Domain Names and IP Addresses: Truy vấn và thông báo cho bạn biết thông tin đăng ký tên miền của người chủ tên miền đó.

- Measure Internet Connection Speed: Kiểm tra, đo lường tốc độ đường truyền hiện thời của modem.

- Advanced Network Tools: Bộ công cụ hữu ích để giải quyết các sự cố truyền như: Advanced TraceRoute, Smart Ping...

Additional Tools
- Places Editor for Microsoft Office: Thêm vào những liên kết để xử lý nhanh các tập tin, thư mục của các chương trình trong bộ Microsoft Office.

- Banner Killer: Ngăn chặn các banner, các trang quảng cáo popup xuất hiện khi duyệt web.

- Windows Power Tools: Truy xuất nhanh một số công cụ có sẵn của Windows như: Microsoft System Information, Test and tune up DirectX, Microsoft System Configuration, Computer Management Tool, Microsoft Perfomance Monitor.

Lưu ý

Với những ai còn ít kinh nghiệm hoặc không muốn mất thời gian tìm hiểu riêng từng tính năng thì ở các thẻ Boost Windows và Boost Programs, tốt nhất nên chọn thẻ Optimize All để chương trình tự thực hiện việc tối ưu và tăng tốc hệ thống theo cách nhanh nhất. Sau đó quan sát phía bên phải, nếu thấy xuất hiện dòng chữ High Performance thì việc thay đổi đã thành công.

Phạm Hồng Quân

Bí quyết sử dụng máy tính bền lâu

Cùng với sự phát triển mạnh mẽ của nhịp sống hiện đại, máy tính ngày càng trở nên gần gũi hơn. Nó mang cả thế giới đến cho bạn nhưng cũng có thể mang thế giới ấy ra đi nếu bạn không chăm sóc, sử dụng nó cẩn thận.

Laptop Samsung Q30 của Samsung.

1. **Vệ sinh chung**: Một trong những nguyên nhân phổ biến của tình trạng máy tính trở nên nóng hừng hực như lò lửa là do bụi bặm, cáu bẩn bám bên trong máy. Do đó, bạn cần giữ cho máy tính luôn sạch sẽ cả bên trong lẫn bên ngoài. Bạn nên dùng một cây cọ mềm để quét sạch các lớp bụi, cáu bẩn. Việc làm này cần được thực hiện tối thiểu một lần/năm.
2. **Sử dụng ổn áp điện**: Máy tính vốn rất nhạy cảm với những thay đổi đột ngột của cường độ dòng điện, chỉ cần một sự cố về điện đột ngột như cúp điện, tăng điện, chập mạch… cũng có thể làm hỏng ổ cứng hay nổ bo mạch… Do đó, bạn nên trang bị cho máy tính một bộ ổn áp điện hay một bộ lưu điện - UPS càng tốt.
3. **Tắt nguồn màn hình**: Hầu hết các loại màn hình hiện nay đều có tính năng tắt tự động khi thoát khỏi hệ điều hành, nhưng như thế không có nghĩa là chúng không sử dụng điện, bằng chứng là công tắc màn hình vẫn sáng hoặc nhấp nháy. Thật ra màn hình chỉ đang "ngủ" và vẫn đang hoạt động (sử dụng điện để "ngủ"). Nếu để tình trạng này xảy ra một thời gian dài, đèn hình sẽ bị yếu (đối với màn hình CRT) hoặc xuất hiện các điểm ảnh hỏng (đối với màn hình LCD). Do đó, bạn hãy chịu khó tắt nguồn màn hình mỗi khi không làm việc với máy tính nữa, để máy có thời gian nghỉ ngơi hồi phục "sức khỏe".
4. **Để hệ thống luôn hoạt động**: Không giống như màn hình nên tắt hẳn mỗi khi thoát khỏi hệ điều hành, hệ thống máy tính luôn cần được hoạt động. Rất nhiều người đã không nhận ra rằng khởi động máy tính từ tình trạng "lạnh ngắt" của các bộ phận như: bộ nguồn, bo mạch, ổ cứng… sẽ làm suy giảm rất nhiều tuổi thọ của chúng. Bạn hãy tưởng tượng một cầu thủ ra sân thi đấu mà không khởi động thì liệu anh ta sẽ đá bóng được trong bao lâu?! Cách giải quyết ở đây là bạn nên cho máy tính ngủ ở chế độ Hibernation thay vì Shutdown hoàn toàn khi không làm việc với nó nữa.
5. **Khám sức khỏe cho ổ cứng**: Công việc này rất đơn giản, từ cửa sổ My Computer, bạn kích chuột phải lên biểu tượng ổ cứng muốn kiểm tra, chọn Properties\Tools\Check now. Bạn cũng có thể dùng các phần mềm chuyên nghiệp khác để kiểm tra kỹ hơn. Nếu chương trình phát hiện ổ cứng có nhiều lỗi hay bad sector thì bạn hãy ngay lập tức sao lưu các dữ liệu quan trọng rồi mới tiến hành sửa chữa.
6. **Phòng chống virus**: Bạn có thể sử dụng các chương trình thuộc hàng VN chất

lượng cao như Bkav 2006, D32 (dung lượng nhỏ, hỗ trợ tiếng Việt) hay hàng ngoại như Norton Antivirus 2006, Panda Titanium 2006, Symantec Antivirus…
7. **Kiểm tra pin CMOS**: Cục pin bé tí này còn được gọi là pin nuôi vì dùng năng lượng của mình để "nuôi" các thông tin thiết lập trong Bios đảm bảo cho hệ thống có thể khởi động được. Để kiểm tra tình trạng pin nuôi, bạn chỉ việc để ý đồng hồ hệ thống, nếu thấy nó bắt đầu chạy chậm thì pin nuôi cũng sắp "tiêu" và bạn nên nhanh chóng thay pin mới đi là vừa.
8. **Cẩn thận khi mở thân máy**: Bất cứ khi nào bạn định mở thân máy, hãy nhớ tắt nguồn và rút hẳn phích cắm điện ra khỏi ổ điện. Khi chạm vào các bộ phận bên trong, bạn hãy để cơ thể mình trực tiếp nối đất hoặc thông qua một vật có khả năng dẫn điện nào đó hoặc đeo vòng khử tĩnh điện nhằm tránh làm hỏng các bo mạch do tương tác tĩnh điện.
9. **Bảo trì chuột**: Sau một thời gian sử dụng, chuột sẽ bị bám đầy bụi và cáu bẩn. Đối với chuột bi, bạn sẽ thấy sự di chuyển của nó không còn trơn tru như lúc mới mua mà bắt đầu "phập phù" lúc đi lúc không, có khi nhảy lung tung. Để vệ sinh nó, bạn sử dụng một cái cạo nhỏ cạo cáu bẩn bám trên các thanh nhựa cuộn (phần tiếp xúc với bi), bánh xe cuộn, đồng thời dùng khăn lau chùi cả viên bi nữa. Đối với chuột quang, bạn chỉ việc cạo sạch bụi đất bám theo bánh xe cuộn là được.
10. **Dọn dẹp Registry**: Bạn thích vọc máy tính nên thường xuyên cài đặt, gỡ bỏ các chương trình thử nghiệm vào hệ thống. Sau một thời gian, bạn sẽ thấy hệ thống trở nên chậm chạp đến khó hiểu. Nguyên nhân chủ yếu là do thông tin của các ứng dụng đã gỡ bỏ vẫn còn tồn tại trong Registry và ngày càng nhiều thêm. Kết quả là Registry phình to ra với khá nhiều rác. Để quét sạch các thứ rác thải này, bạn nên dùng những phần mềm chuyên nghiệp như: Registry Mechanic, Tuneup Utilities 2006...

Theo **Đ.Thiên**
Tuổi trẻ

Một số hỏi đáp trên các báo eChip và Làm bạn với Máy vi tính

Phần 1: Hỏi đáp về phần cứng

(?) Tôi thấy RAM KingMax được bán nhiều trên thị trường. Nay tôi muốn hỏi RAM của KingMax có 3 màu Xanh – đỏ - vàng, vậy 3 loại trên có gì khác nhau, loại nào tốt hơn?

Việc KingMax có nhiều màu là do chính sách kinh doanh của nhà sản xuất. Sắp tới RAM KingMax tại thị trường Việt Nam sẽ chuyển toàn bộ bản mạch thanh RAM sang màu vàng để tránh hàng giả. Khách hàng cần chú ý điểm đặc biệt này. Việc khác màu không có khác nhau gì về chất lượng.

(?) Tôi có lắp ráp một bộ máy vi tính với card màn hình ASUS GF6600 16X DDR-128B, TV-O (EN6600/TD/256), main ASUS A8N5X. Tôi đã cài drive đầy đủ cho máy. Vừa qua tôi Format để cài lại Windows XP SP3. Sau khi cài hệ điều hành mới, tôi cài game thì chỉ nghe tiếng mà không có hình. Lúc khởi động thì máy thông báo là không tìm thấy "graphic card information". (Chú ý: Windows XP SP3 ở đây không phải là bản vá của Microsoft)

Chúng tôi không dám cam đoan về chất lượng của Windows XP SP3 này không phải là bản chính thức của Microsoft, sợ có nhiều trục trặc. Để kiểm tra, bạn nên cài lại Windows XP SP 1 hoặc 2 (bản đúng), sau đó cài lại drive cho các thiết bị đầy đủ. Sau đó vào Device Manager để kiểm tra VGA Card. Nếu thấy màu vàng thì drive chưa cài được. Nếu đã bình thường thì bạn nên kiểm tra cấu hình yêu cầu của game. Nếu vẫn chưa được xin hãy mang đến trung tâm bảo hành.

Tôi đang sử dụng máy MP3 Creative Muvo2. Khi ngắt kết nối với máy tính, máy MP3 liền xuất hiện thông báo "filmware error", sau đó máy liền chuyển sang một dòng thông tin khác: "recovery mode v1.00" Tôi đã thử format hay clean up đều không được mặc dù cổng ÚB vẫn kết nối được.

Nếu khi ngắt mà máy của bạn báo lỗi trên chứng tỏ máy của bạn đã bị lỗi về Software

- Khắc phục : Mang đến trung tâm bảo hành (nếu còn hạn bảo hành) hoặc đem đến dịch vụ sửa chữa.

Tôi đang dùng máy tính mainboard Intel 865 GBF. Mỗi khi cắm điện, máy tự hoạt động 2-3 giây rồi tắt. Sau đó, nếu nhấn vào nút Power máy sẽ hoạt động bình thường.

Đây là hiện tượng của các dòng Mainboard Intel do cấu tạo riêng về BIOS. Khi cắm nguồn điện, BIOS sẽ tự khởi động một vòng sau đó sẽ tắt. Có thể vào BIOS khai báo để máy tự khởi động mà không cần nhấn Power (không nên).

Sau một năm sử dụng. USB Flash 256MB Kingston thỉnh thoảng bị tình trạng không còn file nào (dung lượng 0MB). Rút ra cắm lại thì lại hoạt động bình thường. Sau nhiều lần như vậy tôi format USB thì dung lượng chỉ còn 246MB. Sau đó lại xảy ra tình trạng trên và tôi lại format thì dung lượng chỉ còn 240MB

Do đặc điển của loại USB Flash này, mỗi khi format bằng tiện ích của Windows dung lượng sẽ bị giảm đi. Bạn format bằng chương trình riêng của hãng để giữ nguyên dung lượng.

Hiện nay mỗi khi khởi động, máy tính tự khởi động lại một hai lần mới sử dụng được.

Hiện tượng này có thể do xung đột giữa các chương trình diệt virus, chương trình khởi động cùng Windows hoặc có linh kiện phần cứng bị lỗi.

Máy thường xuyên khởi động lại

Nguyên nhân là do nhiệt độ của Mainboard, CPU,... quá nóng.

Một số hỏi đáp trên các báo eChip và Làm bạn với Máy vi tính

Phần 2: Hỏi đáp về phần mềm và mạng

(?) Máy LAPTOP được chia làm ba phân vùng C, D, E. Trong đó phân vùng E là phân vùng Recovery Windows bản quyền.Dạo này máy tính có hiện tượng mỗi lần khởi động Windows là nó lại chạy CheckDisk phân vùng D. Đã Recovery , cả cài lại Windows nhưng nó không hết hiện tượng trên

Máy bị hiện tượng CheckDisk ổ D là do trong quá trình sử dụng đã có hiện tượng tập tin bị chép lên đĩa không đúng và khi đã có lỗi rồi thì dù cho bạn Recovery lại,

máy cũng chỉ khôi phục hệ điều hành trên đĩa C, vì thế vẫn còn hiện tượng CheckDisk. Hiện tượng CheckDisk chỉ xảy ra khi phân vùng có định dạng FAT / FAT32. Để khắc phục, bạn chuyển phân vùng D sang định dạng NTFS. Cách làm:

- Vào Menu Start / Run, gõ cmd rồi Enter
- Trong Command Prompt gõ lệnh convert D: /FS:NTFS /V rồi thực hiện các bước yêu cầu.

(?) Phần mềm tạo ổ ảo trên Windows Vista

Nên dùng chương trình MagicDisk, một sản phẩm miễn phí kèm theo MagicISO (tải tại www.nguonmovietnam.org dung lượng 1,2MB). Sau khi tải về sẽ bắt gặp nhiều cửa sổ cảnh báo của WinVista do chương trình yêu cầu cài đặt các trình điều khiển quản lý CD/DVD thêm vào hệ thống mà Vista chưa hỗ trợ, bạn cứ ciệc xác nhận tất cả.

(?) Gỡ bỏ thanh công cụ của Internet Explorer và Fire Fox

Trình duyệt IE và FireFox cho phép cài đặt thêm khá nhiều thanh công cụ của các hãng khác nhau để mở rộng chức năng. Tuy nhiên, nhiều thanh công cụ lại có thể là adware hoặc gây lỗi, làm chậm tốc độ, gây rối mắt. Việc gỡ bỏ thủ công chúng không hiệu quả và triệt để. Toolbar Uninstaller sẽ giúp giải quyết vấn đề này chỉ với vài thao tác đơn giản. Chương trình miễn phí, tải tại : www2.tt.xdowns.com/uploadFile/2007-8/Toolbar%20Uninstall.rar

(?) Lấy lại dữ liệu bị ẩn bởi Free Hide Folder

Free Hide Folder, chương trình bảo mật dữ liệu bằng cách ẩn chúng đi. Nhưng nếu hệ thống gặp trục trặc và bắt buộc cài lại Windows trong khi bạn chưa gỡ bỏ FHF hoặc cho các thư mục hiện trở lại thì chúng vẫn ẩn đi và chiếm dung lượng. Trong trường hợp này, sử dụng FreeCommander để thấy được các thư mục bị ẩn.

(?) Làm thế nào để xóa các lệnh trong mục RUN của Windows.

Bấm chuột phải lên thanh Taskbar, chọn Properties. Ở cửa sổ hiện ra, chọn thẻ Start Menu, bấm Customize, bấm Clear rồi OK.

(?) Máy tính của tôi xuất hiện thông báo “vnskb32.exe. Application Error” khi Windows khởi động xong và thông báo “Rundll32” lúc tắt máy.

vnskb32.exe là file thực thi của chương trình VietSpell, file này tự động chạy lúc Windows khởi động. Thông báo trên cho biết file này đã bị lỗi. Do vậy bạn gỡ bỏ hoặc cài đặt lại chương trình này.

(?) Tại sao không Download hình ảnh được trong offline explorer

Offline Explorer là chương trình được dùng để tải nội dung trang web, khi đó các thành phần liên quan như hình ảnh sẽ được tải theo. Nếu bỏ chọn tải text tức là không cho phép tải nội dung các tập tin web từ trang chủ, như vậy tập tin liên quan cũng sẽ không được tải. Khắc phục: Vẫn chọn tải text cho trang web hoặc dùng chương trình chuyên để tải ảnh như: PixGrabber, WebPirate,...

(?) Khi khởi động đến màn hình Welcome của WindowXP thì có thông báo lỗi không tìm thấy file Windows\system32\tools\delfolders.exe

Hiện tượng này xảy ra khi cài drive của mainboard ECS, đây là lỗi do chương trình cài đặt không xóa các file của nó đi sau khi kết thúc quá trình cài đặt. Khắc phục: vào menu Start / Run, gõ lệnh regedit. Trong cửa sổ bên trái, tìm đến khóa HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/Windows/CurrentVersion/RunOnce để xóa dòng lệnh chạy file delfolder.exe. Sau đó vào Start/Programs/Startup để xóa Reboot.exe

....

Cách phân biệt một số loại thẻ nhớ thật và thẻ nhớ nhái

Người viết: nhiếp
Thời gian: 2006-09-01
Biên tập: Bad

Thẻ Kingston

Kingston là thẻ nhớ bị làm giả nhiều nhất ở Việt Nam. Ở tất cả các loại sản phẩm

hàng flash mà Kingston đang bán: MMC mobile, SD, CF.... Mức độ làm giả một cách tinh vi, ngay đến cả người chuyên kinh doanh hàng này cũng không phát hiện ra. Trước đây, bạn chỉ có thể phát hiện bằng cách nhìn tem trên thẻ đưa dưới ánh sáng mặt trời sẽ có ánh cầu vồng (giống như trên các tờ tiền). Nhưng rồi thẻ giả cũng có tem y hệt. Nhưng với một ít kinh nghiệm, bạn vẫn có thể?? đánh giá thẻ xịn hay nhái:
- Thẻ nhái thông thường cũng không có serial in màu xanh nằm ở mặt sau của thẻ, không ghi xuất xứ (China, Taiwan hay Japan) hoặc in bằng mực thường, so với thẻ xịn là in laser chìm, không thể tẩy xóa.
- Hiện tại, **Kingston chưa có kế hoạch sản xuất thẻ SD 4GB**. Các dòng sản phẩm thuộc họ SD của Kingston chỉ có dung lượng tối đa 2GB gồm các tên thương mại:
* SD Standard: có tốc độ ghi tối đa 1.5MB/sec (tương đương 10x), tốc độ đọc tối đa 5.5MB/s.
* SD Elite Pro: Tốc độ đọc/ghi tối đa 7.5MB/s. (50x)
* SD Ultimate Memory Card: Tốc độ đọc/ghi tối đa 133x.

Mức độ làm giả thẻ Kingston đã buộc hãng sản xuất phải thay đổi mẫu mã tem của sản phẩm từ đầu tháng 8 năm nay. Các bạn có thể xem mẫu tem mới của hãng tại đây:
http://www.kingston.com/flash/sd_home.asp

Một số hình ảnh về thẻ Kingston nhái đang có tại Việt Nam

Cách phân biệt một số loại thẻ nhớ thật và thẻ nhớ nhái

Người viết: nhiếp
Thời gian: 2006-09-01
Biên tập: Bad

Thẻ Sandisk

Thẻ nhớ Sandisk, một trong 5 nhà sản xuất thẻ nhớ lớn nhất thế giới cũng không tránh khỏi bị làm nhái. Do Sandisk không có đại diện thương mại tại Việt nam nên sản phẩm này trên thị trường đều được nhập không chính thức từ các nguồn hàng trôi nổi không rõ nguồn gốc. Thẻ Sandisk bị làm giả chủ yếu ở 2 dòng chính: SD và CF. Dưới đây, tôi xin đưa cách phân biệt thẻ nhái SD Sandisk Ultra II: Hàng chính hãng có số Serial Number mầu tr¿??ng, phía dưới thẻ bắt đầu bằng chữ BE0603xxxx và phía dưới là chữ Made in China hoặc Made in USA. Với hàng giả mạo thì không có dòng chữ này. Các tem trên thẻ in nhìn kỹ thì hơi nhạt màu hơn. Thẻ xịn thường làm bằng nhựa dầy, bạn bóp 2 mặt thẻ có cảm giác chắc chắn. Thẻ đểu làm bằng nhựa mỏng, cảm giác ọp ẹp, dùng một thời gian nếu không cẩn thận 2 miếng nhựa bảo vệ vi mạch và chíp nhớ flash bên trong bị tách rời ra. Đặc biệt dùng trong trường hợp truy xuất thẻ lâu gây nóng thẻ. Tốc độ copy của thẻ nhái cực kỳ chậm so với thẻ xịn.

GENUINE = Hàng chính hãng; COUNTERFEIT = Hàng giả mạo

Cách phân biệt một số loại thẻ nhớ thật và thẻ nhớ nhái

Người viết: nhiếp
Thời gian: 2006-09-01
Biên tập: Bad

Thẻ Transcend

Thẻ chính hãng thường có serial number đầy đủ, và serial trên thẻ trùng với hộp

nhựa con. Số serial này bạn có thể kiểm tra trực tiếp trên trang web của hãng theo link dưới. Thẻ hàng nhái thường không có serial hay số serial không thể kiểm tra được từ trang web của hãng sản xuất. Ngoài ra, tem in trên thẻ xịn săc nét, màu xanh tươi và mịn hơn tem trên thẻ nhái. Còn đối với thẻ SD của Transcend cũng bị làm nhái nhọ ?ng với số lượng ít hơn MMC mobile. Cách phân biệt chủ yếu dựa vào serial. Bạn có thể kiểm tra trực tiếp Serial tại địa chỉ: http://www.transcendusa.com/Support/SerialNo.asp?

Hàng nhái - Hàng thật mặt trước

Hàng nhái - Hàng thật mặt sau

Vỏ hộp thẻ nhớ thật

Nâng cấp RAM : Chọn đúng loại bộ nhớ mà máy bạn đang cần

Một trong các phương thức cải thiện đáng kể tốc độ hệ thống PC là nâng cấp RAM. Đôi khi công việc này có vẻ khá đơn giản, chỉ cần tắt điện nguồn, mở thùng máy và nhấn thanh RAM vào slot (khe) của nó. Tuy nhiên, điều này chỉ thực sự đơn giản khi bạn chọn đúng loại RAM cho máy tính của mình.

Thực vậy, trên thị trường hiện nay có quá nhiều loại RAM, và để mua đúng thì bạn cần phải biết mainboard của bạn đang thực sự cần loại nào, SDRAM PC133 hay DDR SDRAM PC2700, PC 3200…?

Để biết được mainboard của mình hỗ trợ loại bộ nhớ nào, hãy tham khảo tài liệu đi kèm máy, nếu bạn lỡ đánh mất tài liệu này thì bạn có thể tìm thấy thông tin chi tiết tại website của hãng sản xuất mainboard. Hoặc đơn giản hơn, hãy đến Website của Crucial Technology hoặc Kingston Technology để tải về các tiện ích giúp bạn tìm ra đúng loại RAM mà máy tính mình đang cần.

Sau đây là một vài thông số mà bạn cần quan tâm trước khi nâng cấp RAM:

Maximum module size: Đây là dung lượng RAM tối đa mà mỗi khe cắm trên mainboard (slot) có thể hỗ trợ. Do đó hãy lưu ý đừng mua những thanh RAM có dung lượng vượt quá khả năng cho phép.

Các loại RAM và khe cắm: Hãy tìm xem mainboard của máy tính sử dụng loại nào trong 4 loại RAM sau đây: DRAM (EDO hoặc FPM), SDRAM, DDR SDRAM, RDRAM. Bốn loại này đều được cắm trên 1 trong 3 loại khe là SIMM, DIMM, RIMM:

+DRAM cắm khe SIMM

+SDRAM và DDR SDRAM cắm khe DIMM

+RDRAM cắm khe RIMM

Trong 4 loại trên thì DRAM hầu như không còn được sử dụng, vì vốn nó chỉ được dùng cho các máy đời 386, 486 . Và để nâng cấp loại bộ nhớ này thì rất khó có thể tìm được linh kiện nâng cấp.

Hiện nay đa số các loại mainboard chỉ hỗ trợ chạy 1 loại RAM duy nhất (cùng 1 loại khe cắm). Tuy nhiên cũng có vài loại mainboard cho phép bạn cắm và chạy cùng lúc nhiều loại RAM khác nhau.

Tốc độ RAM: Các loại SDRAM, DDR SDRAM, RDRAM đều được định tốc độ bằng hoặc hơn tốc độ bus hệ thống (FSB - Front side bus, tốc độ truyền dữ liệu giữa CPU và RAM). Nếu hệ thống bạn đang chạy với SDRAM PC66 thì hãy thay thế nó bằng SDRAM PC100 để đạt tốc độ cao hơn. Tuy nhiên, nếu bạn kết hợp nhiều loại SDRAM ở các tốc độ khác nhau thì hệ thống chỉ chạy được với tốc độ thấp nhất trong số đó.

Thứ tự khe cắm (bank): Trong một vài mainboard thì khe gần CPU nhất (thường là bank 0) phải được gắn RAM đầu tiên, sau đó là các bank tiếp theo. Trong khi đó ở một vài loại khác thì bank 0 phải được gắn thanh RAM có dung lượng cao nhất (nếu bạn dùng nhiều thanh cùng lúc).

Điều này có vẻ không quan trọng lắm, tuy nhiên hãy tìm hiểu thêm về thông số của loại mainboard mà bạn đang sử dụng nếu bạn có nhiều hơn 1 thanh RAM với kích thước không đồng đều.

Nonparity hoặc ECC: Nếu hệ thống hỗ trợ tính năng sửa lỗi (error-correcting code – ECC) và có hơn 512MB Ram thì việc mua các thanh nhớ loại ECC sẽ trở nên đáng giá, vì RAM có dung lượng lớn thường xảy ra các lỗi ngẫu nhiên, vốn có thể được sửa chữa bởi mainboard nếu sử dụng RAM ECC.

Tuy nhiên, bạn có thể chạy đồng thời cả hai loại nonparity và ECC mà không gặp vấn đề gì, và dĩ nhiên là chức năng sửa lỗi sẽ không hoạt động.

Cách đơn giản nhất để nhận thấy RAM của bạn có phải là nonparity hoặc ECC hay không là đếm số chip nhớ trên thanh RAM, nếu con số này chia hết cho 3 thì bạn đang có thanh RAM ECC (parity memory), ngược lại nó là loại nonparity.

Thông số CAS (Column address strobe): Thông số CAS (hoặc CL) càng nhỏ thì RAM càng tốt. SDRAM được sản xuất với CL2 hoặc CL3. Còn DDR SDRAM thì có thông số CL2 hoặc CL2.5 .

Trừ phi mainboard của bạn yêu cầu một loại RAM có thông số CAS hoặc CL nhất định nào đó, còn ngoài ra bạn nên chọn loại RAM có thông số CAS (CL) thấp nhất vì giá cả chênh lệch hoàn toàn không đáng kể.

(Theo PCWorld)

Khởi chạy an toàn chương trình đáng ngờ - 18/8/2006 5h:45

Chắc chắn hầu hết người dùng máy tính đều hiểu rõ sự cần thiết của việc thường xuyên cập nhật chương trình phòng chống virus cũng như đề cao cảnh giác khi tải về các phần mềm từ internet. Tuy nhiên, phải làm sao nếu bạn không thể chắc chắn về tính an toàn của phần mềm mà mình muốn thực thi hay cài đặt? Thật đơn giản, bạn có thể thiết lập khả năng cài đặt "có hạn chế" cho bất kỳ phần mềm đáng ngờ nào bằng cách sử dụng một tính năng hữu ích trong Windows XP.

Hình 1

Để khởi chạy an toàn một chương trình, hãy nhấn phải chuột lên biểu tượng (hay shortcut) của chương trình đó và chọn **Run as** (*Hình 1*). Lưu ý, trong vài trường hợp, bạn cần ấn và giữ phím <*Shift*> để thấy tùy chọn **Run As** khi mở trình đơn nhấn phải. Trong hộp thoại **Run As**, bạn chọn **Current user** và đảm bảo rằng tùy chọn **Protect my computer and data from unauthorized program activity** được đánh dấu (*Hình 2*). Sau đó nhấn **OK**.

Khi được thực thi trong chế độ này, chương trình có thể đọc các thông số cài đặt

Registry, nhưng không thể thay đổi chúng. Ngoài ra, nếu đĩa cứng máy tính được định dạng theo NTFS thì chương trình này sẽ không thể thay đổi bất kỳ tập tin nào gắn với tài khoản người dùng (profile) hiện tại,

bao gồm các cookie và tập tin tạm của trình duyệt, màn hình nền và thư mục *My Documents*. Bên cạnh khả năng bảo vệ máy tính trước các chương trình nguy hại được thực thi trong hệ thống thì tùy chọn này chắc chắn sẽ ngăn cản vài ứng dụng "nghiêm túc" khi có nhu cầu lưu lại cài đặt hay tập tin vào những thư mục nêu trên. Do đó, chỉ nên áp dụng tùy chọn này cho các phần mềm với lai lịch không rõ ràng hay bạn chưa từng sử dụng.

Hình 2

Không những thế, khi bạn khởi chạy trình duyệt Internet Explorer với tùy chọn **Run as**, các website sẽ bị vô hiệu hóa khả năng ghi lại dữ liệu trên đĩa cứng nên máy tính cũng sẽ an toàn hơn. Cũng cần lưu ý, ở chế độ này, bạn không thể sử dụng IE để truy xuất đến bất kỳ website được bảo mật nào (bắt đầu bằng "**https://**"). Tương tự, một vài lệnh (chẳng hạn như "*Open Link in New Windows*" trong trình đơn ngữ cảnh) cũng sẽ không hoạt động.

Bùi Xuân Toại

Theo PC World VN

Windows Hacking Rundll32 Shortcuts

"rundll32 shell32,Control_RunDLL" - Run Control Panel

"rundll32 shell32,OpenAs_RunDLL" - Mở cửa sổ 'Open With...'

"rundll32 shell32,ShellAboutA Info-Box" - Mở 'About Window Window'

"rundll32 shell32,Control_RunDLL desk.cpl" - Open Display Properties

"rundll32 user,cascadechildwindows" - Xếp tầng tất cả cửa sổ

"rundll32 user,tilechildwindows" - Minimize All Child-Windows

"rundll32 user,repaintscreen" - Refresh Desktop

"rundll32 shell,shellexecute Explorer" - Re-Start Windows Explorer

"rundll32 keyboard,disable" - Lock The Keyboard

"rundll32 mouse,disable" - Disable Mouse

"rundll32 user,swapmousebutton" - Swap Mouse Buttons

"rundll32 user,setcursorpos" - Set vị trí con trỏ sang (0,0)

"rundll32 user,wnetconnectdialog" - Hiển thị cửa sổ 'Map Network Drive'

"rundll32 user,wnetdisconnectdialog" - Hiển thị cửa sổ 'Disconnect Network Disk'

"rundll32 user,disableoemlayer" - Hiển thị cửa sổ BSOD
chú ý "'(BSOD) = Blue Screen Of Death "'

"rundll32 diskcopy,DiskCopyRunDll" - Hiển thị cửa sổ Copy Disk

"rundll32 rnaui.dll,RnaWizard" - Run 'Internet Connection Wizard', Nếu run với "/1" - silent mode

"rundll32 shell32,SHFormatDrive" - Run cửa sổ 'Format Disk (A)'

"rundll32 shell32,SHExitWindowsEx -1" - Restart Windows Explorer

"rundll32 shell32,SHExitWindowsEx 1" - Shut Down Computer

"rundll32 shell32,SHExitWindowsEx 0" - Logoff Current User

"rundll32 shell32,SHExitWindowsEx 2" Reboot nhanh Windows9x

"rundll32 krnl386.exe,exitkernel" - Bắt Windows 9x Exit

"rundll rnaui.dll,RnaDial "MyConnect" - Run 'Net Connection' Dialog

"rundll32 msprint2.dll,RUNDLL_PrintTestPage" - Choose & Print Test Page của Printer hiện thời

"rundll32 user,setcaretblinktime" - Set tốc độ của con trỏ

"rundll32 user, setdoubleclicktime" - Set tốc độ DblClick

"rundll32 sysdm.cpl,InstallDevice_Rundll" - Search For non PnP Devices

An toàn với Safe mode

Một ngày nào đó bỗng dưng chiếc máy tính thân quen của chúng ta trở chứng, không chịu khởi động trơn tru để nạp hệ điều hành với giao diện màn hình quen thuộc... Có nhiều lý do dẫn đến điều này.

Sau khi đã loại trừ nguyên nhân từ phần cứng, đừng vội can thiệp bằng cách format ổ đĩa để cài lại hệ điều hành bởi Windows đã chuẩn bị cho người dùng một cách khắc phục an toàn thông qua Safe mode.

Có thể vì bạn đã cài vào máy nhiều phần mềm mới, nạp driver cho thiết bị nào đó và xung đột xảy ra. Hãy tái khởi động máy, khi nhận thông báo Please select the operating system to start hãy ấn phím F8 để bước vào chế độ khởi động với Safe mode, với chế độ này hệ điều hành chỉ nạp vào chương trình những file và trình điều khiển thiết bị căn bản cần thiết nhất. Những gì được coi là thừa sẽ không nạp lên. Sau khi vào được Windows, có thể từ môi trường đồ họa đó xử lý sự cố, cũng có thể vào được Safe mode, kế tiếp chỉ cần tái khởi động máy lại là xong. Với Windows XP chế độ Safe mode bao gồm:

- Safe mode: Nạp driver và các file thiết yếu nhất như đã trình bày.

- Safe mode with Networking: Chạy dưới chế độ này, ngoài việc nạp file, driver như thông thường, sẽ có thêm các dịch vụ giúp chúng ta có thể làm việc trong mạng.

- Safe mode with Command Prompt: Tùy chọn này cho phép chạy chương trình và gọi thêm file cmd.exe để hoạt động trong môi trường giao diện dòng lệnh, tất nhiên người dùng phải thông thạo các lệnh trên Dos.

- Enable Boot Logging: Tất cả những trình điều khiển thiết bị và dịch vụ được nạp lên sẽ ghi lại trong file có tên ntbtlog.txt rất hữu ích để chúng ta có thể đọc và tìm ra chính xác nguyên nhân gây trục trặc cho hệ thống.

- Enable VGA Mode: Khởi động và nạp driver căn bản của Windows cho card tăng tốc đồ họa. Nó khá hữu dụng để xác định có phải trước đó bạn đã cài một driver

mới cho card tăng tốc đồ họa và đó chính là nguyên nhân gây ra sự cố.

- Last Known Good Configuration: Máy tính được khởi động và dùng các thông tin trong Registry mà Windows lưu lại từ lần tắt máy hoàn chỉnh gần đây nhất.

- Directory Service Restore Mode: Khởi động và có thể phục hồi qua System Restore.

- Debugging Mode: Có thể phục hồi thông qua Remote Install Service.

Mặc định của việc chạy chương trình Safe mode là ô sáng nằm ở phần khởi động Windows một cách bình thường, do vậy, muốn chọn 1 trong 8 cách nói trên phải dùng phím mũi tên để di chuyển đến rồi nhấn Enter. Khi máy đã vào được Safe mode, việc tìm nguyên nhân, khắc phục hậu quả để hệ điều hành hoạt động trở lại sẽ nhẹ nhàng hơn là cài đặt mới hệ điều hành. Tất nhiên đó là những lỗi, những xung đột không quá nghiêm trọng mà Windows còn có thể khắc phục.

Tạ Xuân Quan

Thực hiện: Lê Duy

Suỵt! Bạn muốn biết bí mật của họ à? Có nhiều điều các công ty công nghệ không hề công bố cho người dùng. Những bí mật này ít nhiều sẽ giúp ích cho bạn khi mua hàng và khai thác hết tính năng của sản phẩm hiện có.

CPU đang dùng có thể chạy nhanh hơn

Một bí mật của các nhà sản xuất CPU: hầu hết các loại CPU đều có thể ép xung để chạy ở tốc độ nhanh hơn bình thường, tăng tốc độ "miễn phí" cho PC của bạn. Trong vài trường hợp hiếm hoi, các CPU cấp thấp có thể chạy ngang bằng với những CPU có giá cao hơn. Bạn hãy đến các trang web chuyên về ép xung như Anandtech (http://www.anandtech.com/) và HardOCP (www.hardocp.com) để biết các "kỷ lục" ép xung. Nhưng khi ép xung, bạn hãy chú ý đến hệ thống tản nhiệt để không làm tổn hại CPU, hầu hết các điều khoản bảo hành không chịu trách nhiệm về việc này.

Để ép xung cho hầu hết các loại CPU hiện nay, thường người ta tăng tốc độ bus của hệ thống, có thể qua chương trình PC Setup (hoặc BIOS) hoặc thông qua một tiện ích chạy trong Windows như nTune của NVIDIA (xem thêm bài "Bí quyết

tinh chỉnh hệ thống"; ID: A0503_78). Mỗi khi tăng tốc độ, bạn nên dùng một tiện ích giám sát, ví dụ Motherboard Monitor, để kiểm tra nhiệt độ của CPU trong khi chạy ứng dụng "nặng" như mã hóa video hay chơi game 3D. Nếu nhiệt độ CPU tăng lên trên 60 độ hoặc nếu hệ thống mất ổn định (như treo máy, máy tự khởi động lại...), bạn hãy giảm bớt tốc độ của thông số trước.

Trục xuất Messenger

Bạn có biết ai dùng Windows Messenger để chat không? Nhiều người không sử dụng đến tiện ích này nhưng nó lại luôn nằm ở khay hệ thống, thậm chí ngay cả khi bạn đã chỉnh lại thiết lập của nó (chọn Tools.Options, nhấn vào tab Preferences và bỏ chọn "Run Windows Messenger when Windows starts" và "Allow Windows messenger to run in the background"). May thay, bạn có thể cho Messenger vĩnh viễn "biến" khỏi Windows; xem hướng dẫn chi tiết tại find.pcworld.com/49002.

Bỏ chọn những mục này là bước đầu tiên để loại bỏ Messenger.

Không nên gia hạn thời gian bảo hành

Bạn vừa mua một PC hay một thiết bị nào đó và người bán khuyên bạn nên mua thêm thời gian bảo hành cho sản phẩm vì rất có lợi về sau. Tuy nhiên, việc này ít khi mang lại lợi ích thật sự.

Người bán thường lúc nào cũng mạnh miệng khuyên người mua như thế vì số tiền bạn nộp thêm để gia hạn thời gian bảo hành có thể được xem là "lợi nhuận ròng" của họ. Gia hạn thời gian bảo hành thường có giá từ 10% đến 30% giá trị của sản phẩm.

ZOOM SỐ

Không phải mọi tính năng zoom đều như nhau. Trong khi zoom quang sử dụng ống kính của máy ảnh để tăng độ phóng đại thì zoom số dùng phần mềm tích hợp trong máy để phóng đại một khung hình trong ảnh mà ống kính thu vào. Phần mềm này hoạt động bằng cách nội suy điểm ảnh – đưa ra một ảnh mới dựa trên các mẫu điểm ảnh gốc. Quá trình này có thể giảm chất lượng hình ảnh, tạo cho ảnh phóng đại mờ đi và có hạt. Zoom quang mới thực sự là con số bạn nên quan tâm nhiều.

Vài hãng sản xuất máy ảnh quảng cáo trên bao bì kết hợp zoom số và zoom quang.

Khi mua thêm thời gian bảo hành, bạn đánh cược rằng sản phẩm đó sẽ hư và chi phí sửa chữa sẽ đắt hơn so với số tiền mua thêm thời gian bảo hành. Tuy nhiên các nhà lập kế hoạch tài chính khuyên hãy dành chi phí gia hạn thời gian bảo hành vào phí sửa chữa hay thay thế sản phẩm (có thể đến lúc đó bạn cần thay sản phẩm mới).

Còn nếu bạn vẫn muốn gia hạn thời gian bảo hành thì hãy đọc kỹ bản giao kèo; đừng dựa trên lời nói đảm bảo của người bán hàng. Gia hạn bảo hành chỉ đem đến sự an tâm khi dùng sản phẩm hơn là dịch vụ mà bạn có được. Bạn hãy tìm những dịch vụ thực sự có ích khi gia hạn, ví dụ dịch vụ bảo hành cho màn hình bao luôn chi phí thay thế đèn hình, điều này chắc chắn trước sau gì cũng xảy ra.

Tận dụng lỗ hổng bảo mật của Windows

Thời gian đáp ứng và độ tương phản của LCD

Thời gian đáp ứng của LCD có thể nói cho bạn biết màn hình sẽ hiển thị hình ảnh chuyển động nhanh tốt như thế nào. Không may là các nhà sản xuất màn hình LCD đo thời gian đáp ứng theo nhiều cách khác nhau, mà các con số này hầu như vô dụng (xem thêm find.pcworld.com/49062). Số đo tỉ lệ tương phản

cũng không thực sự cần thiết.

Các tiện ích tường lửa, quét virus, dò phần mềm gián điệp, chặn pop-up và lọc thư rác đều đồng ý với nhau 1 điểm: Windows bảo mật kém. Và tình hình này có lẽ cũng không mấy sáng sủa cho đến khi Windows Vista xuất hiện (trước đây là Longhorn) vào năm sau. Trong lúc này ta cũng có vài cách để hoán chuyển tình thế bảo mật kém cỏi của Windows thành lợi thế.

Nếu phải cài đặt lại Windows thì bạn sẽ cần đến mã số bản quyền (license key) đi cùng với đĩa cài đặt. Nhưng không phải ai cũng giữ gìn cẩn thận chuỗi 25 số và chữ ngẫu nhiên đó. Dĩ nhiên bạn không thể sử dụng được Windows nếu không kích hoạt nó. Nhưng nhờ vào tính bảo mật kém của Windows, phần mềm miễn phí Keyfinder 1.41 của Magical Jelly Bean Software sẽ lấy lại license key cho bạn trong tích tắc. Chỉ việc đến website www.pcworld.com.vn để tải về (Download, ID: 051019) và chạy ứng dụng này, và ghi mã số đó ra giấy.

Những bí mật chưa tiết lộ

Trong khi mã số bản quyền có thể thất lạc ở đâu đó thì mật mã trang web của bạn cũng có thể không đúng. Ta có thể thiết lập cho Windows nhớ một đống mật mã của mình để không phải mất thời gian gõ mật mã mỗi khi đến một trang web nào đó, ví dụ như Amazon.com. Dù cho các ký tự mật mã khi ta gõ vào đều hiện ở dạng dấu hoa thị (*) nhưng vì Windows tỏ ra khá "thờ ơ" chuyện bảo mật các mật mã dạng này nên bạn có thể lấy lại các mật mã đó bằng cách tải về tiện ích Revelation 2 của Snadboy Software (www.snadboy.com). Tiện ích sẽ hiện lên bất kỳ mật mã nào ẩn dưới lốt hoa thị. Đây là phần mềm miễn phí mặc dù trang web yêu cầu bạn một khoản tài trợ. Một tiện ích khác giá 15 USD là Aqua Deskperience (www.deskperience.com/aqua) cũng có khả năng hiển thị mật mã và thêm vài tính năng khác như chụp hình màn hình và copy text từ bất cứ ứng dụng nào (bao gồm cả những nơi mà bạn không thể chạy lệnh copy).

Aqua Deskperience giải mã những mật mã ẩn dưới dấu hoa thị.

Cuối cùng, nếu mật mã mà bạn quên chính là mật mã quyền quản trị Windows XP, Microsoft có cách giúp bạn xóa mật mã đó (xem find.pcworld.com/48942).

Bạn có thể tiết kiệm bộn tiền khi mua các gói phần mềm tên tuổi

Giá OEM rẻ hơn giá bán lẻ		
Phần mềm	**Giá bán lẻ (USD)**	**Giá OEM (USD)**
Microsoft Windows XP Pro (SP2)	306	136
Microsoft Windows XP Home (SP2)	199	85

Microsoft Office Pro Edition 2003	380	300
Symantec Norton Internet Security	68	46

OEM: 3 mẫu tự này viết tắt từ "Original Equipment Manufacturer", có thể tiết kiệm cho bạn hơn 50% giá phần mềm (xem bảng). Được điều chỉnh cho hợp với các hệ thống bán kèm, các bản phần mềm OEM hiện nay được bán khá phổ biến, ví dụ tại các cửa hàng trực tuyến như Directron (directron.com) và Newegg (newegg.com). Có những cửa hàng được hỗ trợ để chuyên bán phần mềm OEM đi kèm với phần cứng. Do vậy, với hệ điều hành, bạn phải mua luôn trọn bộ PC thì mới có giá OEM của HĐH đó. Nhưng hầu hết các nhà sản xuất phần mềm cho phép các cửa hàng trực tuyến bán bản OEM cho bất cứ ai mua phần cứng nào, ngay cả chỉ mua 1 con chuột.

Phần mềm OEM thông thường bán ra không có hộp, không có tài liệu hướng dẫn hoặc hỗ trợ kỹ thuật so với phiên bản bán lẻ thông thường. Nhưng bù lại bạn tiết kiệm được khá nhiều tiền.

Điểm chết trên màn hình LCD không thể phục hồi được

Bất kỳ một chi tiết bất thường nhỏ nào xảy ra trong quá trình sản xuất màn hình đều có thể tạo các điểm ảnh chết - điểm luôn sáng hoặc tối bất kể màn hình hiển thị ảnh gì. Từ khi xuất hiện màn hình LCD 19 inch chuẩn có gần 4 triệu các pixel con màu đỏ, xanh dương và xanh lá thì chẳng ngạc nhiên gì khi nhà sản xuất lảng tránh việc thay thế màn hình chỉ có 1 hoặc 2 điểm chết.

Nhưng chuẩn mực màn hình ngày càng cao. Chế độ bảo hành Perfect Panel của Philips và chế độ bảo hành cho màn hình MTXT V6V của Asus sẽ thay thế màn hình ngay cả khi có 1 điểm chết.

Chế độ bảo hành màn hình LCD của phần lớn nhà sản xuất đều đưa ra số lượng điểm chết tối thiểu trước khi họ thay cho người dùng màn hình mới. Thông thường, bạn có thể kiểm tra chính sách bảo hành điểm chết bằng cách tra trên trang web của hãng về thông số "dead pixels" hoặc "pixel criteria". Hoặc bạn có thể thấy chính sách này trong tài liệu PDF trong đĩa hướng dẫn đi kèm màn hình.

Ví dụ, ViewSonic sẽ thay thế màn hình 14 đến 15 inch khi có 4 điểm chết trở lên; màn hình 17 đến 19 inch là 7 điểm chết trở lên; và màn hình từ 20 inch trở lên với 10 điểm. Dell sẽ thay thế màn hình với điều kiện trên 6 điểm chết; NEC yêu cầu 10 điểm. Hầu hết nhà sản xuất cũng sẽ xem xét thay thế màn hình nếu điểm chết đó

nằm ở vùng giữa màn hình.

Điện thoại di động của bạn có vấn đề

Để buộc bạn dùng dịch vụ của họ, các nhà cung cấp dịch vụ thường "khóa" điện thoại để bạn không thể dùng dịch vụ của các nhà cung cấp dịch vụ cạnh tranh khác (hay đôi khi cấm một số tính năng nào đó). Nhưng nếu bỏ ra ít thời gian và công sức, bạn có thể "mở khóa" điện thoại của mình không cần nhà cung cấp dịch vụ tiếp sức. Nhưng hãy cẩn thận, làm vậy có thể làm mất giá trị bảo hành điện thoại. Hãy đọc kỹ chế độ bảo hành.

Tại sao các nhà cung cấp dịch vụ làm như vậy? Lợi nhuận. Thông thường họ tính tiền cho chiếc điện thoại đó thấp hơn so với hãng khác, do vậy họ muốn lấy lại số tiền "bù lỗ". Ví dụ, vài nhà cung cấp dịch vụ gây khó khăn cho người dùng trong việc thiết lập Bluetooth để sử dụng điện thoại như modem quay số cho MTXT hoặc thiết bị cầm tay nào đó (ép bạn phải dùng các dịch vụ truyền dữ liệu vô tuyến khác). Các điện thoại GSM bị khóa cũng làm bạn tốn tiền khi đi du lịch, bạn không thể thay đổi SIM (Subscriber Identity Module, tấm thẻ nhỏ lưu trữ số điện thoại và thông tin định danh điện thoại của bạn) của nhà cung cấp dịch vụ nơi bạn đi du lịch, và vì vậy bị tính tiền dịch vụ chuyển vùng (roaming).

Mạng Cingular không cung cấp mã mở khóa cho điện thoại mà hãng cung cấp

Một kỹ thuật dễ nhất và thông dụng nhất để mở khóa là nhập với các số đặc biệt qua các phím số, cụ thể là một mật mã để mở khóa cộng với số IMEI (International Mobile Equipment Identifier, số định danh thiết bị di động), ESN (Electronic Serial Number, số seri của thiết bị) hoặc mã MSL (Master Subsidy Lock). Với một số model của Samsung và Sony Ericsson, bạn có thể mở khóa bằng cách kết nối chúng với một PC sử dụng một sợi cáp riêng và phần mềm. Cách an toàn nhất để có mã số mở khóa là từ nhà cung cấp dịch vụ.

Nếu nhà cung cấp dịch vụ của bạn từ chối mở khóa, các hãng thứ 3 sẽ bán mã mở khóa cho bạn khoảng từ 30 USD trở lên. Khi tìm với từ " unlock phone", Google sẽ đưa bạn đến Bongo Wireless (www.bongowireless.com), GSM Locker (www.gsmlocker.com) và Mobile Fun (find.pcworld.com/49320), những công ty này đều kinh doanh trên web. Có lẽ bạn nên đi đến cửa hàng điện thoại (đảm bảo là kinh doanh hợp pháp) thì hay hơn vì bạn có thể nói cụ thể cho họ biết vấn đề của mình; hãy hỏi chi tiết về giá và bảo hành. Nếu mã mở khóa không hoạt động, bạn có được nhận lại tiền không? Cửa

hàng đó sẽ xử lý ra sao nếu mã mở khóa làm hỏng điện thoại của bạn?

Tìm trên Google cũng sẽ đưa bạn đến các diễn đàn và blog mà người dùng điện thoại chia sẻ những bí mật mở khóa, ví dụ như Howard Forums (www.howardforums.com, cần đăng ký) và Treonauts (www.treonauts.com) cung cấp cho bạn những mẹo mở khóa máy Palm Treo 650 (find.pcworld.com/49036). Vài trang blog cũng giúp bạn "khai thông" việc chuyển tập tin qua ngõ Bluetooth. Ví dụ, IrishEyes (find.pcworld.com/49035) và RussellBeattie.com (find.pcworld.com/49034) có bản hướng dẫn làm thế nào để thiết lập Bluetooth cho điện thoại Motorola v710.

Các nhà sản xuất thiết bị cao cấp không luôn luôn chế tạo sản phẩm của họ

Ngày nay, thật khó mà biết được thực chất ai sản xuất bất cứ thiết bị nào. Trong tình hình lợi nhuận sút giảm, các hãng lớn như Dell và HP thường tiết kiệm bằng việc gửi thiết kế và sản phẩm mẫu của họ cho các công ty ít tên tuổi gia công (thường là các công ty ở nước ngoài), đôi khi cùng một công ty sản xuất linh kiện cho 2 "ông lớn" cạnh tranh nhau.

Ví dụ, hầu hết các nhà cung cấp màn hình LCD không tự sản xuất panel màn hình. Dell mua panel màn hình 24 inch cho model 2405FPW của mình từ Samsung; HP mua panel màn hình l2335 của Philips. Cũng vậy, một số hãng cung cấp các linh kiện cơ bản cho hầu hết đầu ghi CD và DVD.

Vậy thì có phải màn hình của NEC không tốt hơn model Brand X cũng được sản xuất trên cùng loại panel, hay đầu ghi DVD của Sony cũng chẳng khác biệt gì so với một đầu ghi vô danh nào đó được chế tạo với cùng linh kiện ổ quang? Không hoàn toàn. Câu trả lời phần lớn phụ thuộc vào loại sản phẩm mà bạn mua.

Công suất loa

Các nhà sản xuất loa có cả "rổ" mẹo để thổi phồng con số công suất cho loa của họ. Khi mua loa bạn đừng nên dựa quá nhiều vào chỉ số công suất, đặc biệt là đối với loa máy tính. Bất cứ chuyên gia âm thanh nào cũng đều khuyên bạn cách hay nhất là bạn ngồi nghe thử loa trước khi mua. Vì vậy, hãy bỏ tờ ghi chi tiết kỹ thuật sang một bên, lấy một CD mà bạn hay nghe và nghe nó trước khi chọn mua loa. Còn nếu bạn vẫn khăng khăng dựa vào chi tiết kỹ thuật của loa thì hãy tìm thông số có ghi là Watts RMS mà ghi thông số công suất của từng kênh loa cụ thể, không phải con số ghi công suất của toàn hệ thống.

Ví dụ, với màn hình LCD, các nhà sản xuất có nhiều cách để thêm tính năng và cải

tiến về chất lượng tổng thể của sản phẩm. Các hãng như Dell hay HP có thể đầu tư nhiều hơn công ty vô danh nào đó về thiết kế kiểu dáng công nghiệp, các tùy chọn điều chỉnh và giao diện người dùng để chỉnh thiết lập màn hình.

Đối với các sản phẩm phổ thông như ổ quang, kiểu dáng gần như định hình, không thay đổi và giá giảm khá thấp vì vậy lợi nhuận qua việc cạnh tranh mà nhà sản xuất thu được khá ít, nên các hãng tên tuổi không bỏ nhiều công sức để cải tiến sản phẩm. Dĩ nhiên, vẫn có những khác biệt quan trọng trong chế độ bảo hành, bảo trì, hỗ trợ kỹ thuật và phần mềm đi kèm của riêng mỗi nhà sản xuất. Tuy vậy, tốc độ của 2 sản phẩm dùng cùng loại linh kiện cơ bản thì gần như nhau. Trong trường hợp này, bạn nên chọn sản phẩm chất lượng tốt hơn là chọn sản phẩm theo nhãn hiệu, ví dụ như chọn sản phẩm có tốc độ nhanh nhất hoặc ổ rẻ nhất.

Tìm số điện thoại, địa chỉ thực

Đôi khi việc hỗ trợ kỹ thuật qua e-mail hoặc chat không thể thay việc thảo luận trực tiếp qua điện thoại. Nhưng việc gọi điện thoại như vậy rõ ràng không tiết kiệm chút nào, nên để giảm chi phí cho người dùng, các hãng kinh doanh trên mạng thường ít khi cho số điện thoại, hoặc bạn sẽ rất khó kiếm số điện thoại của họ. Đừng lo, nhiều trang web có thể thay thế cho cuốn danh bạ điện thoại của bạn. Ở Việt Nam, bạn có thể vào www.yp.com.vn của công ty Cổ phần Niên Giám Điện Thoại và Trang Vàng 2 để tra theo địa chỉ, số điện thoại hoặc theo ngành nghề; trangvang.fpt.vn của công ty FPT; hoặc danhba.vdc.com.vn của công ty VDC. Nếu tra theo tên doanh nghiệp, bạn có thể vào www.yellowpages.com.vn của công ty Trang Vàng Việt Nam; www.vidc.com.vn của phòng Thương Mại Và Công Nghiệp Việt Nam... Nếu cần biết số điện thoại của những công ty kinh doanh trực tuyến tên tuổi, trang web Cliché Ideas (www.clicheideas.com) sẽ cung cấp cho bạn.

Máy chơi game PlayStation Portable của Sony vẫn có thể hack

Vô hiệu Security Center

Bạn giữ cho Windows khá an toàn, nhưng đôi khi bạn không thể ngăn Security Center của Windows thông báo hệ thống trong tình trạng không an toàn (ví dụ: "Your computer might be at risk") cứ mỗi sáng khi bạn mở máy. Để vô hiệu hóa thông báo này, bạn vào "Start.Control Panel.Security Center". Sau đó nhấn Change the way security center alerts me, bỏ mọi dấu chọn trong các khung cửa sổ trong mục này.

Có thể hack các hệ máy game console

Các máy game console ngày nay khá mạnh và được trang bị công nghệ cao, vì vậy chẳng ngạc nhiên gì khi các tay hacker lúc nào cũng tìm ra nhiều cách mới để khiến chúng làm được nhiều thứ hơn là chơi game. Ví dụ, Xbox là thuần chất PC với phần cứng đồ họa và âm thanh được cấu hình riêng và một CPU có cách đây vài thế hệ. Chỉ việc hack một chút, bạn có thể cài Linux vào Xbox và sử dụng nó y như một PC bình thường. Xem http://xbox-linux.org/wiki/ để có hướng dẫn từng bước cài Linux trên Xbox và trang web có thể trả lời bạn bất kỳ câu hỏi nào đó liên quan (nhưng tôi không tìm thấy cách đơn giản tương tự để chuyển một Xbox thành PC chạy Windows).

Trong vòng chỉ 1 tuần sau khi được tung ra, PlayStation Portable của Sony đã bị hack để người dùng tùy biến hình nền và lướt web sử dụng một trình duyệt bí mật sẵn có trong game Wipeout Pure. Trang web PSP Hacks (http://www.psp-hacks.com) chỉ tường tận về cách hack này và các kiểu hack khác, như cho phép thiết bị chạy phần mềm nào đó. Khi viết bài này, Sony vừa đưa ra bản cập nhật firmware để thêm vào trình duyệt web và ảnh nền có thể tùy biến, nhưng khóa các kiểu hack mới nhất.

Bạn có thể dùng iPod để chuyển nhạc

Apple không tạo sẵn cho máy nghe nhạc iPod cách sao chép thư viện nhạc từ PC, nhưng bạn có thể làm điều này. Nếu hệ thống bạn chạy Windows, đơn giản chỉ việc cắm iPod vào, tìm iPod trong Windows Explorer, và đảm bảo Windows Explorer có thể nhìn thấy các tập tin ẩn.

Mở thư mục iPod_Control và chép thư mục My_Music vào PC của bạn. Nhập những track nhạc đó vào iTunes và đặt chúng theo thứ tự. Chọn Edit.Preferences, và chọn tab Advanced. Chọn một nơi để chứa thư viện nhạc bằng cách nhấn nút Change, và sau đó chọn Keep iTunes music folder organized.

Một số tiện ích như iPodRip giá 15 USD có bản cho PC và Mac của The Little App Factory (thelittleappfactory.com) có thể tự động thực hiện quá trình trên.

Máy nghe nhạc MP3 mau hết pin

Tốc độ truyền dữ liệu cao nhất

Các nhà sản xuất ổ cứng thích đẩy mấy con số lên cao, ví dụ như tốc độ truyền dữ liệu cao nhất của ổ (bus transfer rate), nhưng con số này ít có ý nghĩa. Một ổ SATA chuẩn có thể truyền dữ liệu cao nhất đạt mức 150MBps trong khi đọc/ghi từ bộ nhớ đệm. Nhưng điều này không thường xảy ra. Một ổ cứng có tốc độ truyền dữ liệu trung bình (thường khoảng 65MBps) thì có nhiều ý nghĩa về tốc độ hơn so với thông số tốc độ tối đa.

Các máy nghe nhạc số hiện nay và các thiết bị di động khác thường có 2 mức tắt máy. Mức đầu là chuyển máy sang chế độ chờ (standby) để bật nguồn trở lại cho nhanh sau một thời gian máy không hoạt động. Nhưng ở chế độ này, mạch điện luôn ở trạng thái hoạt động và cũng liên tục tiêu hao một lượng điện nhất định. Đây là điều mà Jan Schuppius và vài thành viên khác của diễn đàn hỗ trợ MP3 của Creative Labs phát hiện được khi chế độ này giảm thời gian dùng pin của các máy Zen Micro từ 12 giờ xuống thấp hơn 6 giờ (xem thêm tại find.pcworld.com/48956).

Creative đã sửa lỗi này vào đầu tháng 7 khi đưa ra cập nhật firmware, giảm thời gian chờ xuống còn 4 giờ trước khi thiết bị tắt nguồn hoàn toàn, nhưng vấn đề trên vẫn còn xảy ra với IRiver H10. Các nhà sản xuất thiết bị có thể theo chân Creative trong việc giảm thêm thời gian chờ hoặc sửa lại trục trặc này bằng cách cho phép người dùng có thể tắt nguồn hoàn toàn. Nếu được như vậy, nhiều máy nghe nhạc MP3 sẽ cho thời gian dùng pin lâu hơn.

Lê Duy
PC World Mỹ 10/2005

Phương thức bảo vệ thông tin cá nhân với mật khẩu kiên cố

Password là các mã khóa mà bạn sử dụng để truy cập thông tin cá nhân mà bạn đã lưu trên máy tính và trong tài khoản online của bạn.

Nếu các tên trộm hay người dùng nguy hiểm khác lấy trộm thông tin này, họ có thể sử dụng tên của bạn để mở tài khoản credit card của bạn. Và trong nhiều trường hợp bạn không chú ý đến những sự tấn công này cho tới khi nó đã quá muộn. Tuy nhiên, việc tạo một password tốt và bảo vệ chúng là không khó.

Làm gì để tạo một password vững chắc

Với một kẻ tấn công, một password mạnh nên xuất hiện bằng chuỗi các ký tự ngẫu nhiên. Tiêu chuẩn dưới đây có thể giúp password của bạn làm được như vậy:

Tạo chiều dài. Mỗi ký tự mà bạn thêm vào password của mình để tăng sự an toàn, password của bạn nên có chiều dài trên 8 ký tự, 14 ký tự hay hơn nữa là lý tưởng.

Nhiều hệ thống cũng hỗ trợ việc sử dụng space bar trong passwords, vì vậy bạn có thể tạo một nhóm từ được hình thành bằng nhiều từ (gọi là một "pass phase"). Một pass phase này thường dễ nhớ hơn một password đơn, miễn là chúng dài hơn và khó đoán hơn.

Kết hợp các ký tự, số, và các symbol. Sự đa dạng của các ký tự mà bạn có trong password sẽ làm cho nó trở nên khó đoán hơn. Các đặc trưng quan trọng bao gồm:

- Các kiểu ký tự và chiều dài nó nên có trong password. Một chuỗi 15 ký tự gồm các chữ cái và số ngẫu nhiên sẽ tạo cho bạn một password vững hơn khoảng 33.000 lần so với password chỉ có 8 ký tự từ bàn phím. Nếu bạn không thể tạo password bao gồm các symbol thì bạn phải cho nó dài hơn một cách đáng kể để có thể có được mức bảo vệ tương tự. Một password lý tưởng là kết hợp cả hai chiều dài và các loại khác nhau của symbol.

- Sử dụng toàn bộ keyboard, không chỉ các ký tự chung. Các symbol được lấy bằng cách giữ phím "Shift" để lấy các ký tự trên của một phím là rất phổ biến trong password.

Sử dụng các từ và các cụm từ dễ nhớ nhưng khó đoán cho người khác. Cách tốt nhất để nhớ mật khẩu của bạn và các cụm từ là viết chúng ra. Không có gì sai khi

viết các mật khẩu của bạn ra nhưng chúng cần phải được bảo vệ để đảm bảo được độ an toàn và hiệu quả.

Tạo một password an toàn và dễ nhớ theo 6 bước:

1. Nghĩ những câu mà bạn có thể nhớ. Ví dụ: “My son Aiden is three years old”

2. Kiểm tra xem máy tính hay các hệ thống online có hỗ trợ các khoảng trống hay không.

3. Nếu máy tính hay các hệ thống online không hỗ trợ các khoảng trống, thì phải biến đổi nó thành một mật khẩu bằng cách lấy các chữ đầu của mỗi từ trong câu. Ví dụ bằng việc sử dụng ví dụ trên thì bạn sẽ đặt là “msaityo”.

4. Thêm tính phức tạp bằng cách trộn các chữ hoa, chữ thường và số.

5. Cuối cùng, thay một vài kí tự đặc biệt. Bạn có thể sử dụng các symbol trông giống các chữ cái, các từ kết hợp (thay thế các khoảng trống) và các cách khác để làm cho mật khẩu của bạn phức tạp hơn.

6. Kiểm tra mật khẩu của bạn với Password Checker. Password Checker là một trang web không ghi lại mà chỉ giúp bạn xác định sự an toàn mật khẩu của bạn.

Một vài điểm mà password phải tránh:

Có vài phương pháp đã được sử dụng để tạo các mật khẩu lại rất dễ bị đoán bởi các tên tội phạm. Để tránh điểm yếu này, chúng ta phải tránh những trường hợp như sau:

*
Tránh các chuỗi hoặc các ký tự lặp lại: ví dụ 123456, 2222
*
Tránh sử dụng những thay thế giống nhau giữa chữ và số: ví dụ thay i -> 1 hay a -> @
*
Tránh tên đăng nhập của bạn
*
Tránh các từ trong từ điển theo bất kỳ ngôn ngữ nào
*
Sử dụng nhiều hơn một password ở mọi nơi

*
Tránh sử dụng lưu trữ online

Tùy chọn "blank password"

Một "blank password" (không có password) trên account của bạn là an toàn hơn so với các mật khẩu kém như "1234". Các tội phạm có thể dễ dàng đoán một mật khẩu đơn giản, nhưng trên các máy tính sử dụng Window XP, một tài khoản không có password không thể truy cập từ xa bởi mạng nội bộ hay trên Internet (Các tùy chọn này không có sẵn cho Microsoft Window 2000, Windows Me..). Bạn có thể chọn để sử dụng một "blank password" trong account máy tính của bạn nếu máy tính của bạn có những tiêu chuẩn sau:

*
Bạn chỉ có một máy tính hay bạn có vài máy tính nhưng bạn không cần truy cập thông tin trên một máy tính này đến máy tính khác.
*
Máy tính phải bảo đảm về mặt vật lý (bạn phải tin tưởng mọi người đều có truy cập vật lý đến máy tính).

Sử dụng một "blank password" không phải luôn là một ý tưởng tốt. Ví dụ: một máy tính xách tay mà bạn mang theo bạn không thể an toàn về mặt vật lý, vì thế bạn nên cần có một password tốt.

Truy cập và thay đổi password như thế nào

<u>Các account online</u>

Các trang web có các điều khoản khác nhau, các điều khoản này chi phối cách mà bạn có thể truy cập hay thay đổi password của bạn. Bạn sẽ phải tìm một link (như là "My account") trên trang chủ của trang để link tới trang đặc biệt dùng để quản lý mật khẩu và accout của mình.

<u>Các password máy tính</u>

Các file trợ giúp cho hệ thống máy tính của bạn thường cung cấp thông tin về việc tạo, thay đổi và truy cập các user account được bảo vệ mật khẩu. Bạn có thể thử tìm thông tin này online tại các trang của các hãng sản xuất phần mềm. Ví dụ: nếu bạn sử dụng Window XP, phần hỗ trợ có thể hiển thị cho bạn thấy được công việc này như thế nào để quản lý password, thay đổi password.

Giữ mật khẩu của bạn thật bí mật

Hãy giữ thật cẩn thận các mật khẩu của bạn và các pass phrase.

*
Không tiết lộ chúng cho người khác. Giữ các mật khẩu của bạn ẩn so với các bạn của bạn và các thành viên trong gia đình (đặc biệt là trẻ con). Các mật khẩu mà bạn cần để chia sẻ với các người còn lại, như là mật khẩu để account ngành ngân hàng của bạn mà bạn có thể chia sẻ vợ hay chồng của bạn chỉ là các ngoại lệ.
*
Bảo vệ bất kỳ mật khẩu nào được ghi chép. Cần cẩn thận nơi mà bạn giấu mật khẩu mà bạn đã ghi hay viết ra.
*
Không bao giờ cung cấp mật khẩu của bạn trên e-mail hay dựa vào một yêu cầu e-mail.
*
Thay đổi password của bạn một cách thường xuyên
*
Không đánh password của bạn trên máy tính mà bạn không điều khiển nó.

Phải làm gì khi password bị đánh cắp.

Bảo đảm kiểm tra tất cả các thông tin mà bạn bảo vệ với mật khẩu, như là các tuyên bố tài chính hàng tháng của bạn, các bản báo cáo credit, các tài khoản shopping online... Các mật khẩu tốt, dễ nhớ có thể giúp bạn chống lại kẻ gian trá và nhận dạng những tên trộm mà không có các bảo vệ. Nếu một ai đó đột nhập vào hệ thống và lấy mất các thông tin này của bạn thì họ sẽ có được mật khẩu của bạn. Nếu bạn để ý thấy bất cứ một hành động nghi ngờ là có ai đó truy cập thông tin của bạn hãy thông báo cho các chuyên gia biết ngay nếu bạn có thể. Hãy xem thêm thông tin trên “what to do” nếu bạn nghĩ sự nhận dạng của bạn đã bị đánh cắp hay bạn có thể đang giống như bị lừa.

(Theo Microsoft)

Thực hiện: Bùi Xuân Toại

Thỉnh thoảng, tôi nhận được từ Windows một thông báo lỗi cho biết một trong các chương trình của mình đang gặp trục trặc và yêu cầu gửi báo cáo về sự cố này cho Microsoft. Tôi có nên thực hiện theo đề nghị của Windows?

Loại thông báo lỗi trên (được bổ sung vào Windows XP) sẽ cho bạn biết hệ điều hành đã tạm ngưng một chương trình mà nếu bạn tiếp tục cho phép chương trình này hoạt động có thể gây ra tình trạng "treo" Windows. Microsoft khẳng định rằng không sử dụng các thông tin này để theo dõi bạn và các báo cáo đó sẽ rất hữu ích trong việc ngăn chặn các sự cố tương tự xảy ra trong tương lai.

Dù vậy, vẫn còn vài rủi ro về bảo mật. Các cuộc thử nghiệm gần đây của Cục Tư Vấn Về Sự Cố Và Năng Lượng Máy Tính Mỹ cho thấy "đống rác bộ nhớ" được gửi cho Microsoft thỉnh thoảng cũng chứa đựng những thông tin thu gom từ tài liệu của người dùng (để hiểu rõ hơn về vấn đề này, bạn tham khảo find.pcworld.com/56568). Trong mọi trường hợp, bạn có thể nhấn nút Dont Send để nhanh chóng quay trở lại công việc, tuy nhiên Windows không bắt buộc bạn phải quyết định như vậy đối với tất cả sự cố. Bạn có thể thiết lập để Windows gửi hoặc không gửi báo cáo lỗi đến Microsoft.

Quyết định ứng dụng nào trong Windows Vista cần gửi báo cáo lỗi đến Microsoft khi gặp sự cố.

Trong Windows XP, bạn chọn Start.Run, gõ vào lệnh system.cpl và nhấn <Enter>. Trong cửa sổ System Properties, bạn chọn thẻ Advanced và nhấn vào nút Error Reporting.

Bạn có thể vô hiệu hóa tất cả báo cáo lỗi hoặc chỉ những báo cáo lỗi dành cho hệ

điều hành hay ứng dụng cũng như kết hợp cả hai. Nếu muốn kích hoạt tính năng báo cáo lỗi, bạn nhấn nút Choose Programs để bổ sung các ứng dụng cần thông

báo lỗi khi gặp sự cố. Khi đã thực hiện xong, nhấn OK hai lần để kết thúc.

Trong khi đó, thông báo lỗi của Vista không hỏi ý kiến người dùng về việc gửi đi các báo cáo. Mặc định, hệ điều hành này sẽ gửi báo cáo lỗi đến Microsoft trừ khi bạn đã hướng dẫn nó không thực hiện việc này từ trước. Bạn chọn Start, và trong hộp thoại Start Search, gõ vào lệnh problem reports and solutions và nhấn <Enter>, sau đó chọn Change settings.Advanced settings. Trong hộp thoại Advanced settings for problem reporting, bạn có thể tắt tính năng gửi báo cáo, cho phép người dùng khác được quyền tự thiết lập tùy chọn này và liệt kê các chương trình không nên thông báo lỗi mỗi khi gặp sự cố (xem hình). Nhấn OK 2 lần và đóng cửa sổ Problem Reports and Solutions để các thay đổi bắt đầu có hiệu lực.

THU GỌN TRÌNH ĐƠN OFFICE

Làm cách nào để loại bỏ một khoản mục khỏi trình đơn của Microsoft Word?

Loại bỏ các khoản mục không cần dùng sẽ làm cho việc thao tác trên trình đơn trở nên dễ dàng hơn. Thủ thuật sau đây có thể áp dụng cho Word, Excel và các chương trình khác trong Microsoft Office phiên bản 2000, 2002 và 2003.

Trong chương trình có khoản mục trình đơn không dùng đến, bạn chọn Tools.Customize, khi hộp thoại Customize mở ra, nhấn chuột lên thanh trình đơn có chứa khoản mục cần loại bỏ, nhấn phải chuột lên khoản mục tương ứng và chọn Delete. Tiếp theo, bạn nhấn Close để đóng hộp thoại lại.

Office 2007 không cung cấp các trình đơn nên không có gì để bạn tùy biến. Loại bỏ các khoản mục khỏi thanh công cụ dạng ribbon không phải là một phương án tốt. Tuy nhiên, bạn có thể tùy biến thanh công cụ Quick Access Toolbar và các biểu tượng phím tắt trong các ứng dụng Office 2007: nhấn chuột lên biểu tượng Office ở góc trên bên trái màn hình, chọn nút các tùy chọn ở cuối danh sách vừa xuất hiện, sau đó chọn Customize ở khung cửa sổ bên trái.

Bùi Xuân Toại
PC World Mỹ 5/2007

Máy tự động tắt khi chạy nhiều chương trình

Đó hỏi: Không hiểu sao dạo này máy tính em chạy nhiều chương trình 1 lúc thì báo lỗi và tự động tắt ứng dụng đó đi. Vào Start > Run cũng không được. Máy báo "Your system is low on virtual memory....". Vậy em phải làm sao?
<usa007tk09@>

Đây trả lời: Theo như lỗi mô tả thì nguyên nhân là do máy tính của bạn thiếu bộ nhớ ảo (virtual memory). Thông thường khi cài đặt Windows, máy tính sẽ tự điều chỉnh dung lượng của bộ nhớ ảo này mặc định nằm trong phân vùng chứa hệ điều hành, tuy nhiên nếu dung lượng còn lại của phân vùng chứa bộ nhớ ảo này quá nhỏ thì Windows sẽ ra thông báo, đồng thời nếu bạn chạy nhiều ứng dụng máy tính sẽ bị chậm. Để khắc phục hiện tượng này, bạn làm như sau:
- Tăng dung lượng trống của phân vùng cài đặt Virtual memory bằng cách xóa bớt chương trình cài trong phân vùng đó và cài vào phân vùng khác của ổ cứng hoặc dùng tiện ích Disk Cleanup trong Windows để dọn dẹp ổ cứng.
- Điều chỉnh lại phân vùng cài đặt hay dung lượng của Virtual memory: Bạn nhấp chuột phải vào biểu tượng My Computer trên desktop vào Properties > chọn thẻ Advanced > Trong vùng Performance nhấn vào Setting, bạn tiếp tục chọn thẻ Advanced nhấn vào nút Change ở bên dưới, trong cửa sổ Virtual Memory, bạn chọn phân vùng cần thiết lập bộ nhớ ảo (lưu ý: phân vùng này phải có dung lượng trống lớn hơn phân vùng trước đó), chọn tiếp vào mục System managed size hoặc vào Custom size để tự điều chỉnh dung lượng bộ nhớ ảo

Theo Echip

"Tăng lực" cho máy tính

Thực hiện: Bùi Xuân Toại

Thực tế cho thấy, bạn không nhất thiết phải chi nhiều tiền để trang bị cho chiếc máy tính để bàn của mình những tính năng cao cấp vốn chỉ có ở máy tính dành riêng cho nhu cầu chơi game và xử lý đồ họa. Vài biện pháp nâng cấp đơn giản và kinh tế vẫn có thể giúp đẩy hiệu năng hệ thống của bạn lên một tầm cao mới.

Với trình độ sơ đẳng, bạn có thể áp dụng phương pháp ép xung trực tiếp trên bo mạch chủ của máy tính. Việc ép xung có khả năng cải thiện hiệu năng hệ thống

bằng cách yêu cầu bộ vi xử lý (CPU) và chip đồ họa chạy nhanh hơn thiết lập mặc định. Hầu hết CPU đều có thể hoạt động thoải mái ở các tần số cao hơn tần số được các hãng sản xuất máy tính sử dụng.

Nếu là người cẩn trọng, bạn có thể ép xung máy tính mà không gặp phải rủi ro nào. Một khi đã được ép xung, CPU sẽ chạy nhanh hơn và dĩ nhiên cũng nóng hơn, tuy nhiên việc theo dõi và kiểm soát nhiệt độ hệ thống có thể thực hiện khá dễ dàng. Xin lưu ý, việc ép xung sẽ làm hỏng các quy định về bảo hành. Trong vài trường hợp, bạn có thể không nhận thấy bất kỳ sự cải thiện đáng kể nào về hiệu năng và tốt nhất là bạn nên đưa hệ thống về lại tình trạng cũ.

Nếu mua riêng một bo mạch chủ hoặc mua một máy tính sử dụng bo mạch chủ đã "lỗi thời", bạn cần sử dụng một tiện ích chạy trên Windows của hãng thứ 3 để thực hiện ép xung thay vì phải mất công tìm kiếm, tinh chỉnh các thông số trong chương trình PC Setup của máy tính. Đa số các bo mạch chủ đời mới đều cung cấp công cụ ép xung trong đĩa CD đi kèm. Nếu không có cách nào khác, bạn buộc lòng phải mở tiện ích PC Setup bằng cách nhấn một phím được thông báo ngay trước khi Windows được khởi động (thường là phím DEL hay F2). Trong phần cài đặt BIOS, bạn tìm mục thiết lập thông số cho xung nhịp hệ thống và FSB - thường thì chúng nằm trong mục Advanced Chipset Features (hình 1). Cần lưu ý, tên gọi và cách thiết lập các giá trị này có thể khác nhau tùy loại BIOS hoặc máy tính.

Cách duy nhất để tìm ra tốc độ tối đa của CPU là mạo hiểm thiết lập thử. Ngoài ra, bạn cũng có thể tham khảo kinh nghiệm của những người dùng khác từ những diễn đàn mạng chuyên về ép xung như Extreme Overclocking (find.pcworld.com/57353), EarthWeb Hardware (find.pcworld.com/57354) hay Xtremevn.com.

THỰC CHẤT CÔNG VIÊC

Bạn có 2 cách để ép xung CPU, một là tăng hệ số nhân CPU, hai là tăng xung của nhịp bus hệ thống (FSB) - FSB có chức năng kiểm soát bộ nhớ RAM và bo mạch chủ. Trong đó, thay đổi hệ số nhân CPU là phương pháp dễ thực hiện hơn. Ví dụ, nếu FSB của máy tính đang sử dụng được thiết lập ở mức 200MHz và hệ số nhân là 14 thì CPU sẽ chạy ở tốc độ 2,8GHz (hình 2), khi tăng hệ số nhân lên 16 thì tốc độ CPU sẽ đạt 3,2GHz. Tuy nhiên, trừ các CPU cao cấp như dòng Athlon FX của AMD hoặc dòng Extreme Edition của Intel, tất cả CPU đời mới đều bị "khóa" hệ số nhân và đó cũng chính là lý do tại sao hầu hết người yêu thích ép xung hiện nay phải chuyển sang hình thức tăng giá trị xung nhịp FSB - một thủ tục phức tạp hơn rất nhiều so với việc tăng hệ số nhân CPU.

Việc tăng giá trị xung nhịp FSB không những giúp cải thiện hiệu năng CPU mà còn tăng tốc độ truyền nhận dữ liệu giữa bộ nhớ và CPU. Tuy nhiên, thao tác tinh chỉnh này có thể dẫn đến tình trạng "treo" máy, vì thế bạn cũng phải điều chỉnh các thông số liên quan đến RAM và mức điện áp trong BIOS. Bạn cần hết sức thận trọng với các thông số này bởi một sai lầm nhỏ cũng có thể gây ra tai họa khôn lường, do đó tốt hơn hết là bạn nên tham khảo kinh nghiệm thực hiện từ các diễn đàn hay ai đó có kinh nghiệm.

Hình 1: Tìm kiếm và thiết lập thông số ép xung hệ thống trong tiện ích PC Setup.

Để biết hệ thống của mình có thể chạy nhanh hơn đến mức nào, bạn tăng giá trị xung nhịp trong BIOS lên từng bậc, sau đó để máy tính chạy thử một lát và kiểm tra xem có gặp trục trặc nào hay không. Nếu an toàn, bạn tiếp tục tăng giá trị này lên cho đến khi hệ thống xảy ra hiện tượng bất thường. Từ giá trị "chết" này, bạn giảm xung nhịp xuống một bậc hay thậm chí đến một mức thấp an toàn hơn theo quan điểm của riêng bạn.

Làm mát hệ thống

Hình 2: Ép xung chỉ đơn giản là thay đổi giá trị hệ số nhân CPU trong BIOS.

Những máy tính hiệu năng cao thường đòi hỏi một hệ thống làm mát làm việc thật tốt. Quạt làm mát CPU có sẵn trong máy tính thường không đủ "công lực" để đáp ứng cho nhu cầu ép xung. Hệ thống làm mát CPU dùng quạt có giá dưới 30USD, tuy nhiên bạn nên mua sản phẩm của những hãng tên tuổi như Thermaltake hoặc Zalman - dù đắt nhưng chúng ổn định và quan trọng nhất là ít tạo ra tiếng ồn hơn.

Trong khi đó, game thủ và người dùng sử dụng máy tính thường xuyên lại thích trang bị hệ thống giải nhiệt bằng chất lỏng vì chúng hiệu quả hơn. Loại thiết bị này bao gồm một chiếc bơm đơn giản, các ống dẫn, bộ tản nhiệt và một "khối nóng" dùng để hút nhiệt từ CPU.

Nếu lo ngại việc chất lỏng chỉ cách các mạch điện trong máy tính khoảng vài

milimét, bạn có thể sử dụng quạt làm mát Monsoon II Like của Vigor Gaming (130USD, find.pcworld.com/57357). Dù không phải loại tản nhiệt dùng chất lỏng nhưng Monsoon II rất hiệu quả nhờ kết hợp một quạt thông thường với một bộ phận làm mát Peltiler mạnh mẽ. Thiết bị này dễ lắp ráp và chiếm ít diện tích bên trong thùng máy hơn so với nhiều loại quạt mát CPU công suất lớn khác.

ÉP XUNG CARD ĐỒ HỌA

Mỗi card đồ họa có bộ xử lý và RAM riêng, do đó bạn có thể tăng tốc cho từng phần bằng cách sử dụng phần mềm. Tiện ích RivaTuner 2 của 3Dguru (find.pcworld.com/55274) từ lâu đã được những người dùng chuyên ép xung sử dụng để tinh chỉnh hiệu quả đồ họa. Tuy nhiên việc ép xung hiện quá thông dụng cho nên các hãng sản xuất card đồ họa hàng đầu như ATI và nVidia đã cung cấp sẵn các công cụ ép xung trên nhiều loại card đồ họa. Thực ra, trong một số trường hợp, việc sử dụng tiện ích Overdrive của ATI để ép xung không làm mất hiệu lực bảo hành của card đồ họa. Ngoài ra, bạn còn có thể sử dụng tiện ích Coolbits của nVidia hay tham khảo những giải pháp khác được hướng dẫn trong bài viết "Bí quyết tinh chỉnh hệ thống" (ID: A0503_78).

Những lời khuyên dành cho việc ép xung hệ thống cũng có thể áp dụng cho card đồ họa: tham khảo kỹ lưỡng trên các website và diễn đàn chuyên về ép xung để hiểu rõ quy trình áp dụng cho card đồ họa của bạn; luôn ghi nhớ phải tăng xung nhịp lên từng mức nhỏ, kiểm tra thử xem máy có chạy ổn định hay không trước khi tiếp tục tăng giá trị xung nhịp, đồng thời theo dõi kỹ thời điểm máy rơi vào tình trạng quá nhiệt (overheat).

Bạn có thể theo dõi nhiệt độ của card đồ họa bằng thiết bị Digital Thermal Probe của HighSpeed PC (15USD, find.pcworld.com/56489). Nếu nhiệt độ lên quá cao, bạn nên trang bị một thiết bị làm mát card đồ họa như VCool của Antec (20USD, find.pcworld.com/57359, hình 3).

Tuy nhiên, biện pháp hiệu quả nhất để cải thiện hiệu năng xử lý đồ họa cho máy tính vẫn là trang bị một card đồ họa cao cấp. Máy tính giá rẻ với bộ xử lý đồ họa được tích hợp ngay trên bo mạch chủ thường chạy "chậm như rùa" khi chơi các game hành động, biên tập video hoặc xử lý các tập tin đồ họa lớn. Bởi vì những máy tính trên sử dụng RAM hệ thống đồng

Hình 3: Giữ cho card đồ họa luôn mát nhờ quạt thiết kế đặc biệt, ví dụ Antec VCool (20USD).

thời cho tác vụ xử lý đồ họa lẫn các tác vụ chung của hệ thống, cho nên việc lắp thêm một card đồ họa

chuẩn AGP hoặc PCI Exoress – nếu máy tính còn khe cắm trống – sẽ cải thiện được đáng kể khả năng xử lý đồ họa. Để biết máy tính của mình đang sử dụng loại card đồ họa nào, bạn có thể quan sát ở mặt sau máy: nếu cổng tín hiệu VGA hoặc DVI không nằm chung trên một khe cắm card mở rộng thì chắc chắn máy tính của bạn sử dụng card đồ họa tích hợp.

Trước khi mua card đồ họa mới, bạn phải bảo đảm có thể vô hiệu hóa được hệ thống đồ họa trên bo mạch chủ. Trên một số máy tính, điều này sẽ tự động được thực hiện khi bạn lắp card đồ họa rời vào khe cắm, tuy nhiên ở những máy tính khác thì bạn cần phải thay đổi vài thông số trong chương trình PC Setup. Nếu không thể vô hiệu hóa tính năng đồ họa trên bo mạch chủ máy, bạn nên cân nhắc mua một máy tính mới hoặc chí ít cũng là một bo mạch chủ mới.

Thế hệ card đồ họa xuất hiện từ hai năm trước có thể gặp trở ngại đối với vài tựa game mới nhất, đặc biệt là những game đòi hỏi độ phân giải màn hình cao hoặc thậm chí chỉ ở mức vừa phải. Bạn không nhất thiết phải trang bị một card cao cấp như nVidia GeForce 8800 GTX (600USD) mà chỉ cần một card đồ họa có giá phù hợp với ngân sách của mình. Để biết thêm thông tin và hướng dẫn, tham khảo find.pcworld.com/57366 và find.pcworld.com/57367.

Vài lưu ý: Một số card đồ họa chuẩn AGP hiện vẫn còn được bày bán và sử dụng rộng rãi, tuy nhiên công nghệ này đang đi vào giai đoạn "thoái trào". Thậm chí nếu tìm được một card đồ họa AGP ưng ý thì nhiều khả năng bạn không thể tận dụng nó cho chiếc máy tính tương lai của mình (thường thiếu khe cắm AGP), do đó bạn nên cân nhắc mua một bo mạch chủ mới hỗ trợ khe cắm PCI Express. Nếu có ý định sử dụng Windows Vista, bạn phải chắc chắn rằng card đồ họa đó đi kèm trình điều khiển thiết bị cho Vista và hỗ trợ DirectX 10.

Nhiều máy tính chơi game giá khoảng 5.000USD được trang bị hai card đồ họa SLI hoặc CrossFire - thường là loại card đôi (600USD) - hoạt động theo nguyên tắc "xe kéo" để cải thiện khả năng xử lý đồ họa. Tuy nhiên, bạn hoàn toàn có khả năng áp dụng giải pháp này cho máy tính của mình nếu bo mạch chủ đang sử dụng hỗ trợ SLI hoặc CrossFire. Nếu ngân sách eo hẹp, bạn có thể mua trước một card, sau đó sẽ mua tiếp khi có thể.

TRANG BỊ BO MẠCH CHỦ MỚI

Nếu bo mạch chủ đang sử dụng không hỗ trợ các công nghệ hiện đại như PCI

Express (card đồ hoạ), SATA và RAID (đĩa cứng) và bộ xử lý lõi kép thì đây đúng là dịp để bạn mua một máy tính mới. Nếu chưa sẵn sàng cho việc này, bạn có thể cân nhắc chỉ thay mới bo mạch chủ, CPU và RAM. Loại bo mạch chủ sử dụng chipset 650i của nVidia hỗ trợ các card đồ họa, đĩa cứng mới nhất và những thành phần khác. Ví dụ, bo mạch chủ Asus P5N-E SLI (giá dưới 150USD) hỗ trợ PCI Express, cung cấp 2 khe cắm card đồ họa SLI, đầu nối đĩa cứng SATA và hỗ trợ kết nối RAID ngay trên bo mạch chủ. Nếu không cần sử dụng SLI, bạn có thể chọn loại bo mạch chủ như EVGA nForce 650i Ultra ở mức giá 120USD. Cả hai bo mạch chủ này hỗ trợ thế hệ bộ xử lý 2 lõi và 4 lõi của Intel, cũng như Pentium 4 và Celeron (socket 775).

TIỆN ÍCH KHÔNG THỂ THIẾU

Bạn có thể theo dõi sát sao quá trình ép xung hệ thống với các tiện ích miễn phí sau đây.

CPU-Z (find.pcworld.com/57369) giúp bạn kiểm tra tốc độ xung nhịp CPU, cung cấp tất cả cài đặt và thông số quan trọng cho CPU, bo mạch chủ và RAM của hệ thống.

SpeedFan (find.pcworld.com/57370) của Alfredo Milani Comparetti là một chương trình được nhiều người ưa thích, dùng để theo dõi nhiệt độ của CPU và nhiệt độ bên trong thùng máy, đồng thời bạn có thể cài đặt tốc độ quạt sao cho máy được làm mát tốt nhất. Trong khi đó, tiện ích Desktop Utilities (find.pcworld.com/57371) dành cho các máy tính nền Intel sẽ hiển thị đồng thời nhiệt độ bên trong thùng máy và mức điện áp trên một giao diện hết sức thân thiện.

Bạn do dự vì không biết có thể tác động lên bộ xử lý của mình đến mức nào? Hãy sử dụng tính năng độ ổn định của máy tính ở mọi xung nhịp bằng công cụ CPU Stability Test của Jouni Vuorio (find.pcworld.com/57372). Ngoài ra, bạn còn có thể sử dụng tiện ích Prime 95 (find.pcworld.com/57373) của GIMPS Projec (Great Internet Mersenne Primes Search) để kiểm tra máy tính.

Không những thế, bạn còn có thể tham khảo website của hãng sản xuất bo mạch chủ mà mình đang sử dụng để biết các tiện ích tinh chỉnh phù hợp. SysTool (find.pcworld.com/57376) của Tech Power Up sẽ cung cấp các công cụ dùng để ép xung cả CPU lẫn card đồ họa.

Bùi Xuân Toại
PC World Mỹ 8/2007

Bí quyết tiết kiệm với máy in

Chọn máy in: Nếu phải in ấn khá nhiều tài liệu thì nên chọn mua máy in laser. Giá thành của máy in laser khá cao so với máy in phun, nhưng về lâu dài nó sẽ tỏ ra hiệu quả. So sánh chi phí in ấn cho thấy, máy in laser có thể rẻ hơn máy in phun từ 3-5 lần.

- Sử dụng mực bơm: Chọn máy có thể in được mực bơm, cũng như Cartridges mực có thể bơm lại được. Cần lưu ý, mực bơm phải được cung cấp bởi chính hãng sản xuất máy in mà bạn đang sử dụng. Cách này có thể giúp tiết kiệm 5-10 lần so với mua Cartridges mực mới.

- Tăng tốc độ in, tiết kiệm mực bằng cách in một màu nếu tài liệu không cần màu sắc: Vào Start > Settings > Printers, tiếp theo nhấp chuột phải vào biểu tượng máy in rồi chọn Properties, sau đó nhấp chọn một màu nào đó (ví dụ grayscale). Sau cùng nhấn OK. Bây giờ, tốc độ in nhanh hơn khi in tài liệu có màu sắc gấp 3-5 lần và tiết kiệm được khá nhiều mực in.

- Tiết kiệm mực khi in các trang web: Nếu chỉ muốn in một phần nội dung của trang web thì chỉ việc tô chọn nó, tiếp theo nhấp chuột phải vào rồi chọn Print để in. Nếu chỉ cần nội dung, không cần hình nền trang web, bạn vào Tool/Internet Options, tiếp theo nhấp thẻ Advanced, sau đó cuộn xuống tới phần Printing, bỏ dấu chọn vào mục Print background colors and images. Sau cùng nhấn Apply và OK.

- Sử dụng các phần mềm tiết kiệm mực in như InkSaver hay tiết kiệm giấy in như FinePrint, Photo Cool...

(Sưu tầm)

Thủ thuật tối ưu nguồn điện cho laptop

Nguồn PC World

Hiện nay, laptop đã trở thành phổ biến. Phong trào tự lắp ráp laptop đang bùng nổ ở mọi khắp nơi. Vì vậy, để sở hữu một máy tính xách tay phù hợp với khả năng của mình không còn quá khó khăn như trước nữa. Tuy nhiên, trong quá trình sử dụng, người dùng thường thắc mắc: Pin cho laptop của tôi sẽ dùng được bao lâu? Làm thế nào để tiết kiệm năng lượng tối đa?...

Với hầu hết mọi người, một câu trả lời giống nhau dường như là không đủ. Thực ra, có rất nhiều cách giúp cho pin máy tính xách tay của bạn kéo dài thời gian sử dụng hơn. Dưới đây là những thủ thuật giúp tối ưu nguồn năng lượng cho laptop:

Quản lý nguồn điện hiệu quả

Sử dụng phần mềm quản lý nguồn điện trong laptop có thể tiết kiệm nhiều năng lượng và kéo dài thời gian sử dụng pin hơn. Nếu máy có tích hợp chức năng tạo profiles quản lý nguồn riêng thì hãy lựa chọn profiles phù hợp nhất với bạn sao cho tối ưu nhất. Nếu laptop không hỗ trợ thì các chương trình quản lý nguồn của các hãng phần mềm tiện ích cũng rất tốt, nhưng sử dụng tiện ích Power Options có sẵn trong Windows cũng là sự lựa chọn hoàn hảo.

Hãy chọn đúng chế độ nguồn sao cho phù hợp với công việc của bạn. Hãy nhấn *Start-> Control Panel->Performance and Maintenance->Power Options*. Trong *Power Schemes*, lựa *Max Battery* và nhấn *OK*. Lựa chọn này sẽ tắt màn hình sau 1 phút và đưa máy tính xách tay của bạn về chế độ chờ (standby) sau 2 phút không sử dụng. Nếu thấy không thích hợp, hãy chuyển qua lựa chọn *Portable/Laptop*, lựa chọn này sẽ đưa về chế độ chờ sau 5 phút.

Nghỉ ngơi nhanh chóng

Hầu hết các PC đều có chức năng ngủ đông (Hibernate) và chế độ chờ (Suspend hoặc Standby). Hãy tìm các tài liệu đi kèm để tìm hiểu kĩ hơn. Chế độ chờ standby của Windows XP sẽ tạm thời dừng toàn bộ ổ đĩa cứng và màn hình, nhưng mọi thứ trong bộ nhớ hệ thống vẫn còn đó. Trong khi đó, chế độ ngủ đông thì ghi mọi thứ từ trong bộ nhớ vào đĩa cứng và tắt máy hoàn toàn. Windows sẽ phục hồi lại từ chế độ chờ nhanh hơn rất nhiều khi sử dụng chế độ ngủ đông.

Tuy nhiên, nếu máy tính của bạn hết pin khi ở chế độ chờ (standby) thì toàn bộ dữ liệu sẽ biến mất. Vì vậy, bạn cần phải thiết lập tự động sao lưu những công việc đang thực hiện trong các Word, phần mềm quản lý cá nhân PIM (Personal Information Manager), và các phần mềm khác.

Để máy tính về chế độ chờ, hãy nhấn *Start-> Turn Off Computer-> Stand By*. Để cho máy tính về chế độ ngủ đông, hãy chọn *Start ->Turn Off Computer* và chọn *Hibernate* (Nếu không thấy tuỳ chọn này, hãy giữ thêm phím Shift.). Nếu vẫn không thể thiết lập được chế độ ngủ đông, hãy chọn S*tart->Control Panel->Performance and Maintenance -> Power Options->Hibernate* và chọn *Enable*

hibernation.

Giảm độ sáng màn hình

Một máy tính xách tay có màn hình LCD lớn sẽ tiêu tốn nhiều năng lượng. Giảm độ sáng của màn hình sẽ tiết kiệm được nhiều năng lượng pin. Ví dụ: bằng cách giảm bớt độ sáng màn hình trên máy tính xách tay Sony VAIO sẽ kéo dài thời gian sử dụng pin thêm được 45 phút. Hầu hết các máy tính xách tay đều có nút điều khiển, các phím chức năng hoặc các tiện ích phần mềm giúp giảm bớt độ sáng. Nếu màn hình tối hơn sẽ tiết kiệm năng lượng thì tắt màn hình khi không sử dụng tới luôn là phương pháp tiết kiệm nhất.

Tắt các thiết bị không cần thiết

Hãy loại bỏ các PC card và các kết nối USB hoặc FireWire thực sự chưa cần thiết. Máy tính xách tay thường tích hợp sẵn card mạng không dây, những thiết bị này tiêu tốn năng lượng để dò tìm các điểm truy cập (access point), do đó để tiết kiệm năng lượng khi không cần dùng đến hãy tắt thiết bị này.

Tối ưu hiệu năng hệ thống

Tối ưu hiệu năng hệ thống sẽ giảm đáng kể sự tiêu hao năng lượng. Để giữ cho máy tính xách tay sử dụng tài nguyên CPU và bộ nhớ tốt nhất cho các ứng dụng khác, hãy tắt bất cứ các phần cứng và phần mềm nào không cần thiết. Kiểm tra các biểu tượng trong khay hệ thống (system tray). Bạn có thể sử dụng tiện ích có sẵn trong Windows là msconfig để lựa chọn các chương trình muốn tự động nạp trong khi khởi động.

Để kiểm tra lượng tài nguyên, trong HĐH *Windows 2000* và *Windows XP* hãy mở *Ctrl-Alt-Del* và mở *Task Manager*, chọn *Performance* để xem lượng tài nguyên đã sử dụng. Trong *Windows 98* và *Windows Me* hãy mở tiện ích *System Monitor* bằng cách *Start, Programs, Accessories, System Tools, System Monitor*.

Vô hiệu hoá các thiết bị, phần mềm không sử dụng

Tạm thời vô hiệu hoá (disable) các thiết bị không sử dụng sẽ tiết kiệm được khá nhiều năng lượng mặc dù các thiết bị này thực tế vẫn tiêu thụ một ít năng lượng. Những thiết bị này có thể là modem, card mạng, cổng song song (parallel), cổng nối tiếp (serial), ổ đĩa CD-ROM, DVD... Trong *Windows 98/Me* nhấn phím phải vào *My Computer* và chọn *Properties -> Device Manager*. Trong *Windows 2000/XP* nhấn phím phải vào *My Computer* và chọn *Properties->Hardware -> Device Manager*. Tiếp đó, hãy nhấn phím phải vào thiết bị muốn vô hiệu hoá chọn *Disable*.

Lắp thêm bộ nhớ

Thêm bộ nhớ RAM cho laptop cũng làm giảm đáng kể sự cần thiết hoạt động của bộ nhớ ảo. Bộ nhớ ảo sử dụng ổ cứng để lưu tạm các thông tin trong bộ nhớ. Vì vậy, lắp thêm bộ nhớ RAM sẽ làm giảm đáng kể hoạt động của đĩa cứng nên sẽ tiết kiệm được năng lượng hơn.

Lau sạch điểm tiếp xúc

Điểm tiếp xúc giữa pin và máy có thể làm giảm hiệu suất sử dụng của pin. Hãy lau sạch điểm tiếp xúc bằng kim loại giữa pin và máy hàng tháng bằng vải mềm có tẩm cồn. Điều này sẽ giảm thiểu thất thoát năng lượng do tiếp xúc kém.

Hãy mua thêm pin phụ nếu có thể

Đang sử dụng máy tính để soạn thảo một văn bản quan trọng thì hết pin. Thật bực mình! Do đó, luôn mang theo pin phụ sẽ rất hữu ích cho bạn. Nếu khả năng tài chính cho phép, hãy mua thêm pin phụ. Tuỳ thuộc vào chất lượng của pin giá cả có thể từ 85USD cho tới 235USD.

Hãy thường xuyên sạc pin

Hãy mang theo bộ sạc/chuyển đổi AC khi phải đi ra ngoài, và hãy sử dụng bộ sạc này bất cứ lúc nào có thể. Nếu bộ sạc đi kèm theo máy không tốt và có vẻ nặng nề và phiền phức, hãy sử dụng bộ sạc pin hợp thời trang của Belkin và Targus. Những bộ sạc này nhẹ và mỏng. Không những thế, một số model của Targus còn có thể sạc pin cho điện thoại di động nữa.

Xả pin

Nếu MTXT của bạn thuộc thế hệ cũ thì rất có thể loại pin nikel đang được sử dụng. Hãy xả toàn bộ năng lượng và sạc lại pin mỗi tháng/lần để khả năng sạc năng lượng của pin được cao nhất. Hầu hết các máy tính xách tay đời mới hiện nay đều sử dụng pin lithium chuẩn, nên người sử dụng không cần phải xả toàn bộ rồi sạc lại như thế hệ pin nikel trước.

Bạn đang có dự định mua một tính xách tay cho riêng mình? Hãy mua loại máy

tính xách tay có thời gian sử dụng pin lâu nhất, các hệ laptop dựa trên nền tảng Centrino của Intel là sự lựa chọn tốt.

Ngoài ra, các chip đồ hoạ, các thiết bị ngoại vi và còn rất nhiều các yếu tố khác cũng có thể ảnh hưởng lớn tới thời gian sử dụng pin. Hi vọng những nội dung trên phần nào sẽ giúp ích cho bạn tăng thêm thời gian sử dụng pin cho chiếc laptop của mình.

Tổng hợp tăng tốc máy tính hữu hiệu

Tác giả: **nguoixasu**
Bài viết một vài thao tác cơ bản để làm cho máy tính chạy nhanh hơn đặc biệt dùng cho máy yếu.(dành cho newbie).
Máy tôi chỉ có 1.5Ghz nhưng làm theo chỉ dẫn thấy cũng hiệu quả. Vậy các bro làm thử xem thế nào nhé.

Step 1

Một trong những điều quan trọng đầu tiên để tăng tốc máy tính đó là gắn thêm RAM. Như các bạn biết mua RAM không phải ai cũng có tiền mua, nhưng nó thật sự đáng để bạn đầu tư.

Hãy tưởng tượng ổ cứng của bạn là cái hộp lớn chứa đầy thông tin và trò chơi còn RAM như cái bàn lớn để bạn chơi game trên đó. RAM càng lớn thì máy tính của bạn xử lí càng nhanh, và bạn có thể sử dụng nhiều ứng dụng cùng lúc. Ngược lại máy của bạn sẽ chậm hoặc không thể sử dụng, nếu bạn chơi game hay sử dụng các chương trình lớn mà không đủ RAM.

Giá RAM hiện nay đã giảm nhiều so với thời gian trước, bạn còn chờ gì nữa mà không nâng cấp để máy tính của mình hoạt động hiệu quả hơn.

Nếu các bạn muốn tìm hiểu thêm làm thế nào để mua đúng RAM mình cần các bạn có thể tham khảo thêm trang web sau với điều kiện bạn phải biết tiếng Anh.
Website:
http://reviews.cnet.com/4520-3038_7-...lasses.SpeedPC

Để biết RAM máy của bạn là loại nào và model của nó bạn có thể dùng công cụ online:
Website:
http://memory.shopper.com/mfr.asp?class=100|Desktops%2FServers

Ngoài việc nâng cấp RAM thì việc giảm các hiệu ứng không cần thiết là một các dễ dàng để làm cho máy của bạn hoạt động tốt hơn.
Properties ta được như hình sau, trong khung theme: chọn window classic.à+Thứ nhất các bạn kích chuột phải màn hình Desktop--

+Thứ hai các bạn sử dụng tối thiểu các hiệu ứng như fade, shadow… bằng cách làm như sau:
Properties ta vào System Properties.àKích chuột phải My Computer-
Kích vào tab Advanced , chọn Properties như hình:

Bạn chọn Custom , sau đó bỏ chọn tất cả chỉ giữ lại như hình vẽ:

Sau đó chọn hai lần OK xong.
Việc làm trên sẽ giảm thiểu rất nhiều việc sử dụng tài nguyên của máy làm cho máy chạy nhanh hơn.

+Một điều nữa sẽ giúp bạn cảm thấy thoải mái hơn khi bạn truy cập files trong máy là không để cho Window search thư mục và máy in một cách tự động. Bạn làm như sau:
Folder Options bạn chọn View tab như hình vẽ:àTools-àĐúp chuột My Computer-

Bỏ chọn như hình vẽ.
Automatically search for network folders and printers

Step2: Dọn dẹp ổ cứng
Đầu tiên bạn có thể vào My Documents xóa bớt những thứ không cần thiết nhằm làm tăng dung lượng đĩa cứng giúp truy xuất dữ liệu nhanh hơn. Ngoài ra bạn còn có thể làm như sau với cùng mục đích:

• ***Thứ nhất xóa những phần mềm không cần thiết hoặc lâu không dùng, giữ lại***

chỉ nặng máyAdd or Remove Programs như hình vẽ Remove bất cứ soft gì không cần thiết bằng cách chọn Remove như hình.à. Bạn vào Control Panel

• ***Thứ hai di chuyển hoặc lọai bỏ FONT:***
Tạo một folder trong ổ cứng của bạn thường My Documents ví dụ với tên :"Unuse font". Sau đó dùng Window explorer truy cập đến thư mục: C:\WINDOWS\FONTS kéo các fonts không cần thiết vào thư mục Unuse font lúc trước. Điều này tăng tốc một số ứng dụng đáng kể.

• ***Clean disk***: System tools, chọn Disk cleanup như hình. Lựa chọn ổ đĩa rồi OK.àAccessories-àAll programsàChọn Start-

• ***Clean regedit:*** Bạn dùng chương trình sau rất hay đa năng đó là TuneUp Utilities 2006. Thao tác như sau: Chọn Clean Up and Repair

Sau đó chọn TuneUp Registrycleaner rồi làm như hình nó đòi khởi động máy để thực hiện. Hoặc ngoài ra có thể dùng các phần mềm free như : CCcleaner hoặc Easy Cleaner rất dễ sử dụng, dung lượng nhỏ.
TuneUp; CCcleaner; Easy Cleaner bạn có thể search trong diễn đàn

• ***Sử dụng chương trình Defrag:***
àAll Programs-àĐóng tất cả chương trình đang chạy, chọn Start- Disk defragmenter. Chọn ổ đĩa muốn defrag,àSystem toolsàAssessories click Analyze xong chọn Defragment như hình vẽ. Lâu hay chậm còn tùy thuộc vào ô đĩa bạn bị phân mảnh nhiều hay ít và dữ liệu trong đó. Điều này giúp ổ đĩa truy xuất nhanh hơn.

Step3:

• ***Chuyển file hệ thống từ FAT32 sang NTFS:***
chuột phải vào ổ cứng chọn properties được như hình:àĐầu tiên kiểm tra xem file system của bạn là gì bằng cách vào My Computer

Nếu nó là NTFS thì bỏ qua bước này còn không bạn làm như sau:

Run rồi gõ vào box: cmd rồi nhấn Ok bạn sẽ thấy dòng lệnhàClick Start như sau: "C:\WINDOWS" . Tiếp theo bạn gõ vào dòng lệnh sau: convert c: /fs:ntfs nếu ổ cứng của bạn không phải C mà là D, E… thay bằng chữ đó,nhớ có dấu cách giữa : và /. Enter để thực hiện sau đó khởi động lại máy.

• ***Làm cho computer của bạn truyền tải dữ liệu hiệu quả hơn với DMA(direct memory access).***
Hardware sau đó chọn Device Manager như hình vẽ:àPropertiesàChuột phải My Computer

Click vào dấu cộng trước IDE ATA/ATAPI Controllers đúp chuột vào Primary IDE Channel , sau đó click Advanced Setting tabs. Trong box Transfer Mode chọn DMA if available chọn Ok restart lại máy (xem hình).

Step4:
• ***Loại bỏ một số thành phần của Window mà không ảnh hưởng đến hệ thống:***
AddàLoại bỏ MSN Explorer, Window messenger…trong Win vào Control Panel Window Components như hình bỏ chọn những thứ muốnàor Remove Programs- gì bỏ bấm OK hoàn tất.

• ***Tắt một số services tự động chạy:***
Run, đánh vào như sau: services.msc . Click Extended tab rồi chọn tiếp Startup Type như hình vẽ.àClick Start-

Bạn sẽ thấy list các services ở chế độ automatic. Sau đây là list các services bạn có thể thay đổi giúp máy chạy nhanh hơn.

Alerter
Clipbook
Computer Browser
Distributed Link Tracking Client
Error Reporting Service (if you don't want to be asked to send error reports to

Microsoft anymore)

Fast User Switching
Human Interface Access Devices
IPSEC Services
Messenger
NetMeeting Remote Desktop Sharing
Portable Media Serial Number
Remote Desktop Help Session Manager
Remote Procedure Call Locator
Remote Registry
Routing & Remote Access
Secondary Logon
Server
SSDP Discovery Service
Telnet
TCP/IP NetBIOS Helper
Upload Manager
Universal Plug and Play Device Host
Workstation

Cách làm như sau, đúp chuột vào từ cái ví dụ tôi chọn Workstation hiện ra bảng như sau, trong khung startup type bạn chuyển từ automatic sang manual. Click OK

Những cái khác tương tự.

Ngoài ra bạn có thể xóa một số thư mục thừa trong Win mà không sợ ảnh hưởng đến hệ thống:
+Window\Web\Wallpaper.
+File screensavers (*.scr trong Windows\System32)
+Window sound (Windows\Media)
+Window tour (System32\tourstart.exe)
Thêm nữa bạn có thể xóa các files sau nếu không cần thiết dùng:
+System32\magnify.exe
+System32\osk.exe
+System32\accwiz.exe
+System32\utilman.exe
Nếu tin tưởng phần mềm khác có thể xóa các files sau:
+System32\dfrg.msc

+System32\ntbackup.exe
+System32\cleanmgr.exe
+System32\mstsc.exe (remote desktop)
+System32\sndrec32.exe (sound recorder)
+Hyperterminal (Program Files\Windows NT\hypertrm.exe)
Win của bạn sẽ nhẹ đi rất nhiều, chạy nhẹ nhàng hơn.
Step 5: Cải thiện lượt Web

• ***Lấy lại 20% bandwidth:***
Click Start, rồi Run.
Đánh vào gpedit.msc in the box.
Dưới "Local Computer Policy," click vào dấu cộng trước "Computer Configuration," rồi "Administrative Templates."
Click dấu cộng trước "Network" and select "QoS Packet Scheduler."
Ở cửa sổ bên phải, đúp chuột vào "Limit Reservable Bandwidth."
Chọn Settings tab, chọn Enabled.
Trong khung "Bandwidth Limit %", đánh vào 0%. (Đừng quên điều này)
Click OK.

Ngoài ra các bạn có thể dùng TweakXP, TuneUp 2006. Ở đây tôi dùng TuneUp như sau để tối ưu việc kết nôi mạng:
Mở TuneUp 2006 click vào Optimize ỉmpove, chọn TuneUp System Optimize.

Trong TuneUp Sytem Optimize có nhiều mục để bạn chọn ví dụ tôi chọn Optimize Internet Connection, chọn kiểu kết nối của bạn ADSL, DSL hay àmodem 56Kbit

Next để thực hiện thay đổi. Ngoài ra trong này còn có nhiều lựa chọn khác để làm cho máy của bạn tốt hơn, bạn hãy tự khám phá nhé.
Đến bây giờ tôi tin rằng máy của bạn đã khá hơn trước rất nhiều rồi đấy.
Hy vọng nó có ích cho bạn. Lần đầu viết các Admin, Mod có gì sai sửa hộ luôn nhé. Thanks

Bài viết tham khảo CNET.COM; personal computer world.

Tác giả: **Hồng Vy**
PC World Mỹ 6/2006

Nếu chẳng may máy tính rơi vào tình trạng bo mạch chủ "bốc cháy", đĩa cứng ngừng quay, hệ điều hành "ngã quỵ" hay phần mềm gián điệp và virus "thao túng" mọi hoạt động của hệ thống... đừng vội cầu cứu bộ phận hỗ trợ kỹ thuật hay đưa máy tính ra "bệnh viện", hãy tham khảo bài viết bên dưới vì biết đâu bạn sẽ tìm ra được "bí kíp" để hóa giải điều phiền toái đang gặp phải.

MÁY TÍNH KHÔNG KHỞI ĐỘNG

• **Hình như có tiếng động kỳ lạ nào đó phát ra từ máy tính?** Một vài âm thanh có thể là điềm báo trục trặc nghiêm trọng. Nếu nghi ngờ đĩa cứng của mình đang hoạt động trong trạng thái "nhảy cò cò", biện pháp an toàn nhất là tắt máy tính ngay lập tức. Để xác định xem đĩa cứng có phải là nguyên nhân phát ra các âm thanh trên hay không, bạn cần tháo cáp nguồn của ổ đĩa này trước khi bật lại máy tính.

Nếu thủ phạm chính là đĩa cứng, bước kế tiếp bạn cần thực hiện là tải về một tiện ích có khả năng đọc được các mã chẩn đoán SMART (*Self-Monitoring Analysist and Reporting Technology*). Dữ liệu SMART có thể cho bạn biết chính xác hỏng hóc. Hãy tìm tiện ích này từ website của hãng sản xuất đĩa cứng mà bạn đang sử dụng, tham khảo www.ariolic.com/activesmart/low-level-format.html để có thêm thông tin chi tiết.

• **Tại sao tiếng ồn vẫn tồn tại ngay cả khi đã ngắt nguồn của đĩa cứng?** Đến lúc này, dù công việc sẽ khó khăn hơn do mọi thứ trở nên "mơ hồ" nhưng chí ít bạn cũng có thể an tâm rằng dữ liệu vẫn được an toàn. Khi ấy, một biện pháp "bình dân" nhưng hiệu quả để tìm ra trục trặc là sử dụng một ống nghe bằng giấy: bạn hãy đặt một đầu vào tai, đầu còn lại đặt vào thành phần nghi ngờ phát ra tiếng ồn và chăm chú lắng nghe.

• **Liệu nguyên nhân có phải do quạt làm mát?** Nếu bạn lo ngại về những tiếng động bất thường phát ra từ quạt làm mát, hãy sử dụng công cụ miễn phí SpeedFan để xác định xem có phải quạt làm mát gắn trên bo mạch chủ quay quá chậm hay không. Vài thành phần trên bo mạch chủ có thể "bốc cháy" nếu chúng không được làm mát hiệu quả. Đừng tiếc tiền, hãy nhanh chóng thay quạt làm mát mới vì chi phí sẽ ít hơn rất nhiều so với việc phải thay CPU hay bo mạch chủ. Ngoài ra, bạn cũng có thể sử dụng tiện ích CPUCool để theo dõi "nhiệt độ" của hệ thống.

GIÁM SÁT TỐC ĐỘ QUẠT LÀM MÁT

Nếu bạn nghi ngờ quạt làm mát hay đĩa cứng gặp sự cố, hãy thử sử dụng tiện ích SpeedFan. Ngoài khả năng theo dõi tốc độ của quạt (trong hầu hết máy tính, tốc độ quạt sẽ đạt từ 1.000 đến 4.000 vòng quay/phút), SpeedFan còn có thể phân tích dữ liệu SMART của đĩa cứng, nhờ thế bạn có thể tìm ra nguyên nhân hỏng hóc.

• **Tiếng "bíp" gì vậy?** Nếu nghe thấy những tiếng bíp kéo dài không bình thường (hay vài tiếng bíp cùng lúc) khi vừa khởi động máy tính, thì có thể hệ thống đang cố thông báo cho bạn biết một điều gì đó – và thường là tin xấu. Trong khi tiếng bíp ngắn thường xuất hiện ngay trước quá trình khởi động máy sẽ thông báo mọi thứ đã "sẵn sàng" thì những âm thanh báo lỗi lại không tuân theo một quy định nào: chúng có thể khác nhau tùy vào hãng sản xuất BIOS và thỉnh thoảng còn được thay đổi bởi các nhà sản xuất bo mạch chủ. Bạn cần phải tra cứu ý nghĩa của từng tiếng bíp, bằng cách tham khảo tài liệu đi kèm hay trên website của hãng sản xuất. Ví dụ, với máy Dell Dimension XPS Dxxx, một tiếng bíp ngắt quãng và theo sau đó là 2 tiếng bíp khác thông báo card đồ họa gặp sự cố (có thể chưa được gắn đúng vị trí chẳng hạn).

Nếu không tìm thấy thông tin cần thiết tại website của hãng sản xuất, bạn hãy tham khảo BIOS Central (www.bioscentral.com) để xem danh sách và ý nghĩa của từng tiếng bíp được sắp xếp thứ tự theo tên hãng sản xuất BIOS. Ngoài ra, một vài nhà sản xuất (trong đó có Dell) đặt các đèn chẩn đoán ở mặt sau thùng máy, qua đó có thể báo cáo chi tiết hơn những trục trặc đang xảy ra. Chúng có thể khác nhau tùy vào cách thiết kế hệ thống nhưng đèn vàng luôn báo hiệu những triệu chứng không tốt. Một lần nữa, hãy tham khảo website hãng sản xuất để có được câu trả lời chính xác nhất.

• **Trục trặc thiết bị phần cứng có thể ngăn cản quá trình khởi động không?** Nếu bạn trang bị thêm thiết bị phần cứng (gắn trong) mới, như bộ nhớ chẳng hạn, thì bạn cần kiểm tra xem chúng có được lắp đúng vị trí không, hay có xảy ra hiện tượng "lỏng" kết nối ở thiết bị này hay cáp nối không, cũng có thể thiết bị đó bị hỏng hoặc không tương thích với máy tính.

Hãy bắt đầu bằng cách tắt máy và ngắt nguồn điện, tiếp đất cơ thể bằng cách chạm tay vào một thành phần bằng kim loại bên ngoài vỏ máy, sau đó tiến hành mở thùng ra. Bạn cần kiểm tra tất cả dây cáp có được nối chính xác không và đảm bảo bộ nhớ RAM, các card gắn trong được lắp đúng chỗ. Nếu cần thiết, bạn hãy ấn tay dọc theo chiều dài của thanh RAM, hoặc cũng có thể tháo thanh RAM đó ra và sau đó gắn chúng trở lại. Khi đã thực hiện xong, nối lại các cáp nối và khởi động lại máy tính.

Thậm chí nếu thanh RAM được gắn đúng vị trí thì bộ nhớ hệ thống cũng có thể là nguyên nhân trục trặc – do thanh RAM bị hỏng. Hãy sử dụng công cụ miễn phí Memtest86 (www.memtest86.com) tạo một đĩa CD khởi động để kiểm tra các hỏng hóc trên bộ nhớ. Công cụ này thực hiện các kiểm tra chi tiết (và có thể phát hiện nhiều trục trặc mà quá trình kiểm tra BIOS đơn giản thường bỏ sót).

Trong một số ít trường hợp, máy tính không thể khởi động vì xảy ra sự "xung đột" giữa một thiết bị phần cứng mới và các thành phần còn lại trong hệ thống; hay chỉ đơn giản do thiết bị này không hoạt động. Việc này thường xảy ra với các máy tính "đời cũ" cũng như với hầu hết việc nâng cấp. Để kiểm tra tình trạng này, hãy gỡ thiết bị mới ra và gắn trở lại thiết bị cũ. Nếu máy tính vẫn khởi động tốt, nghĩa là bạn gặp rắc rối với thiết bị mới. Hãy liên hệ với nhà sản xuất để có được những trợ giúp cần thiết.

Thỉnh thoảng, máy tính có thể phát ra âm thanh khởi động bình thường (xảy ra khi Windows tải màn hình nền) nhưng bạn vẫn không thấy gì trên màn hình. Đó là báo hiệu cho cả card đồ họa và màn hình. Trước hết, hãy kiểm tra cáp nối màn hình có bị lỏng hay đứt không, hay các chân (pin) của card đồ họa có được cắm chặt không? Nếu mọi thứ vẫn bình thường, hãy nối màn hình này với một máy tính khác để kiểm tra. Nếu màn hình này vẫn hiển thị tốt, bạn cần tìm một màn hình tốt khác để kiểm tra lại máy tính nghi ngờ trước đó. Nếu màn hình tiếp tục "tối om" thì bạn có thể chắc chắn card đồ họa gặp sự cố hay xảy ra hiện tượng lỏng kết nối bên trong máy. Khi đó, hãy tắt điện máy tính, mở thùng máy ra và kiểm tra vị trí của card đồ họa. (Nếu sử dụng card đồ họa tích hợp và nó đang gặp sự cố, bạn cần thay mới bo mạch chủ).

• **Thông báo xuất hiện trên màn hình và máy tính ngưng khởi động?** Nếu màn hình khởi động của máy tính xuất hiện một thông báo lỗi – hay còn được gọi là thông báo BIOS Power-On Self Test, hay POST – thì bạn có thể tra cứu ý nghĩa trong tài liệu hướng dẫn đi kèm bo mạch chủ hay trên website http://www.bioscentral.com/.

Nếu thấy thông báo lỗi "*Non-System disk* ..." ("Không phải đĩa khởi động ...") và hiện không có đĩa nào trong ổ đĩa mềm, bạn hãy tháo bất kỳ đĩa cứng nào gắn ngoài và lấy đĩa CD ra khỏi ổ đĩa, sau đó khởi động lại máy tính. Nếu trục trặc vẫn tiếp diễn, có lẽ sector khởi động hay partition khởi động của đĩa cứng bị hỏng. Tiện ích Partition Table Doctor 3 (39 USD, www.ptdd.com) có thể tạo lại bảng partition (phân vùng đĩa cứng), đây là một phương thuốc hữu hiệu có thể "hồi sinh" máy tính gặp sự cố. Chương trình này cung cấp dưới dạng tập tin ISO, nên bạn có thể sử dụng để tạo đĩa CD khởi động.

CẤM BSOD KHỞI ĐỘNG LẠI

Hãy khởi động máy tính ở chế độ Safe Mode (ấn phím <F8> ngay sau khi quá trình khởi động BIOS và chọn Safe Mode từ trình đơn). Nhấn phải chuột lên biểu tượng My Computer, chọn Properties, nhấn vào thẻ Advanced và chọn nút Settings bên dưới mục Startup and Recovery. Sau đó, bỏ đánh dấu mục Automatically restart và nhấn OK để kết thúc.

• **Phải làm gì khi gặp lỗi màn hình xanh?** Máy tính đang khởi động bỗng nhiên "treo cứng" và xuất hiện một màn hình xanh với thông báo đại loại như "STOP: 0x0000021a Fatal System Error", đây chính là lỗi "màn hình xanh chết chóc" (Blue Screen of Death – BSOD) thường gặp trong Windows. Bạn có thể tìm hiểu chi tiết về lỗi này cũng như cách khắc phục bằng cách tìm kiếm trên web từ một máy tính khác hay giải mã lỗi Stop Error (bao gồm 10 ký tự, được bắt đầu bằng số 0 và chữ x) tại website www.updatexp.com/stop-messages.html.

Nhưng chuyện gì sẽ xảy ra nếu Windows tiến hành khởi động lại ngay khi lỗi màn hình xanh vừa xuất hiện? Có lẽ kỹ sư nào đó phát triển Windows XP nghĩ rằng để hệ thống tự khởi động lại mỗi khi bị "ngã quỵ" nhưng lại không lường đến tình huống sự cố xảy ra trong quá trình khởi động. Điều này có nghĩa là, với người dùng Windows, máy tính sẽ bước vào một vòng lặp vô tận của quá trình "ngã quỵ", khởi động lại và tiếp tục "ngã quỵ". Lúc này, bạn sẽ không bao giờ đọc được mã lỗi hay thông báo lỗi mà qua đó có thể giúp người dùng biết được chuyện tồi tệ gì đang xảy ra. May thay, có một cách dễ dàng khắc phục hiện tượng này được trình bày trong phần "Cấm BSOD khởi động lại".

MÁY TÍNH HOẠT ĐỘNG BẤT THƯỜNG

• **Windows hay ứng dụng thường xuyên "ngã quỵ"?** Bước đầu tiên bạn cần thực hiện là xác định xem trục trặc có thường xuyên xảy ra không và ghi nhận các hành vi làm hệ thống "gãy gánh". Hãy ghi lại trình tự các sự kiện và nội dung của bất kỳ thông báo hay hộp thoại cảnh báo lỗi nào, rồi tìm thông tin về chúng trực tiếp tại website của hãng sản xuất phần mềm hay thông qua các công cụ tìm kiếm web. Một bản sửa lỗi hay nâng cấp cho phần mềm này có khả năng giải quyết được vấn đề đang tồn tại.

Ngoài ra, tiện ích Event Viewer của Windows ghi lại rất chi tiết về nhiều hiện tượng "gãy gánh" của hệ thống và các ứng dụng khác. Nhấn phải chuột lên biểu tượng My Computer, chọn Manage.Expand Event Viewer trong khung cửa sổ bên trái và nhấn chuột vào mục Application (thông thường, tiện ích Event Viewer trong Windows XP ghi nhận 3 loại sự kiện: Application, Security và System). Hãy quan sát những ghi nhận mới nhất, nếu có sự kiện nào xuất hiện với biểu tượng có dấu X màu đỏ thì điều đó có nghĩa là Windows đang gặp một sự cố nghiêm trọng.

Nếu bạn nhấn đúp chuột vào ghi nhận này, một hộp thoại Event Properties với nhiều thông tin hơn sẽ xuất hiện, dù khó để hiểu hết ý nghĩa của chúng. Nếu bạn không thể giải mã chúng, hãy sử dụng cơ sở dữ liệu Event ID của Microsoft tại địa chỉ www.microsoft.com/technet/support/ee/ee_advanced.aspx, hoặc EventID.Net (www.eventid.net/search.asp) – nơi mà người dùng chép lên đó những kinh nghiệm và giải pháp tìm kiếm nguyên nhân gây lỗi. Với phí dịch vụ 9 USD/ 3 tháng, bạn có thể truy cập một cách chi tiết toàn bộ giải pháp và thông tin hữu ích.

• **Phần mềm dở chứng?** Nếu phát hiện ra trang chủ (homepage) trong trình duyệt bị thay đổi, các cửa sổ quảng cáo tự động xuất hiện hay các biểu tượng xuất hiện "lộn xộn" trên màn hình nền của Windows thì gần như chắc chắn máy tính của bạn đã bị nhiễm virus hay phần mềm gián điệp (spyware). Trong trường hợp này, việc chẩn đoán cũng chính là sửa chữa.

Trước tiên, hãy tiến hành quét virus cho máy tính. Nếu chưa cài bất kỳ chương trình phòng chống virus nào, bạn có thể sử dụng dịch vụ quét virus trực tuyến miễn phí Housecall của Trend Micro (http://housecall.trendmicro.com). Nếu bạn đã có chương trình quét virus nhưng muốn trang bị thêm công cụ phát hiện spyware miễn phí, hãy tải về tiện ích Microsoft Windows Defender (trước đây được biết với tên Microsoft Windows AntiSpyware).

• **Thiết bị ngoại vi mất tác dụng?** Nếu bạn đang gặp rắc rối với bàn phím và chuột không dây, hay các thiết bị nhập khác, trước hết hãy kiểm tra lại pin của chúng. Nếu đó là pin sạc, hãy để thiết bị này có chút ít thời gian để "khởi động" và rồi khởi động lại máy.

Nhưng phải làm sao nếu đó là thiết bị dùng dây hoặc pin vẫn tốt? Hãy sử dụng wizard hướng dẫn khắc phục sự cố của Windows: nhấn Start -> Control Panel (hay Start -> Control Panel -> Printers and Other Hardware với chế độ hiển thị Category), chọn Mouse hoặc Keyboard; kế đến, chọn thẻ Hardware và nhấn nút Troubleshoot. Ngoài ra, công cụ chẩn đoán DirectX có thể đánh giá tình trạng của thiết bị nhập: nhấn Start -> Run, gõ vào lệnh dxdiag và nhấn OK. Sau đó, chọn thẻ Input để xem kết quả kiểm tra tất cả thiết bị nhập được gắn vào hệ thống.

Nếu cả tiện ích trợ giúp của Windows và công cụ DirectX đều không thể đưa ra một giải pháp triệt để, bạn cần dùng một con chuột hay bàn phím chuẩn PS/2, sau đó đến website của hãng sản xuất để tải về trình điều khiển thiết bị mới nhất.

• **Máy tính phát nhạc trong im lặng?** Hãy đảm bảo loa máy tính được cấp điện và nối dây tín hiệu một cách chắc chắn. Chạy tiện ích kiểm soát âm lượng Windows Volume Control (bằng cách chọn Start -> All Programs -> Accessories -> Entertainment -> Volume Control) và xác định các hộp thoại đánh dấu Mute có được chọn hay không, nếu có hãy bỏ những đánh dấu này. Nếu vấn đề cũng chưa được giải quyết? Hãy kiểm tra xem card âm thanh có được chọn đúng không (một số máy tính có nhiều thiết bị âm thanh). Trong cửa sổ Volume Control, chọn Options.Properties và đảm bảo mục được liệt kê trong trình đơn thả xuống Mixer Device chính là thiết bị âm thanh của bạn (bất kể đó là card rời hay tích hợp sẵn trên bo mạch chủ).

Ngoài ra, bạn cũng nên xem xét vài vấn đề sau: đầu nối của tai nghe và loa có được cắm đúng vị trí không? Cáp âm thanh có bị lỏng không? Nếu bạn nghe thấy âm thanh bị "ngắt quãng" khi lắc nhẹ đầu nối của tai nghe hay loa, thì đầu nối đó gần như đã hỏng. Nếu đầu cắm audio có thể thoải mái "lắc lư" khi bạn cắm vào hay tháo ra, thì có lẽ cổng âm thanh trong máy tính đã bị gãy và biện pháp duy nhất là thay card âm thanh khác (nếu đang dùng card âm thanh tích hợp, bạn phải kiểm tra xem có còn khe cắm trống nào trên bo mạch chủ hay không).

Nếu đã cài đặt phần cứng hay phần mềm ngay trước khi sự cố xảy ra, bạn cần phải nạp lại trình điều khiển thiết bị (driver) cho card âm thanh. Hãy tham khảo trên website của hãng sản xuất hay Windows Update trong mục Optional Hardware để tiến hành nâng cấp.

Nếu tất cả mọi cố gắng đều thất bại, bạn có thể thử sử dụng công cụ System Restore của Windows XP để đưa máy tính về lại trạng thái "khỏe mạnh" trước đó. Bạn chọn Start -> All Programs -> Accessories -> System Tools -> System Restore và chọn Restore my computer to an earlier time. Windows sẽ tự động tạo các cột mốc khôi phục (tối thiểu là mỗi ngày một lần), vì thế nếu System Restore làm việc (nhưng không phải lúc nào cũng thế!) thì bạn có thể giúp máy tính quay lại tình trạng hoạt động tốt của những ngày trước.

MÁY TÍNH CHẠY CHẬM

• **Dường như Windows làm việc có phần uể oải?** Tuổi tác không phải là nguyên nhân chính làm ảnh hưởng đến tốc độ xử lý của một máy tính: có thể hệ thống đang "gánh vác" quá nhiều ứng dụng chạy ở chế độ nền. Các chương trình "lén lút" hay các tiến trình của Windows bao gồm các tiện ích in ấn và lập chỉ mục đĩa cứng sẽ "chén sạch" tài nguyên CPU và bộ nhớ chính. Chúng cũng có thể làm cho quá trình khởi động và tắt máy ngày càng "ì ạch" hơn. Tiện ích MSConfig (chọn Start.Run và gõ vào lệnh msconfig) sẽ liệt kê danh sách một số ứng dụng được nạp trong quá trình khởi động, tuy nhiên danh sách này chưa thật hoàn chỉnh. Thay vào đó, hãy sử dụng tiện ích miễn phí StartupList có khả năng liệt kê tất cả chương trình được khởi động cùng với Windows. Ngoài ra, tiện ích Autoruns của hãng Sysinternals không những có thể nhận dạng các ứng dụng tự khởi động mà còn có khả năng vô hiệu hóa chúng.

Để giành lại tài nguyên của hệ thống, hãy đóng, xóa hoặc giấu các applet trên khay hệ thống mà bạn không cần. Về vấn đề này, bạn nên tham khảo mục "Thanh lọc Desktop và menu" trong bài viết "Thuần phục Windows" (ID: A0410_92).

DỌN DẸP VÀ TĂNG TỐC TRÌNH ĐƠN NGỮ CẢNH

Hãy tiến hành quét Registry của Windows bằng công cụ ShellExView. Khi tiện ích này thực hiện xong, hãy sắp xếp danh sách có được theo dạng Type. Lần lượt, chọn một trình đơn ngữ cảnh trong danh sách và ấn phím <F7> để vô hiệu hóa chúng. Sau đó, hãy thu nhỏ

tối đa (minimize) cửa sổ của chương trình này và nhấn phải chuột lên màn hình nền của Windows để xem trình đơn ngữ cảnh mở ra nhanh hơn không. Nếu chưa hài lòng, tiếp tục thực hiện công việc như trên cho các mục còn lại trong danh sách.

Ví dụ, với vài applet, bạn chỉ cần nhấn phải chuột lên biểu tượng trên khay hệ thống và chọn Options hay Properties. Sau đó, bỏ đánh dấu tương ứng với tùy chọn Place icon in the taskbar hay mục có ý nghĩa tương đương. Để xem danh sách tất cả chương trình đang chạy trên hệ thống, bạn nhấn chuột vào nhãn Processes trong tiện ích Task Manager. Tương ứng với mỗi chương trình là dung lượng bộ nhớ sử dụng, giá trị càng cao thì càng không tốt. Để ngưng một chương trình trong Task Manager, nhấn chuột lên tên chương trình đó và nhấn vào nút End Process. Tuy nhiên, vấn đề đặt ra ở đây là bạn không thể xác định được chương trình này có nhiệm vụ gì? Tiện ích miễn phí Quick Access InfoBar sẽ đặt một biểu tượng vào cạnh mỗi chương trình đang chạy trong Task Manager, bạn hãy nhấn chuột lên biểu tượng đó để biết đây là chương trình gì và có an toàn không nếu bạn tiến hành chấm dứt hoạt động của nó.

• **Gặp rắc rối về đồ họa khi xem phim hoặc chơi game?** Trước hết, hãy đảm bảo bạn đang sử dụng driver mới nhất cho card đồ họa. Việc làm tưởng chừng như đơn giản này thường sửa được nhiều trục trặc đối với card đồ họa. Bạn có thể tìm được các driver mới nhất tại website của nVidia hay ATI, và driver tại 2 website này thường mới hơn so với phiên bản được nhà sản xuất card đồ họa cung cấp. Tuy nhiên, card đồ họa trên máy tính xách tay là trường hợp ngoại lệ, bạn cần liên hệ với hãng sản xuất máy tính để được trợ giúp cụ thể.

Bạn cũng có thể thực hiện vài kiểm tra cơ bản thiết bị đồ họa bằng cách sử dụng tiện ích chẩn đoán DirectX. Tại nhãn Display (nhấn Start.Run, gõ vào lệnh dxdiag và nhấn OK), thực hiện cả kiểm tra DirectDraw và Direct3D để xác định có trục trặc gì về driver, hay có gì đó được cài đặt không chính xác không. Hãy để tất cả kiểm tra hoàn tất và tham khảo kết quả ở phần hộp thoại Notes bên dưới.

Nếu trục trặc vẫn "cứng đầu" tiếp diễn, hãy sử dụng Task Manager (ấn tổ hợp phím <Ctrl> - <Alt> - <Del>) để đóng tất cả chương trình và tác vụ chạy ở chế độ nền trước khi xem phim hay chơi game. Nếu biện pháp này có thể giải quyết được thì hãy nghĩ đến việc bổ sung bộ nhớ RAM cho máy tính. Tương tự, bạn nên sắp xếp

lại các tập tin đang nằm "tứ tán" bằng cách thực hiện dồn (defrag) ổ đĩa cứng – cách này sẽ giúp việc xem các tập tin video dung lượng lớn mượt mà hơn. Để thực hiện dồn đĩa, bạn chọn Start -> All Programs -> Accessories -> System Tools -> Disk Defragmenter. Ngoài ra, bạn có thể thử nhiều kiểm tra khác như hướng dẫn

tại địa chỉ
http://www.pcworld.com/news/article/0,aid,115049,pg,9,findid,52594,00.asp.

• **Trình đơn ngữ cảnh đáp ứng chậm?** Hiện tượng này không phải do phần mềm độc hại (malware) gây ra, mà do tiện ích bổ sung Windows được viết quá tồi. Trình đơn ngữ cảnh là một dạng của tiện ích bổ sung (shell extension) cho Windows. Hãy sử dụng công cụ miễn phí NirSoft ShellExView để vô hiệu hóa tiện ích bổ sung cho Windows. Sau khi cấm những tiện ích tồi, trình đơn ngữ cảnh sẽ trở lại trạng thái nhanh nhẹn vốn có.

• **Việc ghi đĩa CD/DVD diễn ra chậm hay dừng lại trước khi hoàn tất?** Có lẽ, CPU đang gặp phải tình trạng quá tải. Trước khi tiến hành ghi đĩa, hãy mở tiện ích Task Manager và chọn thẻ Tab. Quan sát biểu đồ để xem mức độ sử dụng CPU có đạt mức 100% trong khi ghi đĩa hay không. Hãy thử đóng một số ứng dụng, như tiện ích phòng chống virus/spyware và công cụ lập chỉ mục tìm kiếm trên máy tính của Google, Yahoo hay các hãng khác. Nên nhớ khởi động lại tiện ích phòng chống virus ngay sau khi thực hiện ghi đĩa xong. Ngoài ra, bạn có thể tham khảo nhiều thông tin về thủ thuật ghi đĩa cũng như định dạng video tại website Video-Help.com.

GIẢI MÃ EVENT ID TRỰC TUYẾN
Các mã Event ID báo cho người dùng nguyên nhân sự cố được ghi lại trong tiện ích Event Viewer của Windows, tuy nhiên chúng hầu như rất khó hiểu. EventID.net sẽ chỉ cho bạn biết chuyện gì đang xảy ra. Nhập mã Event ID vào biểu mẫu trên website này và bạn sẽ thấy một trang web liệt kê tất cả những gì người dùng khác chia sẻ về lỗi này, bên cạnh đó là cách giải quyết.

MẠNG MẤT KẾT NỐI

• **Máy tính và thiết bị ngoại vi không tìm thấy mạng?** Nếu kết nối Internet băng rộng không hoạt động (do modem mất kết nối), hãy thử tắt rồi bật lại điện cấp cho modem. Cách này thường có thể giải quyết được trục trặc. Nếu có sử dụng thiết bị mạng như router hay hub kết nối với modem, bạn cần thực hiện thao tác như trên cho modem trước, rồi sau đó thực hiện cho các thiết bị này.

• **Máy in mạng không hoạt động?** Trước hết, hãy đảm bảo bạn đã thực hiện chia

sẻ máy in. Nhấn Start.Control Panel và chọn Printers and Faxes. Nhấn phải chuột lên máy in cần chia sẻ, rồi chọn Sharing. Ở thẻ Sharing, nhấn Share Name và gõ vào tên máy in. Lưu ý, nếu máy in được gắn vào một máy tính nối mạng thì bạn cần luôn bật máy tính này. Hoặc để giảm chi phí trả tiền điện, bạn có thể trang bị một print server (có giá từ 30 đến 50 USD), giúp kết nối trực tiếp máy in với hệ thống mạng.

• **Kết nối mạng "chập chờn"?** Nếu mạng chạy quá chậm, hay thậm chí không làm việc, trước hết bạn cần sử dụng tính năng giải quyết sự cố mạng của Windows XP: nhấn Start -> Help and Support, và bên dưới mục Pick a Help topic nhấn Networking and the Web, rồi sau đó chọn Fixing network or Web problems, và cuối cùng chọn Home and Small Office Networking Troubleshooter. Tính năng này sẽ hỏi bạn một loạt câu hỏi để giúp chỉ ra trục trặc, khi bạn đã thực hiện xong phần trả lời, máy tính sẽ chạy một chương trình chẩn đoán để chỉ ra nguồn gốc của sự cố.

• **Máy tính xách tay khó kết nối vào mạng Wi-Fi?** Trước hết, hãy đảm bảo mạng không bị "kẹt" bởi những dữ liệu khác. Hoặc hãy tìm xem có thiết bị nào kết nối vào mạng đang thực hiện tải về nhạc và phim không? Những việc này có thể làm giảm tốc độ kết nối mạng của máy tính bạn. Thậm chí, một số thiết bị sử dụng sóng radio cũng có thể gây nên tình trạng tương tự và tiện ích Netstumbler sẽ giúp bạn khắc phục trục trặc này. Tiện ích có khả năng kiểm tra nhiều nguồn phát sóng, từ thiết bị gia dụng như lò viba hay điện thoại cordless. NetStumbler cũng có thể dò ra tất cả mạng không dây có trong khu vực sử dụng chung kênh tần số với bạn, thông báo độ mạnh yếu của từng nguồn phát và giúp tìm ra một mạng không dây công cộng miễn phí. Băng tần 2,4Ghz có 3 kênh không trùng nhau là 1, 6 và 11, bạn nên chọn kênh nào ít người dùng nhất. Ngoài ra, bạn cũng cần kiểm tra lại tín hiệu từ máy tính xách tay của mình. Nếu có thể, bạn cần di chuyển lại gần nguồn phát sóng hơn.

• **Kết nối Wi-Fi chậm?** Có thể ai đó đang "xài ké" mạng không dây của bạn để truy cập Internet. Giải pháp cần thực hiện ngay là kích hoạt tính năng bảo mật của gateway không dây. Điều này đòi hỏi bạn phải thực hiện vài tác vụ như thay đổi mật khẩu mặc định của gateway, kích hoạt tính năng mã hóa WPA PreShared Key. Các bước cài đặt bảo mật này có thể khác nhau tùy vào hãng sản xuất, tuy nhiên bạn sẽ nhận được những hướng dẫn chi tiết tại website GetNetWise (http://spotlight.getnetwise.org/wireless/wifitips/). Ngoài ra, bạn cũng có thể cập nhật tính năng bảo mật bằng cách nâng cấp firmware cho thiết bị không dây, tham khảo hướng dẫn tại đây.

• **Tường lửa có vấn đề?** Phần mềm tường lửa thỉnh thoảng sẽ ngăn cản chương trình mà bạn muốn sử dụng để truy xuất Internet. Bạn có thể vô tình nhấn chuột vào tùy chọn "Keep blocking this program" (nếu sử dụng phần mềm Windows Firewall) hay "Block" (với phần mềm tường lửa của ZoneAlarm) thay vì "Unblock the program" hay "Allow" ở lần đầu tiên chạy chương trình này.

Để khắc phục lỗi này với Windows Firewall, chọn Start -> Run, gõ vào lệnh wscui.cpl và nhấn OK. Sau đó, nhấn tiếp vào mục Windows Firewall, chọn thẻ Exceptions và rồi nhấn Add Programs. Tiếp đến, chọn các ứng dụng mà bạn muốn tính năng tường lửa bỏ qua việc kiểm tra từ danh sách có sẵn, hay nhấn Browse để xác định chúng.

Với ZoneAlarm, nhấn đúp chuột vào biểu tượng ZA trên khay hệ thống, chọn Program Control Program ở khung cửa sổ bên trái và nhấn vào thẻ Programs. Cuộn qua danh sách để tìm ra chương trình cần sử dụng, và nếu bạn thấy một dấu X màu đỏ bên cạnh biểu tượng của chương trình này, hãy nhấn chuột lên đó và chọn Allow từ trình đơn thả xuống.

KIỂM TRA SÓNG WI-FI VỚI NETSTUMBLER
NetStumbler có thể thông báo cho bạn biết sóng radio có ảnh hưởng đến gateway không dây hay không. Hãy lưu ý đến chỉ số SNR (signal-to-noise): nhiễu càng cao thì giá trị SNR càng thấp và vấn đề này có thể do một gateway không dây gần đó sử dụng cùng kênh (channel) với thiết bị gateway của bạn.

Cần biết khi tự ráp máy tính

Khi tự ráp máy vi tính PC, bạn sẽ được lợi nhiều hơn là mua máy ráp sẵn. Nhưng nó cũng đòi hỏi bạn nhiều thứ trong đó quan trọng nhất là lòng ham mê tìm hiểu vì nếu thiếu cá tính nầy bạn sẽ mau bỏ cuộc khi gặp trục trặc (là chuyện thường xảy ra).

Bài viết nầy có mục đích khuyến khích các bạn trẻ tự ráp máy hay tự nâng cấp máy bởi vì chỉ có qua việc làm nầy các bạn mới học hỏi được nhiều về cấu trúc máy, cách hoạt động cũng như cách xử lý khi có hư hỏng.

Tuy nhiên chúng tôi xin khuyên bạn nào không ham thích về kỹ thuật là đừng nên tự ráp máy vì trong quá trình ráp máy có vô số vấn đề phức tạp xảy ra chớ không đơn giản hễ ráp là chạy đâu.

ƯU ĐIểM:

Tiết kiệm cho bạn rất nhiều tiền, theo kinh nghiệm của chúng tôi là khoảng 10% trị giá máy.

Linh kiện do bạn tự chọn lựa nên hợp với tình hình kinh tế của bạn và chất lượng món hàng cũng do bạn quyết định. Ngoài ra do mua lẻ nên bạn sẽ có đầy đủ các sách **hướng dẫn**, đĩa driver và bao bì cho từng linh kiện.

Các thao tác lắp ráp sẽ được tiến hành kỹ lưỡng hơn ngoài tiệm và cách sắp xếp trong máy cũng hợp ý hơn.

Bạn hiểu rõ về máy của bạn hơn và mạnh dạn sửa chữa máy khi có trục trặc nhỏ như: lỏng chân Card, lỏng chấu cắm, các mối nối tiếp xúc không tốt...

Sau khi ráp thử một lần, bạn sẽ có hứng thú giúp đỡ bạn bè và tự nâng cao trình độ về phần cứng máy tính.

KHUYếT ĐIểM:

Tốn nhiều công sức đi lùng mua linh kiện cho vừa ý, thời gian ráp máy nếu chưa có kinh nghiệm có thể kéo dài cả ngày. Đó là chưa kể linh kiện không dùng được phải đem đổi.

Đòi hỏi phải có kiến thức căn bản về phần cứng, phải có tính kỹ lưỡng, kiên nhẫn khi lắp ráp.

Phải biết cách xử lý những va chạm giữa các linh kiện với nhau. Thí dụ: Ngắt, địa chỉ, DMA...

Sau đây là phần trình bày theo thứ tự thực tế để bạn dễ tiếp thu.

LắP RáP CáC PHầN CƠ BảN Để TEST MáY:

KIểM TRA Bộ NGUồN:

Bạn nối dây điện nguồn (dây cáp bự màu đen có 4 dây con) đến công tắc Power, chú ý là có 2 loại công tắc là nhấn và bật lên xuống, bạn phải xem sơ đồ **hướng**

dẫn trên nhãn bộ nguồn để nối cho đúng vì cách xếp đặt chân 2 loại khác nhau. Nối dây cấp điện 5VDC cho mặt hiện số (xem cách nối trong tờ giấy **hướng dẫn** kèm theo thùng máy). Sau đó đóng công tắc nguồn, quạt của bộ nguồn phải quay và bảng hiện số phải sáng (bạn không điều khiển được do chưa nối dây vào mainboard) nếu bộ nguồn tốt. Bộ nguồn không được phát tiếng động lạ như: hú, rít, lạch xạch...

RáP ổ ĐĩA:

Ráp các ổ đĩa mềm, ổ đĩa cứng, ổ đĩa CD-ROM vào thùng máy, gắn các dây cáp tín hiệu cho chúng nhưng khoan gắn cáp cấp điện.

RáP MAINBOARD:

Ráp mainboard lên miếng sắt đỡ bên hông thùng máy. Gắn đầy đủ các chốt đệm bằng nhựa. Cố gắng bắt đủ 2 con ốc cố định cho mainboard, tốt nhất là nên lót thêm miếng lót cách điện cho phần ốc đế và ốc xiết để tránh chạm điện khi mainboard xê dịch.

Căn cứ vào sách **hướng dẫn**, bạn kiểm tra và set lại các Jumper cho đúng với loại CPU của bạn. Bạn cần quan tâm tới Jumper Volt vì nếu set sai CPU sẽ nổ trong 1 thời gian ngắn (thường điện thế của Pentium là 3V).

RáP RAM:

Mainboard 486 cho phép bạn sử dụng từ 1 cây SIMM đến 4 cây (có 4 bank). Mainboard Pentium bắt buộc phải gắn 1 cặp 2 cây SIMM cho 1 Bank (có 2 bank). Bạn xác định chiều gắn SIMM bằng cách đặt đầu chân khuyết cạnh của SIMM vào đầu có gờ chặn của bank. Bạn không nên trộn lẫn vừa EDORAM vừa DRAM, chỉ nên xài 1 loại cho "bảo đảm".

RáP CáC DÂY CắM CủA THùNG MáY:

Bạn nên ráp các dây cắm của thùng máy lên mainboard trước khi ráp Card để tránh vướng và khi ráp card bạn dễ chọn Slot hơn. Đọc kỹ sách **hướng dẫn** của mainboard để cắm các đầu đây cho đúng. Đối với đèn báo khi không lên bạn chỉ cần xoay ngược đầu cắm lại, không sợ hư hỏng. Đối với nút Turbo khi nút có tác dùng ngược, bạn cũng làm như trên. Dây Reset và dây Loa không phân biệt đầu, cắm sao cũng được.

Chú ý là có mainboard không có đầu nối cho nút Turbo (Turbo vĩnh viễn), có khi bạn phải tách dây đèn Turbo từ bảng đèn cắm trực tiếp vào đầu cấm Turbo Led trên mainboard.

RáP CARD:

Bình thường máy cấu hình chuẩn chỉ có card màn hình PCI. Bạn cắm card vào slot nào trong 4 slot PCI cũng được. Các card bổ sung như: Sound, Modem, Netware, MPEG, thường là cắm vào 4 Slot ISA. Trước khi cắm bạn chú ý đặt card vào Slot để xem thử có khớp không, nếu không phải xê dịch mainboard hay miếng sắt đỡ cho khớp rồi mới đè cho phần chân ăn sâu vào Slot. Nên đè luân phiên từ đầu một cho dễ xuống.

Chúng tôi khuyên bạn nên ráp chỉ một mình card màn hình cho dù bạn có nhiều card . Sau khi máy đã khởi động tốt bạn mới ráp các card khác tiếp tục.

RáP CPU:

Gắn CPU vào quạt trước khi gắn CPU vào mainboard, chú ý cắm cạnh khuyết của CPU vào đúng cạnh khuyết của ổ cắm (cạnh khuyết là cạnh thiếu 1 chân hay lỗ ở góc vuông). Khi cắm, bạn so khớp chân với lỗ rồi thả nhẹ nhàng CPU xuống. Khi CPU không tự xuống có thể do cần gạt chưa gạt lên hết cỡ hay chân CPU bị cong cần phải nắn lại. Nếu ổ cắm còn mới, bạn chỉ cần đè nhẹ tay là xuống. Tuyệt đối không được dùng sức đè CPU xuống khi nó không tự xuống được, bạn có thể làm gẫy chân CPU (coi như bỏ !).

RáP CáP TíN HIệU CủA ổ ĐĩA:

Bạn chỉ cần nối cáp cho ổ đĩa mềm khởi động trước để test máy. Bạn cắm cáp tín hiệu vào đầu nối FDD trên mainboard hay trên Card I/O rời. Phải chú ý đấu cho đúng đầu dây số 1 của cáp vào đúng chân số 1 của đầu nối.

RáP DÂY CáP CấP ĐIệN CHO ổ ĐĩA:

Đầu tiên chỉ nên ráp dây cáp cấp điện cho ổ đĩa mềm khởi động để Test máy. Sau khi máy chạy tốt mới nối cho các ổ đĩa còn lại.

RáP CáP CấP ĐIệN CHO MAINBOARD:

Khi nối cáp cấp điện cho mainboard, bạn chú ý là 4 dây đen phải nằm sát nhau và nằm giữa. Ráp ngược cáp có thể làm hư mainboard hay chết các con chip.

LINH TINH:

Tóm gọn các dây nhợ lại thành từng bó, cột và cố định vào chỗ nào gọn. Tránh để dây chạm vào quạt giải nhiệt của CPU, tạo khoảng trống tối đa cho không khí lưu thông dễ dàng trong thùng máy.

KHởI ĐộNG LầN ĐầU TIÊN:

Đây là thời điểm quan trọng nhất trong quá trình ráp máy. Bạn kiểm tra lần cuối cùng rồi bật máy. Nếu mọi việc đều ổn, trong vòng 10 giây, màn hình phải lên và Bios tiến hành kiểm tra máy. Nếu trong 10 giây , màn hình không lên là có chuyện gay go, bạn phải lập tức tắt máy và kiểm tra lại các thành phần sau:

Jumper: Kiểm tra lại các jumper tốc độ mainboard, tốc độ CPU, điện thế CPU có đúng chưa?

DRAM: Coi chừng Ram chưa cắm khớp vào đế, cắm lại Ram thật cẩn thận. Đây là lỗi thường xảy ra nhất.

CPU: Kiểm tra lại chiều cắm của CPU, kiểm tra xem có chân nào cong do cố nhấn xuống đế không? Lỗi nầy hiếm nhưng vẫn xảy ra cho những người ít kinh nghiệm. Khi nắn lại chân phải nhẹ nhàng và dứt khoát, tránh bẻ đi bẻ lại nhiều lần sẽ làm gẩy chân.

Card màn hình: Kiểm tra xem chân card màn hình xuống có hết không?, hay thử đổi qua Slot khác xem sau. Trường hợp card màn hình bị hư hay đụng mainboard rất hiếm.

Nếu tất cả đều đúng nhưng máy vẫn không khởi động được, bạn cần liên hệ với nơi bán mainboard vì xác xuất lỗi do mainboard là cao nhất trong các thành phần còn lại. Có trường hợp mainboard bị chạm do 2 con ốc đế không được lót cách điện. Có trường hợp cần phải set các jumper khác với sách **hướng dẫn** (chỉ có người bán mới biết). Có khi bạn phải ôm cả thùng máy ra chỗ bán mainboard nhờ kiểm tra dùm.

Nếu máy khởi động tốt là bạn đỡ mệt và tiến hành ráp hoàn chỉnh máy. Chú ý trong giai đoạn nầy bạn nên sử dụng xác lập mặc nhiên (default) trong Bios, khi nào máy hoàn chỉnh và chạy ổn định mới set Bios lại sau.

RáP Bổ SUNG Để HOàN CHỉNH MáY:

Nối cáp tín hiệu và cáp điện cho các ổ đĩa còn lại.

Nối các cổng COM và LPT. Chú ý là phải sử dụng bộ dây được cung cấp kèm theo Mainboard, dùng bộ dây khác có thể không được do thiết kế khác nhau. Nối Mouse và máy in.

Ráp các Card còn lại: Nguyên tắc chung khi ráp các Card bổ sung là chỉ được ráp từng Card một, khởi động máy, cài đặt các driver điều khiển. Nếu Card hoạt động tốt mới ráp tiếp Card khác. Cách làm nầy giúp bạn xác định chính xác Card nào trục trặc trong quá trình ráp, không phải đoán mò.

Trước khi ráp Card bổ sung cần cẩn thận kiểm tra các jumper so với sách **hướng dẫn** để tránh bị đụng ngắt, địa chỉ, DMA...

KHởI ĐộNG LạI Và KIểM TRA Kỹ LƯỡNG:

Sau khi ráp hoàn chỉnh, các bạn cho khởi động máy. Tiến hành kiểm tra các thiết bị ngoại vi như sau:

KIểM TRA ổ ĐĩA MềM:

Cách kiểm tra triệt để nhất là Format chừng 2 hay 3 đĩa mềm còn mới và bạn biết chắc là tốt sau đó ghi thử lên đĩa và đem qua máy khác đọc. Có trường hợp ổ đĩa mềm đọc, ghi bình thường nhưng không format được hay khi format báo đĩa hư nhiều. Có trường hợp đĩa ghi bằng máy mới khi đem qua máy khác không đọc được hay ổ đĩa mới không đọc được đĩa máy khác - Đây là do đầu từ bị lệch so với các ổ đĩa khác. Có trường hợp ổ đĩa hoạt động bình thường nhưng không thể khởi động máy được, thay ổ đĩa khác vẫn như vậy - Đây là do Mainboard. Có trường hợp ổ đĩa đọc ghi được một thời gian rồi bắt đầu phát tiếng kêu lớn và không đọc được đĩa nữa hay lúc được lúc không - ổ đĩa hư cần thay ổ khác, đừng cố xài sẽ hư đĩa mềm.

KIểM TRA CáC THàNH PHầN KHáC:

Dùng chương trình PCCHECK chứa trên đĩa mềm để kiểm tra toàn bộ máy, kể cả ổ đĩa CDROM.

LINH TINH:

Tiến hành **Fdisk** và format đĩa cứng.

CàI ĐặT Hệ ĐIềU HàNH:

Cài đặt hệ điều hành vào ổ đĩa cứng để chấm dứt tình trạng khởi động bằng ổ đĩa mềm. Theo kinh nghiệm của chúng tôi hệ điều hành dùng để xác định chất lượng máy tốt nhất là Windows 95 và Windows NT. Máy nào cài được coi như đã có xác nhận chất lượng cao. Trên thực tế, các máy ráp linh kiện rẻ tiền và không chuẩn sẽ khó lòng cài Windows 95 chứ nói gì đến Windows NT. Có nhiều chỗ bán máy "dỏm" không dám cài Windows 95 khi có yêu cầu của khách vì họ sợ không cài được. Bạn chỉ cần cài thử để kiểm tra chất lượng máy rồi xoá chứ không cần sử dụng luôn, đây cũng là dịp cho bạn thử hệ điều hành mới ngoài Dos và Windows 3.xx.

Sau khi cài hệ điều hành xong, bạn mới có thể tiến hành việc tăng tốc máy và set lại Bios theo ý bạn

Đọc xong - vọc liền

"XỬ" CÁC GÃ HDD BẰNG DM

"VỌC SĨ" PHẠM HỒNG PHƯỚC

KHI TẬU MỚI MỘT GÃ Ổ ĐĨA CỨNG (HDD) hay bị virus khủng bố khiến phải "tắt đèn làm lại" cả ổ đĩa, bạn chẳng có lối thoát nào khác hơn tiến hành định dạng (format) và phân vùng (chia partition) cho HDD. Nếu không được siêng hay có gì xài nấy, người ta thường nhờ vả tới công cụ FDISK của MS-DOS. Nhưng nếu muốn "xử" HDD cho triệt để và tối ưu, bạn nên sử dụng công cụ cài đặt HDD (như Disk Manager) do từng hãng sản xuất HDD cung cấp.

DISK MANAGER (DM) là một chương trình chạy ngoài MS-DOS. Vì thế, nó hoàn toàn không bị lệ thuộc hoặc bị giới hạn chi đối với Windows. Nhờ vậy, bạn có thể dễ dàng cài đặt một ổ đĩa cứng mới vào hệ thống, phó linh hồn và thể xác nó cho CMOS của mainboard quản lý, trước khi cài đặt Windows. Điều này thiệt tiện lợi khi bạn gắn ổ cứng mới, ráp máy mới hay trong trường hợp Windows bị "tan tác đời hoa" vì virus. Chỉ với một đĩa mềm, bạn có thể boot máy và chạy DM để xử lý ổ cứng, như định dạng, phân vùng,... Ngoài ra, để giải quyết các hạn chế về BIOS ở các máy hơi bị "xưa rồi Diễm", DM chia ổ đĩa cực kỳ nhanh. Đặc biệt là nó định dạng HDD với dung lượng chính xác nhất và được coi là tối ưu trong chuyện "xử" các gã HDD có dung lượng khổng lồ.

Thế nhưng có một điều lưu ý cực kỳ quan trọng: Mặc dù hầu hết công cụ DM đều có xuất xứ một lò là Ontrack nhưng chúng đều có những thay đổi khác nhau cho

phù hợp với các thông số và tiêu chuẩn kỹ thuật của từng nhà sản xuất HDD. Bởi vậy, bạn chỉ được sử dụng DM của đúng nhãn hiệu ổ cứng. HDD Seagate thì xài DM Seagate. Bạn có thể tải các phần mềm DM này từ các website của hãng sản xuất HDD.

* Seagate (DM 9.56a, dung lượng 1,1MB): http://www.seagate.com/support/disc/download/dmgr956a.exe
* IBM (DM 9.61, dung lượng 1,7MB): http://www.hgst.com/downloads/DMDISK.EXE
* Maxtor (Max Blast 3, dung lượng 1,8MB): http://www.maxtor.com/en/support/downloads/files/maxblast3.exe
* Western Digital (Data Life Guard 10.0, dung lượng 1,4 MB): http://support.wdc.com/download/dlg/dlginstall_10_0.exe

Tạo đĩa mềm chạy phần mềm định dạng HDD có khả năng boot:

Bạn nạp một đĩa mềm trắng vào ổ. Kích hoạt file phần mềm DM và bắt đầu làm theo các bước được hướng dẫn trên màn hình. Tất cả các dữ liệu cũ đang có trên đĩa mềm này sẽ bị xóa sạch. Sau khi hoàn tất, bạn đã có trong tay một đĩa mềm DM để xử gã HDD của mình. Để sử dụng nó, bạn chỉ việc nạp vào ổ và khởi động lại máy.

Định dạng và phân vùng HDD:

1. Disk Manager cho các HDD IBM, Seagate và Quantum:

Giai đoạn ban đầu của mỗi DM tuy có thể khác nhau, nhưng phần cơ bản cũng tương tự nhau. Hiện nay, hầu hết các đĩa mềm DM đều tự boot và tự chạy. Sau những thủ tục ban đầu, bạn chọn chức năng Install HDD. Ở DM của IBM, bạn phải chọn ngay tác vụ cần thực hiện. Nếu muốn định dạng HDD, bạn nhấn phím số 2 để chọn tác vụ DM.

* Menu Disk Manager Main Menu có bốn mục:
- (E)asy Disk Installation: Định dạng đơn giản.
- (A)dvanced Options: Các tùy chọn nâng cao.
- (V)iew/Print Online Manual: Xem và in hướng dẫn sử dụng on-line.
- Exit Disk Manager: Thoát khỏi DM.

Bạn chọn mục 2 (A)dvanced Options để định dạng ổ HDD.

* Menu Advanced Options gồm bốn mục:
- (A)dvanced Disk Installation: Cài đặt đĩa nâng cao.
- (M)aintenance Options: Các tùy chọn bảo dưỡng.
- (U)pgrade Disk Manager: Nâng cấp DM.

Bạn chọn mục 1 (A)dvanced Disk Installation để cài đặt HDD nâng cao.

* DM nhận diện HDD đang có trong hệ thống của bạn. Chọn Yes để xác nhận. Khi trong máy có tới hai HDD, bạn phải cẩn thận chọn đúng HDD mình muốn "xử".

* Trên màn hình chọn loại hệ điều hành, bạn chọn loại dự định sử dụng. Có các tùy chọn:
- Windows 95, 95A, 95 OSR1 (FAT 16)
- Windows 95 OSR2, 98, 98SE, Me, 2000 (FAT 16 or 32)
- Windows NT 3.51 (or earlier)
- Windows NT 4.0 (or later) or OS/2
- DOS/Windows 3.1x (FAT 16)
- Other Operating System

Bạn nên chọn mục 2 Windows 95 OSR2, 98, 98SE, Me, 2000 (FAT 16 or 32) cho nó rộng đường "binh" sau này.

* DM hỏi bạn có đồng ý cho nó format HDD bằng hệ thống file FAT 32 hay không? Nên chọn Yes.

* Trên menu Select a Partition Option, bạn chọn một tùy chọn phân vùng (hay gọi là chia partition) mà mình muốn.

* Nếu muốn để nguyên HDD làm một partition, bạn chọn OPTION (A). Nếu để DM chia thành bốn partition bằng nhau, bạn chọn OPTION (B). Còn trong trường hợp muốn phân các vùng có dung lượng khác nhau theo ý mình, bạn chọn OPTION (C).

Xin lưu ý: Khi chia HDD ra càng nhiều vùng, bạn sẽ càng mất nhiều tài nguyên cho chuyện quản lý từng vùng và tốc độ HDD sẽ bị chậm lại. Với các HDD có dung lượng lớn, dứt khoát bạn phải chia vùng để những phần mềm hệ thống cũ chẳng bị "sốc", có thể nhận diện được; đồng thời khi cần xóa phân mảnh (defragment), công cụ này chạy nhẹ hơn và nhanh hơn. Bạn lần lượt gõ dung lượng từng vùng vào hộp Size of Partition (tính bằng MB). Đầu tiên là ổ đĩa gốc C:. Sau đó, bạn cấp mặt bằng lần lượt cho từng vùng khác.

* Xong xuôi, bạn chọn mục Save and Continue để lưu các thiết đặt lại.

* Một menu đỏ mang tính cảnh báo xuất hiện. Nó báo rằng tất cả các dữ liệu đang có trên HDD sẽ bị xóa sạch. Bạn được yêu cầu kiểm tra lại tên HDD xem chính xác chưa để "hạ thủ bất huờn". Chắc như bắp rồi thì bạn nhấn tổ hợp phím ALT+C để
cho DM bắt đầu xử HDD.

* Bạn nên chọn Yes ở hộp thoại Fast Format để DM định dạng nhanh.

* Chọn Yes để sử dụng giá trị cluster mặc định.

* Trước khi tiến hành xóa HDD, DM hỏi lại bạn lần nữa. Chọn Yes để tiếp tục.

Sau khi DM hành xử xong, việc thiết lập các partition đã hoàn tất. Sau khi bạn boot máy, mỗi partition này sẽ được truy xuất như một tên ổ luận lý (logical drive letter), hay còn gọi là ký tự ổ đĩa. Bây giờ thì HDD của bạn đã sẵn sàng để sử dụng, có thể cài đặt hệ điều hành.

2. Max Blast 3 cho HDD Maxtor:

Giao diện của Max Blast 3 (MB3) mang tính đồ họa, thân thiện, giống như một ứng dụng Windows.

Sau khi khởi động và MB3 đã được nạp, bạn chọn bước Partitioning and Formatting để phân vùng và định dạng HDD Maxtor. Nhấn nút chọn ổ đĩa muốn xử. Bạn chọn hệ điều hành mà mình tính cài đặt. Bất luận thế nào, nên chọn sẵn là Windows 98 or ME. Có hai tùy chọn:

- Standard Partitions (các vùng tiêu chuẩn). Hình thành số partition tối thiểu mà hệ điều hành cho phép.
- For Advanced Users (dành cho những người dùng hơi bị có nghề). Cho phép bạn tùy biến quá trình định dạng HDD.

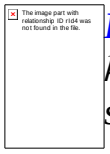
Trên màn hình Drive Information, bạn nhấn nút ADD nếu muốn chia thêm các partition. MB3 tuyệt hơn DM ở chỗ cho phép bạn kéo thanh trượt để xác định dung lượng từng partition. Cứ mỗi lần nhấn nút ADD, bạn có thể tạo một partition mới. Bạn cứ việc làm theo hướng dẫn từng bước tới khi kết thúc.

3. Data Life Guard cho HDD Western Digital:

Data Life Guard (DLG) cũng có giao diện đồ họa thân thiện, nhưng không có màu sắc như Max Blast. Sau khi nạp lên ở MSDOS, nó yêu cầu bạn chọn tác vụ cài đặt đĩa hay các công cụ xử lý đĩa. Làm theo hướng dẫn từng bước của DLG

PARTITION MAGIC (PHIÊN BẢN 8): "BỬU BỐI" CỦA NHỮNG NGƯỜI THÍCH... "VỌC"

DUY THÔNG



PARTITION MAGIC (PM) là một phần mềm không thể thiếu trong "túi càn khôn" đối với những người làm công tác "bảo trì" máy tính hay các "vọc sĩ" tại... gia.

Đây là một phần mềm chuyên dùng để phân chia và tái... phân chia ổ cứng mà không làm mất dữ liệu đã có trong ổ cứng (dĩ nhiên là theo lý thuyết). Phần mềm này có thể làm việc với "gần như" mọi hệ điều hành hiện có và chuyển đổi các dạng thức phân vùng ổ cứng một cách dễ dàng.

Nếu phân tích tỉ mỉ mọi tính năng của phần mềm này, chắc phải viết thành một cuốn sách dày. Ở đây, e-CHÍP chỉ xin đề cập đến những tính năng căn bản và quan trọng, các bạn có thể tự nghiên cứu thêm để làm "chủ" phần mềm này. Chú ý: PM sẽ có một phiên bản cho DOS bao gồm tất cả các file nằm trong thư mục Program Files\Power Quest\PartitionMagic 8.0\Dos. Bạn có thể chép các file này ra đĩa mềm hay đĩa CD để chạy độc lập. Cách sử dụng phiên bản cho DOS và cho Win

hoàn toàn giống nhau.

1. Tạo phân vùng (partition)

Trên một ổ đĩa, bạn có thể tạo bốn phân vùng Primary, hay ba phân vùng Primary và một phân vùng Extended. Trong phân vùng Extended, bạn có thể tạo bao nhiêu phân vùng con (logic) cũng được.

Cách làm: Chọn ổ đĩa, chọn Partition/Create, chọn Logical Partition hay Primary Partition, chọn Partition Type, đặt tên (Label), chỉ định kích thước (Size), chọn vị trí đầu hay cuối đĩa (Beginning of unallocated space hay End of unallocated space) và bấm OK.

2. "Nhân bản" (Copy) phân vùng

Bạn có thể tạo phân vùng mới là bản sao của phân vùng đang có. Chức năng này được dùng khi: Di chuyển nhanh nội dung của ổ đĩa này sang ổ đĩa khác. Sao lưu dự phòng.

Thay đổi vị trí phân vùng... Cách làm: Chọn ổ đĩa và phân vùng, chọn Partition/Copy, chọn vị trí, bấm OK.

3. Chuyển đổi (convert) phân vùng

- FAT sang FAT32 (Windows 9x/Me/2000/XP). FAT sang NTFS (Windows NT/2000/XP).
- FAT32 sang FAT, FAT32 sang NTFS (Windows 2000/XP).
- NTFS sang FAT hay FAT32. Chú ý: Không thể chuyển đổi được nếu phân vùng NTFS có sử dụng những tính năng đặc biệt như: compressed, sparse, reparse points, encrypted hay có lỗi đĩa như: lost clusters, cross-linked...
- Primary thành Logical và ngược lại.

Cách làm: Chọn phân vùng, bấm Partition/Convert, chọn dạng thức cần chuyển.

4. Sáp nhập (Merge) phân vùng

Bạn có thể sáp nhập hai phân vùng FAT, FAT32 hay NTFS để giảm bớt số lượng phân vùng đang có mà không làm mất dữ liệu. Bạn cũng có thể sáp nhập phân vùng logic vào primary. Chú ý: Giữa hai phân vùng cần sáp nhập không được có phân vùng thứ ba. Bạn không thể sáp nhập phân vùng FAT/FAT32 với phân vùng NTFS.

Cách làm: Chọn ổ đĩa và phân vùng, chọn Partition/Merge để mở hộp thoại Merge Adiacent Partitions, chọn phân vùng muốn sáp nhập trong phần Merge Option. Nội dung của phân vùng nầy sẽ trở thành thư mục (folder) trong phân vùng kia. Đặt tên cho thư mục lưu trữ nội dung của phân vùng bị mất khi sáp nhập trong phần Merge Folder, chọn kiểu bảng FAT cho phân vùng sau khi sáp nhập, OK.

5. Chia tách (Split) phân vùng

Bạn có thể chia một phân vùng FAT hay FAT32 thành hai phân vùng có cùng định dạng. Bạn có thể chọn dữ liệu từ phân vùng "gốc" để đưa sang phân vùng mới, chọn kích thước, vị trí cũng như đặt tên cho phân vùng mới.

Cách làm: Chọn phân vùng, chọn Partition/Split, chọn bảng Data, chọn file/thư mục cần di chuyển, đặt tên cho phân vùng mới, chọn dạng thức, chọn bảng Size,chỉ định kích thước, chọn OK.

[Đầu trang]

6. Thay đổi kích thước/Di chuyển (Resize/Move) phân vùng

Bạn có thể thay đổi kích thước hay di chuyển phân vùng với một số chú ý sau:
- Không thể thu nhỏ phân vùng nếu trong phân vùng không còn không gian trống.
- Không thể mở rộng phân vùng nếu không có không gian trống ở kề bên phân vùng.
- Trong thời gian điều chỉnh kích thước hay di chuyển phân vùng NTFS, nếu có trục trặc phân vùng này có thể bị hư hỏng.

Cách làm: Chọn ổ đĩa và phân vùng, chọn Partitiopn/Resize/Move, dùng chuột để điều chỉnh khoảng trống ở đầu đĩa/cuối đĩa qua thanh công cụ Partition Map (hay gõ số dung lượng vào các ô kích thước). Di chuyển phân vùng qua vị trí khác bằng cách đưa chuột vào giữa rồi bấm, giữ và kéo chuột đi.

7. "Giấu" (Hide) phân vùng

Bạn có thể giấu phân vùng đĩa hay cho "hiện" (unhide) nếu bạn... thích. Chú ý: Nếu bạn có nhiều phân vùng Primary, chỉ phân vùng khởi động "hiện" còn các phân vùng khác sẽ tự động "ẩn".

Cách làm: Chọn ổ đĩa và phân vùng, chọn Partition/Advanced/Hide Partition hay Unhide Partition, OK.

8. Phục hồi phân vùng bị xoá (Undelete)

Bạn có thể phục hồi phân vùng FAT, FAT32, NTFS và Linux. Chú ý: Bạn chỉ phục hồi khi không gian của phân vùng bị xoá chưa được sử dụng. Bạn phải phục hồi lần lượt nếu có nhiều phân vùng bị xoá vì chương trình chỉ hiển thị danh sách từng phân vùng mỗi lần chạy. Bạn không thể phục hồi nếu phân vùng bị xoá có lỗi ở hệ thống file. Bạn không phục hồi được phân vùng primary nếu ổ đĩa có đến bốn phân vùng primary.

Cách làm: Trên disk map hay danh sách phân vùng, chọn phần không gian trống (unallocated space), chọn Partition/Undelete, chọn phân vùng cần phục hồi, OK.

9. Cài Hệ điều hành mới

Partition Magic còn có chức năng giúp bạn cài đặt thêm hệ điều hành (HĐH) mới để chạy song song với HĐH đang có. Chương trình sẽ giúp bạn tính toán dung

lượng sao cho phù hợp với HĐH và tạo phân vùng Primary mới từ không gian lấy ở các phân vùng đang có.

Chú ý: Bạn phải tự cài đặt HĐH lên phân vùng mới và cài đặt trình quản lý Boot nếu cần thiết.

10. Thay đổi thông tin ổ đĩa cho phần mềm

Trong bộ PM8 có "khuyến mại" phần mềm Drive Mapperv có chức năng tự động thay đổi tên ổ đĩa, trong các file lưu trữ thông tin về địa chỉ của các phần mềm chạy trong Windows. Thí dụ: Bạn có nhiều phần mềm cài trên ổ đĩa D, nay vì gắn thêm một ổ cứng nên ổ D bị đổi thành F, tất cả sẽ không còn chạy được do sai địa chỉ. Phần mềm nầy sẽ tự động thay đổi tất cả địa chỉ lưu trữ từ D (cũ) thành F (mới) để các phần mềm này tiếp tục chạy.
Chức năng nầy đặc biệt có ích khi bạn chia lại (thêm, bớt, di chuyển...) phân vùng trên ổ cứng, thay đổi số lượng ổ cứng trong máy mà không muốn cài đặt lại các phần mềm.
Khi chạy chương trình, bạn có chọn lựa:
- Typical Operation: Cho phép bạn thay đổi ký tự ổ đĩa theo ý muốn. - Merge Operation: Cho phép bạn thay đổi ký tự ổ đĩa bằng đường dẫn đến một thư mục.
- Split Operation: Cho phép bạn thay đổi ký tự ổ đĩa bằng đường dẫn đến một file hay thư mục.

LẮP RÁP VÀ SỬ DỤNG Ổ CỨNG

LÊ HOÀN

Lắp ráp

Máy tính cá nhân (PC) hiện nay cho phép bạn sử dụng bốn ổ đĩa cứng có giao tiếp IDE/ EIDE cùng lúc. Để phân biệt các ổ đĩa trên cùng một cáp tín hiệu, chúng ta phải xác lập bằng cách nối tắt các chân cắm được quy định cụ thể trên từng ổ đĩa (set jumper). Nhà sản xuất luôn cung cấp sơ đồ set jumper kèm theo ổ đĩa của mình vì nếu thiếu, chỉ có cách là set "mò" hay dựa trên ổ đĩa khác. (Chú ý: ổ đĩa CD-ROM theo chuẩn giao tiếp IDE cũng được tính vào tổng số này.)

Nếu muốn sử dụng trên bốn ổ đĩa trong một máy, bạn có thể mua card Ultra ATA gắn vào Slot PCI còn trống trên mainboard. Mỗi card Ultra ATA cho phép gắn thêm bốn ổ đĩa cứng và mainboard sẽ quản lý các ổ đĩa này tương tự các ổ đĩa SCSI. Chú ý: Bạn phải cài driver dành cho từng phiên bản Windows của nhà sản xuất cung cấp kèm theo card.

Các quy ước khi lắp ráp, kết hợp ổ đĩa:

- Dây cáp: Cáp tín hiệu của ổ đĩa cứng IDE/EIDE (40 dây) có ba đầu nối giống y nhau. Một đầu để gắn vào đầu nối EIDE trên mainboard, hai đầu còn lại để gắn vào đầu nối trên hai ổ đĩa cứng. Khi cắm dây, chú ý cắm sao cho vạch màu ở cạnh cáp

nối với chân số 1 của đầu nối. Thường chân số 1 được quy ước trên mainboard là cạnh có ghi số 1 hay có dấu chấm tròn, hoặc dấu tam giác. Trên ổ đĩa là cạnh có ghi số 1, hay cạnh nằm sát dây cắm nguồn. Có hãng sản xuất đã ngừa trường hợp cắm ngược cáp bằng cách bỏ bớt một chân ở đầu nối trên mainboard, và bít một lỗ tương ứng ở đầu nối trên cáp. Khi nối cáp, cố gắng xoay trở đầu cáp sao cho đoạn dây đi từ mainboard đến ổ đĩa cứng là ngắn nhất. Thậm chí, bạn có thể nối đầu giữa lên Mainboard, hai đầu bìa lên ổ đĩa cứng. Chú ý: Đối với cáp Ultra ATA (80 dây) ta phải cắm đúng quy định của nhà sản xuất (thường các đầu cắm phân biệt bằng màu sắc).
Giữa hai nhóm ổ đĩa 1, 2 và 3, 4 phân biệt bởi hai dây cáp gắn vào hai đầu nối Pri (thứ nhất 1, 2) hay Sec (thứ nhì 3, 4). Giữa ổ đĩa 1, 2 hay 3, 4 phân biệt bằng cách set Jumper trên mỗi ổ đĩa là Master (1, 3) hay Slave (2, 4).

- Trên ổ đĩa có các set sau: Master (single): Ổ đĩa chính duy nhất. Master (dual): Ổ đĩa chính nhưng có kết hợp với ổ khác.
Slave: Ổ đĩa phụ.
Cable Select: Xác lập master hay slave bằng vị trí đầu cáp.
Có một số mainboard bắt buộc ổ đĩa khởi động phải được set là Master và được gắn vào cáp Pri (1). Có một số mainboard đời mới cho phép bạn vào BIOS xác lập khởi động bằng ổ đĩa nào cũng được hay tự động dò tìm ổ đĩa khởi động theo thứ tự do bạn quy định trong BIOS (ổ mềm, CD ROM, SCSI, ổ cứng C hay D, E, F...).
Có trường hợp hai ổ đĩa không chịu chạy chung với nhau khi gắn cùng một cáp. Bạn phải sử dụng hai cáp cho hai ổ đĩa này.

Sử dụng

Để sử dụng được ổ đĩa cứng với hệ điều hành DOS/Win, bạn phải tiến hành các thủ tục sau:
Fdisk: Phân vùng đĩa.
Format: Định dạng đĩa.
Trong trường hợp bạn mới ráp máy hay làm lại ổ đĩa, bạn phải khởi động bằng đĩa mềm rồi dùng chương trình chứa trên đĩa mềm tiến hành thao tác với ổ đĩa cứng.

Cách làm đĩa mềm khởi động như sau:
* Đưa đĩa mềm vào ổ đĩa A, đánh lịnh Format A: /S
* Chép tối thiểu các file sau lên đĩa mềm: Fdisk, Format, Sys. Bạn có thể chép thêm NC, các chương trình chống Virus, các chương trình tiện ích...tuỳ theo nhu cầu và dung lượng đĩa mềm còn trống.

FDISK

Khi bạn đánh lệnh Fdisk, màn hình đầu tiên sẽ hỏi bạn có sử dụng FAT32 hay không (DOS 7 hỗ trợ FAT32) rồi đến màn hình có các mục dưới đây:
1. Create DOS partition or Logical DOS Drive

2. Set active partition
3. Delete partition or Logical DOS Drive
4. Display partition information
5. Change current fixed disk drive
Giải thích:
* Create DOS partition or Logical DOS Drive: Tạo khu vực trên đĩa (có thể là một phần, có thể là toàn bộ) và tạo ổ đĩa Logic Dos.
Trong mục nầy còn có các mục con:
a. Create Primary DOS Partition
b. Create Extended DOS Partition
c. Create Logical DOS Drive(s) in the Extended DOS Partition
* Đầu tiên, bạn phải tiến hành mục a tức là tạo Partition DOS thứ nhất. Vùng nầy có đặc điểm là chỉ chứa một ổ đĩa duy nhất có dung lượng chiếm toàn bộ không gian vùng và chỉ ổ đĩa nầy được phép khởi động. Nếu bạn không chia nhỏ ổ đĩa cứng vật lý thì bạn cho vùng nầy chiếm toàn bộ và quá trình fdisk kể như hoàn tất, Fdisk sẽ tự động chỉ định cho ổ đĩa nầy là ổ khởi động. Nếu bạn muốn chia nhỏ ổ đĩa, bạn chỉ định kích thước cụ thể cho vùng này rồi tiến hành mục b.
* Mục b tạo vùng đĩa mở rộng dành cho DOS. Dung lượng là không gian còn lại của ổ đĩa vật lý hay chỉ một phần nếu bạn muốn dự trữ một vùng riêng ngoài tầm kiểm soát của DOS (dành cho hệ điều hành khác) gọi là vùng Non DOS. Vùng DOS mở rộng nầy sẽ chứa tất cả các ổ đĩa Logic mà bạn muốn tạo và bạn tiến hành tạo chúng bằng mục c.
2. Set active partition: Chỉ định ổ đĩa được phép khởi động. Theo quy định của DOS, chỉ có ổ đĩa nằm trong Pri Partition mới được phép active (ổ đĩa C). Mục này chỉ dùng khi bạn không cho vùng Pri chiếm toàn bộ dung lượng ổ đĩa vật lý.
3. Delete partition or Logical DOS Drive: Xoá bỏ những gì bạn tạo trong mục 1. Theo quy định của DOS, quá trình xóa phải ngược lại với quá trình tạo, nghĩa là cái gì tạo đầu tiên phải được xoá sau cùng và ngược lại.
Trong mục nầy có các mục con:
a. Delete Primary DOS Partition
b. Delete Extended DOS Partition
c. Delete Logical DOS Drive(s) in the Extended DOS Partition
d. Delete Non-DOS Partition
Trong mục nầy, bạn phải tiến hành ngược từ dưới lên trên tức là tiến hành theo thứ tự 4,3,2,1.
4. Display partition information: Hiển thị tình trạng hiện tại của ổ đĩa cứng. Mục này bạn nên chọn đầu tiên để tránh tình trạng thao tác lộn ổ đĩa.
5. Change current fixed disk drive: Chọn ổ đĩa vật lý để thao tác.
Chú ý: Khi bạn Fdisk trên ổ đĩa cứng nào (logic hay vật lý) toàn bộ dữ liệu trên ổ

đĩa đó sẽ bị xoá. Fdisk chỉ dùng cho ổ đĩa cứng, bạn không thể Fdisk ổ đĩa mềm.

[Đầu trang]

FORMAT

Format được dùng cho đĩa cứng lẫn đĩa mềm và gần như là chương trình thông dụng khi sử dụng máy tính. Nhưng Format có hai tính năng chưa được đánh giá đúng mức là format triệt để (/u): quá trình kiểm tra đĩa kỹ lưỡng nhất, và format /q (format nhanh): cách xoá đĩa có nhiều file nhanh nhất.

Công dụng chính của Format /u là xóa mọi dữ liệu cũ, định dạng lại ổ đĩa giống như khi mới mua. Trong quá trình định dạng lại nó còn kiểm tra đánh dấu các vị trí xấu không sử dụng được.

Công dụng của Format /q là không làm gì ảnh hưởng đến dữ liệu hiện có trong ổ cứng, nó chỉ làm một việc đơn giản là xoá các thông tin dùng để quản lý dữ liệu. Khi nào cần ghi dữ liệu mới thì dữ liệu cũ bị xoá đi. Do đó, nếu format /q, bạn vẫn có thể phục hồi dữ liệu lại được nếu chưa ghi dữ liệu mới đè lên.

Ký tự cho ổ đĩa

Trên máy có từ hai ổ cứng trở lên mà mỗi ổ cứng lại chia thành nhiều phân vùng (partition) thì việc đặt tên đĩa của DOS dễ làm bạn "rối" vì chúng được gán theo một thứ tự "kỳ cục": DOS chỉ định ký tự ổ đĩa cho các phân vùng chính (pri) trước rồi mới đến các phân vùng mở rộng (ext). Thí dụ: Có ba ổ đĩa, mỗi ổ đĩa chia hai phân vùng thì tên của chúng được gán là C cho phân vùng pri của ổ 1, D cho phân vùng pri của ổ 2, E cho phân vùng pri của ổ 3, F cho phân vùng ext của ổ 1, G cho phân vùng ext của ổ 2, H cho phân vùng ext của ổ 3. Đối với những người sử dụng máy tính ít kinh nghiệm, họ khó mà biết ký tự ổ đĩa được gán thuộc về ổ cứng nào (trừ ổ C).

Bạn có thể tránh được rắc rối này bằng cách chỉ chia phân vùng ext cho các ổ cứng từ ổ thứ hai trở đi. Khi đó, DOS sẽ gán ký tự ổ đĩa theo đúng trật tự vật lý của chúng, nghĩa là lần lượt từ ổ thứ nhất đến ổ cuối cùng (vì chỉ có một phân vùng pri trên ổ 1).
Biện pháp này có một nhược điểm là tất cả các ổ đĩa không có phân vùng pri sẽ không khởi động được và không thể dùng làm ổ C nếu mang sang các máy tính khác.

Nếu đang sử dụng Windows 98 trên máy Pentium MMX trở lên, bạn có thể áp dụng cách đơn giản sau: Không khai báo ổ cứng thứ nhì trở đi trong BIOS. Khi vào Windows, hệ điều hành nầy tự phát hiện ra các ổ cứng đó và sẽ quản lý với các ký tự ổ đĩa được sắp xếp tiếp theo ổ cứng thứ nhất (thí dụ: C là phân vùng pri trên ổ 1; D là phân vùng ext trên ổ 1; E là phân vùng pri trên ổ 2; F là phân vùng ext trên ổ 2).
Biện pháp này có nhược điểm là không sử dụng được ổ cứng thứ hai khi khởi động với DOS, nhưng có ưu điểm là bạn vẫn chia ổ đĩa như bình thường (có thể dùng làm ổ C để khởi động khi chạy trên máy khác).

Nếu chạy Windows NT/2000/XP, bạn có thể vào Computer Manager/Disk Management và thay đổi ký tự ổ đĩa tuỳ ý.

Format cấp thấp đĩa cứng (low level format)

Thông thường, nhà sản xuất đã format cấp thấp cho ổ đĩa trước khi xuất xưởng, format cấp thấp đĩa cứng (low level format) sẽ ghi lại thông tin định dạng lên từng sector đĩa cứng về mặt vật lý phù hợp với trạng thái đầu từ ghi/đọc lúc đó và "loại bỏ" các sector hư hỏng (nếu có) khỏi danh sách quản lý của mạch điều khiển (tránh trường hợp ghi vào đây làm mất dữ liệu). Sau thời gian sử dụng, có thể có một số sector bị hư hỏng hay tình trạng đầu từ đọc/ghi bị thay đổi (do các chi tiết cơ khí bị mài mòn), chúng ta nên format cấp thấp lại để cập nhật "tình trạng vật lý" mới cho ổ đĩa. Ảnh hưởng của nó tương đương với một lần ghi dữ liệu và không hề làm giảm tốc độ hay tuổi thọ của ổ cứng, tuy nhiên chúng ta cần chú ý các vấn đề sau:
- Format cấp thấp đĩa cứng sẽ phát hiện các sector hỏng và sẽ giấu chúng về mặt vật lý (mạch điều khiển ổ đĩa) để tất cả các chương trình (kể cả hệ điều hành) không bao giờ dùng được các sector này, do đó mỗi lần format cấp thấp lại, có thể dung lượng đĩa hữu dụng sẽ bị giảm (nếu có thêm sector hỏng mới).
- Trong một số mainboard, BIOS có chức năng format cấp thấp và quá trình thực hiện việc format này rất chậm.
- Có một số phần mềm chuyên dùng để format cấp thấp của các hãng sản xuất ổ cứng chạy rất nhanh và có thể sử dụng cho nhiều loại ổ khác nhau. Tuy nhiên, chức năng giấu sector hỏng không được hoàn hảo lắm (khi được, khi không...).
- Quá trình format cấp thấp là một quá trình ghi đọc đĩa toàn diện và trên toàn bộ

bề mặt vật lý của đĩa cho nên có thể nói đây cũng là một quá trình kiểm tra tình trạng hoạt động khá nặng nề đối với các ổ đĩa cũ (ổ nào quá "yếu" thì có thể "tắt thở" luôn do không chịu nổi thử thách). Do đó, không nên format ở mức Low Level nhiều lần, mà chỉ thực hiện khi thật cần thiết.

ThemeXP.org: Thiên đường hay địa ngục?

Thực hiện: Nguyễn Tiến Dũng

Thiên đường của vẻ đẹp

Nếu là một người yêu cái đẹp chắc hẳn bạn không còn quá xa lạ với địa chỉ ThemeXP.org. Đây là một website lớn, cung cấp những giao diện ba chiều độc đáo, hình nền, biểu tượng, con trỏ, màn hình khởi động, đăng nhập... cho hệ điều hành Widows XP, thứ nào cũng đều tuyệt đẹp. Lần đầu vào ThemeXP.org ai cũng ngỡ ngàng trước vẻ đẹp thanh thoát hiện đại trên đó. Nếu chú ý một chút bạn sẽ nhận ra rằng việc tải tệp tin thật đơn giản vì chỉ cần nhấn vào dòng chữ Download luôn thường trực dưới các hình thu nhỏ (thumbnail), mọi thứ đều miễn phí và được sắp đặt theo từng thể loại rất rõ ràng (**Hình 1**). Chẳng thế mà có người ví von rằng đây chẳng khác nào một "thiên đường" dành cho những người dùng Windows XP. Và hễ nói về ThemeXP.org là người ta lại nhắc đến phần mềm StyleXP 3.18 giá 19,95 USD của TGTSoft (**Hình 2**).

Quả lừa ngoạn mục!

Nếu dừng lại ở đây thì bài viết này cũng chỉ là một bài ca tụng ThemeXP.org giống như bao bài báo khác. Đã bao giờ bạn nghĩ rằng mình phải trả gì cho những vẻ đẹp miễn phí này chưa? Sự thực ngoài cái đẹp bạn sẽ nhận thêm một chú trojan và những phần mềm quảng cáo bất hợp pháp... Thật vậy, người viết bài này đã không thể tin vào mắt mình trước cảnh báo của những phần mềm diệt virus/spyware hàng đầu thế giới. Để làm sáng tỏ điều này chúng ta hãy cùng lướt qua quá trình cài đặt các tệp tin thực thi mà website này cung cấp. Cách thực hiện khá đơn giản, sau khi chạy và nhấn Next hai lần bạn sẽ nhận được thông báo về việc ThemeXP.org được

hỗ trợ bởi phần mềm New.net và bạn bắt buộc phải đánh dấu vào ô I agree to install New.net Domains Software nếu không nút I agree sẽ bị ẩn đi và không cài tiếp được. Nếu trước đó máy tính đã được bảo vệ bởi một phần mềm diệt virus/spyware mạnh với chế độ tự động diệt thì đôi khi thông báo Application.Adware.NewDotNet.B.Dropper được hiện ra (**Hình 3**), New.net chính là một phần mềm quảng cáo bất hợp pháp. Tiếp đến bạn cũng phải đồng ý cho phần mềm Hyperlinker hoặc SaveNow được cài đặt. Với Hyperlinker (**Hình 4**) bạn nhận được con trojan Downloader Small BKE (**Hình 5**) và có thể cả adware Link Maker, còn adware SaveNow vẫn cho kết quả âm tính với BitDefender 9 Pro mặc dù đã bị phát hiện là tự ý chỉnh sửa registry để khởi chạy cùng Windows. Tuy vậy nó vẫn tỏ ra rất ranh ma khi đưa ra thông báo (**Hình 6**) khuyên bạn hãy chọn Allow (đồng ý) hoặc Ignore (bỏ qua) trước những cảnh báo của phần mềm tường lửa, diệt virus/spyware, và không ngại ngùng giải thích Ezthemes_WhenUSaveNow_Installer.exe đang cố gắng kết nối Internet một cách đúng đắn cho việc tải những thành phần cần thiết để hoàn tất quá trình cài đặt. Thật nực cười khi trước đó SaveNow còn tự quảng cáo rằng "sẽ giúp bạn so sánh giữa những quảng cáo và lời đề nghị đặc biệt, sự riêng tư của bạn sẽ được bảo vệ một cách nghiêm túc" (**Hình 7**). Thực ra bạn sẽ bị theo dõi vì chúng luôn chạy nền với danh nghĩa là phần mềm hữu ích. Cuối cùng "nhẹ nhàng" nhất là EZ shopper (**Hình 8**) có tác dụng làm giả shortcut của Internet Explorer trong menu Start và desktop (**Hình 9**) hay My.Freeze.com (**Hình 10**) làm thay đổi website mặc định của trình duyệt web... Thậm chí những công cụ diệt virus/spyware mạnh nhất hiện nay cũng không nhận ra mối hiểm họa khi nó vẫn còn nằm trong tệp tin cài đặt (**Hình 11**). Một lời khuyên thường được nêu ra mỗi khi bạn cài đặt bất kỳ phần mềm nào là "hãy tắt tất cả các ứng dụng nặng", trong đó tất nhiên phải kể đến chế độ tự động bảo vệ vốn bị coi là nguyên nhân làm chậm máy, thế nên người ta thường chọn "disable" để quá trình hoạt động trơn tru hơn. Sau khi có tệp tin nén bạn sẽ nhận được một lời mời khác (**Hình 12**) cùng yêu cầu mặc định là khởi động lại máy (**Hình 13**). Thực hiện thành công kết nối Internet, chỉnh sửa registry và chạy nền... thì việc cài đặt các tệp tin thực thi khác trở nên thật dễ dàng, các thành phần gây hại không được nhắc đến nữa, cũng dễ hiểu vì bạn đã bị "dính" rồi.

Phát hiện âm mưu

Đây chính là một ví dụ về sự "phá cách" của những chương trình gây hại, thay vì

bí mật, lén lút theo dõi, phá hoại, chúng lại trình bày tất cả trước mắt bạn sự hữu dụng, vẻ đẹp đồng thời gắn tên tuổi của mình với những phần mềm nổi tiếng, mượn danh một công ty trong sạch khác để chiếm được lòng tin của người sử dụng. Khi đã có được những thứ mình muốn bạn sẽ chẳng buồn để ý tới chúng nữa. Tuy nhiên đó là một lý do, mục đích chính của những website phát tán adware chính là kiếm tiền, nhưng họ chỉ nhận được thù lao từ các công ty quảng cáo khi bạn biết và đồng ý cho các chương trình được cài đặt (bạn được khuyên hãy đọc thật cẩn thận nhưng dĩ nhiên chẳng có một từ adware nào được nhắc tới, chỉ toàn những lời đường mật). Tại sao họ phải mất công như vậy? Đơn giản là để bạn không thể kiện những công ty trên khi biết mình đã bị lừa một cách trắng trợn, tuy nhiên việc phát tán trojan thì lại khác, quan trọng phải có người dám tố cáo hành động xấu.

Trong khi chờ đợi những người dũng cảm xuất hiện, bạn có thể tự mình vạch mặt những kẻ thù ranh ma này không? Tất nhiên là có, ngoài tính đa nghi bạn cần phải đặt câu hỏi cho những điểm bất hợp lý đang diễn ra trước mắt mình, phân tích thật kỹ để tìm ra một lời giải thích có lý.

Tất cả những thứ miễn phí được tung ra đều đem lại một lợi ích nào đó cho người tạo ra chúng, có thể là để quảng cáo cho phiên bản thương mại, thúc đẩy quá trình phát triển của những dịch vụ có phí liên quan hay với mục đích gây dựng, khuếch trương tên tuổi, thương hiệu... cuối cùng tệ hại nhất là phát tán các phần mềm gây hại, theo dõi, ăn cắp thông tin cá nhân... phục vụ cho việc buôn bán và quảng cáo bất hợp pháp. Bạn cần nhận ra lợi ích của họ để xem có hại gì cho mình hay không, nếu đôi bên cùng có lợi, dĩ nhiên chúng ta nên chấp thuận.

Trở lại với ThemeXP.org, nếu nói đây là một website thu lợi nhuận chính từ việc quảng cáo hợp pháp thì nó đã đi ngược với nguyên tắc chung của những website loại này. Thay vì cố kéo dài thời gian lướt web của khách bằng các liên kết chằng chịt hay bắt đăng ký để thu thập thông tin cho việc gởi thư tiếp thị, ThemeXP.org lại hào phóng để bạn lấy về thứ mình muốn một cách dễ dàng. Hơn nữa các banner không cố định mà thường thay đổi khi chuyển trang, cuối cùng đặc biệt nhất là một cảnh báo giả dạng hộp thoại của hệ thống có thể sẽ hiện ra khi bạn vừa mới mở trang web (**Hình 14**) hay mỗi lần liên kết bị "lag" (**Hình 15**), (thực ra đây chỉ là lag giả vì nếu đã lag thì sao lại có hình ảnh). Thế nên mặc dù mọi người có thể đóng

góp 10 USD một năm cho ban quản trị website nhưng bạn dễ nhận ra ThemeXP.org không bán sản phẩm và được hưởng nhiều lợi nhuận từ hoạt động quảng cáo hợp pháp, ngay cả StyleXP, một "bàn đạp" quan trọng, cũng chỉ được giới thiệu sơ qua bằng liên kết mà không có bất kỳ hình ảnh nào quảng bá cho phần mềm này. Cũng dễ hiểu vì ThemeXP.org không liên quan tới TGTSoft, một công ty phát triển và bán những phần mềm có phí, ThemeXP.org chỉ đứng ra với danh nghĩa một website miễn phí cung cấp thêm các "vật liệu" cho việc "make up" Windows XP. Về sự nổi tiếng thì ThemeXP.org có thừa, số lượt người xem và tải về dưới mỗi thumbnails mới cũng thường lên tới hàng chục ngàn, chỉ riêng địa chỉ website cũng đã đủ gây dựng lòng tin nơi người dùng. Chưa kể hàng loạt bài báo trong và ngoài nước hướng dẫn bạn đọc sử dụng website này mà không có sự kiểm tra chu đáo. Mặc dù ThemeXP.org có giới thiệu tác giả đã hào phóng c

ho phép họ đóng gói tệp tin để làm giảm hao phí, nên có lẽ họ không phải trả tiền bản quyền cho tác giả, nhưng để có thể duy trì sự hoạt động cũng như thường xuyên cập nhật những "vật liệu" mới thì nhất định họ phải được tài trợ từ một nguồn nào đó.

Làm thế nào?

Dẫu biết nguy hiểm nhưng nếu phải chia tay với những "bộ cánh" tuyệt đẹp chắc bạn không đành lòng, để ý một chút bạn dễ nhận ra người viết bài này cũng đang sử dụng giao diện từ ThemeXP.org. Sự thực chúng ta có thể dễ dàng "hút" những "giọt mật" hấp dẫn từ "cái bẫy" mà "bông hoa ăn thịt" ThemeXP.org đã giăng. Nhưng "cẩn tắc vô áy náy", hãy đọc bài "Vũ khí chống virus mới" (TGVT A 3/2006, tr.90) với hai ứng cử viên sáng giá là BitDefender 9 Standard giá 30 USD và McAfee VirusScan 2006 giá 40 USD. Đến đây sẽ có 2 trường hợp:

Nếu đây là lần đầu tiên bạn sử dụng ThemeXP.org thì việc cài đặt tại điểm truy cập Internet là một sự lựa chọn sáng suốt. Bạn không phải lo rằng sẽ tiếp tay cho kẻ xấu, chỉ cần khởi động máy là mọi thứ trở lại như cũ vì tất cả các máy tính công cộng đều được bảo vệ bởi một phần mềm "đóng băng" nào đó. Thế nên bạn chỉ được khởi động lại máy sau khi cài đặt xong tất cả, muốn vậy cần lưu ý tránh sử dụng nút Enter trên bàn phím vì tất cả các lựa chọn mặc định đều theo hướng có lợi cho các chương trình gây hại nhất là lựa chọn khởi động lại máy để hoàn tất quá trình cài đặt. Tiếp theo cần chép các tệp zip vào thiết bị lưu trữ để giải nén vào thư mục X:\WINDOWS\Resources\Themes (X là phân vùng mà hệ điều hành đang chạy) hay sử dụng với StyleXP 3.18, trên máy vi tính ở nhà. Qua thử nghiệm của người viết, các giao diện mà ThemeXP.org cung cấp không tương thích với hệ điều hành Windows Media Center 2005, để khắc phục vấn đề này bạn cần cài đặt StyleXP 3.18 hoặc phần mềm miễn phí Vista Inspirat 1.1. Với sự hướng dẫn của khá nhiều bài báo tiếng Việt về ThemeXP.org bạn sẽ không gặp khó khăn. Xin lưu ý trong những tệp tin thực thi từ những năm trước (bây giờ vẫn có thể tải chúng) đều có trojan Downloader Small BKE, bạn nên quét virus/trojan cho thiết bị lưu trữ của mình, còn tới thời điểm hiện nay sẽ luôn có các adware SaveNow và Newdotnet, tuy nhiên SaveNow đã lên "đời" mới có hình người màu xanh nhạt thay vì những đường tròn đồng tâm như phiên bản cũ (**Hình 16**), việc lây nhiễm cả hai bản cùng lúc vẫn thường xảy ra.

Bạn đã dùng ThemeXP.org từ lâu và đang sử dụng máy tính có kết nối Internet, hãy cẩn thận! Nếu không được bảo vệ, thông tin riêng tư của bạn và người thân đã và đang bị xâm phạm. Việc cần làm là sử dụng những công cụ chống virus mạnh thường kiêm luôn tính năng antispyware để quét thật kỹ thư mục Program Files (và

tất cả các dữ liệu), đồng thời lập tường lửa hay tạm ngắt kết nối Internet tránh để chúng gọi "quân tiếp viện" đến hỗ trợ. Không nên sử dụng các tệp tin gỡ bỏ cài đặt được cung cấp sẵn, nó có thể làm mọi thứ trở nên trầm trọng hơn. Ví dụ, tệp uninst.exe được hướng dẫn là để gỡ Hyperlinker lại chính là adware Link Maker (**Hình 17**). Qua thử nghiệm, tuy BitDefender 9 tự động nhận diện và tiêu diệt các adware, trojan ngay lập tức nhưng adware SaveNow chỉ bị phát hiện đã chỉnh registry (**Hình 18**) mà vẫn "bình an vô sự" chạy nền (**Hình 19**), đôi khi trojan Downloader Small BKE chưa được tự động diệt nên bạn phải tự quét (**Hình 20**). McAfee VirusScan 2006 không nhanh bằng BitDefender 9 Standard, sau vài phút mới tự nhận ra adware Newdotnet (**Hình 21**) nhưng lại tóm được cả SaveNow. Sau khi quét và sao chép các tệp tin nén, trong Program Files bạn cần xóa các thư mục sau nếu có: Hyperlinker, e-zshopper, Ezthemes_WhenUSaveNow_Installer, Save, VVSN, themexp... Cuối cùng đặt lại địa chỉ mặc định của trình duyệt web, xóa hai shortcut làm giả Internet Explorer và hai shortcut có biểu tượng e-zshopper màu xanh lá trong Start menu, Desktop. Bạn nên tìm đọc bài "Internet Explorer luôn truy cập trang web lạ" (trang 154) và "Đĩa cứng bị chậm" (trang 148) trên TGVT A 4/2006. Khi muốn sử dụng thêm các tệp tin thực thi, hãy làm với máy công cộng như hướng dẫn trên, bạn không nên cài trực tiếp trên cỗ máy yêu quý của mình, việc gỡ bỏ đôi khi rất khó khăn, trong tương lai ThemeXP.org sẽ nhận thêm các "đơn đặt hàng" mới mạnh mẽ và nguy hiểm hơn.

Thế nên không gì có thể đảm bảo sự an toàn tuyệt đối khi bạn vẫn tiếp xúc với ThemeXP.org. Giải pháp an toàn là mua giao diện từ những hãng nổi tiếng như Stardock, TGTSoft... với giá khoảng 7,95 - 14,95 USD. Nếu thấy chưa vừa ý với số lượng theme ít ỏi (vỏn vẹn có 21 cái) mà TGTSoft cung cấp (**Hình 22**), bạn nên dành 19,95 USD cho phần mềm StyleBuilder 2.0 cũng của TGTSoft, nếu StyleXP 3.18 có tác dụng quản lý thì StyleBuilder 2.0 (**Hình 23**) lại chính là công cụ chuyên dùng cho việc tạo ra các giao diện. Bỏ ra một chút thời gian với nó bạn sẽ có những theme độc đáo, không bị "đụng hàng" và quan trọng hơn là do chính bạn làm ra nên chẳng có trở ngại nào cho việc chia sẻ, khoe chúng với người thân, bạn bè. Sẽ thật tự hào khi mọi người trầm trồ khen ngợi "đứa con tinh thần" của mình. Tuy nhiên đừng vội quay lưng với những sản phẩm miễn phí, chúng rất thích hợp nếu bạn đang "viêm màng túi" hay lo ngại về phương thức thanh toán qua mạng vẫn còn là việc khó thực hiện với nhiều người. Bạn nên "ghé mắt" qua Vista Inspirat 1.1 của CrystalXP và Stardock CursorXP Free (**Hình 24**), xin dám chắc CursorXP Free đẹp, sinh động hơn bất kỳ con trỏ nào mà ThemeXP.org cung cấp. Thậm chí bạn còn có thể tùy ý điều chỉnh việc đổ bóng cho con trỏ (**Hình 25**).

ThemeXP.org chỉ là một trong rất nhiều website phát tán các chương trình gây hại trên Internet, người viết bài chọn làm thí dụ vì nó khá nổi tiếng và ít bị mọi người

đề phòng trước vẻ ngoài lịch sự và thân thiện. Với những trang web dạy hack, cung cấp patch, keygen để bẻ khóa phần mềm hay chứa các nội dung đồi trụy, cờ bạc hoặc các chương trình "bẻ" sẵn chứa trong đĩa "lậu" được bán với giá rất rẻ so với giá trị thực mà nhà sản xuất đề ra đều có thể đem lại "điều chẳng lành", đặc biệt với những người ít kinh nghiệm. Việc bẻ khóa có thể làm mất đi tính ổn định của chương trình và loại đĩa CD rẻ tiền thường được dùng để ghi phần mềm "lậu" có tuổi thọ rất thấp, khó đọc so với đĩa gốc của phần mềm có bản quyền. Do cũng bắt nguồn từ Internet nên nguy cơ lây nhiễm từ những chiếc đĩa lậu này là khá cao. Thí dụ như những chiếc đĩa CD cài đặt trò chơi MU Offline luôn chứa trojan StartPage KR (**Hình 26**). Việc sử dụng phần mềm bị bẻ khóa chỉ mang lại cái lợi trước mắt, hậu quả mà nó gây ra không nhỏ chút nào cho chính người sử dụng, nhà sản xuất và xã hội. Cách giải quyết tốt nhất mà mọi người nên làm là mua và sử dụng phần mềm có bản quyền từ những công ty có uy tín, khi đó bạn sẽ không phải phấp phỏng lo sợ việc kiểm tra bản quyền, những kẻ thù giấu mặt trong các tệp tin cài đặt, hay gặp phiền phức khi PC biến thành "zombie" như trường hợp của bài "Máy tính bị oan?" (TGVT A tháng 4/2006, tr.12)... đồng thời nhận được nhiều chế độ hậu mãi từ phía nhà sản xuất cũng như sự giúp đỡ trực tiếp nếu có vấn đề nảy sinh (ví dụ điển hình là chương trình ưu đãi Windows Genuine Advantage của hãng Microsoft). Đó là một hành động đẹp, góp phần xây dựng nền công nghiệp phần mềm và uy tín của nước nhà trước bè bạn thế giới.

Tên phần mềm - Phiên bản	Địa chỉ tải về	Nhà sản xuất	Dung lượng tệp cài đặt (MB)	Giá (USD)
StyleBuilder 2.0 beta	http://download.tgtsoft.com/StyleBuilderInstall.zip	TGTSoft	2,68	19,95
StyleXP 3.18 Ladies	http://download.tgtsoft.com/StyleXPInstallFemale.zip	TGTSoft	22,4	19,95
StyleXP 3.18 Men	http://download.tgtsoft.com/StyleXPInstallMale.zip	TGTSoft	18,5	19,95

Style XP 64-bit Ladies (AMD64)	http://download.tgtsoft.com/StyleXPFemaleAmd64.zip	TGTSoft	19,3	19,95
Style XP 64-bit Mens (AMD64)	http://download.tgtsoft.com/StyleXPMaleAmd64.zip	TGTSoft	15,3	19,95
Vista Inspirat 1.1	http://www.crystalxp.net/dl/en.gal.130.htm http://download.softpedia.com/software/desktop/Pack_Vista_Inspirat_1.1.exe /Pack_Vista_Inspirat_1.1.exe	CrystalXP	27,1	miễn phí
Stardock Cursor XP Free	http://www.stardock.com/products/cursorxp/downloads.asp downloads.asp	Stardock	2,38	miễn phí

Nguyễn Tiến Dũng

Những vị trí ẩn núp của virus và trojan trong quá trình khởi động - 17/8/2006 8h:30

1. Thư mục START-UP:

Windows mở tất cả các chương trình từ thư mục Start Up trong Start Menu. Thư mục này rất dễ thấy trong phần Programs của Start Menu.

Chú ý là tôi không nói Windows "khởi chạy" mọi chương trình nằm trong thư mục Start Up. Tôi nói rằng nó "mở". Ở đây có sự khác biệt quan trọng.

Tất nhiên là các chương trình điển hình trong thư mục Start Up sẽ chạy. Nhưng bạn có thể có các shortcut của chúng trong Start Up dưới dạng tài liệu chứ không phải là chương trình.

Ví dụ nếu bạn đặt một tài liệu dạng Word trong thư mục Start Up, Word sẽ chạy và

tự động mở nó trong quá trình khởi động hệ thống. Nếu bạn đặt một file WAV, phần mềm nghe nhạc sẽ chạy bản nhạc đó khi máy khởi động. Và nếu bạn đặt một Web-page Favourites, Internet Explorer (hay một browser khác bạn chọn) IE sẽ chạy và mở trang Web cho bạn tương tự như trên. (Các ví dụ dẫn ra ở đây có thể đặt shortcut một cách dễ dàng như là một file WAV, một tài liệu Word, v.v…)

2. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "Run" của Windows Registry. Các thành phần trong "Run" (và trong các phần khác của Registry trong danh sách bên dưới) có thể là các chương trình hay các file mà máy tính mở như trong giải thích của phần 1 ở trên.

3. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "RunServices" của Registry.

4. REGISTRY: Windows thực hiện tất cả các lệnh trong phần "RunOne" của Registry.

5. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "RunServicesOne" của Registry. (Windows dùng hai khu vực "Runone" chỉ để chạy các chương trình thời gian đơn, thông thường trong phần khởi động hệ thống tiếp theo sau khi cài đặt một chương trình).

6. REGISTRY: Windows thực hiện các lệnh trong khu vực HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %* của Registry. Lệnh nhúng ở đây sẽ mở khi bất kỳ file chạy nào được thực thi.

Có thể có những file khác:

[HKEY_CLASSES_ROOT\exefile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\comfile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\batfile\shell\open\command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] ="\"%1\" %*"
[HKEY_CLASSES_ROOT\piffile\shell\open\command] ="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] ="\"%1\"

%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command]
="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]
="\"%1\"

%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command]
="\"%1\"
%*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command]
="\"%1\"
%*"

Nếu các khoá không có giá trị **"\"%1\" %*"** như trên và bị thay đổi một số thứ kiểu như **"\"somefilename.exe %1\" %*"** thì chúng sẽ tự động gọi một file đặc tả.

7. File BATCH: Windows thực hiện tất cả các lệnh trong các file Winstart BAT đặt trong thư mục Windows. (Hầu hết những người sử dụng và phần lớn những người thành thạo Windown đều không biết đến file này. Nó có thể không tồn tại trong hệ thống của bạn, nhưng bạn có thể tạo ra nó một cách dễ dàng. Chú ý rằng một số phiên bản của Windows gọi thư mục Windows là "WinNT"). Tên file đầy đủ là: ***WINSTAR.BAT***.

8. File INITIALIZATION: Windows thực hiện các lệnh tại dòng "RUN=" trong file WIN.INI đặt ở thư mục Windows (hay WinNT).

9. File INITIALIZATION: Windows thực hiện các lệnh tại dòng "LOAD=" trong file WIN.INI đặt ở thư mục Windows (hay WinNT).

Nó cũng chạy các lệnh tại "*shell=*" trong ***System.ini*** hoặc ***c:\windows\system.ini***.

[boot]
shell=explorer.exe C:\windows\filename

Tên file theo kiểu ***explorer.exe*** sẽ bắt đầu bất cứ khi nào Windows khởi động.

Với Win.ini, các tên file có thể được dành cho một không gian đáng kể, mỗi tên lưu trữ trên một dòng. Nó làm giảm khả năng các tên file có thể bị tìm thấy. Thông thường đường dẫn đầy đủ của file nằm trong mục nhập vào này, nếu không hãy kiểm tra lại trong thư mục Windows.

10. RELAUCHING: Windows khởi chạy lại các chương trình đang sử dụng khi hệ thống Shutdown. Windows không thể làm điều này với phần lớn các chương trình không phải của Microsoft. Nhưng nó thực hiện dễ dàng với Internet Explorer

và với Windows Explorer, chương trình quản lý file và folder xây dựng trong Windows. Nếu bạn đang mở Internet Explorer khi hệ điều hành tắt, Windows sẽ mở lại đúng trang đó sau khi bạn khởi động lại hệ thống. (Nếu điều này không xảy ra trong máy tính của bạn, một người nào đó đã tắt tính năng này. Dùng *Tweak UI,* chương trình quản lý giao diện người dùng miễn phí của Microsoft Windows để tái kích hoạt thiết lập "*Remember Explorer settings*" hay dưới tên gọi nào đó khác trong phiên bản Windows của bạn).

11. TASK SCHEDULER: Windows thực hiện các lệnh chạy tự động trong *Windows Task Scheduler* (hay bất kỳ bộ lập lịch nào khác bổ sung hay thay thế *Task Scheduler*). *Task Scheduler* là một bộ phận chính thức của tất cả các phiên bản Windows, ngoài trừ phiên bản đầu tiên của Windows 95. Nhưng nếu cài đặt thêm *Microsoft Plus Pack* thì Windows 95 cũng có *Task Scheduler*.

12. SECONDARY INSTRUCTIONS: Các chương trình Windows khởi chạy tại thời điểm khởi động có thể tự do khởi chạy các chương trình "con" bên trong nó. Về mặt kỹ thuật, đây không phải là các chương trình do Windows khởi chạy. Nhưng chúng thường không thể phân biệt được với các chương trình tự động chạy thông thường nếu chúng được khởi chạy ngay sau khi chương trình "cha" chạy

13. Phương pháp C:\EXPLORER.EXE

C:\EXPLORER.EXE

Windows tải chương trình *explorer.exe* (luôn đặt trong thư mục Windows) trong suốt tiến trình khởi động. Tuy nhiên, nếu *c:\explorer.exe* tồn tại nó sẽ được thực thi thay vì Windows *explorer.exe*. Nếu *c:\explorer.exe* bị ngắt, người dùng thực tế bị lock out khỏi hệ thống của họ sau khi chúng khởi động lại.

Nếu *c:\explorer.exe* là một trojan, nó sẽ được thực thi. Không giống như các phương thức tự động khởi động lại máy trong các virus khác, nó không cần bất kỳ file hay thanh ghi nào thay đổi. File này đơn giản chỉ phải đặt lại tên là: *c:\explorer.exe*.

14. Các phương thức Additional:

Các phương thức tự động khởi động lại máy Additional. Hai phương thức đầu tiên được dùng bởi Trojan SubSeven 2.2.

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed

Components
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\explorer\Usershell folders

Icq Inet
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
"Path"="test.exe"
"Startup"="c:\\test"
"Parameters"=""
"Enable"="Yes"

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]
This key specifies that all applications will be executed if ICQNET Detects an Internet Connection.

[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap] ="Scrap object"
"NeverShowExt"=""

Khoá này thay đổi đuôi mở rộng file của bạn.

T.Thu - Quản Trị Mạng

Xử lý những sự cố máy tính xấu nhất

Thực hiện: Đông Quân

Máy tính không khởi động? Quên mật khẩu đăng nhập Windows? Ổ cứng hỏng, dữ liệu cá nhân biến mất, mất kết nối mạng... hoặc bạn vừa gửi nhầm thư "ca cẩm" đến địa chỉ email của sếp? Tệ hơn nữa, bạn lại làm tình hình thêm nghiêm trọng khi cố gắng giải quyết một cách vội vàng. Bạn nên chuẩn bị tinh thần cho những tình huống này. Hãy đọc kỹ, giữ gìn cẩn thận "cẩm nang" này để khi xảy ra sự cố thì lấy ra và làm theo hướng dẫn. Những thủ thuật trong bài không giải quyết hết tất cả những trục trặc. Tuy nhiên, chúng sẽ giúp bạn vượt qua một số tình huống tồi tệ nhất trên máy tính bằng những thủ thuật "độc chiêu" bạn chưa từng nghĩ đến như cho ổ đĩa cứng vào tủ lạnh để cứu dữ liệu, làm khô điện thoại di động bằng lò vi sóng hoặc thiết lập thời gian chờ trước khi email tự động gửi đi để có thời gian

đọc lại nội dung email.

Máy tính không khởi động

Nguyên nhân có thể (NN). Do bất cứ thứ gì; lỗi của Windows, xung đột giữa các phần mềm, trình điều khiển (driver) thiết bị gây tranh chấp hoặc do phần cứng hỏng hóc.

Khắc phục (KP). Trong trường hợp này, bạn thử trổ tài thám tử Sherlock Holmes để xác định chính xác "thủ phạm". Hãy sử dụng phương pháp loại suy bằng cách thay thế từng phần cứng "khả nghi".

- Đầu tiên, bạn cần kiểm tra tất cả cáp (cáp nguồn, cáp dữ liệu và cả cáp gắn vào mạch điện tử) để chắc chắn mọi thứ đã gắn chặt và đúng cách.

- Kế tiếp, kiểm tra bộ nguồn. Lắng nghe tiếng quạt tản nhiệt hoạt động, tiếng đầu đọc ổ đĩa cứng di chuyển. Nếu không nghe tiếng động, có thể bộ nguồn gặp trục trặc, cần thay thế. Để chắc chắn hơn, hãy kiểm tra điện thế ra với một thiết bị kiểm tra chẳng hạn như ATX power supply tester (giá 10USD) (find.pcworld.com/57276).

Hình 1. Jumper xóa thiết lập CMOS thường nằm gần pin (nuôi) CMOS

- Nếu bộ nguồn vẫn hoạt động tốt nhưng màn hình không hiển thị, bạn thử mượn màn hình khác (tất nhiên phải còn hoạt động tốt) kiểm tra để loại trừ nguyên nhân màn hình. Nếu ổ đĩa cứng vẫn hoạt động bình thường, card màn hình là thủ phạm. Tháo card màn hình rời và sử dụng card đồ họa tích hợp (nếu bo mạch chủ có) để kiểm tra. Để thay card màn hình, tham khảo hướng dẫn tại find.pcworld.com/57260. Lưu ý khi mở thùng thùng máy, kiểm tra để chắc chắn quạt tản nhiệt phần cứng (CPU, card đồ họa...) vẫn hoạt động tốt, có thể nguyên nhân do các linh kiện bị "đốt" nóng.

- Trường hợp màn hình làm việc tốt nhưng BMC không nhận dạng được ổ đĩa cứng nên không hiển thị (hoặc có hiển thị nhưng PC bị treo ở quá trình khởi động). Hãy thử thiết lập lại trạng thái ban đầu cho CMOS. Tắt máy, rút cáp nguồn, đeo vòng khử tĩnh điện (có thể chạm vào thùng máy để cân bằng tĩnh điện trong người)

trước khi tháo pin CMOS. Đợi khoảng 5 phút, gắn pin vào và khởi động lại, xem kết quả. Nếu máy tính vẫn không nhận được ổ cứng, có thể nó đã hỏng. Tham khảo cách xử lý trong phần "Ổ cứng hỏng" bên dưới. Lưu ý: Bạn phải thiết lập lại các thông số trong BIOS Setup sau khi tháo pin. Xem tài liệu đi kèm với mainboard để biết vị trí jumper, pin CMOS và cách thiết lập lại các thông số.

- Nếu máy tính vẫn không hoạt động, có thể RAM là thủ phạm. Lần lượt gắn từng thanh RAM ở các vị trí khác nhau để kiểm tra. Sử dụng máy tính khác để kiểm tra RAM bằng một trong những tiện ích như Memtest86+, DocMemory, GoldMemory... có trong đĩa Hiren's BootCD.

- Nếu các bước trên không thành công, nguyên nhân có thể do BMC hoặc CPU hỏng, cần phải thay mới.

Ghi chú: Nếu không có kinh nghiệm về phần cứng, bạn nên đem đến dịch vụ sửa chữa có uy tín kiểm tra; nhất là với MTXT.

Nếu các phần cứng vượt qua "kỳ kiểm tra", chúng ta sẽ tiếp tục với các nguyên nhân có liên quan đến phần mềm, chẳng hạn như Windows không thể khởi động hoặc hệ thống treo khi HĐH đang khởi động. Lưu ý: cẩn tắc vô áy náy, với những dữ liệu cá nhân bạn nên gắn ổ đĩa cứng sang máy tính khác và sao lưu chúng trước khi tiếp tục kiểm tra.

- Khởi động Safe Mode. Nhấn F8 để vào giao diện tùy chọn khởi động của Windows, chọn Safe Mode. Thông thường, Windows sẽ tự sửa chữa một số lỗi khởi động ở Safe Mode. Nếu sử dụng Windows Vista, bạn chọn mục "Repair Your Computer". Nếu máy tính không có tùy chọn này, hãy khởi động bằng đĩa cài đặt Vista và chọn "Startup Repair".

- Nếu chưa khắc phục được, hãy thử chọn "Last Known Good Configuration". Tùy chọn này rất hữu ích nếu bạn thường xuyên thay đổi phần cứng và cập nhật trình điều khiển (driver). Nếu khởi động thành công, tiến hành gỡ bỏ phần cứng mới (có thể do không tương thích) và khôi phục driver cũ trong Device Manager bằng cách: nhấn phải chuột trên My Computer (hoặc Computer trong Vista), chọn Properties để vào System Properties. Trong tab Hardware, chọn mục Device

Manager. Nhấn phải chuột trên phần cứng mới, chọn Properties. Chọn mục Roll Back Driver trong tab Driver để khôi phục.

- Nếu Windows chỉ khởi động ở Safe Mode (không khởi động ở chế độ thường – Normal Mode), thử sử dụng tiện ích System Restore của Windows (Start. Programs. Accessories. System Tools) hoặc trong Vista, chọn Start, gõ từ khóa system trong mục Run. Chọn System Restore liệt kê trong danh sách Programs để phục hồi hệ thống trở lại thời điểm nó làm việc tốt. Bạn cũng nên chạy phần mềm chống virus, spyware trong Safe Mode để kiểm tra.

- Nếu Windows vẫn không thể khởi động, bạn thử khởi động máy bằng đĩa cứu hộ khẩn cấp như Knoppix (find.pcworld.com/57261) hoặc Active Boot Disk (find.pcworld.com/57262) và sao lưu dữ liệu cá nhân sang thiết bị lưu trữ khác trước khi cài lại Windows (trong bước tiếp theo).

- Nếu PC vẫn làm không làm việc tốt, cài lại Windows là giải pháp tốt nhất. Tham khảo hướng dẫn tại find.pcworld.com/57277 hoặc find.pcworld.com/57278 nếu sử dụng Vista.

Phòng tránh (PT). Máy tính có thể "đột tử" bất cứ lúc nào, vì vậy bạn nên kích hoạt System Restore, lưu trữ cẩn thận những đĩa CD dùng để cứu hộ, khôi phục hệ thống. Giữ lại đĩa cài đặt những phần mềm quan trọng, thường xuyên sao lưu và nếu được, nên "thủ sẵn" 1 ổ đĩa cứng, bộ nguồn dự phòng khi máy tính gặp sự cố. Sử dụng tiện ích tạo ảnh đĩa như Acronis True Image 10 (giá 50USD, www.acronis.com) hoặc Norton Ghost (giá 70USD, find.pcworld.com/57279) là giải pháp tốt để sao lưu, phục hồi hệ thống, dữ liệu của bạn một cách nhanh chóng.

BẠN VỪA GỬI EMAIL "CA CẨM" SẾP VÀ HỐI TIẾC VỀ ĐIỀU ĐÓ	
NN. Bạn thất vọng vì một số khoản phúc lợi bị cắt giảm. **KP.** Một số mail server hỗ trợ tính năng recall (hoặc replace) cho phép người dùng lấy lại email vừa gửi. Tuy nhiên, bạn chỉ sử dụng tính năng này nếu biết chắc nó được kích hoạt và người nhận chưa đọc email. Trên thực tế, khả năng recall email thành công không nhiều. Nếu mail server không hỗ trợ tính năng này, bạn nên đến phòng sếp, bày tỏ sự hối tiếc và sẵn sàng đón nhận cơn thịnh nộ. **PT.** Hãy nhớ rằng tự kềm chế là đức tính tốt. Hãy kiềm chế cảm xúc của bạn khi kiểm tra mail; nếu không, rất dễ để châm ngòi cho một cuộc chiến. Bạn cũng nên có thói quen xem lại nội dung email trước khi gửi. Và tất nhiên,	Thiết lập thời gian chờ cho bạn cơ hội sửa chữa sai lầm

giải pháp kỹ thuật sẽ giúp bạn tránh lâm vào hoàn cảnh này một lần nữa. Để thiết lập khoảng thời gian chờ trước khi email tự động gửi đi, trong MS.Outlook, chọn Tools. Options. tab Mail Setup, bỏ tùy chọn mục Send immediately when connected, chọn Send/Receive và thay đổi thời gian chờ trong mục

Schedule an automatic send/receive every, tốt nhất là 10 phút hoặc hơn. Bạn sẽ có thời gian xem lại nội dung email trước khi gửi.

Không thấy máy tính khác trên mạng

NN. Có thể do Windows hoặc thậm chí do phần cứng bị lỗi. Cách kiểm tra đơn giản nhất là thử truy cập Internet, nếu được, bạn có thể loại trừ nguyên nhân do phần cứng và driver.

KP. Nếu không thấy bất cứ máy tính nào trong mạng, hãy kiểm tra xem máy của bạn có cùng "nhóm" (workgroup) với các máy khác không. Lưu ý: khác với Windows XP, Vista có thay đổi tên workgroup mặc định. Trong Start. Run, gõ lệnh sysdm.cpl và nhấn Enter. Chọn Change trong tab Computer Name và xem tên workgroup.

Nếu các máy cùng workgroup, bước kế tiếp bạn kiểm tra khả năng trùng địa chỉ IP giữa 2 máy tính. Windows luôn hiển thị cảnh báo trong trường hợp này. Để khắc phục, thử khởi động lại máy tính hoặc router sẽ giải quyết được vấn đề. Tuy nhiên, nếu gán địa chỉ IP tĩnh, sử dụng lệnh "ipconfig" để kiểm tra xem IP có trùng với các IP được router gán tự động cho các máy tính khác trong mạng không. Trên từng máy tính, chọn Start.Run, gõ lệnh "cmd /k ipconfig" và nhấn Enter để xem địa chỉ IP đang sử dụng.

Nếu chưa khắc phục được, thử chạy tính năng Windows Update trên tất cả các máy tính (nhất là những máy cài đặt Windows XP). Để chắc ăn, bạn nên kiểm tra cáp mạng, kết nối WiFi (nếu có) cũng như máy tính cần truy cập có trên mạng không.

Cuối cùng, hãy chắc rằng máy in hoặc thư mục đã chia sẻ và cấp quyền truy cập.

Bạn cần sử dụng tài khoản thuộc nhóm quản trị (Administrators) để truy cập. Để chia sẻ thư mục, trong Windows Explorer, nhấn phải chuột trên thư mục cần chia sẻ, chọn Share. Với máy in, chọn Start.Printers and Faxes (hoặc Printers với Vista), nhấn phải chuột trên máy in, chọn Sharing. Lưu ý: Cách chia sẻ của Vista hơi khác với XP, kiểm tra thiết lập chia sẻ tập tin và máy in được kích hoạt trong Network and Sharing Center.

PT. Một khi những vấn đề trên được khắc phục, bạn sẽ không gặp lại chúng. Tuy nhiên, nếu chúng bất ngờ xuất hiện lại, hãy thử khởi động lại máy tính một vài lần sẽ khắc phục vấn đề.

Mất kết nối mạng

NN. Modem/router quá nóng, không thể truy cập các trang web.

KP. Hãy bắt đầu với những nguyên nhân nằm trong "tầm tay" của bạn. Modem/router lỗi thường xuyên làm mất kết nối mạng, trong trường hợp này, tắt nguồn, khởi động lại modem/router sau 30 giây có thể giải quyết vấn đề.

- Đầu tiên, thử truy cập Internet bằng máy tính khác để kiểm tra card mạng máy bạn có bị hỏng không. Nếu không thể truy cập, hãy kiểm tra mạng cục bộ; nếu mạng cục bộ bình thường, thủ phạm là router/modem. Thử khởi động lại hoặc thay mới (nếu việc khởi động lại không có tác dụng).

Hình 2. Chọn Repair để "làm mới" kết nối mạng

- Kế tiếp, kiểm tra cáp mạng và xem thông báo lỗi (bằng đèn hiển thị trạng thái) của modem/router DSL. Nếu gặp lỗi, hãy rút cáp mạng, tắt máy tính và khởi động lại.

- Vẫn không có tác dụng? Hãy thử "làm mới" kết nối mạng. Trong Win XP, chọn Start.Run, gõ lệnh "cmd" (với Vista, gõ "cmd" trong khung Search). Sau đó gõ lệnh "ipconfig /renew" trong cửa sổ cmd vừa xuất hiện. Ngoài ra, bạn có thể thực hiện tương tự bằng cách nhấn phải chuột trên biểu tượng kết nối ở khay hệ thống, chọn Repair. Tuy nhiên, thường thì lệnh "ipconfig /renew" tỏ ra hiệu quả hơn.

- Nếu đang kết nối bằng card mạng không dây (wireless card), hãy thử chuyển sang kết nối trực tiếp với router bằng cáp mạng (RJ45). Nếu sử dụng kết nối mạng

chung với truyền hình cáp, kiểm tra tín hiệu TV và chắc chắn rằng bạn đã thanh toán cước đầy đủ.

- Nếu các thao tác trên không có tác dụng. Hãy gọi nhà cung cấp dịch vụ (ISP) yêu cầu kiểm tra kết nối. Một số ISP có khả năng kiểm tra từ xa, chẳng hạn như gửi tín hiệu để thiết lập lại modem của bạn. Thông thường, những nguyên nhân "nằm ngoài ngôi nhà bạn" chỉ là tạm thời, tuy nhiên vấn đề sẽ được giải quyết nhanh hơn nếu bạn liên tục "nhắc khéo".

PT. Hãy dự phòng một vài thứ để dùng tạm khi mất kết nối mạng như wireless card (cùng chuẩn hoặc tương thích) với router WiFi/access point để dùng ké nhà hàng xóm hoặc sử dụng kết nối tạm bằng Internet card.

Máy ảnh, điện thoại, MTXT hoặc bàn phím bị "nhúng" nước.

NN. Bạn không thể phàn nàn Microsoft trong trường hợp này.

KP. Cần lưu ý mạch điện tử và nước "kị rơ" nhau, tuy nhiên đây không phải là chuyện to tát nếu bạn sơ ý để chúng dính một ít nước. Trên thực tế, tỷ lệ các đồ dùng/vật dụng có thể khôi phục hoàn toàn không nhiều, tuy nhiên nếu thao tác cẩn thận, bạn vẫn có thể sửa chữa lỗi lầm của mình.

- Trước hết, nhanh chóng tắt thiết bị (nếu nó vẫn còn hoạt động), tháo pin, đĩa CD, thẻ nhớ, thẻ SIM. Nếu là MTXT, tháo các thiết bị gắn ngoài như PC card, ổ quang và lau sạch chất lỏng bằng khăn khô. Kiểm tra và nhanh chóng "rã" thiết bị nếu bạn vẫn nghe tiếng chất lỏng ở bên trong; điều này là rất cần thiết để làm khô thiết bị (cả bên trong lẫn bên ngoài) càng nhanh càng tốt.

Các hướng dẫn tiếp theo sẽ giúp bạn làm khô thiết bị. Hãy chọn cách nào thuận tiện và phù hợp. Cần lưu ý rằng những phương thức dưới đây có thể làm thiết bị "đi tong" hơn là cứu vãn; tuy nhiên may mắn vẫn có thể xảy ra.

- Hãy thử với những chất hút ẩm. Đặt thiết bị vào túi kín với một ít gói bột hút ẩm bên trong. Lưu ý: nên sử dụng những gói hút ẩm mới; những gói cũ ít hiệu quả hơn. Cách thức này cũng có thể áp dụng với gạo hoặc muối ăn và tránh đừng làm

rơi những hạt gạo hoặc muối vào trong thiết bị. Tốt nhất là bọc chúng trong những khăn giấy.

- Hơi nóng có thể làm chất lỏng bốc hơi. Đặt thiết bị trên thanh chắn bùn xe hơi vào buổi chiều trong khoảng 1 tiếng. Can đảm hơn nữa, bạn thử đặt thiết bị vào lò nướng trong 1 giờ hoặc để điện thoại trong túi quần cả ngày cũng đủ làm nóng thiết bị; giống như dùng máy sấy tóc vậy (lưu ý không dùng chế độ mạnh hoặc quá nóng sẽ nướng chín thiết bị). Ghi chú: bạn phải chắc chắn pin đã được tháo khỏi thiết bị nếu thử một trong những cách trên.

- Sử dụng cồn để hút nước. Nếu cảm thấy "run tay", bạn không nên dùng cách này. Nhúng toàn bộ thiết bị vào một chậu chứa đầy cồn (loại cồn nguyên chất 99%, không dùng loại thấp hơn). Cách này sẽ làm nước bốc hơi hết trong thiết bị. Hãy làm điều này thật nhanh vì cồn có thể phá hỏng một số phần được làm bằng nhựa.

- Nếu là bàn phím máy tính, úp ngược thiết bị xuống để nước có thể chảy ra ngoài.

- Nếu làm đổ những chất có đường như nước Soda vào MTXT, điện thoại di động, bạn phải lau thật sạch những chất này. Mở phần thiết bị ra và lau sạch chúng với cồn 99%, nếu không thiết bị sẽ bị chập mạch vì những chất dính này.

PT. Nên cẩn thận khi vừa làm việc vừa nhấm nháp trà, café. Sử dụng thiết bị không thấm nước như bàn phím có lớp nhựa phủ bên ngoài. Sử dụng vỏ bọc chống thấm cho máy ảnh khi dạo chơi trên biển, đặt điện thoại di động, máy nghe nhạc trong túi nhựa sẽ giúp bạn thoát khỏi những rắc rối sau này.

Bạn nhận được đơn kiện của RIAA/MPAA

NN. Chúng ta sẽ không đi sâu vào tìm hiểu nguyên nhân. Bạn có thể tham khảo thông tin liên quan trong bài Hollywood chống PC (ID: A0211_18, A0603_20).

KP. Bạn có thể phi tang vật chứng như vứt máy tính xuống hồ nước, định dạng ổ đĩa cứng nhiều lần hoặc nghiền nát cái iPod đáng ghét... tuy nhiên, đây không phải là hành động thích hợp ở thời điểm này, hãy gọi điện cho luật sư của mình hoặc tìm "đồng minh" tại Directory of Lawyers Defending Against RIAA Lawsuits

(find.pcworld.com/57266).

PT. Kiểm tra và thiết lập bảo mật kết nối mạng không dây. Không chia sẻ các thư mục phim ảnh trên máy tính và gỡ bỏ các ứng dụng chia sẻ tập tin mạng ngang hàng không tuân thủ với luật bản quyền.

Quên mật khẩu Windows

NN. Nên tham khảo ý kiến bác sỹ để chẩn đoán bệnh hay quên.

KP. Với mỗi phiên bản Windows, việc phục hồi mật khẩu khác nhau đôi chút và

phức tạp hơn do những cải tiến về bảo mật của Microsoft. Tuy nhiên, vẫn còn hy vọng cho bạn trước khi chọn giải pháp cài mới Windows.

- Nếu có đặt mật khẩu Windows, bạn thử đăng nhập với một tài khoản người dùng khác (cũng thuộc nhóm quản trị); có thể là một tài khoản được cài sẵn khi mua máy tính, thường thì tài khoản này không có mật khẩu. Với Windows XP, bạn thử đăng nhập với tài khoản là Administrator, mật khẩu để trống xem. Nếu được, xóa mật khẩu tài khoản kia. Trường hợp XP không hiển thị đầy đủ tài khoản người dùng, thử nhấn tổ hợp phím Ctrl + Alt + Del để quay lại màn hình đăng nhập của Windows NT.

- Nếu không có tài khoản khác trên máy tính, bạn phải dùng đến những công cụ có khả năng cài lại (hoặc xóa luôn) mật khẩu. Ophcrack là công cụ bạn nên dùng để phục hồi lại mật khẩu đã mất. Sử dụng máy tính khác tải về phần mềm miễn phí từ http://ophcrack.sourceforge.net và ghi nó lên đĩa CD khởi động được. Khởi động bằng đĩa này, tùy thuộc vào độ dài của mật khẩu, nó có thể phục hồi được toàn bộ mật khẩu các tài khoản trên máy tính chỉ trong ít phút hoặc lâu hơn.
- Bạn có thể dùng công cụ khác để xoá mật khẩu nếu việc phục hồi mật khẩu không hiệu quả. Cần lưu ý rằng khi sử dụng các công cụ này, nguy cơ mất hoặc hỏng dữ liệu có thể xảy ra (dù rất ít). Nếu quen làm việc với những dòng lệnh, 2 công cụ miễn phí Offline NT Password & Registry Editor (find.pcworld.com/57275) và Emergency Boot CD (ebcd.pcministry.com) khá thích hợp cho bạn.

PT. Bạn là người đãng trí, dễ quên thì hãy viết nó vào tờ giấy và cất kỹ vào ví, thậm chí cất trong két sắt (nếu cẩn thận) hoặc để ở nhà cho an toàn... Bất cứ cách nào miễn sao bạn không bị mất mật khẩu.

XÓA NHẦM MỘT TẬP TIN QUAN TRỌNG VÀ KHÔNG CÓ BẢN DỰ PHÒNG

NN. Bạn không tỉnh táo do thiếu ngủ.

KP. Chúng ta đều biết rằng khi Windows xóa một tập tin hay thư mục nào đó trong hệ thống, thực chất tập tin chỉ được đánh dấu "đã xóa" cho đến khi dữ liệu mới được ghi vào, lúc này dữ liệu cũ mới thực sự bị xóa đi và ghi đè bằng dữ liệu mới. Như vậy, bạn vẫn còn cơ hội phục hồi cả khi nó không còn trong Recycle Bin.

- Dừng ngay việc sử dụng máy tính. Đóng tất cả những ứng dụng đang mở và các dịch vụ lập chỉ mục theo thời gian thực (real-time indexing services) như X1, Google desktop hoặc Windows Index Service, vì chúng có thể ghi đè lên tập tin cần phục hồi.
- Sử dụng một trong những phần mềm phổ biến như QueTek's File Scavenger (giá 49USD, find.pcworld.com/57270) hoặc Diskeeper's Undelete (giá 30USD, find.pcworld.com/57271) để phục hồi dữ liệu.
- Nếu phần mềm phục hồi không có tác dụng, hãy nghĩ đến việc lấy lại bằng những cách khác. Bạn đã gửi tập tin này cho ai chưa? Kiểm tra mục Send Items hộp thư của bạn hoặc nhờ người nhận gửi lại cho bạn. Tập tin là hình ảnh hay đoạn phim?

Tính năng Shadow Copy hữu ích khi bạn xóa nhầm

Kiểm tra thẻ nhớ trong máy ảnh, máy quay hoặc bạn có đưa chúng lên Flickr, YouTube không? Rất nhiều tập tin vẫn còn hiện hữu trong các thư mục tạm nằm rải rác trong ổ đĩa cứng của bạn.

Nếu đang sử dụng Windows Vista, bạn có thể sử dụng tình năng Shadow Copy (mặc định được kích hoạt). Nhấn phải chuột trên thư mục chứa tập tin bị xóa, chọn Restore previous versions và chọn thời điểm phục hồi.

PT. Thường xuyên sao lưu dự phòng. Nếu là dữ liệu quan trọng, nên sao lưu theo thời gian thực. Ngoài ra, cài đặt một phần mềm khôi phục, chẳng hạn như Undelete để kiểm soát các tập tin cho đến khi chúng thực sự bị xóa.

Tràn ngập cửa sổ pop-up khi khởi động

NN. Máy tính bị nhiễm virus, spyware, adware.

KP. Đây chẳng phải là tin tốt lành nhưng trong hầu hết các trường hợp đều có thể khắc phục.

- Rút cáp mạng khỏi máy tính hoặc ngắt kết nối mạng không dây.

- Khởi động Safe Mode (nhấn F8 để vào giao diện tùy chọn khởi động của Windows, chọn Safe Mode).

- Chạy phần mềm phòng chống virus ở chế độ đầy đủ (full system scan). Sau đó lần lượt chạy 2 phần mềm chống spyware: Ad-aware (www.lavasofttusa.com) và Spybot (www.spybot.info). Khắc phục những lỗi do virus, spyware gây ra sau khi diệt. Gắn cáp mạng, khởi động lại máy, cập nhật danh sách virus, spyware mới và tiếp tục quét lần nữa. Ngoài ra, bạn có thể quét virus trực tuyến, chẳng hạn như dịch vụ của Symantec.

- Trường hợp máy tính nhiễm virus, spyware quá nặng, khả năng làm sạch và khôi phục hoàn toàn hệ thống là không thể do một số spyware có khả năng ngăn chặn chương trình diệt virus hoạt động cả trong Safe Mode. Bước tiếp theo, sử dụng HijackThis (find.pcworld.com/57267), một tiện ích khá mạnh có khả năng xác định chính xác các ứng dụng đang kiểm soát máy tính của bạn. HijackThis sẽ tạo một tập tin nhật kí hoạt động (log file), hãy cung cấp tập tin này khi tìm kiếm sự giúp đỡ trên các diễn đàn (find.pcworld.com/57268), bạn sẽ nhận được những lời khuyên hữu ích. Nếu đang vội, bạn thử tham khảo bảng mô tả tại find.pcworld.com/57267. Trang web này có những phân tích tự động log file của bạn và cung cấp một số công cụ cần thiết. Tuy nhiên, bạn vẫn cần sự giúp đỡ của người có kinh nghiệm để lựa chọn công cụ phù hợp.

Nếu tất cả những bước trên không thành công, thử sử dụng System Restore để khôi phục hệ thống. Nếu không hiệu quả, giải pháp cuối cùng là cài lại Windows. Ghi chú: kết quả thường là thành công nếu kiên nhẫn thực hiện từng bước theo hướng dẫn, bạn sẽ không cần đến giải pháp cuối cùng.

PT. Không mở những tập tin đáng ngờ đính kèm trong email, các cửa sổ pop-up hoặc đường link đến những website không rõ nội dung. Nâng mức bảo mật của trình duyệt web (trong Tools. Internet Options. Security) hoặc sử dụng các trình duyệt khác an toàn hơn. Luôn cập nhật phần mềm diệt virus và spyware. Bật tính

năng System Restore. Giải quyết dứt điểm ngay khi máy tính gặp sự cố (vì virus, spyware thường lây nhiễm rất nhanh) và giữ lại đĩa cài đặt các phần mềm phòng chống virus, spyware.

Hình 3. HijackThis cung cấp cho bạn báo cáo chi tiết về những gì đang chạy trên máy tính

Ổ cứng hỏng

NN. Ổ cứng bị rơi? Quá nóng? Hoặc không làm việc vì "quá già". Thực tế, ổ đĩa cứng là phần cứng máy tính dễ hỏng nhất.

KP. Cách giải quyết phụ thuộc vào từng tình huống cụ thể.

Hình 5. TackTech cung cấp nhiều công cụ hữu ích trong việc khắc phục lỗi ổ đĩa cứng

Nếu ổ đĩa cứng hoạt động thất thường, dữ liệu của bạn có thể bị sai lệch, không sử dụng được. Thử một trong những cách sau để cứu dữ liệu và sao chép sang ổ đĩa cứng khác trước khi nó ngưng hoạt động.

- Cáp IDE rất dở và dễ hỏng. Nếu sử dụng ổ đĩa cứng giao tiếp IDE, hãy bắt đầu bằng việc kiểm tra cáp đã được gắn chặt và đúng cách, thay mới nếu cần thiết.

- Thử khởi động bằng đĩa cứu hộ khẩn cấp Knoppix (xem phần Máy tính không khởi động) hoặc bằng ổ đĩa cứng khác và cố gắng sao chép dữ liệu sang ổ đĩa cứng này. Format ổ đĩa cứng bị lỗi xem có khắc phục được vấn đề không.

- Trường hợp ổ đĩa cứng bị lỗi sector, thử dùng tiện ích HDD Regenerator (ww.dposoft.net) kiểm tra và xác định sector bị lỗi. Tải về bản dùng thử và ghi vào đĩa CD khởi động. Nếu phát hiện sector lỗi, bạn phải trả 60USD cho phiên bản đầy đủ để phục hồi sector lỗi và khôi phục hoạt động ổ đĩa cứng.

- Trang web TackTech (find.pcworld.com/57272) cung cấp khá đầy đủ những công cụ miễn phí hữu ích trong việc chẩn đoán và khắc phục lỗi ổ đĩa cứng. Bạn chỉ việc tìm và tải về công cụ phù hợp với nhà sản xuất ổ đĩa cứng đang sử dụng (Conner, Fujistu, Hitachi, IBM, Maxtor, Quantum, Samsung, Seagate, Toshiba, Western Digital)

- Nếu ổ đĩa vẫn không khởi động được, hãy sử dụng phần mềm phục hồi dữ liệu (giá dao động từ 40USD cho đến 200USD) để cố gắng lấy lại dữ liệu đã mất. QueTek's File Scavenger và Stellar Phoenix (find.pcworld.com/57273) là 2 tên tuổi đáng giá trong lĩnh vực này.

- Bạn sẽ làm gì với một ổ đĩa cứng không hoạt động? Hãy thử một số thủ thuật sau. Đây là những nỗ lực cuối cùng và khả năng thành công khá mỏng manh. Ghi chú: Nếu ổ đĩa cứng vẫn không hoạt động, không nên tiếp tục thử mà hãy đem đến dịch vụ cứu dữ liệu. Đừng cố gắng vỗ hoặc đập vào ổ đĩa, đừng tháo rời từng phần, mở ổ đĩa cứng ra. Cách này chẳng những không có tác dụng mà còn làm ổ đĩa cứng hỏng nặng hơn, khả năng mất dữ liệu cao hơn.

Hình 4. QueTek's File Scavenger có khả năng cứu dữ liệu từ ổ cứng hỏng

- Giữ chặt ổ đĩa và xoay tròn cánh tay thật nhanh, song song với hướng của những phiến đĩa (giống trò ném đĩa Frisbee). Lặp lại nhiều lần và tránh đừng để ổ đĩa cứng đập mạnh vào bất cứ vật gì. Hành động này sẽ giải quyết được vấn đề "stiction" (sự ma sát tĩnh điện), giúp ngăn các phiến đĩa cứng không quay tròn.

- Thử tăng điện áp cấp cho ổ đĩa cứng, "tuyệt chiêu" cuối này có thể giúp ổ đĩa cứng hoạt động lần cuối cùng.

- “Thủ thuật đông lạnh” có thể áp dụng trong trường hợp ổ đĩa cứng chỉ nghe “tíc tíc” chứ không nghe tiếng quay. Cho ổ đĩa cứng vào 1 túi đông bằng nhựa (nhớ gói nó trong khăn giấy để ngăn hơi ẩm cũng như tránh nước) và làm lạnh nó trong vài

giờ. Sau đó lấy ra, để nó tự rã lạnh bằng nhiệt độ trong phòng. Hiện vẫn chưa có thời gian đông lạnh ổ đĩa cứng hiệu quả nhất. Vì vậy, hãy bắt đầu với 1 giờ và thử lại cho đến tối đa là 24 giờ để xem ổ đĩa cứng có "chịu" quay lần cuối không.

Lưu ý: nếu bạn làm cho ổ đĩa cứng hỏng quay lần cuối thì cố gắng đừng để nó ngưng cho đến khi bạn đã sao lưu những dữ liệu quan trọng.

Nếu tất cả cách trên không hiệu quả và dữ liệu thực sự rất quan trọng với bạn. Tốt nhất nên gửi nó đến dịch vụ cứu dữ liệu như DriveSaver (http://www.drivesaver.com/).

Tất nhiên chi phí không hề rẻ tí nào nhưng thực sự điều kỳ diệu đã xảy ra khi những cách thức của khách hàng không mang lại hiệu quả.

PT. Thường xuyên sao lưu những dữ liệu quan trọng. Để an toàn hơn, có thể thiết lập RAID cho ổ đĩa cứng để giảm tối thiểu rủi ro mất dữ liệu, tiết kiệm thời gian. Giải pháp rẻ tiền hơn là sử dụng phần mềm có khả năng cảnh báo những tai họa ổ đĩa cứng sắp xảy đến như HDD Health (www.panterasoft.com), SMART (công nghệ tự theo dõi, chuẩn đoán và báo cáo lỗi ổ đĩa cứng).

TÀI LIỆU TRÌNH BÀY BỊ LỖI KHI ĐANG THUYẾT MINH

NN. Tập tin lỗi, router mất nguồn, không tương thích khi trình diễn trên máy tính người khác, thực sự không phải là vấn đề nghiêm trọng. Bạn cũng không có thời gian để tìm hiểu nguyên nhân tại sao.
KP. Nếu can đảm, bạn có thể tiếp tục thuyết trình với tài ăn nói và sự khéo léo mà không cần tài liệu minh họa.
Nếu vẫn cần những tài liệu minh họa nhưng việc khởi động lại máy tính không giúp được bạn, thử sử dụng OpenOffice.org (www.openoffice.org). Với một chút khéo léo để "câu giờ", bạn có thể tải về và cài đặt mất khoảng từ 10 – 15 phút và tiếp tục phần thuyết trình.
Cách giải quyết tốt hơn trong trường hợp này là sử dụng bộ OpenOffice.org portable (find.pcworld.com/57274). Bạn có thể trực tiếp khởi chạy chúng mà không cần cài đặt. Hãy giữ sao lưu 1 bản trên thiết bị lưu trữ di động USB sẽ giúp bạn thuyết trình bất cứ lúc nào, trên mọi máy tính.
PT. Luôn sẵn sàng. In ra giấy tất cả các tài liệu minh họa để phát cho mọi người khi tài liệu trình bày bị lỗi. Sao chép bộ OpenOffice.org portable vào thiết bị lưu trữ di động USB.

Đông Quân
PC World Mỹ 07/2007

Kinh nghiệm xử lý lỗi khó xác định nguyên nhân

MÁY TÍNH TỰ KHỞI ĐỘNG LẠI

Hiện tượng máy tính tự khởi động lại mà không có thông báo lỗi là vấn đề "đau đầu" của nhiều bạn đọc. Cùng một hiện tượng nhưng do nhiều nguyên nhân khác nhau: có thể do lỗi của Windows, xung đột giữa các phần mềm, trình điều khiển thiết bị phần cứng gây tranh chấp hoặc phần cứng kém chất lượng, không ổn định. Hiện tượng này xảy ra bất kể là máy mới mua, mới ráp hoặc máy cũ, đang sử dụng, chỉ xảy ra thỉnh thoảng hay xảy ra liên tục. Tự khởi động lại khi máy đang shutdown hay bất kể lúc nào. Lúc khởi động hoặc khi chạy những ứng dụng chiếm nhiều tài nguyên hệ thống...

Vì chúng xảy ra không theo một quy luật nào cả, để xác định nguyên nhân chính xác đòi hỏi bạn phải có phần cứng thay thế, thời gian và tính kiên nhẫn. Trong trường hợp này, chúng tôi thường sử dụng phép thử đúng sai để loại suy dần các nguyên nhân có thể gây ra hiện tượng máy tính tự khởi động lại.

Kiểm tra phần mềm

Tiến hành kiểm tra phần mềm nếu hiện tượng này xảy ra sau khi bạn chỉnh sửa hệ thống, cài đặt hoặc gỡ bỏ ứng dụng, phần mềm... (Lưu ý những thao tác có ảnh hưởng đến hệ thống). Với Windows 2000/XP, đăng nhập với quyền Administrator, vào Control Pannel\Administrative Tools\Event Viewew để xem thông báo lỗi. Đây là một trong những nơi cần tham khảo, tìm hiểu nguyên nhân để biết cách khắc phục.

Trong trường hợp cần thiết, tải về từ website của nhà sản xuất và cập nhật các trình điều khiển thiết bị phần cứng như chipset, card đồ họa, card âm thanh, card mạng... Bạn nên chọn những driver tương thích với phiên bản hệ điều hành đang sử dụng. Tham khảo thêm thông tin tại www.microsoft.com/whdc/whql/default.mspx.

Thiết lập mặc định Windows NT/2000/XP sẽ tự khởi động lại máy khi gặp lỗi liên quan đến hệ thống (kể cả trong quá trình shutdown). Giải pháp tạm thời là tắt tính năng này, thực hiện như sau:

+ Nhấn phải chuột trên My Computer, chọn Properties để vào System Properties.

+ Chọn Tab Advanced, trong mục Start and Recovery, chọn Settings.

+ Bỏ dấu tùy chọn mục "Automatically Restart".

+ Nhấn OK để xác nhận thay đổi và khởi động lại.

Việc bỏ tùy chọn Automatically Restart sẽ làm hệ thống bị treo hoặc hiển thị "màn hình xanh chết chóc" khi gặp lỗi (hình 1). Điều này sẽ giúp bạn dễ xác định được nguyên nhân gây lỗi hơn. Để khắc phục, hãy cài lại Windows với tùy chọn R (Repair) để Windows tự sửa lỗi. Nếu không thể khắc phục bằng việc cài lại, bạn nên format phân vùng đĩa cứng và cài mới Windows. Tham khảo thêm thông tin về cách cài đặt trong mục Làm mới Windows, bài viết "Trẻ hóa Windows" (ID:A0305_103).

Kiểm tra phần cứng

Hinh 1

Chúng ta không thể (hoặc không dám) can thiệp sâu vào phần cứng, chỉnh sửa hoặc thay đổi như phần mềm. Vì vậy, "thay và thử" là giải pháp chúng tôi áp dụng nhằm xác định nguyên nhân. Trong trường hợp này, RAM và bộ nguồn (Power Supply Unit - PSU) là hai phần cứng bạn cần quan tâm đặc biệt.

Kinh nghiệm thực tế cho thấy, với hệ thống P3 (hoặc tương đương), RAM là phần cứng đầu tiên cần kiểm tra nhưng với các hệ thống P4 hiện nay, phần cứng đầu tiên cần kiểm tra là bộ nguồn.

RAM

Một số phần mềm (miễn phí hoặc có phí) sẽ giúp bạn kiểm tra RAM như Memtest86 (www.memtest86.com), Gold Memory (www.goldmemory.cz). Tuy nhiên, việc sử dụng phần mềm kiểm tra sẽ mất nhiều thời gian với những thanh RAM có dung lượng lớn (512MB hoặc 1GB). Vì vậy, "thay và thử" sẽ giúp bạn tránh khỏi cảnh "đợi chờ" nếu có sẵn RAM thay thế.

Bộ nguồn

Hình 2

Bộ nguồn là một thiết bị phần cứng quan trọng, cung cấp năng lượng hoạt động cho toàn hệ thống. Tuy nhiên, việc lựa chọn bộ nguồn đã không được người dùng quan tâm trong một thời gian dài. Với hàng loạt công nghệ mới chạy đôi hoặc "2 trong 1" như RAM dual channel, đĩa cứng RAID, đồ họa SLI/CrossFire, dual monitor, CPU dual core... Bộ nguồn càng trở nên quan trọng hơn bao giờ hết bởi nó quyết định sự ổn định của hệ thống, tuổi thọ của các thiết bị phần cứng khác. Gánh nặng này đã vượt quá khả năng "chịu đựng" của những bộ nguồn không tên tuổi trên thị trường, kể cả những bộ nguồn được dán nhãn 600 - 700W. Vì vậy, bạn đừng tiếc tiền khi đầu tư cho bộ nguồn của hệ thống vì chúng tránh cho bạn những sự cố đáng tiếc khi xảy ra quá tải. Tham khảo thêm thông tin liên quan việc lựa chọn bộ nguồn hợp lý trong bài "Giải bài toán nguồn điện (ID: A0505_131)" và bài "Bộ nguồn - Gánh PC tải nặng" (ID: A1205_56).

Lưu ý

- Trong quá trình kiểm tra, bạn phải lưu ý vấn đề tĩnh điện và tiếp đất của cơ thể để tránh gây hỏng hóc cho các thiết bị, linh kiện.

- Sao lưu những dữ liệu quan trọng để tránh mất mát khi kiểm tra.

- Việc kiểm tra phần cứng đòi hỏi phải có chuyên môn và kinh nghiệm, nếu có thể, bạn nên nhờ người có kinh nghiệm giúp đỡ.

- Điện áp trồi sụt cũng là nguyên nhân làm máy tính không ổn định. Điện áp quá cao hay quá thấp có thể làm hư hỏng thiết bị phần cứng. Nếu có thể, bạn nên trang bị ổn áp hoặc hoặc tốt hơn là UPS cho "cục cưng" của mình.

XP LUÔN KIỂM TRA ĐĨA CỨNG

Thật bực mình khi Windows XP luôn chạy checkdisk (tương tự scandisk của Win98) mỗi khi khởi động dù bạn đã tắt máy đúng cách. Nếu không muốn phiền phức, bạn có thể tắt tính năng này; tuy nhiên, bạn phải chắc rằng hệ thống vẫn hoạt

động tốt (trừ việc luôn chạy checkdisk). Trước khi sử dụng giải pháp này, chúng ta thử thực hiện một số thao tác sau.

- Trước hết, bạn hãy kiểm tra các ứng dụng tự động chạy trong Scheduled Tasks. Chọn Start.Programs.Accessories.System Tools.Scheduled Task để xem những chương trình nào đang sử dụng tính năng này. Xóa tất cả những thứ liên quan đến Chkdsk hoặc Autochk.

- Thực hiện việc kiểm tra đĩa cứng một lần nữa với tiện ích checkdisk để Windows tự kiểm tra và sửa lỗi. Thực hiện như sau: Trong Windows Explorer, nhấn phải chuột trên phân vùng cần kiểm tra, chọn Properties. Trong tab Tools, chọn Check Now trong mục Error Checking. Đánh dấu các tùy chọn trong Check Disk Options trước khi nhấn Start. Với phân vùng hệ thống (phân vùng cài đặt Windows), checkdisk chỉ kiểm tra trong lần khởi động kế tiếp (hình 2).

- Nếu checkdisk không thể hoàn tất quá trình kiểm tra (treo máy) hoặc không khắc phục được lỗi, hãy sử dụng tiện ích checkdisk (chkdsk.exe), fixmbr và fixboot của Recovery Console (bộ tiện ích có trong đĩa cài đặt Windows) để kiểm tra Master Boot Record (MBR) và các tập tin hệ thống. Tham khảo cách sử dụng Recovery Console trong bài "Recovery Console - DOS trong XP" (ID: A0203_71).

- Một trường hợp khác là cấu trúc logic của phân vùng đĩa cứng bị lỗi, bạn nên copy tất cả dữ liệu sang phân vùng khác, sau đó format phân vùng bị lỗi rồi chép dữ liệu trở lại.

- Kế đến, kiểm tra trường hợp lỗi của các phần mềm. Chọn Start.Run để mở cửa sổ DOS Prompt; gõ vào lệnh "msconfig" và nhấn OK để mở cửa sổ System Configuration Utility. Trong giao diện System Configuration Utility, chọn tab Startup và bỏ tất cả các tùy chọn được liệt kê trong Startup Item (tương ứng với các ứng dụng được nạp trong quá trình khởi động). Nhấn OK và chọn Restart để khởi động lại máy. Khi Windows khởi động lại, cửa sổ System Configuration Utility sẽ xuất hiện. Nếu không có bất kỳ trục trặc nào xảy ra, đánh dấu chọn Dont show this message or launch the System Configuration Utility và nhấn OK. Kiểm tra xem hiện tượng checkdisk còn xuất hiện không. Nếu không, mở cửa sổ System Configuration Utility, lần lượt đánh dấu chọn từng mục trong Startup Item và khởi

động lại để kiểm tra cho đến khi phát hiện được phần mềm gây lỗi. Gỡ bỏ chúng và cài đặt phiên bản mới hơn hoặc thay thế bằng phần mềm khác có tính năng tương đương.

TẮT TÍNH NĂNG SCANDISK/CHECKDISK

- Với Windows 98 và 98SE. Chọn Start.Run, gõ lệnh "msconfig" và nhấn OK. Trong cửa sổ System Configuration Utility, chọn mục Advanced trong tab General và đánh dấu chọn Disable ScanDisk after bad shutdown.
- Với Windows ME. Chọn Start.Run, gõ lệnh "regedit.exe" và nhấn OK để mở cửa

sổ Registry Editor. Tìm đến khóa DisableScandiskOnBoot theo đường dẫn HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro l\FileSystem, thay đổi Value data thành 01 (00 nếu muốn kích hoạt lại tính năng này). Khởi động lại máy tính để những thay đổi có hiệu lực.
Với Windows 2000/XP. Trong Registry Editor (regedit.exe), tìm đến nhánh HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro l\Session Manager\BootExecute, xóa dòng lệnh trong Value data. Khởi động lại máy tính để thay đổi có hiệu lực.
Lưu ý: Trước khi tiến hành chỉnh sửa Registry, bạn hãy thực hiện sao lưu Registry (tham khảo bài "Chăm sóc và bảo dưỡng Windows Registry", ID: A0205_90).

Ebook Sưu Tầm và Đóng gói bởi
Phạm Tiến Vượng
Email:phamtienvuong.tk@gmail.com
Ebook tập hợp những bài học dành cho những bạn theo học mạng Cisco

IP v6

Tác giả: Đặng Quang Minh

IPv6

Hai vấn đề lớn mà IP v.4 đang phải đối mặt là việc thiếu hụt các địa chỉ, đặc biệt là các không gian địa chỉ tầm trung (lớp B) và việc phát triển về kích thước rất nguy hiểm của các bảng định tuyến trong Internet.

Trong những năm 1990, CIDR được xây dựng dựa trên khái niệm mặt nạ địa chỉ (address mask). CIDR đã tạm thời khắc phục được những vấn đề nêu trên. Khía cạnh tổ chức mang tính thứ bậc của CIDR đã cải tiến khả năng mở rộng của IPv.4. Mặc dù có thêm nhiều công cụ khác ra đời như kỹ thuật subnetting (1985), kỹ thuật VLSM (1987) và CIDR (1993), các kỹ thuật trên đã không cứu vớt IP v.4 ra khỏi một vấn đề đơn giản: không có đủ địa chỉ cho các nhu cầu tương lai. Có khoảng 4 tỉ địa chỉ IPv.4 nhưng khoảng địa chỉ này là sẽ không đủ trong tương lai với những thiết bị kết nối vào Internet và các thiết bị ứng dụng trong gia đình có thể yêu cầu địa chỉ IP.

Một vài giải pháp tạm thời, chẳng hạn như dùng RFC1918 trong đó dùng

một phần không gian địa chỉ làm các địa chỉ dành riêng và NAT là một công cụ cho phép hàng ngàn hosts truy cập vào Internet chỉ với một vài IP hợp lệ. Tuy nhiên giải pháp mang tính dài hạn là việc đưa vào IPv.6 với cấu trúc địa chỉ 128-bit. Không gian địa chỉ rộng lớn của IPv.6 không chỉ cung cấp nhiều không gian địa chỉ hơn IPv.4 mà còn có những cải tiến về cấu trúc. Với 128 bits, sẽ có 340,282,366,920,938,463,463,374,607,431,768,211,456 địa chỉ.

Trong năm 1994, IETF đã đề xuất IPv.6 trong RFC 1752. IPv.6 khắc phục vào một số vấn đề như thiếu hụt địa chỉ, chất lượng dịch vụ, tự động cấu hình địa chỉ, vấn đề xác thực và bảo mật. Đối với một doanh nghiệp đã dùng hạ tầng mạng theo IPV4, để chuyển sang IPv6 không phải là việc dễ dàng. Một giao thức IP mới sẽ yêu cầu các phần mềm mới, các phần cứng mới và các phương pháp quản trị mới. Cũng có thể, IPv4 và IPv6 sẽ cùng tồn tại, ngay cả bên trong một Autonomous System trong khoảng thời gian sắp tới.

IP v.6 có các đặc điểm và lợi ích như sau:

- Không gian địa chỉ rộng lớn
- Địa chỉ unicast và địa chỉ multicast
- Tổng hợp địa chỉ (address aggregation)
- Tự động cấu hình
- Renumbering
- Cấu trúc header đơn giản, hiệu quả
- Bảo mật
- Cơ động
- Các tuỳ chọn để chuyển đổi từ IPv4 sang IPv6

Như được định nghĩa trong RFC1884 và RFC2373, các địa chỉ IPv6 là 128-bit dùng để nhận dạng cho các cổng của routers và tập các cổng của

routers. Có ba kiểu địa chỉ tồn tại:

- Unicast: là địa chỉ cho một giao tiếp. Một gói dữ liệu được gửi tới một địa chỉ Unicast sẽ được phân phối tới cổng giao tiếp được chỉ ra bởi địa chỉ đó.

- Anycast: là địa chỉ cho tập hợp các cổng giao tiếp. Các tập này thông thường thuộc về các node khác nhau. Một gói dữ liệu được gửi tới một địa chỉ anycast sẽ được phân phối đến cổng giao tiếp gần nhất hay đầu tiên trong nhóm anycast.

- Multicast: địa chỉ cho một tập hợp các cổng giao tiếp (thông thường thuộc về các node khác nhau). Khi một gói được gửi đến một địa chỉ multicast, tất cả các cổng giao tiếp sẽ nhận được gói dữ liệu này.

Để viết một địa chỉ dạng 128-bit ở dạng dễ đọc hơn, kiến trúc của IPv6 đã loại bỏ dạng cú pháp dấu chấm thập phân của IPv4 mà chỉ dùng dạng thập lục phân. Vì vậy, IPv6 có thể được viết bao gồm 32 ký tự dạng hex với dấu hai chấm ':' tách địa chỉ ra thành tám phần, mỗi phần có chiều dài 16-bit.

Theo các kế hoạch hiện tại, các node chạy IPv6 kết nối vào Internet sẽ dùng một kỹ thuật gọi là địa chỉ khả kết toàn cục (aggregatable global unicast address). Trong đó có nhiều điểm tương đồng với kỹ thuật summary như trong version 4. Địa chỉ tích hợp của IPv6 có ba mức:

- Mức public topology: là tập hợp các nhà cung cấp kết nối Internet.
- Mức vùng: mức này là cục bộ đối với các tổ chức.
- Mức cổng giao tiếp: mức này ảnh hưởng đến các cổng giao tiếp riêng lẽ. Link-local address là địa chỉ chỉ được sử dụng trên 1 kết nối (hay 1 cổng của router) và địa chỉ này phải duy nhất trong liên kết đó. Địa chỉ này có thể được sử dụng trong mạng cục bộ (các máy có chung địa chỉ mạng)và có thể không có router trong mạng này. Địa chỉ này có dạng :FE80::<MAC>. Subnet ID của lọai địa chỉ này được gán =0. Do đó lọai địa chỉ này không thể được sử dụng để giao tiếp ra khỏi subnet cục bộ được.

Dạng địa chỉ của IPv6

Địa chỉ IPv6 thì rất khác so với địa chỉ IPv4. Không chỉ khác nhau về kích thước (dài hơn gấp 4 lần) mà sự khác nhau còn trong dạng biểu hiện ở dạng thập lục phân so với dạng thập phân. Các dấu ':' sẽ tách các số dạng thập lục phân là các thành phần của địa chỉ 128-bit. Một ví dụ của địa chỉ Ipv6 là như sau:

4021:0000:240E:0000:0000:0AC0:3428:121C

Để tránh nhầm lẫn, lỗi và các trạng thái phức tạp không cần thiết, các luật sau sẽ được xác định:

- Các số dạng thập lục phân không phân biệt chữ thường và chữ hoa.
- Bất cứ một số 0 nào đứng trước các vùng 16 bit có thể được bỏ qua và được tượng trưng bằng dấu ':'. Một cặp dấu :: chỉ ra rằng các giá trị 16 bit của các số 0 đã được rút gọn. Quá trình nhận dạng số sẽ dễ dàng nhận ra số chữ số 0 đã bị thu gọn bằng cách thêm vào số chữ số 0 cho đến khi nào thu được một địa chỉ dài 128-bit
- Chỉ có một cặp các dấu ':' là cho phép tồn tại trong một địa chỉ bởi vì quá trình nhận dạng sẽ không thể chỉ ra có bao nhiêu số 0 trong mỗi vị trí.

Ví dụ địa chỉ **4021:0000:240E:0000:0000:0AC0:3428:121C** có thể được viết ở dạng **4021:0:240E::0AC0:3428:121C**

Mặc dù không thể có hai phiên bản của hai dấu '::', các vùng với nhiều chữ số 0 chỉ có thể được biểu diễn như 0. Trong ví dụ nêu trên, các chữ số 0 trong vùng thứ hai của địa chỉ được thu gọn lại thành một chữ số 0. Nếu một địa chỉ không có phần host, địa chỉ có thể kết thúc ở dạng '::'. Ví dụ 4021:0:240E::.

IPv6 có thể có nhiều dạng và nó có khả năng giải quyết các hạn chế của IPv4.

Cấu trúc ba mức này được thể hiện thông qua cấu trúc của địa chỉ tích hợp của IPv6, trong đó bao gồm các vùng sau:

Vùng tiền tố FP: 3 bit của FP sẽ được dùng để chỉ ra kiểu của địa chỉ (là unicast. Multicast…). Giá trị 001 chỉ ra đây là địa chỉ toàn cục

Vùng TLA ID (top level aggregation) được dùng để chỉ ra mức thẩm quyền cho địa chỉ này. Các Internet Router sẽ duy trì các bảng cần thiết cho tất cả các giá trị TLA. VớI 13-bit, vùng này có thể có đến 8,192 TLAs.

RES field (8 bits): kiến trúc của IPv6 định nghĩa vùng dành riêng sao cho các giá trị TLA hoặc NLA có thể mở rộng. Hiện tại, giá trị này bằng zero

NLA ID (24 bits): vùng này được dùng để chỉ ra ISP. Vùng này có thể được sắp xếp để phản ánh mối quan hệ giữa các ISP.

LSA ID (16 bits): được dùng bởi các tổ chức để tạo ra các kiến trúc địa chỉ bên trong của nó và để chỉ ra các mạng con.

Interface ID (64 bits): chỉ ra các cổng giao tiếp riêng lẽ trên một kết nối. Vùng này là tương tự như vùng host trên IPv4 nhưng nó được dẫn xuất từ dạng địa chỉ IEEE EUI-64 bit. Dạng địa chỉ này tương tự như địa chỉ MAC nhưng thêm vào một vùng 16 bit.

Thêm vào dạng địa chỉ tích hợp toàn cục nêu trên, IPv6 hỗ trợ các địa chỉ nội bộ, tương tự như các địa chỉ RFC1918. Nếu một node không được gán một địa chỉ toàn cục hay một địa chỉ cục bộ nêu trên, nó có thể được định vị bằng địa chỉ kết nối cục bộ, chỉ ra một phân đoạn mạng. Local–Use Unicast address: được gọi là địa chỉ đơn hướng dùng nội bộ, được dùng cho một tổ chức có mạng máy tính riêng (dùng nội bộ) chưa nối với mạng Internet tòan cầu hiện tại nhưng sẵn sàng nối được khi cần. Ngòai ra địa chỉ này còn được chia thành 2 loại là Link-Local (nhận dạng đường kết nối local) và Site local (nhận dạng trong phạm vi nội bộ có thể nhiều nhóm Node – Subnet). Link-local, sẽ được sử dụng ngay lần đầu khi thiết bị IPv6 bật lên. Do khả năng tự cấu hình của IPv6, nên khi thiết bị được bật lên, tự động một địa chỉ là link-local sẽ được gán. Chú ý là địa chỉ này không phải do ta gán mà do máy tự gán để giao tiếp trong nội bộ kết nối, nghĩa là với các host có chung địa chỉ subnet. Sau đó, khi thấy có router tồn tại trong mạng thì máy sẽ gửi các gói tin router solicitation và advertising để xin router 1 subnet ID để tạo site-local để sử dụng giao tiếp giữa các

subnet. Chú ý là 2 địa chỉ này không được định tuyến ra internet.

IPv6 Multicast Addresses

Một địa chỉ multicast là một địa chỉ xác định một nhóm các cổng của router, thông thường trên các hệ thống đầu cuối khác nhau. Các gói tin sẽ được phân phối đến tất cả các hệ thống được chỉ ra trong địa chỉ multicast. Sử dụng địa chỉ multicast thì hiệu quả hơn địa chỉ broadcast, trong đó yêu cầu tất cả các hệ thống đầu cuối phải ngừng tất cả các việc đang xử lý. Bởi vì một địa chỉ multicast là một địa chỉ của một nhóm các máy tính, nếu một máy tính không phải là thành viên của nhóm địa chỉ này, nó sẽ drop các gói ở layer 2. Tuy nhiên broadcast vẫn được xử lý trước khi các hệ thống xác định rằng dạng broadcast này là không liên quan đến nó. Các thiết bị lớp 2 thường lan truyền các broadcast bởi vì các địa chỉ broadcast không được lưu trữ trong bảng CAM. Không giống như router (hành động mặc định của router là drop các gói tin trong đó phần địa chỉ là không biết), switch sẽ phát tán tất cả các frame với phần địa chỉ là không xác định ra tất cả các cổng của switch. Về mặt lý thuyết, điều này cũng đúng với các địa chỉ multicast mặc dù một vài thiết bị có các cơ chế thông minh để giới hạn các dạng truyền multicast.

IPv6 không dùng cơ chế broadcast mà chỉ dựa vào địa chỉ multicast. Mặc dù IPv4 dùng địa chỉ multicast như định nghĩa RFC2356, nó sử dụng theo một cách khác. Các địa chỉ IPv6 có các dãy địa chỉ khác nhau. Tất cả các địa chỉ IPv6 bắt đầu với 8 bit đầu tiên gán bằng 1. Vì vậy tất cả các địa chỉ multicast sẽ bằng đầu với giá trị F. Dãy địa chỉ multicast là FF00::/8 - FFFF::/8

Giá trị octet thứ hai, theo sau octet đầu tiên, chỉ ra tầm vực và thời gian sống của địa chỉ multicast. Theo cách này, IPv6 có hàng triệu nhóm địa chỉ multicast.

Tóm tắt địa chỉ (Address Aggregation)

Quá trình tóm tắt các route, bất cứ khi nào có thể, là quan trọng trong Internet. Bảng định tuyến thì dễ quản lý hơn với cách hiện thực CIDR. Mặc dù tất cả các sơ đồ địa chỉ trong IPv6 cho phép cấp phát hầu như vô tận các địa chỉ, kiến trúc của IPv6 vẫn cho phép triển khai theo dạng có

cấu trúc sao cho nó không bị quá tải. Như trong IPv4, các bit bên trái của địa chỉ được dùng để tóm tắt các địa chỉ mạng xuất hiện ở phía phải của cấu trúc địa chỉ. Như vậy, địa chỉ IPv4 140.108.128.0/17 có thể bao gồm các subnets 140.108.225.0/24. Điều này có nghĩa là bảng định tuyến có thể route đến tất cả các subnets nhưng thay vì có 128 địa chỉ subnet nằm trong bảng định tuyến, chỉ còn 1 dòng duy nhất tượng trưng cho tất cả các route. Để chỉ ra một subnet nhỏ hơn, các qui luật thông thường trong định tuyến vẫn được tuân theo và gói tin được gởi tới cho router quảng bá network 140.108.128.0/17. Router này trong bảng định tuyến của nó có nhiều thông tin chi tiết hơn, sẽ chuyển gói cho đến khi nó đến được network đích.

Trong IPv6, kiến trúc địa chỉ cho phép điều chỉnh tốt hơn dạng địa chỉ được dùng trong Internet. Địa chỉ thì rất dài và mỗi phần phục vụ một chức năng khác nhau. 48-bit đầu tiên của địa chỉ được dùng bởi IANA cho quá trình định tuyến động trong Interner để tạo ra các địa chỉ khả kết toàn cục. Ba bit đầu tiên được gán giá trị 001 để chỉ ra một địa chỉ toàn cục.

Tự động cấu hình (Autoconfiguration)

Các địa chỉ cục bộ hay các router kết nối trực tiếp gửi prefix ra các kết nối cục bộ và ra tuyến đường mặc định. Các thông tin này được gửi đến tất cả các node trên hệ thống mạng, cho phép các host còn lại tự động cấu hình địa chỉ IPv6. Router cục bộ sẽ cung cấp 48-bit địa chỉ toàn cục và SLA hoặc các thông tin subnet đến các thiết bị đầu cuối. Các thiết bị đầu cuối chỉ cần đơn giản thêm vào địa chỉ lớp 2 của nó. Địa chỉ L2 này, cùng với 16-bit địa chỉ subnet tạo thành một địa chỉ 128-bit. Khả năng gắn một thiết bị vào mà không cần bất cứ một cấu hình nào hoặc dùng DHCP sẽ cho phép các thiết bị mới thêm vào Interner, chẳng hạn như dùng cellphone, dùng các thiết bị wireless và. Mạng Internet trở thành plug-and-play.

Tái cấu hình địa chỉ (Renumbering)

Khả năng kết nối đến các thiết bị ở xa một cách tự động cho phép đơn giản hóa nhiều tác vụ trước đây là các cơn ác mộng cho các nhà quản trị. Tính năng tự động cấu hình của IPv6 cho phép các router cung cấp tất cả các thông tin cần thiết đến tất cả các host trên mạng của nó. Điều này có nghĩa là các thiết bị có thể cấu hình lại địa chỉ của nó dễ dàng hơn. Trong IPv6,

các thay đổi này là trong suốt đối với người dùng cuối.

Header đơn giản và hiệu quả

Phần header của IPv6 đã được đơn giản hóa để tăng tốc độ xử lý và tăng hiệu quả cho router. Các cải tiến bao gồm:

- Có ít vùng hơn trong header.
- Các vùng bao gồm 64bits.
- Không còn phần kiểm tra lỗi checksum.

Do có ít vùng hơn, quá trình xử lý cũng ngắn hơn. Bộ nhớ dùng hiệu quả hơn với các field 64 bits. Điều này cho phép quá trình tìm kiếm trở nên rất nhanh bởi vì các bộ xử lý ngày nay cũng là các bộ xử lý 64 bit. Trở ngại duy nhất là việc sử dụng địa chỉ 128-bit, lớn hơn kích thước một word hiện hành. Việc loại bỏ phần check sum cũng giảm thiểu thời gian xử lý nhiều hơn nữa.

Error!

Error!

Bảo mật (Security)

Với các kết nối trực tiếp thông qua các không gian địa chỉ rộng lớn, vấn đề bảo mật là một chọn lựa nhiều thực tế cho IPv6. Bởi vì nhu cầu dùng firewall và các quá trình NAT giữa các thiết bị đầu cuối là giảm, các giải pháp về bảo mật có thể được thực hiện bằng cách mã hóa giữa các hệ thống. Mặc dù IPSec đã sẵn có trong IPv4, nó đã trở thành một thành phần trong IPv6. Việc sử dụng các thành phần mở rộng cho phép một giao thức cung cấp giải pháp end-to-end.

Tính cơ động

Địa chỉ IPv6 được thiết kế với tính cơ động được tích hợp vào trong Mobile IP. Mobile IP cho phép các hệ thống đầu cuối thay đổi vị trí mà không mất các kết nối. Đặc điểm này rất cần thiết cho những sản phẩm

wireless chẳng hạn như IP phone và các hệ thống GPS trong xe hơi. Định dạng phần header cho phép các thiết bị đầu cuối thay đổI địa chỉ IP bằng cách dùng một địa chỉ gốc như là nguồn của gói tin. Địa chỉ gốc này là ổn đinh, cho phép các địa chỉ duy trì tính cơ động.

Chuyển đổi IPv4 to IPv6

Chìa khóa cho thành công của IPv6 không chỉ nằm trong chức năng của nó mà còn trong khả năng chuyển đổi các hệ thống mạng hiện tại sang một giao thức mới. Điều này đòi hỏi nhiều thứ, bao gồm địa chỉ mới, cài đặt giao thức mới, các ứng dụng có thể giao tiếp với giao thức mới.

Lý thuyết cho vấn đề này là bạn nên bắt đầu triển khai IPv6 ở ngoài rìa của mạng và di chuyển dần vào lớp core theo một cách chậm, kiểm soát được. Điều này có nghĩa là một trong ba chọn lựa trên phải xảy ra: các traffic của IPv6 cần phải được mang thông qua các mạng IPv4 sao cho IPv6 cần thiết chạy trên toàn mạng. Điều này có nghĩa là cả IPv4 và IPv6 có thể cùng tồn tại hay một giao thức có thể cần được chuyển đổi sang một giao thức khác.

IPv6 tunnel qua ipv4: Cơ chế này được thực hiện đóng gói một gói tin IPv6 theo chuẩn IPv4 để có thể mang gói tin đó trên nền kiến trúc IPv4. Trong cơ chế tunneling, các nodes IPv6/IPv4 sẽ thực hiện việc đóng gói các datagram IPv6 vào thành phần dữ liệu trong datagram IPv4. Do đó gói tin này sẽ có thể được truyền qua nền IPv4.

Các kết nối có thể áp dụng cơ chế tunneling là:

- Router-to-router.
- Host-to-router.
- Host-to-host.

Trong 2 phương thức router-to-router và host-to-router, gói tin IPv6 được tunnel đến địa chỉ cuối cùng là tại router. Do đó, điểm cuối cùng của quá trình tunnel là các router trung gian. Các router này phải có nhiệm vụ “ mở gói” tin được tunnel và chuyển nó tới đích cuối cùng. Địa chỉ trong gói tin IPv6 được tunnel, không hỗ trợ địa chỉ IPv4 của điểm cuối cùng tunnel. Thay vào đó thì địa chỉ điểm cuối cùng tunnel phải được quyết định từ các

thông tin cấu hình trên nodes thực hiện đóng gói. Theo cơ chế xác định địa chỉ cuối như vậy, ta gọi là "tunnel configured". Có nghĩa là địa chỉ điểm cuối cùng của quá trình tạo tunnel đã được khai báo trước.

Gói tin IPv6 được tunnel trên tất cả hành trình của chúng cho tới khi đến được đích theo 2 phương thức sau: host-to-host và router-to-host . Theo cơ chế này, nodes cuối cùng được xác định địa chỉ đích của gói tin IPv6. Vì vậy, điểm cuối cùng của tunnel có thể quyết định từ địa chỉ đích của gói tin IPv6. Nếu địa chỉ này là một địa chỉ tương đương với địa chỉ IPv4, theo cấu trúc của địa chỉ này thì 32 bits thấp sẽ được lấy làm địa chỉ của nodes đích, và được sử dụng làm địa chỉ đích của nodes cuối cùng được tunnel. Kỹ thuật này tránh được việc khai báo trước địa chỉ đích của nodes cuối cùng được tunnel, gọi là "automatic tunneling".

Cả 2 kỹ thuật tự động và cấu hình có khác nhau cơ bản nhất là việc quyết định địa chỉ cuối của quá trình tunnel. Còn lại về cơ bản hoạt động của 2 cơ chế này là giống nhau.

- Điểm khởi tạo tunnel (điểm đóng gói tin) tạo một header IPv4 đóng gói và truyền gói tin đã được đóng gói.
- Nodes kết thúc của quá trình tunnel (điểm mở gói tin) nhận được gói tin đóng gói, xóa bỏ phần đầu header IPv4, sửa đổi một số trường của header IPv6, và xử lý phần dữ liệu này như một gói tin IPv6.

- Nodes đóng gói cần duy trì các thông tin về trạng thái của mỗi quá trình tunnel, ví dụ các tham số MTU để xử lý các gói tin IPv6 bắt đầu thực hiện tunnel. Vì số lượng các tiến trình tunnel co thể tăng lên một số lượng khá lớn, trong khi đó các thông tin này thường lặp lại, và do đó có thể sử dụng kỹ thuật cache và được loại bỏ khi cần thiết.

Các giao thức định tuyến cho IPv6

Các giao thức định tuyến hỗ trợ IPv6 là RIPng, OSPF, IS-IS, and BGP-4. Các giao thức này được hỗ trợ trong IOS 12.2T. Giao thức RIPng là một giao thức nội và được hỗ trợ bởi Cisco IOS. Chức năng của nó tương đương với RIPv2. RIPng là một giao thức nhóm distance vector nên có sử dụng split horizon và poison reverse, maximum hop count.Giao thức BGP-4+ là một giao thức ngoại vùng. Nó được dùng để kết nối các AS khác

nhau trên Internet.

RIPng có các đặc điểm sau:

- Dùng địa chỉ multicast cho các routing update.
- IPv6 prefix.
- Các routing update được gửi đi sẽ đóng gói trong IPv6.

MÔ HÌNH MẠNG OSI

Tác giả: Trần Văn Thành

I.Mô hình OSI

Cùng với sự phát triển rực rỡ của công nghệ vi mạch tích hợp là động lực không nhỏ vào sự phát triển của các hệ thống mạng máy tính. Nhưng có một bất cập là mỗi hệ thống lại sử dụng những chuẩn phần cứng và phần mềm riêng của mình. Những điều đó khiến cho việc kết nối giữa những hệ thống này với nhau gặp rất nhiều khó khăn. Trước tình hình đó tổ chức tiêu chuẩn quốc tế ISO đã đề xuất ra một mô hình mà các nhà thiết kế mạng có thể dựa vào đó để thiết lập các hệ thống có khả năng tưng thích với nhau, đó chính là mô hình tham chiếu OSI.

Mô hình tham chiếu hệ thống mở OSI (Open System Interconnection Reference Mode) là mô hình kiến trúc gồm 7 lớp, mỗi lớp đều có chức năng mạng xác định như: gán địa chỉ, điều khiển luồng, điều khiển lỗi, đóng gói và truyền gói tin một cách tin cậy trên mạng.

Các nguyên lý được áp dụng cho 7 tầng như sau:

(1) Mỗi lớp cần thiết phi tạo ở mức độ khác nhau của khái niệm trừu tượng.

(2) Mỗi lớp phi thực hiện một chức năng xác định rõ ràng.

(3) chức năng của mỗi lớp phi được chọn theo quan điểm hướng tới các giao thức chuẩn quốc tế đ• được định nghĩa.

(4) Ranh giới giữa các lớp phi được chọn để tối thiểu luồng thông tin đi qua các giao diện

Error!

Một số ưu điểm của việc sử dụng mô hình phân lớp đó là:

- Tách hoạt động thông tin trên mạng thành những phần nhỏ hơn, đơn giản hơn.
- Nó chuẩn hóa các thành phần mạng để cho phép phát triển một mạng từ nhiều nhà cung cấp sn phẩm.
- Cho phép các loại phần cứng phần mềm khác nhau thông tin được với nhau.
- Cho phép người thiết kế chuyên môn hoá và phát triển chức năng theo kiểu modul.
- Nó giúp cho việc học tập về mạng được dễ dàng hơn.

Error!

Trong mô hình OSI, bốn lớp dưới định nghĩa cách để các trạm thiết lập kết nối để trao đổi với nhau dữ liệu. Còn 3 lớp trên định nghĩa các ứng dụng trong phạm vi đàu cuối sẽ giao tiếp với nhau và với user như thế nào.

I.1. Lớp vật lý

Lớp vật lý cung cấp các phưng tiện điện, c các, thủ tục để kích hoạt, duy trì và gii phóng liên kết vật lý giữa các hệ thống.

Thuộc tính điện liên quan đến sự biểu diễn các bit (mức tín hiệu điện thế) và tốc độ truyền bit.

Thuộc tính c liên quan đến các chuẩn về giao diện vật lý kích thước, cấu hình.

Thuộc tính thủ tục liên quan đến giao thức điều khiển việc truyền các chuỗi bit qua đường vật lý.

Lớp vật lý là dưới cùng trong mô hình OSI giao diện với đường truyền không có PDU (Protocol Data Unit), không có phần header chứa thông tin điều khiển (PCI Protocol Control Information), dữ liệu được truyền theo dòng bit.

I.2. Lớp liên kết dữ liệu (Data Link Layer)

Lớp liên kết dữ liệu cung cấp các phưng tiện để truyền thông tin qua lớp vật lý đm bo độ tin cậy thông qua các c chế đồng bộ, kiểm soát lỗi và kiểm soát luồng dữ liệu.

Ngoài ra, lớp liên kết dữ liệu còn được chia làm 2 lớp con là:

+MAC (Media Access Control).

+LLC (Logical Link Control).

Các chức năng của lớp 2 gồm: tạo khung dữ liệu để truyền trên các đường vật lý, truy nhập các phưng tiện vật lý nhờ các địa chỉ MAC, phát hiện lỗi nhưng không sửa được lỗi.

I.3. Lớp mạng (Network Layer)

Lớp mạng được các nhà chuyên gia đánh giá lớp phức tạp nhất trong tất c các lớp trong mô hình OSI. Lớp mạng cung cấp phưng tiện để truyền các đn vị dữ liệu qua mạng hay liên mạng. Bởi vậy, nó phi đáp ứng nhiều kiểu cấu hình mạng và nhiều dich vụ cung cấp bởi các mạng khác nhau.

Các dịch vụ và giao thức cho lớp mạng phi phn ánh được tính phức tạp đó. Hai chức năng chủ yếu của lớp mạng đó là:

+Định tuyến (Routing).

+Chuyển tiếp (Relaying).

Mỗi node trong mạng đều phi thực hiện các chức năng này, do đó, chúng phi ở trên lớp liên kết dữ liệu để cung cấp một dịch vụ "trong suốt" đối với lớp giao vận. Chức năng định tuyến em sẽ giới thiệu trong phần giao thức TCP/IP.

Công nghệ IP là một công nghệ tiêu biểu và ưu việt nhất của lớp mạng cho nên, hiện tại và tưng lai các công nghệ ở các lớp khác đều phi tiến tới ci tiến để tối ưu trong sự liên lạc với IP.

I.4. Lớp giao vận (Transport Layer)

Trong mô hình OSI, 4 lớp thấp quan tâm đến việc truyền dữ liệu qua hệ thống đầu cuối (end systems) qua các phưng tiện truyền thông còn 3 lớp cao tập trung đáp ứng các yêu cầu và các ứng dụng của người sử dụng. Lớp giao vận là lớp cao nhất của 4 lớp thấp, nhiệm vụ của nó la cung cấp dịch vụ truyền dữ liệu sao cho các chi tiết cụ thể của các phưng tiện truyền thông được sử dụng ở dên dưới trở nên "trong suốt" đối với các lớp cao. Do đó nhiệm vụ của lớp giao vận rất phức tạp. Nó phi được tính đến kh năng thích ứng với một phạm vi rất rộng các đặc trưng mạng. Chẳng hạn, một mạng có thể là "connection-oriented" hay "connectionless", có thể là đáng tin cậy (reliable) hay không đáng tin cậy (unreliale). Nó phi biết được yêu cầu về chất lượng dịch vụ của người sử dụng đồng thời, cũng phi biết được kh năng cung cấp dịch vụ của mạng bên dưới.

I.5. Lớp phiên (Session Layer)

Nhiệm vụ của lớp phiên là cung cấp cho người sử dụng các chức năng cần thiết để qun trị các "phiên" ứng dụng của họ, cụ thể như sau:

Điều phối việc trao đổi dữ liệu giữa giữa các ứng dụng bằng cách thiếp lập và gii phóng (một cách logic) các phiên (hay còn gọi là các hội thoại-dialogues).

Cung cấp các điểm đồng bộ hoá để kiểm soát việc trao đổi dữ liệu.

Áp đặt các quy tắc cho các tưng tác giữa các ứng dụng của người sử dụng.

Cung cấp c chế nắm quyền trong quá trình trao đổi dữ liệu.

Việc trao đổi dữ liệu có thể được thực hiện theo 1 trong 3 phưng thức:

Đn công

Bán song công

Song công

Tóm lại, nhiệm vụ của lớp phiên là thiết lập, quản lý và kết thúc các phiên giao tiếp giữa các thực thể lớp trình bày.

I.6. Lớp trình diễn (Presentation Layer)

Mục đích của lớp trình diễn là đm bo cho các hệ thống đầu cuối có thể truyền thông có kết qu ngay c khi chúng sử dụng các cách biểu diễn dữ liệu khác nhau.

I.7. Lớp ứng dụng (Application Layer)
Lớp ứng dụng là lớp gần gũi với người dùng hn hết, nó cung cấp các dịch vụ mạng cho các ứng dụng của người dùng.

Là lớp cao nhất trong mô hình OSI, cho nên lớp ứng dụng có một số đặc điểm khác với các lớp dưới nó.Trước hết, nó không cung cấp một dịch vụ cho một lớp trên nào như các lớp bên dưới. Do đó ở lớp không có khái niệm điểm truy nhập lớp dịch vụ. Lớp ứng dụng là ranh giới giữa môi trường nối kết các hệ thống mở và các tiến trình ứng dụng (Application Process). Các tiến trình ứng dụng thuộc các hệ thống mở khác nhau muốn trao đổi thông tin phi thông qua tầng ứng dụng thuộc các hệ thống mở khác nhau

Tác giả: Trần Văn Thành

II. Mô hình TCP/IP

TCP/IP có cấu trúc tương tự như mô hình OSI, tuy nhiên để đảm bảo tính tương thích giữa các mạng và sự tin cậy của việc truyền thông tin trên mạng, bộ giao thức TCP/IP được chia thành 2 phần riêng biệt: giao thức IP sử dụng cho việc kết nối mạng và giao thức TCP để đảm bảo việc truyền dữ liệu một cách tin cậy.
Hình 1.3 bên dưới cho thấy sự giống và khác nhau giữa 2 mô hình OSI và TCP/IP.

Error!

Lớp ứng dụng: Tại mức cao nhất này, người sử dụng thực hiện các chương trình ứng dụng truy xuất đến các dịch vụ hiện hữu trên TCP/IP Internet. Một ứng dụng tương tác với một trong những protocol ở mức giao vận (transport) để gửi hoặc nhận dữ liệu. Mỗi chương trình ứng dụng chọn một kiểu giao vận mà nó cần, có thể là một dãy tuần tự từng thông điệp hoặc một chuỗi các byte liên tục. Chương trình ứng dụng sẽ gửi dữ liệu đi dưới dạng nào đó mà nó yêu cầu đến lớp giao vận.

Lớp giao vận: Nhiệm vụ cơ bản của lớp giao vận là cung cấp phưng tiện liên lạc từ một chương trình ứng dụng này đến một chưng trình ứng dụng khác. Việc thông tin liên lạc đó thường được gọi là end-to-end. Mức chuyên trở có thể điều khiển luông thông tin. Nó cũng có thể cung cấp sự giao vận có độ tin cậy, bảo đảm dữ liệu đến nơi mà không có lỗi và theo đúng thứ tự. Để làm được điều đó, phần mềm protocol lớp giao vận cung cấp giao thức TCP, trong quá trình trao đổi thông tin nơi nhận sẽ gửi ngược trở lại một xác nhận (ACK) và nơi gửi sẽ truyền lại những gói dữ liệu bị mất. Tuy nhiên trong những môi trường truyền dẫn tốt như

cáp quang chẳng hạn thì việc xy ra lỗi là rất nhỏ. Lớp giao vận có cung cấp một giao thức khác đó là UDP.

Lớp Internet: Nhiệm vụ cơ bản của lớp này là xử lý việc liên lạc của các thiết bị trên mạng. Nó nhận được một yêu cầu để gửi gói dữ liệu từ lớp cùng với một định danh của máy mà gói dữ liệu phi được gửi đến. Nó đóng segment vào trong một packet, điền vào phần đầu của packet, sau đó sử dụng các giao thức định tuyến để chuyển gói tin đến được đích của nó hoặc trạm kế tiếp. Khi đó tại nơi nhận sẽ kiểm tra tính hợp lệ của chúng, và sử dụng tiếp các giao thức định tuyến để xử lý gói tin. Đối với những packet được xác định thuộc cùng mạng cục bộ, phần mềm Internet sẽ cắt bỏ phần đầu của packet, và chọn một trong các giao thức lớp chuyên trở thích hợp để xử lý chúng. Cuối cùng, lớp Internet gửi và nhận các thông điệp kiểm soát và sử lý lỗi ICMP.

Lớp giao tiếp mạng: Lớp thấp nhất của mô hình TCP/IP chính là lớp giao tiếp mạng, có trách nhiệm nhận các IP datagram và truyền chúng trên một mạng nhất định. Người ta lại chia lớp giao tiếp mạng thành 2 lớp con là:

+Lớp vật lý: Lớp vật lý làm việc với các thiết bị vật lý, truyền tới dòng bit 0, 1 từ ni gửi đến nơi nhận.

+Lớp liên kết dữ liệu: Tại đây dữ liệu được tổ chức thành các khung (frame). Phần đầu khung chứa địa chỉ và thông tin điều khiển, phần cuối khung dành cho viêc phát hiện lỗi.

Hình 1.4 dưới đây sẽ mô tả chi tiết hơn về kiến trúc của mô hình TCP/IP.

Error!

II.1. The Process/Application Layer Protocols

II.1.1. Dịch vụ đăng nhập từ xaTELNET

Telnet là ứng dụng sử dụng giao thức telnet cho phép người dùng có thể đăng nhập vào một hệ thống ở xa và làm việc giống như đang sử dụng máy tính nội bộ vậy. Người sử dụng dùng chương trình Telnet Client (chưng trình Telnet trên máy tính trên máy khách) thực hiện một số kết nối TCP với một Telnet Server (chương trình phục vụ telnet trên máy chủ) ở cổng 23.

Error!

II.1.2. Dịch vụ truyền file FTP

Dịch vụ truyền File FTP (File Transfer Protocol) là một trong những dịch vụ sớm nhất ứng dụng giao thức TCP/ IP. FTP cho phép người dùng thực hiện các chức năng.

+ Sao chép.
+ Đổi tên.
+ Xóa file.
+ Tạo thư mục …..ở một hệ thống ở xa.

Hệ thống FTP ở xa thường yêu cầu người dùng cung cấp định danh ID và mật khẩu trước khi truy nhập hệ thống. Các máy chủ thường cung cấp hai dạng dịch vụ truy nhập.

Truy nhập vào các file công cộng dùng chung qua tài khoản ẩn danh (Anonymous).

Truy nhập vào các file riêng chỉ dành cho những người sử dụng với quyền truy nhập ở mức hệ thống.

FTP sử dụng cổng TCPở lớp Transport để truyền file một cách tin cậy. Tại FTP Server thì sẽ được gán các cổng cố định là 20, 21, còn ở Client thì sẽ được gán giá trị bất kỳ lớn hơn 1023. Để có thể hoạt động FTP thiết lập 2 kết nối. Một cho login và theo đó là giao thức Telnet. Hai là cho quản lý truyền dữ liệu.

II.1.3. Trivial File Transfer Protocol (TFTP)

Mặc dù FTP là giao thức truyền tập tin tổng quát nhất trong bộ giao thức TCP/IP, nhưng nó rất phức tạp. Nhiều ứng dụng không cần đến tất c các tính năng mà FTP cung cấp. Do đó người ta đưa ra một giao thức thứ hai cung cấp dịch vụ ít tốn kém và không phức tạp. Được biết dưới tên Trivial File Transfer Protocol (TFTP), giao thức này không cần đến những tưng tác phức tạp giữa client và server. TFTP giới hạn thao tác chỉ trong việc truyền tập tin và không cung cấp việc xác minh.

Không giống như FTP, TFTP không cần dịch vụ chuyển tin đáng tin cậy. Mà nó sử dụng giao thức UDP của tầng Transport, có sử dụng timeout và việc truyền lại để đảm bảo dữ liệu được truyền đến nơi. Bên gửi truyền một tập tin theo những khối có kích thước cố định (512 byte) và đợi lời đã nhận của mỗi trước khi gửi tiếp. Bên phía nhận gửi tr lời đã nhận sau khi nhận được mỗi khối.

II.1.4 Network File System (NFS)

Được phát triển đầu tiên bởi công ty Sun Microsoft, Hệ tập tin mạng (Network File System-NFS) cung cấp việc truy xuất trực tuyến các tập tin dùng chung. Người sử dụng có thể thực hiện một chưng trình ứng dụng bất kỳ và sử dụng bất kỳ một tập tin nào trong việc xuất nhập. Bản thân tên các tập tin không cho biết chúng cục bộ hay ở xa. NFS là một RPC (Remote Procedure Call).

II.1.5. Simple Mail Transfer Protocol (SMTP)

Giao thức SMTP là giao thức tiêu chuẩn trên Internet cho việc chuyển thư điện tử giữa các máy tính. SMTP được thiết kế để chuyển giao những thông điệp text và

cũng hỗ trợ những ứng dụng multimedia. SMTP thực hiện bên trên một phiên kết nối Telnet NVT.

Có hai thành phần chính trong SMTP: nơi gửi và nơi nhận. Nơi gửi được coi như là máy khách thực hiện lập một kết nối TCP với nơi nhận đóng vai trò là máy chủ. Cổng tiêu chuẩn để thực hiện kết nối TCP là 25. Trong một phiên của SMTP, nơi gửi & nhận trao đổi một chuỗi các lệnh và trả lời.

II.1.6. Simple Network Management Protocol (SNMP)

Giao thức quản lý mạng chuẩn của TCP/IP là SNMP định nghĩa giao thức quản lý cấp để quản lý hai thao tác cơ sở: trích giá trị từ một biến và lưu trữ giá trị vào một biến.

II.1.7. Domain Name Service (DNS)

Đối với những người truy nhập Internet, việc nhớ nhiều địa chỉ IP cùng một lúc là rất khó. Do đó, các nhà thiết kế tạo nên những tên dễ nhớ như: www.yahoo.com, www.home.vnn.vn, www.vnn.vn, www.ipmac.com.vn...

Người dùng muốn truy nhập đến địa chỉ nào thì chỉ việc gõ bàn phím những tên đó vào. Tuy nhiên, giao thức lớp mạng IP chỉ có thể hiệu và làm việc được với địa chỉ IP. Do vậy cần có sự chuyển đổi qua lại giữa tên và địa chỉ IP. Việc chuyển đổi tên thành địa chỉ được thực hiện qua hệ thống tên miền (Domain Name System – DNS). Hệ thống DNS thực chất là những CSDL (DNS database) chứa tên và địa chỉ tưng ứng cùng với các thông tin khác đi kèm.

II.1.7. Dynamic Host Configuration Protocol (DHCP)/BootP (Bootstrap Protocol)

Giao thức Bootstrap, gọi là BOOTP, cung cấp một cách khác với RARP cho máy tính nào cần xác định địa chỉ IP của nó. BOOPTP tổng quát hơn RARP vì nó sử dụng UDP, nên có thể mở rộng việc bootstrap đi qua bộ định tuyến. BOOTP cũng cho phép máy tính xác định địa chỉ của bộ định tuyến, địa chỉ server và tên của chương trình mà máy tính phải chạy. BOOTP được thiết kế đủ nhỏ và để chứa được trong bootstrap ROM. Client sử dụng địa chỉ Broadcast có giới hạn để thông tin liên lạc với Server, có trách nhiệm truyền lại nếu Server không trả lời. BOOTP hiệu quả hơn RARP bởi vì một thông điệp BOOTP xác định nhiều dữ liệu cần thiết vào lúc khởi động, bao gồm địa chỉ IP của máy tính, địa chỉ của bộ định tuyến, và địa chỉ của Server.

Được thiết kế như là bước nối tiếp của BOOTP, Dynamic Boat Configuration Protocol (DHCP) là sự mở rộng của BOOTP trên một số phương diện. Quan trọng nhất là DHCP cho phép server cấp phát địa chỉ IP một cách động. Việc cấp phát động là cần thiết đối với những môi trường mạng không giây (wireless), trong đó máy tính có thể kết nối và tách ra khỏi mạng một cách nhanh chóng.

II.2. The Internet Layer Protocols

II.2.1. Internet Protocol (IP)

Giao thức IP là một giao thức lớp mạng, được sử dụng phổ biến cho các mạng tham gia Internet. Thực chất, Internet là mạng của các mạng nối với nhau qua bộ định tuyến (Router). IP là giao thức được sử dụng để hướng các gói dữ liệu đến nút mạng mà nó cần đến. Mục đích ra đời của IP là để thống nhất việc sử dụng các máy chủ và router từ các hãng sản xuất khác nhau. Cho nên, IP cho phép kết nối nhiều loại mạng có đặc điểm khác nhau mà không làm gián đoạn hoạt động của mạng và kết nối với Internet.

Giao thức IP có ba nhiệm vụ chính đó là:

Thứ nhất: giao thức IP định nghĩa đơn vị cơ sở của lớp Internet.

Thứ hai : thực hiện chức năng định tuyến(routing), chọn ra con đường đi tối ưu mà dữ liệu cần gửi đi.

Thứ ba : điều khiển và xử lý lỗi.

II.2.1.1. Định dạng IP

Trên một mạng vật lý, đơn vị truyền dữ liệu là một frame bao gồm phần đầu và phần sữ liệu, với phần đầu cung cấp địa chỉ nguồn và địa chỉ đích (vật lý). Internet gọi đn vị truyền dữ liệu của nó là IP datagram hoặc là datagram (có những tài liệu thì lại gọi là packet). Cũng giống như một frame trong mạng vật lý, một datagram bao gồm 2 phần:

Phần tiêu đề (header).

Phần dữ liệu (data).

Error!

Sau đay ta sẽ tìm hiểu chi tiết nội dung từng trường một trong header của IP datagram.

Error!

Trong đó:

VERS (4-bit): chỉ phiên bản hiện hành của IP được sử dụng. Với IP thông thường là 4, thế hệ IP tiếp theo là 6.

HLEN(4-bit): chỉ độ dài phần tiêu đề của datagram tính theo đơn vị từ (32bit). Độ dài tối thiểu là 5 (20 octet).

Service Type: là chỉ số chất lượng dịch vụ yêu cầu cho IP datagram. Trường này bao gồm những thông tin sau:

Total Length: xác định độ dài của toàn bộ datagram,c header và data.

Identification: cùng với các tham số khác như Source IP addres, Destinaton IP address dùng để định danh duy nhất cho một datagram trong khong thời gian gói tin tồn tại trên mạng, dùng để tập hợp fragmented datagram.

Flags: Liên quan đến sự phân đoạn của datagram.

Error!

Trong đó:

+0: chưa sử dụng và luôn bằng 0.

+DF(Do not Fragment): bằng 0 có nghĩa là cho phép phân mnh, bằng 1 là không cho phép phân mnh.

+ MF (More Fragments): = 0 đây là đoạn phân mnh cuối cùng (the last fragment). = 1 đây là phân đoạn tiếp theo (more fragments).

Fragment Offset (13 bit): chỉ vị trí của đoạn (fragment) trong datagram ban đầu, tính theo đn vị 8 octet. Mỗi đoạn (trừ đoạn cuối cùng) phi chứa vùng dữ liệu là bội số của 8 octet.

Time to Live (8-bit): quy định thời gian tồn tại (tính bằng giây) của datagram trên mạng để tránh tình trạng datagram không đến được đích và cứ đi lòng vòng trên mạng. Thời gian này được thiết lập bởi trạm gửi và gim đi mỗi đi datagram đi qua một nút mạng. TTL = 0 gói dữ liệu sẽ bị discard.

Protocol Number: This field indicates the higher level protocol to which IP should deliver the data in this datagram. These include:

- 0: Reserved
- 1: Internet Control Message Protocol (ICMP)
- 2: Internet Group Management Protocol (IGMP)
- 3: Gateway-to-Gateway Protocol (GGP)
- 4: IP (IP encapsulation)
- 5: Stream
- 6: Transmission Control Protocol (TCP)
- 8: Exterior Gateway Protocol (EGP)
- 9: Private Interior Routing Protocol
- 17: User Datagram Protocol (UDP)
- 41: IP Version 6 (Ipv6)
- 50: Encap Security Payload for Ipv6 (ESP)
- 51: Authentication Header for Ipv6 (AH)
- 89: Open Shortest Path First

Source IP Address (32bit): địa chỉ IP của trạm gửi.

Destination IP Address(32 bit):địa chỉ IP của trạm nhận.

Header Checksum (16 bit): m• kiểm soát lỗi 16 bit theo phưng pháp CRC, chỉ áp dụng cho vùng header. Trường này luôn được cập nhật khi một gói tin đi qua router trung gian.

Options: khai báo các tuỳ chọn do ni gửi yêu cầu. Trường option không bắt buộc phi có trong mọi datagram và chủ yếu dùng để kiểm tra lỗi trên mạng. Option là một phần quan trọng của giao thức IP nên mọi tiêu chuẩn thực hiện phi dựa trên IP phi bao gồm tiến trình xử lý trường này. Độ dài của trường Option thay đổi tuỳ thuộc vào các tham số đi kèm. Khi các Option xuất hiện trong datagram, nó sẽ kéo dài liên tục mà không có sự ngắt quãng.

II.2.1.2. Định tuyến

Một trong những chức năng của giao thức IP là có kh năng thiết lập kết nối giữa các mạng vật lý khác nhau. Đó chính là định tuyến. Một hệ thống thực hiện chức năng này được gọi là IP router. Sẽ trình bày cụ thể trong phần 2.

II.2.1.3. Điều khiển và xử lý lỗi

Như ta đã biết giao thức IP cung cấp dịch vụ "unreliable", chuyển dữ liệu connectionless bằng cách dàn xếp cho mỗi bộ định tuyến chuyển dữ liệu. Mỗi packet sẽ di chuyển từ bộ định tuyến này đến bộ định tuyến khác cho đến bộ định tuyến mà có thể chuyển packet trực tiếp đến đích cuối cùng của nó. Nếu một bộ định tuyến không thể gửi một packet, hay nếu nó phát hiện một dấu hiệu không bình thường có nh hưởng đến việc truyền dữ liệu (ví dụ: nghẽn mạch trên mạng), bộ định tuyến cần phải thông báo cho nơi xuất phát của packet, để tránh hoặc khắc phục lỗi. Do đó cần phải một cơ chế để thông báo lỗi cho bên gửi gói tin.

Giao thức bn tin điều khiển liên mạng ICMP (Internet Control Message Protocol) ra đời để giải quyết vấn đề trên. ICMP cũng giúp cho các host định tuyến trên mạng và cho phép các nhà qun lý mạng theo dõi tình trạng các node trên mạng. Tất cả các host và Router đều phải có khả năng tạo và xử lý các bản tin ICMP nhận được.

II.2.2. Giao thức bản tin điều khiển liên mạng (ICMP)

Giao thức IP hoạt động tại lớp Network được sử dụng bởi IP cho nhiều dịch vụ khác nhau. Bản tinICMP được mang trực tiếp trong gói tin IP với trường Protocol Number bằng 1.

Có rất nhiều trường hợp khiến cho gói tin IP bị loại bỏ: Đường truyền có sự cố, trường Time-to-Live hết hạn, không phân mảnh được gói tin kích thước lớn hn MTU cho phép....Khi một gói tin cần loại bỏ, bn tin ICMP được sử dụng để thông báo về địa chỉ gửi gói tin.

Tuy nhiên, không phi trường hợp nào ICMP cũng cần phi báo lỗi.Sau đây là một số trường hợp mà khi xảy ra sự cố, ICMP không cần báo lỗi:

Định tuyến hay chuyển giao bản tin ICMP.

Phát quảng bá hay phát theo nhóm gói tin IP.

Các phân đoạn gói tin khác với phân đoạn đầu tiên.

Bn tin có địa chỉ nguồn không xác định một host duy nhất (ví dụ: 127.0.0.1, 0.0.0.0).

Định dạng của bn tin ICMP như sau :

Error!

Bản tin ICMP được mang trogn phần dữ liệu của gói tin IP. Mặcdù mỗi bản tin ICMP có dạng riêng của nó, nhưng chúng đều bắt đầu với ba trường sau:

TYPE (8bit): là một số nguyên 8bit để xác định thông điệp.

CODE (8bit):cung cấp thêm thông tin về kiểu thông điệp.

CHECKSUM(16bit) : ICMP sử dụng thuật giải checksum như IP, nhưng ICMP checksum chỉ tính đến thông điệp ICMP.

Hơn nữa, các thông điệp ICMP thông báo lỗi luôn luôn bao gồm phần đầu và 64bit đầu tiên của packet gây nên lỗi. Lý do có thêm phần đầu này cùng với phần đầu packet là để cho phép nơi nhận xác định chính xác hơn những giao thức nào và chương trình ứng dụng có trách nhiệm đối với packet.

Trường TYPE của ICMP xác định ý nghĩa của thông điệp cũng như định dạng của nó.Các kiểu bao gồm:

- 0: Echo reply
- 3: Destination unreachable
- 4: Source quench
- 5: Redirect
- 8: Echo

- 9: Router advertisement
- 10: Router solicitation
- 11: Time exceeded
- 12: Parameter problem
- 13: Timestamp request
- 14: Timestamp reply
- 15: Information request (obsolete)
- 16: Information reply (obsolete)
- 17: Address mask request
- 18: Address mask reply
- 30: Traceroute
- 31: Datagram conversion error
- 32: Mobile host redirect
- 33: Ipv6 Where-Are-You
- 34: Ipv6 I-Am-Here
- 35: Mobile registration request
- 36: Mobile registration reply
- 37: Domain name request
- 38: Domain name reply
- 39: SKIP
- 40: Photuris

II.2.3. ARP và RARP

II.2.3.1. ARP

a/ Khái niệm

Địa chỉ IP được dùng để định danh các trạm và mạng tưng ứng với tưng ứng lớp mạng của mô hình OSI và không phải địa chỉ vật lý của trạm đó trên một mạng cục bộ LAN (Ethernet, Token Ring....). Trên một mạng LAN như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải có cơ chế ánh xạ giữa địa chỉ IP (32bit) và địa chỉ vật lý (48bit).

Để giải quyết vấn đề trên, người ta xây dưng nên một giao thức ARP. Các thiết bị trên mạng LAN sử dụng ARP để tìm ra thông tin về địa chỉ vật lý của các thiết bị đó trên mạng.

ý tưởng về giải địa chỉ động dua ARP : khi máy A muốn gii địa chỉ IP là IB, nó phát đi một thông điệp quảng bá trên toàn mạng trong đó có chứa địa chỉ IP và vật lý của nó và địa chỉ IP của B. Tất cả các trạm đều nhận được, nhưng chỉ có B nhận ra địa chỉ IP của mình và sẽ trả lời A bằng một thông điệp trong đó có chứa địa chỉ vật lý của B.

Tuy vậy không phải lúc nào khi cần truyền dữ liệu, A đều phát đi thông điệp quảng bá để yêu cầu địa chỉ vật lý của trạm nào đó. Việc phát thông điệp quảng bá như vậy sẽ tốn rất nhiều băng thông trên mạng thậm chí có thể gây ra tình trạng tắc

nghẽn không đáng có ở những mạng có tốc độ truyền tải chậm. Do đó, mỗi trạm đều có một bộ đệm ARP (ARP cache) để lưu giữ những địa chỉ IP và vật lý tương ứng tìm được gần đây nhất. Mỗi khi một trạm nhận được một thông điệp ARP yêu cầu hoặc trả lời của một trạm khác, nó đều cập nhật trong ARP cache của mình. Khi truuyền một gói dữ liệu, trạm sẽ tìm xem trong bộ đệm ARP của nó có chứa địa chỉ vật lý tương ứng hay chưa. Nếu tìm thấy, nó sẽ không phát quảng bá ARP nữa. Các địa chỉ trong ARP cache sẽ bị xoá bỏ sau một khoảng thời gian nhất định để đề phòng sự cố xảy ra đối với một trạm nào đó. Ví dụ: một trạm có card mạng bị hỏng, cần thay thế và như vậy địa chỉ vật lý của trạm đó sẽ thay đổi. Nhưng các trạm không biết gì về sự cố đó nên vẫn giữ địa chỉ cũ của trạm này. Đó là lý do vì sao cần phi cài đặt một bộ đếm thờn gian và thông tin trạng thái sẽ bị xoá bỏ sau khi thời gian hết hạn. Ví dụ bất cứ khi nào thông tin về địa chỉ liên kết được đặt vào bộ đệm ARP, giao thức này sẽ yêu cầu thời gian bắt đầu đếm, thông thường là 20 phút. Khi hết hạn (sau 20 phút) thông tin phi được xoá bỏ. Sẽ có 2 khả năng xảy ra khi xoá bỏ.

Nếu không còn dữ liệu được gửi tới máy tính đích này, thì không có gì xy ra nữa.

Nếu vẫn còn dữ liệu được gửi tới máy tính đích này và không còn thông tin về địa chỉ này trong bộ đệm ARP, máy tính sẽ phi lặp lại địa chỉ thông thường là broadcast một yêu cầu ARP và lấy lại thông tin địa chỉ. Nếu máy tính đích vẫn còn đó, thông tin địa chỉ lại được đặt vào bộ đệm ARP. Nếu không, nI gửi sẽ phát hiện được rằng máy đích không còn nối mạng nữa.

b/ Định dạng gói tin ARP

Error!

Hardware address space (16bit): xác định loại giao diện sử dụng trên mạng ví dụ: Ethernet, Packet Radio Net.

Protocol address space: xác định loại giao thức ở lớp trên được sử dụng, nó có giá trị080016 dành cho địa chỉ IP.

Hardware address length: Xác định độ dài địa chỉ vật lý trong gói tin ví dụ : IEEE 802.3 và IEEE 802.5 là 6.

Protocol address length: xác định độ dài của địa chỉ của giao thức lớp 3 tương ứng trong mô hình OSI. ví dụ IP là 4.

Operation code: xác định một trong 4 loại thông điệp:

+ARP yêu cầu (ARP request)-1

+ARP tr lời (ARP reply)-2

+RARP yêu cầu (RARP request)-3

+RARP tr lời (RARP reply)-4

Source/target hardware address: bao gồm địa chỉ vật lý của mạng, ví dụ với IEEE 802.3 là 48-bit addresses.

Source/target protocol address: gồm địa chỉ của giao thức, ví dụ với TCP/IP là 32-bit IP addresses.

II.2.3.2. RARP

a/ Khái niệm

Ngược lại với giao thức ARP, giao thức RARP (Reverse ARP) được dùng để tìm địa chỉ IP khi biết địa chỉ vật lý của một trạm. Điều này thường xảy ra khi một số trạm không có đĩa cứng để lưu giữ địa chỉ IP của mình. Những trạm chỉ có địa chỉ vật lý lưu ở trong ROM của card mạng. Chúng phải tìm địa chỉ IP ở trong server quản lý địa chỉ IP khi khởi động. RARP cũng tương tự như ARP gồm 2 loại thông điệp:

+RARP yêu cầu địa chỉ (RARP request).

+ RARP tr lời (RARP reply).

ý tưởng: một máy khi cần biết địa chỉ của nó dưới dạng Broadcast, trên mạng sẽ có RARP server sẽ trả lời bằng cách cấp cho máy của bạn một địa chỉ IP. Định dạng gói tin RARP

Định dạng của RARP giống hệt ARP, tương ứng trường Operation code bằng 3,4.

II.3. The Host-to-Host Layer Protocols

Giao thức IP được thiết kế để thực hiện một chức năng : tạo gói tin và định tuyến đến nơi nhận. Không có cơ chế nào trong giao thức IP đảm bảo các gói tin không bị thất lạc trên đường truyền và đến đúng với thứ tự được truyền đi. Nhiệm vụ đó do giao thức TCP ở tầng giao vận đảm nhiệm. TCP bảo đảm dữ liệu được phân phát tin cậy, theo thứ tự, và không có lỗi.

Một giao thức khác cũng rất phổ biến ở lớp giao vận là giao thức UDP, UDP có đơn vị truyền dữ liệu đơn giản hơn và độ tin cậy kém hơn TCP rất nhiều. UDP thường dùng cho những ứng dụng yêu cầu về tốc độ nhiều ho8n là độ tin cậy.

II.3.1Transmission Control Protocol (TCP)

II.3.1.1. Khái niệm

Một kết nối TCP sẽ được thực hiện khi ứng dụng ở một host truyền và nhận dữ liệu đến một host khác. TCP cung cấp khả năng truyền song công (full-duplex) giữa hai ứng dụng ở hai đầu kết nối.

TCP phi có nhiệm vụ chuyển dữ liệu của lớp ứng dụng thành các đơn vị dữ liệu có thể truyền để có thể đóng gói thành packet ở lớp Internet. Ưng dụng chuyển dữ liệu đến TCP và TCP đặt vào bộ đệm gửi. TCP chia nhỏ dữ liệu và thêm phần tiêu đề (header) tạo thành đơn vị dữ liệu gọi là segment. Kích thước của segment phi luôn được điều chỉnh ở mức tối ưu với tài nguyên hiện có trên mạng. TCP sẽ chờ cho đến khi nhận đủ dữ liệu từ lớp trên trước khi tạo một segment có kích thước phù hợp.

Một máy khách phải được xác định được loại dịch vụ yêu cầu từ máy chủ. Điều này được thực hiện bằng việc sử dụng cặp địa chỉ IP và số hiệu cổng TCP. Cổng TCP nằm trong khong từ 0 đến 65535. Từ 0 đến 1023 là các cổng cho những dịch vụ thông thường.
Sự kết hợp giữa địa chỉ IP và số hiệu cổng tạo thành cặp địa chỉ socket. Một kết nối TCP giữa hai đầu cuối được nhận diện hay phân biệt nhờ địa chỉ socket này. Trong header của packet chứa thông tin địa chỉ nguồn và địa chỉ đích, số hiệu cổng nằm trong segment của TCP.
TCP là một giao thức Connection-Oriented nên để truyền được dữ liệu thì trước đó nó phải thiết lập kết nối rồi duy trì kết nối và sau khi hết dữ liệu cần gửi nó phải giải phóng kết nối. Trong quá trình truyền dữ liệu có sử dụng cơ chế điều khiển luồng (flow control) và điều khiển lỗi.
II.3.1.2. Định dạng dữ liệu của TCP
Mỗi segment của giao thức TCP bao gồm phần tiêu đề (header) và phần dữ liệu (data).

Error!

Trong đó:

Source port (16 bit) và Destination port (16 bit): số hiệu cổng của host nguồn và đích.

Sequence Number (32 bit): số hiệu xác định vị trí byte đầu tiên của segment khi bit SYN không được thiết lập. Nếu bit SYN được thiết lập thì đây là số hiệu tuần tự khởi đầu của dữ liệu.

Ackknowledgment Number (32 bit): ký hiệu là ACK, là số hiệu của segment kế tiếp trong dòng dữ liệu mà bên nhận đang chờ. Data Offset (4 bit): chỉ kích thước của phần header TCP tính theo đn vị từ 32 bit. Trường này đồng thời cũng xác định vị trí bắt đầu của phần dữ liệu.

Reserved (6 bit): trường này hiện vẫn dự phòng và luôn bằng 0.

Flags (6 bit): là các bit cờ có ý nghĩa như sau:

-URG: bằng 1 nếu có dữ liệu khẩn. Dữ liệu khẩn sẽ được chỉ ra trong trường Urgent Pointer. Ngược lại thì bằng 0.
-ACK: bằng 0 nếu là segment khởi đầu và khi đó trường ACK Number mới có hiệu lực.
-PSH: thông báo dữ liệu cần chuyển đi ngay.
-RST: xác định lỗi, đồng thời để khởi động lại kết nối.
-SYN:bằng 1 khi thiết lập kết nối.
-FIN: bằng 1 khi trạm nguồn hết thông tin.

Window (16 bit): Đây là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong trường ACK Number mà trạm nguồn sẵn sàng để nhận.

Checksum (16bit): m• kiểm soát lỗi theo phương pháp CRC của toàn bộ segment.

Urgent Pointer (16 bit): đây là con trỏ tới số hiệu tuần tự của byte đi sau dữ liệu khẩn, cho phép bên nhận biết được độ dài của dữ liệu khẩn. Trường này có hiệu lực khi bit URG được thiết lập 1.

Padding (độ dài thay đổi): Phần mềm chèn thêm vào header để đảm bảo header luôn kết thúc ở một mốc 32 bit. Phần chèn thêm này luôn = 0.

Data (độ dài thay đổi): chứa dữ liệu cần gửi đi của lớp trên TCP.

Options (độ dài thay đổi): khai báo các tuỳ chọn của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.

II.3.2. User Datagram Protocol (UDP)

II.3.2.1. KháI niệm

Giao thức UDP là giao thức kết nối không định hướng (connectionless) được sử dụng trên lớp IP theo yêu cầu của ứng dụng. Khác với TCP, UDP không có quá trình thiết lập và giải phóng kết nối. UDP cũng không hỗ trợ chức năng báo nhận (acknowledgement), không sắp xếp tuần tự các đơn vị dữ liệu (packet) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu (packet) mà không hề có thông báo lỗi cho ứng dụng sử dụng UDP. Có thể nói UDP không cung cấp các dịch vụ truyền tin tin cậy như TCP.

Giống như TCP, UDP cũng hoạt động dựa trên chế sử dụng các số hiệu cổng (port number) để định danh duy nhất một ứng dụng chạy trên một máy tính nối mạng. Do có it chức năng phức tạp nên UDP có tốc độ truyền và nhận nhanh hơn TCP trong các mạng có độ tin cậy cao như LAN. UDP thường dùng cho các ứng dụng đơn giãn.

II.3.2.2. Định dạng dữ liệu của UDP

Error!

Trong đó:

Source port (16 bit) và Destination port (16 bit): số hiệu cổng của host nguồn và đích.

Length: chỉ độ dài của bn tin UDP bao gồm c phần header và data.

Checksum: sử dụng kiểm tra lỗi cho phần header.

MỘT SỐ GIAO THỨC ĐỊNH TUYẾN CỤ THỂ

Tác giả: Trần Văn Thành

Các giao thức cổng nội (Interior Routing Protocols)

I. Classfull routing protocol

I.1. RIPv1

Routing Information Protocol (RIP) là giao thức định tuyến vector khoảng cách (Distance Vector Protocol) xuất hiện sớm nhất. Nó suất hiện vào năm 1970 bởi Xerox như là một phần của bộ giao thức Xerox Networking Services (XNS). Một điều kỳ lạ là RIP được chấp nhận rộng rải trước khi có một chuẩn chính thức được xuất bản. Mãi đến năm 1988 RIP mới được chính thức ban bố trong RFC1058 bởi Charles Hedrick. RIP được sử dụng rộng rãi do tính chất đơn giản và tiện dụng của nó.

1. Định nghĩa

RIP là giao thức định tuyến vector khoảng cách điển hình, là nó đều đăn gửi toàn bộ routing table ra tất cả các active interface đều đặn theo chu kỳ là 30 giây. RIP chỉ sử dụng metric là hop count để tính ra tuyến đường tốt nhất tới remote network. Thuật toán mà RIP sử dụng để xây dựng nên routing table là Bellman-Ford.

2. Các giá trị về thời gian (RIP Timers)

Trước khi đi vào tìm hiểu hoạt động của RIP, tôi xin giới thiệu một số khái niệm về thời gian:

Route update timer: là khoảng thời gian trao đổi định kỳ thông tin định tuyến của router ra tất cả các active interface. Thông tin định tuyến ở đây là toàn bộ bảng routing table, giá trị thời gian là 30 giây.

Route invalid timer: là khoảng thời gian trôi qua để xác định một tuyến là invalid. Nó được bắt đầu nếu hết thời gian hold time mà không nhận được update,

sau khoảng thời gian route invalid timer nó sẽ gửi một bản tin update tới tất cả các active interface là tuyến đường đó là invalid.

Holddown timer: giá trị này được sử dụng khi thông tin về tuyến này bị thay đổi. Ngay khi thông tin mới được nhận, router đặt tuyến đường đó vào trạng thái hold-down. Điều này có nghĩa là router không gửi quảng bá cũng như không nhận quảng bá về tuyến đường đó trong khong thời gian Holddown timer này. Sau khoảng thời gian này router mới nhận và gửi thông tin về tuyến đường đó. Tác dụng về giá trị này là giảm thông tin sai mà router học được. Giá trị mặc định là 180 giây.

Route flush timer: là khoảng thời gian được tính từ khi tuyến ở trạng thái không hợp lệ đến khi tuyến bị xoá khỏi bảng định tuyến. Giá trị Route invalid timer phải nhỏ hơn giá trị Route flush timer vì router cần thông báo tới neighbor của nó về trạng thái invalid của tuyến đó trước khi local routing được update.

3. Hoạt động của RIPv1

Tất cả các bản tin của RIP đều được đóng gói vào UDP segment với cả hai trường Source and Destination Port là 520. RIP định nghĩa ra hai loại bản tin Requestmessages and Response messages.

Request message: được sử dụng để gửi một yêu cầu tới router neighbor để gửi update.

Response message: mang thông tin update.

a/ Khởi động RIP

RIP gửi broadcast bản tin Request ra tất cả các active interface. Sau đó lắng nghe hay đợi Response message từ router khác. Còn các router neighbor nhận được các Request message rồi gửi Response message chứa toàn bộ routing table.

b/ Xử lý thông tin update của router

Sau khi xây dựng xong routing table lúc khởi động, khi router nhận được thông tin update về route tới một mạng nào đó. Nếu route tới mạng đó đã tồn tại trong routing table, route đang tồn tại sẽ bị thay thế bởi route mới nếu route mới có hop count nhỏ hơn. Nó sẽ lờ đi nếu route mới có hop count lớn hơn. Nếu hết thời

gian Holddown time thì bất kể route mới có giá trị như thế nào thì nó vẫn được lưu vào routing table.

c/ Định dạng bản tin của RIP (RIP Message Format)

Định dạng bản tin RIP được mô tả trong hình dưới. Mỗi bản tin RIP đều bao gồm trường command, version và có thể chứa được tới 25 tuyến đường (route entries). Mỗi route entry bao gồm address family identifier, the IP address reachable by the route, and the hop count for the route.Nếu router phi một update với hn 25 route entries thì multiple message được sử dụng.

Chú ý, phần đầu gồm 4 octet cộng và mỗi route entry là 20 octet. Do đó kích thước tối đa của message là 4 + 25*20 + 8 = 512 octet. Header của UDP segment là 8 octet.

Error!

Các trường cụ thể trong bản tin RIP:

Command: có giá trị là 1 cho biết đây là một Request message, có giá trị là 0 cho biết đây là Response message.

Version: là 1 cho biết đây là version 1.

Address Family Identifier: có giá trị là 2 nếu là IP.

IP Address: là địa chỉ đích của tuyến đường.

Metric: là hop count như đã đề cập.

d/ Đặc trưng của RIP

RIP thường được sử dụng cho những mạng nhỏ với kiến trúc đơn giản, RIP rất ít khi được sử dụng cho những mạng lớn, phức tạp vì những lý do sau:

Metric của RIP có giá trị tối đa là 15, 16 có nghĩa là mạng unreachable (không tới được).

Metric của RIP là hop count nên không giải quyết tốt được vấn đề lưu lượng.

Thời gian hội tụ Convergence time là rất lớn. Khi một sự cố xy ra trên mạng, RIP phải cần một khoảng thời gian khá lớn để tìm được tuyến đường thay thế. Giá trị này ít nhất phi lớn hơn Flush time là 240 giây.

I.2. Interior Gateway Routing Protocol (IGRP)

1. Định nghĩa

Trước những nhược điểm vốn có của RIP như: metric là hop count, kích thước mạng tối đa là 15 hop. Cisco đã phát triển một giao thức độc quyền của riêng mình là IGRP để khắc phục những nhược điểm đó. Cụ thể là metric của IGRP là sự tổ hợp của 5 yếu tố, mặc định là bandwidth và delay:

Bandwidth

Delay

Load

Reliability

Maximum transfer unit (MTU)

IGRP không sử dụng hop count trong metric của mình, tuy nhiên nó vẫn theo dõi được hop count. Một mạng cài đặt IGRP thì kích thước mạng có thể nên tới 255 hop.

Ưu điểm nữa của IGRP so với RIP là nó hỗ trợ được unequal-cost load sharing và thời gian update lâu hơn RIP gấp 3 lần.

Tuy nhiên bên cạnh những ưu điểm của mình so với RIP, IGRP cũng có những nhược điểm đó là giao thức độc quyền của Cisco.

2. Hoạt động và đặc trưng

IGRP có rất nhiều điểm chung với RIP, chúng cùng là classfull distance vector protocol cũng như định kỳ gửi toàn bộ routing table ra tất cả active interface.

Cũng giống như RIP, IGRP cũng broadcasd Request packet ra tất cả các active interface khi khởi động và cẩn thận check các paket update nhận được xem source

address của packet đó có cùng subnet mà update được nhận. Giống như RIP nó cũng không gửi subnetmask trong thông tin định tuyến.

Nếu như RIP dùng port 520 của giao thức UDP để trao đổi thông tin định tuyến, thì IGRP thì làm điều này trực tiếp trong gói tin IP với trường Protocol number là 9.

IGRP sử dụng khái niệm Autonomous System (AS), một IGRP AS là một IGRP process domain_tập hợp các router có chung routing protocol là một IGRP process. Cho phép multiple IGRP AS tồn tại bên trong một AS có nghĩa là người quản trị có phân đoạn mạng tốt hơn. Người quản trị có thể tạo một IGRP AS cho mỗi routing domain, giúp cho việc điều khiển thông tin giữa các mạng tương tác tốt hơn.

IGRP thừa nhận 3 loại tuyến đường trong thông tin update:

Interior route: mạng nối trực tiếp với router.

System route: là đường tới địa chỉ mạng mà bị summary bởi network border router.

Exterior route: là đường học qua IGRP từ IGRP AS khác, nó cung cấp thông tin sử dụng bởi default route.

a/ IGRP Timer

Chu kỳ update của IGRP là 90 giây, IGRP có sử dụng nhân tố random 20% để ngăn chặn sự đồng bộ update timer. Khoảng thời gian giữa 2 lần update biến đổi từ 72 đến 90 giây.

Khi một tuyến đường đầu tiên được học, invalid timer cho tuyến đó là 270 giây hay là gấp 3 lần update timer. Flush timer được thiết lập với giá trị là

630 giây_ gấp 7 lần update timer. Mỗi lần tuyến được được update thì những thông số thời gian này được khởi động lại. Nếu như invalid timer trôi qua mà tuyến đường đó không nhận được một update thì tuyến đường đó sẽ bị đánh dấu là không đến được. Tuyến đường đó sẽ được giữ trong routing table và quảng bá với thông tin là tuyến đó không đến được cho đến khi flush timer trôi qua, tuyến đó sẽ được xoá khỏi routing table.

Update timer của IGRP gấp 3 lần RIP, điều đó chứng tỏ IGRP tốn it băng thông hơn cho việc gửi update. Nhưng thời gian hội tụ của IGRP sẽ lớn hơn RIP.

b/ IGRP Metrics

Metric của IGRP là tổ hợp của các thành phần sau: bandwidth, delay, load, reliability. Mặc định của metric là bandwidth và delay, bạn hãy tưởng tượng liên kết dữ liệu (data link) như là một cái ống thì bandwidth như là chiều rộng của ống còn delay như là chiều dài của ống. Nói cách khác bandwidth là thước đo khả năng mang thông tin và delay độ trễ cần thiết để một bít truyền đến đích.

Bandwidth: được biểt diễn với đơn vị là kbps, là một thông số được sử dụng để IGRP sử dụng để chạy thuật toán Bellman-Ford. Nó là một thông số tĩnh có thể thay đổi bởi người quản trị không liên quan gì đến bandwidth thật của đường truyền.

BW = [10000000/(bandwidth in Kbps)]

Delay: giống như bandwidth là một thông số tĩnh có thể được cấu hình bằng tay.

Delay = [Delay in 10s of microseconds]

Reliability: là một thông số động, được biểu diễn bởi một số 8bit. được tính số lượng gói tin đến đích mà không bị hỏng. Reliability có giá trị 255 có nghĩa là 100% gói tin không bị hỏng, giá trị nhỏ nhất là 1.

Load: là một phần băng thông sử dụng trên đường truyền, được biểu diễn bởi một số 8 bit. Load có giá trị là 255 nghĩa là sử dụng 100%, 1 là giá trị nhỏ nhất.

Mặc định: K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0. Các hăng số trên có thể được thay tuỳ theo mục đích của người quản trị.

c/ IGRP Packet Format

Định dạng gói tin IGRP được biểu diễn như hình sau:

Error!

Như ta thấy bản tin IGRP update mang nhiều thông tin hơn so với RIP. Mỗi bản tin IGRP update có thể chứa tối đa 104 muc nhập (entry) với mỗi mục nhập có kích thước 14octet và header của IGRP update là 12 octet. Ta có maximum của IGRP packet là 12 + 104*14 = 1468 byte.

Các trường của IGRP có ý nghĩa là:

Version: luôn luôn có giá trị bằng 1.

Opcode: có giá trị là 1 cho IGRP Request packet và có giá trị là 2 cho IGRP Update packet. Chú ý Request packet không chứa mục nhập (entry).

Edition: giá trị được tăng lên bởi nơi gửi bất cứ khi nào có một thay đổi về thông tin định tuyến. Giá trị này giúp cho router tránh update nhầm thông tin update cũ sau khi nhận thông tin update mới.

Autonomous System Number: là ID number của IGRP process. Thông số này cho phép multiple IGRP process trao đổi thông tin định tuyến qua một liên kết dữ liệu chung.

Number of Interior Routes: là số mục nhập trong update, là những subnet của những network nối trực tiếp.

Number of System Routes: số tuyến đường tới những mạng mà không nối trực tiếp. Hay nói cách khác, là những tuyến đường đã được summary

bởi router biên.

Number of Exterior Routes: là số tuyến đường tới những mạng mà được học bởi default route.

Checksum: được tính trên IGRP header và tất cả các mục nhập.

Destination: là trường đầu tiên của mỗi mục nhập. Có một chú ý là trường destination chỉ có 3 octet trong khi địa chỉ IP có 4 octet. Điều này được thực hiện do những nguyên nhân sau. Nếu mục nhập là một interior route thì ít nhất octet đầu tiên của địa chỉ IP luôn luôn được xác định từ địa chỉ IP của interface mà nó nhận được update. Tương tự như vậy nếu mục nhập là system hay external route thì route sẽ bị summary và ít nhất là octet cuối cùng là toàn zero. Do đó trường destination chỉ cần biểu diễn 3 octet đầu là đủ.

Delay: trường này bao gồm 24 bit.

Bandwidth: trường này bao gồm 24 bit.

MTU: là Maximum Transmission Unit nhỏ nhất của bất kỳ link nào trong tuyến đường đến đích. Mặc dù đây là một thông số nhưng không bao giờ được sử dụng để tính route.

Reliability, Load: có giá trị biến đổi từ 0x01 đến 0xFF.

Hop Count: có giá trị biến đổi từ 0x01 đến 0xFF cho biết số hop của tuyến đường đến đích.

d/ Unequal-Cost Load Balancing

Load balancing là cách router gửi lưu lượng qua nhiều đường để đến cùng đích. Nó được sử dụng để giảm lưu lượng qua single path. Không giống như RIP, IGRP không những chỉ hỗ trợ equal-cost balancing mà còn hỗ trợ cả unequal-cost balancing. Điều này được thực hiện nhờ sử dụng thông số variance. Những route nào có metric nhỏ hơn hoặc bằng metric*variance sẽ được chọn là feasiable route (metric tốt nhất). Thông số Maximum Paths xác định tối đa có bao nhiêu route tham gia load balancing.

MPLS Traffic Engineering

Tác giả: Nguyễn Tuấn Vũ

I. Tổng quan về quản lý lưu lượng MPLS

Quản lý lưu lượng là quá trình điều khiển các tắt nghẽn trong mạng, xử lý, tính toán, kiểm soát lưu lượng, tối ưu hóa các tài nguyên mạng theo yêu cầu cho các mục đích khác nhau.

Trước khi MPLS ra đời, người ta thực hiện quản lý lưu lượng trên mạng IP và ATM.

IP traffic engineering điều khiển lưu lượng dựa trên đơn giá của đường truyền, không điều khiển được lưu lượng đến (traffic from), mà chỉ điều khiển được lưu lượng đi (traffic to).
ATM traffic engineering sử dụng các PVC để truyền cho phép quản lý lưu lượng tốt hơn. Tuy nhiên cần phải xây dựng full-mesh PVC và phải điều chỉnh kích cỡ, vị trí của các PVC tuỳ vào loại traffic tại mỗi thời điểm, khi một kết nối bị down sẽ tạo ra flooding rất lớn.

MPLS traffic engineering kết hợp những lợi điểm của ATM TE với tính linh hoạt, mềm dẻo của mạng IP cho phép xây dựng đường chuyển mạch nhãn LSP (còn gọi là TE tunnel) để truyền lưu lượng.

MPLS TE tránh được vấn đề flooding mà ATM gặp phải do MPLS TE sử dụng cơ chế gọi là autoroute để xây dựng bảng định tuyến thông qua các tunnel mà không cần dựa vào full-mesh of routing như ATM.

II. Yêu cầu để cấu hình MPLS TE

- Router và IOS có hỗ trợ MPLS TE.
- Mạng có hỗ trợ Cisco Express Forwarding (CEF).
- Giao thức định tuyến link-state: OSPF hay IS-IS

- Kích hoạt traffic engineering ở global mode và ở interface mode
Router(config)#mpls traffic-eng tunnels
Router(config-if)#mpls traffic-eng tunnels
- Interface loopback để làm routerID (RID) trong MPLS TE
int lo0
ip address 10.1.1.1 255.255.255.255
- Cấu hình TE tunnel, ví dụ:
int Tunnel0
ip unnumbered Loopback0
tunnel mode mpls traffic-eng
tunnel destination <địa chỉ IP đích>
…

III. Hoạt động của MPLS TE

Gồm 3 quá trình: Phân phối thông tin tài nguyên hiện có, thiết lập đường truyền và vận chuyển lưu lượng theo các tunnel.

1 Information Distribution

Ta cần giải quyết 3 vấn đề: thông tin gì được phân phối, khi nào thì thực hiện phân phối thông tin và thông tin được phân phối như thế nào? (What/When/How information is distributed)

1.1 What information is distributed?

MPLS TE sử dụng OSPF/IS-IS để phân phối thông tin về tài nguyên hiện có. Các thông tin phân phối bao gồm:
- Thông tin về băng thông hiện có trên interface
Router(config-if)# ip rsvp bandwidth <kbps>
- Độ ưu tiên của tunnel
Tunnel có priority mang giá trị từ 0 đến 7, giá trị càng thấp thì càng ưu tiên, chia làm 2 loại Setup priority và Holding Priority. Setup priority quyết định khi nào thì chấp nhận 1 tunnel. Setup priority của tunnel mới được dùng để so sánh với Hold Priority của tunnel cũ để ra quyết định sẽ chọn tunnel nào.
Router(config-if)# mpls traffic-eng priority 1 7

Ví dụ ta có tunnel1 và tunnel2 cùng yêu cầu sử dụng băng thông, cả 2 đều có SP = 1 và HP = 7. Khi đó:

1. Tunnel1 đến trước và chiếm dụng băng thông với HP=7.
2. Tunnel2 đến sau, so sánh SP của tunnel 2 (1) <HP của tunnel 1(7) nên sẽ ưu tiên cho tunnel2 và đẩy Tunnel1 ra khỏi đường truyền, tunnel2 chiếm dụng băng thông với HP=7.
3. Tunnel1 đến, so sánh SP> HP của tunnel 2 nên sẽ đẩy tunnel2 ra khỏi đường truyền và chiếm dụng băng thông với HP=7.

Quá trình lặp lại…

Recommend: Ta thường cấu hình giá trị Setup Priority > Hold Priority.

- Các thuộc tính cờ (attribute flags)
Attribute flag gồm 32 bit chỉ trạng thái, tính chất của đường truyền.
Router(config-if)#mpls traffic-eng attribute-flags 0x3
(Phần này chưa rõ lắm)

-Trọng số (administrative weight) của interface
Giải thuật SPF sử dụng cost để tính toán đường đi. Mặc định TE cost = IGP cost. Giả sử kết nối 2 router có TE metric = IGP metric = 1. Để thay đổi TE cost mà không đổi IGP cost ta sử dụng lệnh:
Router(config-if)# mpls traffic-eng administrative-weight 3
Khi đó TE metric = TE admin weight = 3, IGP metric = 1

Một vấn đề đặt ra là khi nào thì thông tin được phân phối?

1.2 When information is distributed?

Khi mạng không dùng MPLS TE, IGP sẽ flood các thông tin đường truyền khi: thay đổi trạng thái kết nối (a link goes up or down), khi cấu hình kết nối thay đổi (link cost is modified, or link's configuration is changed,…), khi đến chu kỳ flooding dữ liệu.

MPLS TE có thêm 1 yếu tố nữa để ra quyết định flooding là khi băng thông thay đổi đáng kể. Tunnel được thiết lập hay loại bỏ dựa vào sự thay đổi băng thông dành trước trên interface. Nhưng khi nào thì router sẽ thông báo sự thay đổi băng thông này? Nếu router sẽ thông báo khi có sự thay đổi băng thông thì với số lượng lớn tunnel thay đổi, thông tin flooding này cũng sẽ chiếm đầy tài nguyên mạng chẳng khác gì so với IGP. Do đó ta phải định ra ngưỡng giới hạn để điều khiển quá trình này, có 3 cách xác định ngưỡng:

- Flood significant changes immediately
Router(config-if)#mpls traffic-eng flooding thresholds {up|down} <list of threshold percentages>
Percent là phần trăm băng thông dành cho kết nối.
Up/Down là nếu sử dụng băng thông vượt qua ngưỡng/thấp hơn ngưỡng thì sẽ thực hiện flooding.

- Flood insignificant changes periodically, but more often than the IGP refresh interval
Router(config)# mpls traffic-eng link-management timers periodic-flooding <0-3600s>
Mặc định, sau 3 phút sẽ kiểm tra TE Link Manager, nếu có sự thay đổi về yêu cầu dự trữ băng thông thì sẽ tiến hành flooding.

Recommend: Không nên thay đổi chu kỳ flooding, nếu ta thay đổi chu kỳ quá thấp như 1s thì router sẽ làm việc liên tục và hậu quả sẽ khó lường.

- If a change that has not yet been flooded is known to cause an error, flood immediately
Khi có error do RSVP gửi về khi thiết lập đường truyền thì sẽ tiến hành flooding thông tin đi để thông báo trạng thái.

Kế tiếp ta xem xét thông tin sẽ được phân phối như thế nào?

1.3 How Information Is Distributed?
ở đây ta quan tâm đến MPLS TE trong OSPF.
Router ospf 1
Mpls traffic-eng router-id Loopback0
Mpls traffic-eng area 0
LSA mờ(opaque LSA – LSA type 10) định nghĩa thêm trường TLV (Type/Length/Variable) được sử dụng để trao đổi thông tin.

1. How SPF Works
Giả sử ta có mạng như hình 1, khi tính toán SPF, mỗi router sẽ xây dựng 2 danh mục PATH list(chứa danh mục các shortest path để đến đích) và TENT list(chứa danh mục các next-hop trong quá trình tính toán). Trong đó, (node, cost, next-hop) sẽ biểu diễn kết quả tính toán trên mỗi router.

----------PATH list ---------TENT list-----
B1:.....(A,0,0)……(empty)

B2:.....(A,0,0)……(B,5,B), (C,10,C)

B3:.....(A,0,0)……(C,10,C)
.....(B,5,B)

B4:.....(A,0,0)
.....(B,5,B)……(C,8,B), (D,13,B)

B5:.....(A,0,0)…….(D,13,B)
.....(B,5,B)
.....(C,8,B)

B6:.....(A,0,0)
.....(B,5,B)……(D,12,C)
.....(C,8,B)

B7:.....(A,0,0)……..(empty)
.....(B,5,B)
.....(C,8,B)
.....(D,12,C)

Khi đó, bảng định tuyến trên router A là:
Node---------Cost---------Next Hop
A……0…….Self
B……5…….B (directly connected)
C……8…….B
D……..12…….C

Khi đó các đường đi xuất phát từ A là A—B, A—B—C, A—B—C—D

2. How CSPF Works
Đường đi ngắn nhất trong MPLS TE còn phải dựa vào các yếu tố về bandwidth, link attributes và administrative weight.

Giả sử băng thông cấp phát cho các kết nối như sau: A-B(100Mbps), A-C(100), B-C(50), B-D(90), C-D(60). Xem hình 2

Khi đó đường đi từ A—B—C—D có cost là 12 sẽ chỉ cho phép băng thông cao nhất là 60Mbps.

Giải thuật CSPF có đưa tham số bandwidth để tính toán (node, cost, next-hop, bandwidth)

--------PATH list -----TENT list-----
B1:…(A,0,self,N/A)……(empty)

B2:…(A,0,self,N/A)……(B,5,B,100), (C,10,C,100)

B3:…(A,0,self, N/A)…(C,10,C,100)
……(B,5,B,100)……(D,13,B,90)

B4:…(A,0,self, N/A)……(D,13,B,90)
……(B,5,B,100)
……(C,10,C,100)

B5:…(A,0,self, N/A)…….(empty)
……(B,5,B,100)
……(C,10,C,100)
……(D,13,B,90)

Khi đó, bảng định tuyến trên router A là:
Node-------Cost--------Bandwidth---------Next Hop
A.....0.....N/A.....Self
B.....5.....100.....B (directly connected)
C.....8.....100.....C
D.....12.....90.....B
Các đường đi xuất phát từ A: A—B, A—C, A—B—D

3. Resource Reservation Protocol (RSVP)
Sau khi tính toán xong đường đi bằng giải thuật CSPF sẽ thực hiện thiết lập đường truyền thông qua giao thức dự trữ tài nguyên RSVP.

Xét ví dụ hình 3, giả sử ta muốn dự trữ tài nguyên theo đường hầm R1-R2-R3-R5-R6-R7, các bước thực hiện như sau:

1. R1 gửi PATH message đến R2, R2 nhận thông điệp, kiểm tra định dạng thông điệp, kiểm tra trạng thái kết nối TE Link Manager để đảm bảo có đủ băng thông yêu cầu cấp phát. Nếu có sai sót, R2 sẽ gửi error message về lại R1. Nếu tất cả đều tốt, chuyển sang bước 2.
2. R2 gửi PATH mess đến R3, kiểm tra tương tự R1
3. R3 gửi PATH mess đến R5, kiểm tra tương tự
4. R5 gửi PATH mess đến R6, kiểm tra tương tự
5. R6 gửi PATH mess đến R7, kiểm tra tương tự
6. R7 là cuối tunnel, sẽ gửi RESV message về lại R6 báo rằng nhãn R7 sẽ

cấp phát cho các gói trên đường truyền này là explicit-null.
7. R6 gửi RESV mess đến R5 và báo là muốn nhận nhãn đến mang giá trị 42. Nghĩa là trên đường truyền R5-R6, traffic sẽ nhận nhãn 42 và thực hiện loại bỏ nhãn tại R6 (label swaping) để gửi đến R7.
8. R5 gửi RESV mess đến R3, báo nhãn cho R3 là 10921.
9. R3 gửi RESV mess đến R2, báo nhãn cho R2 là 21.
10. R2 gửi RESV mess đến R1, báo nhãn cho R1 là 18.

Khi R1 nhận thông điệp RESV, đường hầm từ R1 đến R2 sẽ sẵn sàng và ta biết được giá trị nhãn sử dụng trong tunnel.

Còn rất nhiều các vấn đề khac như điều khiển lưu lượng đi qua tunnel dựa vào static route, policy routing, autoroute, vấn đề sử dụng chung băng thông, cân bằng tải và điều khiển metric trong đường hầm TE tunnel, vấn đề chất lượng dịch vụ trong MPLS TE, Fast Reroute (FRR)…

Bài viết Multi Layers Switching

Tác giả: Đặng Quang Minh

GIỚI THIỆU CHUNG:

Trong một hệ thống mạng máy tính, switch đóng vai trò thiết bị kết nối trung tâm và thường hoạt động ở layer 2 của mô hình OSI. Đối với một số dòng switch cao cấp như Catalyst 4000 trở về trước của Cisco hay Switch Procurve 8000 trở về trước của HP, một vài chức năng của layer 3 như là Broadcast control, IP Multicast,.QoS (IP Precedence, Protocol filter) được bổ sung để đáp ứng các nhu cầu ngày càng cao của hệ thống…Tuy nhiên các switch này không có được một số chức năng quan trọng của layer 3 như chức năng routing, IP dynamic VLAN… Do vậy các VLAN do các switch này tạo ra thường là static VLAN hay MAC dynamic VLAN. Mặc khác các VLAN không thể liên lạc được với nhau nếu không có router trung gian.

Hình sau cho thấy các VLAN muốn giao tiếp với nhau phải thông qua 1 router trung gian.

Error!

Như vậy để 2 VLAN giao tiếp được với nhau, hệ thống mạng sẽ trở nên rắc rối hơn, khó quản lý hơn.

Khái niệm multilayer switch (MLS) nói chung là một switch có thể thực hiện được một số các chức năng của các tầng cao hơn. Ở đây, chúng tôi chỉ trình bày các chức năng hoạt động ở tầng thứ 3 của mô hình OSI mà các switch trước đây không thực hiện được. MLS cung cấp một cách hiệu quả khả năng hoạt động ở layer 3 cho phần cứng của switch thông qua vi mạch chuyên dụng application-specific (ASIC) được tích hợp với phần cứng trong switch và bộ xử lý của router. Các chức năng của layer 3 có được trong switch loại này là do tích hợp thêm một vài thiết bị phần cứng như là RSM (Routing Switch Module), NFFC (NetFlow Feature Card),

NRFC (Network Routing Feature Card)…vào switch truyền thống. Các thiết bị phần cứng này sẽ được đề cập chi tiết trong phần sau.

Ví dụ sau cho ta thấy một switch có chức năng MLS sẽ kết nối được các VLAN như thế nào::

Host A, B và C nằm trên các VLAN khác nhau : host A thuộc VLAN Sales, host B thuộc VLAN Maketing, host C thuộc VLAN Engineering. Thông qua một switch duy nhất (đã có thêm phần cứng là RSM) các host này đã giao tiếp được với nhau. Bảng tạo ra ở phần trên của hình chính là bảng routing do thiết bị phần cứng thêm vào switch đã tạo ra.

Error!

Ta nhận thấy thiết bị phần cứng thêm vào switch đóng vai trò như một router. Nên việc tìm đường cũng dựa vào các routing protocol như Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), và Intermediate System-to-Intermediate System (IS-IS).

Khái niệm switch layer 3 sẽ góp phần làm cho hệ thống đỡ phức tạp do giảm bớt các thiết bị (thay vì để 2 VLAN liên lạc được với nhau hệ thống cũ trước đây phải có 2 switch và 1 router thì bây giờ hệ thống chỉ cần quản lý 1 switch duy nhất). MLS còn có khả năng thống kê lưu lượng lưu thông các gói tin để giúp cho việc quản trị mạng. Thêm vào đó, hệ thống mạng với các switch này sẽ được cải thiện về tốc độ và giá thành.

Đối với các sản phẩm switch Catalyst của Cisco, tính năng Multilayer switching tạo nên sự khác biệt giữa dòng sản phẩm 4000 và các dòng sản phẩm 5000 và 6000. Các dòng sản phẩm 5000, 6000 còn có một số chức năng bổ sung như Server Load Balancing, Enhanced QoS, FlexWAN… nhưng tính năng MultiLayer Switching đóng vai trò quan trọng nhất.

CẤU HÌNH PHẦN CỨNG CẦN THIẾT ĐỂ CÓ CHỨC NĂNG MULTILAYER SWITCH

Tài liệu này phân tích riêng về các sản phẩm switch Catalyst của Cisco. Các switch của các hãng khác khi muốn có thêm chức năng multilayer switching cũng có thể thêm vào các phần cứng có chức năng tương tự nhưng có thể có những tên gọi khác. Trong tài liệu này đề cập đến 2 dòng switch mới mà có thêm vào chức năng multilayer switch đó là Catalyst 5000 và Catalyst 6000.

Đối với Switch Catalyst 5000 :

Các thành phần cung cấp tính năng MLS gồm có :

MLS-SE (Multilayer Switching – Switch Engine) : cụ thể là NetFlow Feature Card (NFFC) hoặc là NFFC II trong Supervisor Engine III or III F hoặc là Supervisor Engine II G / III G, và Catalyst đời 2926G. MLS-SE cung cấp dịch vụ Layer 3 LAN-switching.

MLS-RP (Multilayer Switching – Router Processor) : là RSM hoặc RSFC hoặc là những router nối ngoài như Cisco 7500, 7200, 4700, 4500, or 3600 với phần mềm hỗ trợ IP MLS MLS-RP. MLS-RP cung cấp các dịch vụ về Cisco IOS-based multiprotocol routing và network.

MLS-RP hoạt động như một router. Nó bao gồm một trong những thiết bị phần cứng sau:

Route Swittch Module (RSM):

Catalyst 5500, 5505, 5509 có thêm một module vật lý RSM. Module này có khả năng hoạt động tương tự như một router. Có thể lắp module này vào bất kì slot nào trên switch ngoại trừ slot 1 và 2 (dành cho Supervisor và redundant supervisor engine).

Hình Route Switch Module

Error!

Bảng những đặc điểm kĩ thuật của RSM

Mô tả	**Đặc điểm**
Bộ xử lý	2 bộ xử lý Mips R4700 RISC[1] có tốc độ external là 50 MHz và tốc độ internal là 100 MHz.
Bộ nhớ: DRAM[2] NVRAM Flash SIMM Flash Card Boot ROM	 32-MB (minimum), 64-MB, or 128-MB main and shared memory. Chấp nhận 8-MB (8 x 4), 16-MB (16 x 2 or 16 x 4), or 32-MB (32 x 4) SIMMs. 128-KB nonvolatile EPROM cho file cấu hình hệ thống. 8-MB or 16-MB onboard Flash SIMMs cho Cisco IOS images. 16-MB or 20-MB PCMCIA card cho Cisco IOS images. RSM có 2 slot PCMCIA cung cấp kích thước lớn nhất cho bộ nhớ 40-MB Flash card. 256-KB EPROM cho chương trình quản lý ROM.

Những cổng giao tiếp	1 port serial console 1 port serial auxiliary Backplane interface: 2 SAGE ASICs
Regulatory compliance: Safety EMC Network xác nhận	 UL1950, CSA22.2-950, EN60950 FCC-Part15-Class A, EN55022-Class B, CISPR22-Class B, VCCI-Class 2, CE Marking Net 1, Net 2, Net 3

[1]RISC = Reduced Instruction Set Computing
[2]DRAM = dynamic random-access memory

Route Switch Feature Card (RSFC)

Đối với họ switch Catalyst 5000, supervisor module là module tùy chọn. Có nhiều loại supervisor như Supervisor II, Supervisor II G, Supervisor III F, Supervisor III G… Trong đó Supervisor II G và Supervisor III G hỗ trợ cho RFSC. RFSC có thể gắn thêm vào các module này để phục vụ cho các chức năng ở layer 3 của switches.

Error!

RSFC được xem như 1 module logic.Nếu Supervisor engine được gắn vào slot 1 thì RSFC được xem là module thứ 15. Nếu Supervisor engine được gắn vào slot 2 thì RSFC được xem là module thứ 16.

Bảng những đặc điểm kĩ thuật cũa **RSFC**

Mô tả	Đặc điểm

Bộ xử lý (Processor)	1 bộ sử lý Mips R4700 RISC với tốc độ 200 MHz.
Cổng giao tiếp	1 cổng serial console (trên mặt trước của supervisor engine).
Bộ nhớ	
DRAM[1]	64-MB or 128-MB main and shared memory.
NVRAM	128-KB nonvolatile EPROM cho file cấu hình hệ thống
Flash SIMM	16-MB onboard Flash SIMMs cho Cisco IOS images.
Boot ROM	256-KB EPROM cho chương trình quản lý ROM.
Regulatory Compliance	
Safety	UL1950, CSA22.2-950, EN60950
EMC	FCC-Part15-Class A, EN55022-Class B, CISPR22-Class B, VCCI-Class 2, CE Marking
Network xác nhận	Net 1, Net 2, Net 3

[1]DRAM = dynamic random-access memory

Đối với Switch Catalyst 6000 :

Để switch có chức năng của layer 3, hai phần cứng quan trọng được thêm vào là: Policy Feature Card (PFC) và Multilayer Switch Feature Card (MSFC)

PFC :

PFC chứa bảng Layer 3 switching (the Layer 3 MLS cache). MSL cache chưa thông tin luồng dữ liệu cho tất cả mọi hoạt động.

PFC của switch 6000 có chức năng tương tự như MLS-SE của switch 5000.

MSFC:

MSFC được gắn bên trong supervisor engine, chạy phần mèn Cisco IOS router để liên lạc với những phần logic còn lại trên supervisor engine thông qua Interprocessor Communication (IPC) bus. Như thế, switch có MSFC có khả năng MLS (Layer 3 switching).

MSFC của switch 6000 có chức năng tương tự nhu MLS-RP của switch 5000.

MSFC được xem như là module logic thứ 15 nếu supervisor engine được gắn vào trong slot 1 và được xem như là module logic thứ 16 nếu supervisor engine được gắn vào trong slot 2.

Hình mô tả chức năng của Multilayer Switch Feature Card

Error!

Hoạt động của MSFC :

Packet đầu tiên đi từ nguồn đến đích theo cách routing thông thường. Ngay khi nó đến đích, supervisor engine học được tất cả thông tin mà nó cần để gởi đi những packet tiếp theo bằng con đường khác thông qua phần cứng của chính nó và bô xử lý router. Supervisor trình bày lại theo cách trình bày của layer 3 và thiết bị nơi nhận nghĩ rằng nó nhận được packet từ 1 router. Hoạt động này sẽ được trình bày chi tiết ở phần sau.

NHỮNG CHỨC NĂNG CỦA LAYER 3 :

Tất cả những phần cứng mà vừa trình bày ở trên đều cho switch có thêm các chức năng ở layer 3. Ở phần này ta sẽ khảo sát kĩ hơn để xem các phần cứng đó hoạt động ra sao để có các chức năng layer 3 đó. Đồng thời nghiên cưu các cách cấu hình cho các chức năng layer 3.

INTERVLAN Routing

Giới thiệu :

Hệ thống mạng với các switch layer 2 thì các thiết bị trên những VLAN khác nhau không thể liên lạc trực tiếp với nhau. Chức năng layer 3 trên switch giúp các VLAN có thê liên lạc được với nhau mà không cần phải gián tiếp qua router.

Các khái niệm :

Trước khi đi qua phần khảo sát kĩ hoạt động của các phần cứng để có chức năng inter VLAN thì ta xem qua các khái niệm sau đây :

Khái niệm luồng dữ liệu (flow):

Khái niệm luồng dữ liệu tức là một hướng truyền và nhận dữ liệu duy nhất và các packet trên hướng đó phải cùng 1 giao thức. Nói cách khác, những luồng này là khác nhau nếu giao thức hoặc địa chỉ đầu gửi và nhận khác nhau. Tức là hướng packet đi từ A đến B khác packet đi từ B đến A. Packet đi từ A đến B với giao thức FTP khác packet từ A đến B với giao thức HTTP. Khái niệm luồng thông tin chỉ ở trên layer 3. Đặc điểm này cho phép các lưu thông IP từ những người dùng hoặc ứng dụng đến 1 đích xác định chỉ cần đi theo1 luồng dữ liệu duy nhất.

Khái niệm Layer 3 MLS Cache:

NFFC (hoặc NFFC II) chứa bảng Layer 3 switching (còn gọi là Layer 3 MLS cache) để chứa những thông tin về luồng dữ liệu. Cache này cũng bao gồm các thông tin về lưu lượng trên. Sau khi MLS cache được tạo, packet được nhận ra dựa vào thông tin luồng lưu trong bảng cache.

Một mục trong cache sẽ được tạo mới ngay khi switch nhận được packet có luồng dữ liệu không giống tất cả các mục đã hiện diện trong cache.

Mỗi một mục lưu thông tin về luồng dữ liệu có quy định thời gian tồn tại. Ta cũng có thể thay đổi thời gian đó.

Kích thước lớn nhất của cache là 128K.

Hoạt động của các phần cứng để có chức năng interVLAN:

Khi 1 packet được chuyển đi ở layer 3 thì Switch (Switch ở đây đối với họ switch 5000 là MLS-SE, đối với họ 6000 là NFC) trình bày thông tin trong packet lại dưới dạng học được từ Router (Router ở đây đối với họ switch 5000 là MLS-RP, đối với họ 6000 là NSFC) và lưu giữ packet đó ở trong MLS cache.

Nếu Host A và Host B khác VLAN. Host A gửi packet đến router để định được con đường đến Host B, switch nhận ra packet được gửi đến router nnờ vào địa chỉ MAC của router ở trên packet. Switch kiểm tra lại MLS cache thấy con đường chưa được xác định.

Packet switch nhận có dạng như sau:

Frame Header		**IP Header**				**Payload**	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
SWITCH MAC	*Host A MAC*	*Host B IP*	*Host A IP*	*n*	*calculation 1*		

Switch viết lại header của frame thuộc layer 2, thay đổi địc chỉ MAC của nơi đến thành địa chỉ MAC của Host B và địc chỉ MAC của nơi đi thành địa chỉ MAC của Router (những địc chỉ MAC này được lưu giữ trong MLS cache). Địa chỉ IP của Layer 3 vẫn tương tự như vậy, nhưng Time to Live (TTL) tăng 1 và checksum được tính toán lại.

Switch chuyển tiếp packet vừa được viết lại đến VLAN của Host B và Host B nhận packet.

Packet sau khi được switch viết lại có dạng như sau:

Frame Header		**IP Header**				**Payload**	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
Host B MAC	*MLS-RP MAC*	*Host B IP*	*Host A IP*	*n+1*	*calculation 2*		

Sau khi packet đầu tiên đã được chuyển đến Host B. Thông tin về dòng dữ liệu đã được lưu trong MLS cache. Những packet sau đó sử dụng lại những thông tin này để chuyển tiếp đến đích.

Cụ thể hơn, ta mô tả lại quá trình hoạt động của Router và Switch đối với gói tin đầu tiên mà switch layer 3 nhận được để tạo ra một mục trong MLS cache qua 4 bước sau đây:

Bước 1:

Error!

Bước 2 :

Error!

Bước 3 :

Error!

Bước 4:

Error!

Những phần mềm và phần cứng cần thiết :

IP MLS đòi hỏi những phần mềm sau:

Supervisor engine software release 4.1(1) hoặc những đời sau.

Phần mềm IOS cho router Cisco:

IOS release 12.0(3c)W5(8a) or later on the Route Switch Feature Card (RSFC)

IOS release 12.0(3c)W5(8) or later on the MLS-RP if running MLS over ATM media

IOS release 12.0(2) or later on Cisco 3600 series routers

IOS release 11.3(2)WA4(4) or later on the Route Switch Module (RSM), or Cisco 7500, 7200, 4700, and 4500 series routers

Nếu chạy MLS trên ATM media, Catalyst 5000 family ATM module software release 11.3(8)WA4(11) or later, or release 12.0(3c)W5(10) or later

IP MLS đòi hỏi những phần cứng sau:

Catalyst đời 2926G switch, hoặc Catalyst 5000 switch với Supervisor Engine II G or III G, or Supervisor Engine III or III F với NetFlow Feature Card (NFFC) or NFFC II

RSM, RSFC, hay là những router ngoài như Cisco 7500, 7200, 4700, 4500, or 3600.

Họ Catalyst 5000 với ATM module và router với cổng ATM nếu hoạt động MLS trên ATM media.

(Tùy chọn) Những module có khả năng inline-rewrite ---Những module này có phần cứng onboard có khả năng cưc đại hoá khả năng IP MLS. Lệnh **show port capabilities** sẽ xác định được phần cứng hỗ trợ inline rewrite.

Configuration

IP MLS thường được cài đặt mặc định. Nhưng ta cũng có thể thay đổi cấu hình trên các cổng bằng các lệnh sau:

Task	**Command**
Tắt khả năng IP MLS trên 1 cổng	Router(config-if)# **no mls ip**
Bật khả năng IP MLS trên 1 cổng	Router(config-if)# **mls ip**

Trình bày chi tiết IP MLS của mọi cổng	**show ip** [*interface*]

Ví dụ:

Router(config-if)# **no mls ip**

Router(config-if)# **mls ip**

Router(config-if)#

· **Thiết lập INTERVLAN với RSM**

Lệnh session *mod_num* (slot lắp RSM) giúp truy cập vào RSM thông qua CLI.

Ví dụ :

Console> (enable) **session 5**

Trying Router-5...

Connected to Router-5.

Escape character is '^]'.

User Access Verification

Password:

Router>**exit**

Console> (enable)

§ Thiết lập IP Intervlan với RSM:

Thực hiện tiếp những lệnh sau trong chế độ configuration

Task	**Command**
Step 1 (tùy chọn) Bật IP routing trên router.	**ip routing**
Step 2 (tùy chọn) Xác định một IP routing protocol.	**Router** *ip_routing_protocol*

Step 3 Xác định cổng VLAN trên RSM.	**Interface** *vlan-id*
Step 4 Xác định địa chỉ IP cho VLAN.	**ip address** *n.n.n.n mask*
Step 5 Thoát khỏi chế độ configuration.	Ctrl-Z

Ví dụ :

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ip routing**

Router(config)#**router rip**

Router(config-router)#**network 10.0.0.0**

Router(config-router)#**interface vlan 100**

Router(config-if)#**ip address 10.1.1.1 255.0.0.0**

Router(config-if)#^**Z**

Router#

- Thiết lập IPX Intervlan với RSM

Thực hiện những lệnh sau trong chế độ configuration

Task	**Command**
Step 1 (tùy chọn) Bật IPX routing trên router.	**Ipx routing**
Step 2 (tùy chọn) Xáx định một IPX routing protocol.	**router** *ipx_routing_protocol*
Step 3 Xác định cổng VLAN trên RSM.	**Interface** *vlan-id*

Step 4 Xác định một network number cho VLAN.	**ipx network** [*network* |unnumbered] **encapsulation** *encapsulation-type*
Step 5 Thoát khỏi chế độ configuration.	Ctrl-Z

Ví dụ :

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ipx routing**

Router(config)#**ipx router rip**

Router(config-ipx-router)#**network all**

Router(config-ipx-router)#**interface vlan100**

Router(config-if)#**ipx network 100 encapsulation snap**

Router(config-if)#**^Z**

Router#

- **Thiết lập INTERVLAN với RSFC**

Lệnh session *mod_num* (module logic của RSFC) giúp truy cập vào RSFC thông qua CLI.

Ví dụ:

Console> (enable) **session 15**

Trying Router-15...

Connected to Router-15.

Escape character is '^]'.

User Access Verification

Password:

Router>**exit**

Console> (enable)

- § Thiết lập IP Intervlan với RSFC

Thực hiện những lệnh sau trong chế độ configuration

Task	**Command**
Step 1 (tùy chọn) Bật IP routing trên router.	**ip routing**
Step 2 (tùy chọn) Xáx định một IP routing protocol.	**router** *ip_routing_protocol*
Step 3 Xác định cổng VLAN trên RSM.	**interface** *vlan-id*
Step 4 Xác định địa chỉ IP cho VLAN.	**ip address** *n.n.n.n mask*
Step 5Thiết lập tình trạng “up” cho cổng, nếu cần	**no shutdown**
Step 6 Thoát khỏi chế độ configuration.	Ctrl-Z

Ví dụ:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip routing

Router(config)#router rip

Router(config-router)#network 10.0.0.0

Router(config-router)#interface vlan 100

Router(config-if)#ip address 10.1.1.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#^Z

Router#

- § Thiết lập IPX Intervlan với RSFC

Thực hiện những lệnh sau trong chế độ configuration

Task	**Command**
Step 1 (tùy chọn) Bật IPX routing trên router.	**Ipx routing**
Step 2 (tùy chọn) Xáx định một IPX routing protocol.	**router** *ipx_routing_protocol*
Step 3 Xác định cổng VLAN trên RSM.	**interface** *vlan-id*
Step 4 Xác định một network number cho VLAN	**ipx network** [*network* |unnumbered] **encapsulation** *encapsulation-type*
Step 5Thiết lập tình trạng “up” cho cổng, nếu cần	no shutdown
Step 6 Thoát khỏi chế độ configuration.	Ctrl-Z

Ví dụ:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ipx routing

Router(config)#ipx router rip

Router(config-ipx-router)#network all

Router(config-ipx-router)#interface vlan100

Router(config-if)#ipx network 100 encapsulation snap

Router(config-if)#no shutdown

Router(config-if)#^Z

Router#

· **Thiết lập INTERVLAN với MSFC (họ switch 6000)**

Để truy cập vào MSFC từ cổng switch command-line, thực hiện lệnh:

Console> (enable) **switch console** [*mod_num*]

Với *mod_num* là số thứ tự module logic của MSFC

§ Thiết lập IP Intervlan với MSFC

Task	**Command**
Step 1 (tùy chọn) Bật IP routing trên router.	Router(config)# **ip routing**
Step 2 (tùy chọn) Xáx định một IP routing protocol.	Router(config)# **router** *ip_routing_protocol*
Step 3 Xác định cổng VLAN trên RSM.	Router(config)# **interface** *vlan-id*
Step 4 Xác định địa chỉ IP cho VLAN.	Router(config-if)# **ip addr**ess *n.n.n.n mask*

Step 5 Thoát khỏi chế độ configuration.	Router(config-if)# Ctrl-Z

Ví dụ:

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# ip routing

Router(config)# router rip

Router(config-router)# network 10.0.0.0

Router(config-router)# interface vlan 100

Router(config-if)# ip address 10.1.1.1 255.0.0.0

Router(config-if)# ^Z

Router#

- Thiết lập IPX Intervlan với MSFC: các lệnh cũng tương tự như với RSM

Ví dụ:

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# ipx routing

Router(config)# ipx router rip

Router(config-ipx-router)# network all

Router(config-ipx-router)# interface vlan100

Router(config-if)# ipx network 100 encapsulation snap

Router(config-if)# ^Z

Router#

IP MULTICAST MUTILAYER SWITCHING (IP MMLS)

Giới thiệu:

IP MMLS cũng tương tự như IP MLS, cung cấp 1 cách hiệu quả khả năng layer 3 cho phần cứng của switch thông qua vi mạch application-specific (ASIC) được tích hợp với phần cứng trong switch và bộ xử lý của router.

Chúc năng multicast được hỗ trợ khi địa chỉ của phần nơi gưi thuộc về nhóm những địa chỉ multicast. Những packet không được hỗ trợ đường dẫn đến đích thì vẫn được chuyển tiếp bằng phần mềm trên router.

Giao thức Independent Multicast (PIM) được dùng để tìm đường (route).

Hình sau cho thấy một mô hình IP multicast cơ bản gồm có switch layer 3 và một router nối ngoài:

Error!

Hình sau cho thấy một mô hình IP multicast cơ bản gồm có 1 switch layer 3 với RMS

Error!

Khái niệm về Layer 3 Multicast MLS Cache

Switch (tức là PFC trong họ catalyst 6000 và MMLS-SE trong họ catalyst 5000) nằm trong Layer 3 MLS cache chứa các luồng thông tin muticast. Mỗi phần tử trong cache có dạng: {source IP, destination group IP, source VLAN}.

Router và Switch trao đổi thông tin qua giao thức multicast Multilayer Switching (multicast MLSP).

Khi router nhận được 1 luồng thông tin mới, nó cập nhật bảng multicast routing và chuyển tiếp thông tin mới đó đến Switch bằng multicast MLSP. Ngoài ra, nếu 1 phần tử trong bảng multicast routing bị quá hạn, router sẽ xóa phần tử đó và chuyển tiếp thông tin vừa cập nhật cho Switch.

Lệnh **clear ip mrouter** để xóa bảng multicast routing.

Lệnh **no ip multicast-routing** để tắt quá trình IP multicast routing.

Quá trình hoạt động của IP MMLS

Quá trình hoạt động của IP MMLS cũng tương tự như quá trình hoạt động của IP MLS.

Switch (tức là MMLS-SE đối với họ switch 5000 hoặc là NFC đối với họ 6000), nhận được multicast packet có dạng như sau :

Frame Header		**IP Header**				**Payload**	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
Group G1 MAC	*Server A MAC*	*Group G1 IP*	*Server A IP*	*n*	*calculation 1*		

Sau đó Switch sửa lại packet thành dạng sau :

Frame Header		**IP Header**				**Payload**	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
Group G1 MAC	*MSFC MAC*	*Group G1 IP*	*Server A IP*	*n-1*	*calculation 2*		

Những phần mềm và phần cứng cần thiết

Supervisor engine software---Software release 5.1(1) or later

Cisco IOS router software---IOS release 12.0(3c)W5(8) or later

Catalyst 5000 family switch có Supervisor Engine II G or III G, or Supervisor Engine III or III F với NetFlow Feature Card II (NFFC II)

Routing platform hỗ trợ IP multicast MLS:

Họ Catalyst 5000 Route Switch Module (RSM) hoặc Route Switch Feature Card (RSFC)

Cisco 7500, 7200, 4500, hoặc 3600 router sử dụng cho kết nối bên ngoài.

Catalyst 8500 campus switch router (CSR) sử dụng cho kết nối bên ngoài.

Configuration

· **Configuring IP MMLS trên Router**

(Router ở đây tức là MLS-RP đối với họ switch Catalyst 5000 hoặc là MSFC đối với họ Catalyst 6000)

Bật chế độ IP multicast routing :

Task	**Command**
Bật chế độ IP multicast routing trên router.	Router(config)# **ip multicast-routing**

Ví dụ :

Router(config)# **ip multicast-routing**

Router(config)#

Ø Lưu ý : IP PIM (Protocol Independent Multicast) phải được bật trên các cổng cũa router kết nối đến switch trước khi có chức năng IP MMLS trên những cổng này

Task	**Command**
Bật IP PIM trên những	Router(config-if)# **ip pim** {**dense-mode** |

cổng của router.	**sparse-mode** | **sparse-dense-mode**}

Ví dụ bật PIM trên các cổng ở chế độ default(**sparse-dense-mode**):

Router(config-if)# **ip pim**

Router(config-if)#

Ví dụ bật PIM trên các cổng ở chế độ sparse:

Router(config-if)# **ip pim sparse-mode**

Router(config-if)#

Task	**Command**
Trình bày thông tin IP MMLS cho 1 cổng MSFC IP PIM trên router.	**show ip pim interface** [*type number*] **count**
Trình bày tình trạng hoạt động của IP MMLS trên một cổng của router.	**show ip interface**

Tắt IP MMLS

Task	**Command**
Tắt IP MMLS trên các cổng của router.	Router(config-if)# **no mls ip multicast**

Ví dụ:

Router(config-if)# **no mls ip multicast**

Router(config-if)#

Trình bày bảng IP multicast

Task	**Command**
Trình bày bảng IP multicast routing.	**show ip mroute** [*group*[*source*]]	[**summary**]	[**count**]	[**active** *kbps*]

Ví dụ:

Router# **show ip mroute**

IP Multicast Routing Table

Flags:D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned

R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT

Outgoing interface Flags: H - Hardware switched

Timers:Uptime/Expires

Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 224.0.1.40), 00:01:15/00:00:00, RP 0.0.0.0, flags:DJCL

Incoming interface:Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan800, Forward/Dense, 00:01:15/00:00:00

(*, 224.1.1.1), 00:01:14/00:02:59, RP 0.0.0.0, flags:DJC

Incoming interface:Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan5, Forward/Dense, 00:01:15/00:00:00

Vlan4, Forward/Dense, 00:01:15/00:00:00

Vlan3, Forward/Dense, 00:01:15/00:00:00

Vlan2, Forward/Dense, 00:01:15/00:00:00

(2.1.1.2, 224.1.1.1), 00:01:06/00:02:53, flags:CT

Incoming interface:Vlan800, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan2, Forward/Dense, 00:01:06/00:00:00, H

Vlan3, Forward/Dense, 00:01:06/00:00:00, H

Vlan4, Forward/Dense, 00:01:06/00:00:00, H

Vlan5, Forward/Dense, 00:01:06/00:00:00, H

Trình bày chi tiết thông tin MMLS trên router :

Task	**Command**
Trình bày chi tiết IP MMLS trên tất cả các cổng.	**show mls ip multicast** [[*group*[*source*][*vlan-id*]] | [*****]]
Trình bày tổng thể thông tin IP MMLS.	**show mls ip multicast summary**
Trình bày bảng thống kê IP MMLS.	**show mls ip multicast statistics**

Ví dụ cho thấy cách trình bày thông tin một mục IP MMLS trên router:

Router# **show mls ip multicast 224.1.1.1**

Multicast hardware switched flows:

(1.1.13.1, 224.1.1.1) Incoming interface: Vlan13, Packets switched: 61590

Hardware switched outgoing interfaces: Vlan20 Vlan9

MFD installed: Vlan13

(1.1.9.3, 224.1.1.1) Incoming interface: Vlan9, Packets switched: 0

Hardware switched outgoing interfaces: Vlan20

MFD installed: Vlan9

(1.1.12.1, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 62010

Hardware switched outgoing interfaces: Vlan20 Vlan9

MFD installed: Vlan12

(1.1.12.3, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 61980

Hardware switched outgoing interfaces: Vlan20 Vlan9

MFD installed: Vlan12

(1.1.11.1, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430

Hardware switched outgoing interfaces: Vlan20 Vlan9

MFD installed: Vlan11

(1.1.11.3, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430

Hardware switched outgoing interfaces: Vlan20 Vlan9

MFD installed: Vlan11

Total hardware switched installed: 6

Router#

Ví dụ sau trình bày thông tin tổng thể IP MMLS trên router:

Router# **show mls ip multicast summary**

7 MMLS entries using 560 bytes of memory

Number of partial hardware-switched flows:2

Number of complete hardware-switched flows:5

Router#

- **Configuring IP MMLS trên Switch**

(Switch ở đây tức là MLS-SE đối với họ switch Catalyst 5000 hoặc là PFC đối với

họ Catalyst 6000)

Để bật IP MMLS trên switch, làm những bước sau trong chế độ privileged:

Task	**Command**
Bật IP MMLS trên switch.	**set mls multicast enable**
Kiểm tra lại MMLS.	**show mls multicast**

Ví dụ:

Console> (enable) set mls multicast enable

Multilayer Switching for Multicast is enabled for this device.

Console> (enable)

Tắt IP MMLS trên Switch

Khi tắt IP MMLS trên switch, switch dừng quá trình multilayer switching IP multicast, bỏ tất cả những thông tin IP MMLS trong Layer 3 cache, và dừng tiến trình gửi multicast messages từ Router.

Để tắt IP MMLS trên switch :

Task	**Command**
Tắt IP MMLS trên switch.	**set mls multicast disable**
Kiểm tra lại MMLS.	**show mls multicast**

Ví dụ:

Console> (enable) set mls multicast disable

Multilayer Switching for Multicast is disabled for this device.

Console> (enable)

Trình bày thông tin IP cấu hình MMLS :

Task	**Command**
Trình bày 1 cách tổng thể thông tin cấu hình IP MMLS.	**show mls multicast**

Ví dụ:

Console> (enable) show mls multicast

Admin Status: Enabled

Operational Status: Active

Configured flow mask is {Destination-source-vlan flow}

Active Entries = 10

Router include list :

1.1.9.254 (Active)

1.1.5.252 (Active)

Console> (enable)

Trình bày bảng thống kê thông tin IP MMLS:

Task	**Command**
Trình bày bảng thống kê IP multicast trên Router.	**show mls multicast statistics** [*ip_addr*]

Ví dụ:

Console (enable) show mls multicast statistics

Router IP Router Name Router MAC

1.1.9.254 ? 00-50-0f-06-3c-a0

Transmit:

Delete Notifications: 23

Acknowledgements: 92

Flow Statistics: 56

Receive:

Open Connection Requests: 1

Keep Alive Messages: 72

Shortcut Messages: 19

Shortcut Install TLV: 8

Selective Delete TLV: 4

Group Delete TLV: 0

Update TLV: 3

Input VLAN Delete TLV: 0

Output VLAN Delete TLV: 0

Global Delete TLV: 0

MFD Install TLV: 7

MFD Delete TLV: 0

Router IP Router Name Router MAC

1.1.5.252 ? 00-10-29-8d-88-01

Transmit:

Delete Notifications: 22

Acknowledgements: 75

Flow Statistics: 22

Receive:

Open Connection Requests: 1

Keep Alive Messages: 68

Shortcut Messages: 6

Shortcut Install TLV: 4

Selective Delete TLV: 2

Group Delete TLV: 0

Update TLV: 0

Input VLAN Delete TLV: 0

Output VLAN Delete TLV: 0

Global Delete TLV: 0

MFD Install TLV: 4

MFD Delete TLV: 0

Console (enable)

Xóa bảng thống kê IP MMLS:

Task	**Command**
Xóa bảng thống kê IP MMLS trên switch.	**clear mls multicast statistics**

Ví dụ:

Console> (enable) clear mls multicast statistics

All statistics for the MLS routers in include list are cleared.

Console> (enable)

· **Trình bày những mục IP MMLS:**

Trình bày những mục IP MMLS của switch :

Task	**Command**
Trình bày những mục IP MMLS của switch	**Show mls multicast entry** [[[*mod*] [vlan *vlan_id*] [group *ip_addr*] [source *ip_addr*]]	[all]]

Ví dụ cho thấy cách trình bày tất cả những mục IP MMLS của switch :

Console> (enable) show mls multicast entry all

Router IP	Dest IP	Source IP	Pkts	Bytes	InVlan	OutVlans
1.1.5.252	224.1.1.1	1.1.11.1	15870	2761380	20	
1.1.9.254	224.1.1.1	1.1.12.3	473220	82340280	12	
1.1.5.252	224.1.1.1	1.1.12.3	15759	2742066	20	
1.1.9.254	224.1.1.1	1.1.11.1	473670	82418580	11	
1.1.5.252	224.1.1.1	1.1.11.3	15810	2750940	20	
1.1.9.254	224.1.1.1	1.1.12.1	473220	82340280	12	
1.1.5.252	224.1.1.1	1.1.13.1	15840	2756160	20	

1.1.9.254 224.1.1.1 1.1.13.1 472770 82261980 13

1.1.5.252 224.1.1.1 1.1.12.1 15840 2756160 20

1.1.9.254 224.1.1.1 1.1.11.3 473667 82418058 11

Total Entries: 10

Console> (enable)

Ví dụ cho thấy cách trình bày tất cả những mục IP MMLS cho một Router đặc biệt :

Console> (enable) show mls multicast entry 15

Router IP Dest IP Source IP Pkts Bytes InVlan OutVlans

--- --- --- --- --- --- ---

1.1.5.252 224.1.1.1 1.1.11.1 15870 2761380 20

1.1.5.252 224.1.1.1 1.1.12.3 15759 2742066 20

1.1.5.252 224.1.1.1 1.1.11.3 15810 2750940 20

1.1.5.252 224.1.1.1 1.1.13.1 15840 2756160 20

1.1.5.252 224.1.1.1 1.1.12.1 15840 2756160 20

Total Entries: 5

Console> (enable)

Ví dụ cho thấy cách trình bày tất cả những mục IP MMLS của 1 nhóm địa chỉ đích đến multicast :

Console> (enable) show mls multicast entry group 226.0.1.3 short

Router IP Dest IP Source IP InVlan Pkts Bytes OutVlans

--- --- --- --- --- --- ---

171.69.2.1 226.0.1.3 172.2.3.8 20 171 23512 10,201,22,45

171.69.2.1 226.0.1.3 172.3.4.9 12 25 3120 8,20

Total Entries: 2

Console> (enable)

Ví dụ cho thấy cách trình bày tất cả những mục IP MMLS của một Router và 1 nhóm địa chỉ nơi đi multicast

:

Console> (enable) show mls multicast entry 15 1.1.5.252 source 1.1.11.1 short

Router IP Dest IP Source IP Pkts Bytes

InVlan OutVlans

--- --- --- --- ---

--- ---

172.20.49.159 224.1.1.6 1.1.40.4 368 57776

40 23,25

172.20.49.159 224.1.1.71 1.1.22.2 99 65142

22 30,37

172.20.49.159 224.1.1.8 1.1.22.2 396 235620

22 13,19

Console> (enable)

Ví dụ về InterVLAN Routing

Ví dụ này bao gồm các phần sau

· **Example Network Topology**

- **Catalyst 5509 Configuration**
- **Catalyst 5505 Configuration**
- **RSFC Configuration**
- **Example Network Topology**
  - 03 VLANs (IP subnets):
    - VLAN 50 (172.16.50.0/24)
    - VLAN 150 (172.16.150.0/24)
    - VLAN 250 (172.16.250.0/24)
  - 03 VLAN interface cấu hình trên RSFC:
    - Interface vlan50 (172.16.50.1)
    - Interface vlan150 (172.16.150.1)
    - Interface vlan250 (172.16.250.1)
  - Cấu hình của Catalyst 5509:
    - Supervisor Engine III G và RSFC trên slot 1
    - 12 port 100-Mbps Fast Ethernet module trên slot 2
    - 2-slot 48 port 10-Mbps Ethernet module trên slot 6
  - Cấu hình của Catalyst 5505:
    - Supervisor Engine III và Gigabit Ethernet uplink ports trên slot 1
    - 2-slot 48 port 10-Mbps Ethernet module trên slot 3
  - Catalyst 5509 và Catalyst 5505 kết nối với nhau thông qua Gigabit EtherChannel ISL trunk link trên ports 1/1-2.
  - VTP domain: "Corporate"
  - Catalyst 5509: VTP server và Catalyst 5505: VTP client

Error!

Các bước cấu hình

1. Cấu hình VTP server và gán VTP domain name cho switch 5509
2. Cấu hình VTP client và gán VTP domain name cho switch 5505.
3. Tạo VLANs trên Catalyst 5509.
4. Cấu hình Gigabit EtherChannel ISL trunk link
5. Gán các port vào VLAN
6. Trên RSFC, tạo và gán IP addresses cho VLAN interfaces

Sau khi cấu hình xong, tất cả các port jtrên switch có thể kết nối được với nhau.

· **Catalyst 5509 Configuration**

Cat5509> (enable) **set VTP domain Corporate mode server**

VTP domain Corporate modified

Cat5509> (enable) **set vlan 50**

Vlan 50 configuration successful

Cat5509> (enable) **set vlan 150**

Vlan 150 configuration successful

Cat5509> (enable) **set vlan 250**

Vlan 250 configuration successful

Cat5509> (enable) **set port channel 1/1-2 desirable**

Port(s) 1/1-2 channel mode set to desirable.

Cat5509> (enable) **set trunk 1/1 desirable isl**

Port(s) 1/1 trunk mode set to desirable.

Port(s) 1/1 trunk type set to isl.

Cat5509> (enable) **set port duplex 2/1 full**

Port 2/1 set to full-duplex.

Cat5509> (enable) **set vlan 50 2/1**

VLAN 50 modified.

VLAN 1 modified.

VLAN Mod/Ports

---- ----------------------

50   2/1

Cat5509> (enable) **set port duplex 6/1 full**

Port 6/1 set to full-duplex.

Cat5509> (enable) **set vlan 150 6/1**

VLAN 150 modified.

VLAN 1 modified.

VLAN Mod/Ports

---- ----------------------

150   6/1

Cat5509> (enable)

- **Catalyst 5505 Configuration**

Cat5505> (enable) **set VTP domain Corporate mode client**

VTP domain Corporate modified

Cat5509> (enable) **set port duplex 3/1 full**

Port 3/1 set to full-duplex.

Cat5505> (enable) **set vlan 250 3/1**

VLAN 250 modified.

VLAN 1 modified.

VLAN Mod/Ports

---- ----------------------

250   3/1

Cat5505> (enable)

- **RSFC Configuration**

Console> (enable) **session 15**

Trying Router-15...

Connected to Router-15.

Escape character is '^]'.

RSFC>**enable**

RSFC#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

RSFC(config)#**interface vlan50**

RSFC(config-if)#**ip address 172.16.50.1 255.255.255.0**

RSFC(config-if)#**no shutdown**

RSFC(config-if)#**interface vlan150**

RSFC(config-if)#**ip address 172.16.150.1 255.255.255.0**

RSFC(config-if)#**no shutdown**

RSFC(config-if)#**interface vlan250**

RSFC(config-if)#**ip address 172.16.250.1 255.255.255.0**

RSFC(config-if)#**no shutdown**

RSFC(config-if)#^**Z**

RSFC#

Nâng cấp IOS image cho Catalys switch dùng TFTP Server

Tác giả Trương Quang Dũng

Error!

Dùng một máy trạm chạy hệ điều hành Windows có cài đặt phần mềm TFTP server.

Các IOS image lưu trữ tại đây

Kết nối TFTP server vào một port trên Management Vlan (Vlan 1)

Yêu cầu:

Cấu hình địa chỉ IP cho Management Vlan và , địa chỉ IP trên TFTP server

Error!

(Hai địa chỉ IP này cùng mạng) Đứng từ switch phải Ping thành công TFTP server,và ngược lại

Error!

TFTP server ping thành công Catalyst Switch

Chú ý:*Khi tiến hành nâng cấp IOS image, người dùng thường gặp một số vấn đề như sau:*

- *Đang load giữa chừng, xảy ra lỗi khiến cho IOS image mới không hoạt động được.*
- *Load thành công IOS image mới, nhưng phiên bản IOS image này không tương thích với dòng sản phẩn đang sử dụng, dẫn đến không dùng được.*

Trong cả hai trường hợp, IOS image cũ có thể bị ghi đè(overwrite) nếu dung lượng Flash memory không đủ lớn để chứa cả hai IOS image cùng lúc.

Kết quả, Switch/Router chỉ có thể hoạt động ở chế độ "rommon", tức hoạt động ở mức tối thiểu

Vì lý do đó, để tránh trường hợp này,trước khi load IOS image mới vào Flash memory của Switch, cần phải lưu lại IOS image hiện hành trên Flash menmory vào TFTP server để dự phòng, khi cần thiết, có thể khôi phục lại phiên bản IOS ban dầu cho thiết bị

Quy trình thực hiện:

- Khởi động phần mềm TFTP server, kiểm tra đường dẫn đến file IOS image
- Kiểm tra vị trí lưu trữ IOS image trên switch, ghi nhận lại các thông số về dung lương củng như tên của IOS image hiện hành. Cũng cần phải lưu ý xem dung lương của flash memory đủ lớn để chứa IOS

image mới hay không.

- Sao lưu IOS image hiện hành lên TFTP server để dự phòng.
- Load IOS image từ TFTP server vào flash memory.

Quy trình này giống nhau đối với các dòng sản phẩm Catalys Switch và Router của Cisco

Một số lưu ý khác:

-Tên của các phiên bản IOS image thường ký hiệu bằng các ký tự và kết thú là"**.bin**"

Mỗi ký tự thường thể hiện các tính năng mà phiên bản IOS image hỗ trợ.

Do đó khuyếnn cáo người dùng nên giữ nguyên tên của IOS image khi di chuyển các file này, và luôn nhớ kết thúc tên file là "**.bin**"

VD: **c2950-i6q142-mz.121-11.bin**

Bước 1: Khởi động phần mềm TFTP server

Error!

Bước 2: Kiểm tra vị trí lưu trữ IOS image, ghi nhận chính xác tên của IOS image hiện hành. Bên cạnh đó, kiểm tra xem dung lượng của Flash memory có đủ sức chứa IOS image mới hay không..

Switch#dir flash:

Directory of flash:/

2 -rwx 0 Mar 01 1993 00:59:13 env_vars

3 -rwx 3993344 Mar 01 1993 00:29:59 c3550-i5q3l2-mz.121-13.EA1a.bin

4 -rwx 43 Mar 01 1993 00:59:13 system_env_vars

6 -rwx 1625 Mar 01 1993 00:13:57 starup-config

15998976 bytes total (12001792 bytes free)

Switch#

**Ghi nhận đường dẫn*

flash:c3550-i5q3l2-mz.121-13.EA1a.bin

Bước 3:Sao lưu IOS image hiện hành lênn TFTP ser ver để dự phòng

Switch#copy flash:c3550-i5q3l2-mz.121-13.EA1a.bin tftp

Address or name of remote host []? 10.0.0.2

Destination filename [c3550-i5q3l2-mz.121-13.EA1a.bin]? y

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!!!!!!!!!!!!!!!!!!!!!!

3993344 bytes copied in 19.972 secs (199947 bytes/sec)

Switch#

*Trong quá trình sao chép, khai báo địa chỉ TFTP server, trong trường hợp này, giữ nguyên tên của IOS image khi sao lưu lên TFTP server

Bước 4:Upgrade IOS image từ TFTP server vào Flash memory

*Cần chú ý: filename của các tập tin loại này luôn phải kết thúc "**.bin**"

Switch#copy tftp:**c3550-i5q3l2-mz.121-13.EA1a.bin** nvram

Address or name of remote host [10.0.0.2]?

Source filename [**c3550-i5q3l2-mz.121-13.EA1a.bin**]?

Destination filename [nvram]? **c3550-i5q3l2-mz.121-13.EA1a.bin**

%Warning:There is a file already existing with this name

Do you want to over write? [confirm]y

Accessing tftp://10.0.0.2/**c3550-i5q3l2-mz.121-13.EA1a.bin**...

Loading **c3550-i5q3l2-mz.121-13.EA1a.bin** from 10.0.0.2 (via Vlan1):

!O!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

!!!

[OK - 3993344 bytes]

3993344 bytes copied in 105.760 secs (37759 bytes/sec)

Switch#

Quy trình cũng tương tự khi sao chép các file khác nhau trên switch, chỉ khác nhau ở vị trí.

Làm việc với các File khác

Switch#dir nvram:

Directory of nvram:/

382 -rw- 1483 <no date> startup-config

383 ---- 5 <no date> private-config

393216 bytes total (391676 bytes free)

Switch#

Lưu file **startup-config** từ NVRAM vào TFTP server.

Switch#copy nvram:startup-config tftp

Address or name of remote host []? 10.0.0.2

Destination filename [switch-confg]? y

!!!!

1483 bytes copied in 0.032 secs (46344 bytes/sec)

Switch#

Đây là một trong những cách sao lưu cấu hình mạng rất hiệu quả. Về sau, muốn cấu hình nhanh, người dùng chỉ cần kết nối thiết bị theo đồ hình cũ, sau đó Download cấu hình từ TFTP server về để hệ thống hoạt động

Download cấu hình từ TFTP server vào NVRAM

Switch#copy tftp:**cauhinhmau** nvram

Address or name of remote host []? 10.0.0.2

Destination filename [nvram]? **startup-config**

Accessing tftp://10.0.0.2/**cauhinhmau**...

Loading **cauhinhmau** from 10.0.0.2 (via Vlan1):

!!!!

[OK - 1483 bytes]

1483 bytes copied in 0.056 secs (26482 bytes/sec)

Open Shortest Path First (OSPF)

Tác giả: Trần Văn Thành

Open Shortest Path First (OSPF) được phát triển bởi Internet Engineering Task Force (IETF) như một sự thay thế những hạn chế cũng như nhược điểm của RIP.

OSPF là một link state protocol, như tên gọi của mình nó sử dụng thuật toán Dijkstra'' Shortest Path First (SPF) để xây dựng routing table và open nói nên tính phổ biến của nó. OSPF đã được John Moy đưa ra thông qua một số RFC, gần đây nhất là RFC 2328.

Giống như các link state protocol, OSPF có ưu điểm là hội tụ nhanh, hỗ trợ được mạng có kích thước lớn và không xảy ra routing loop. Bên cạnh đó OSPF còn có những đặc trưng sau:

Sử dụng area để giảm yêu cầu về CPU, memory của OSPF router cũng như lưu lượng định tuyến và có thể xây dựng hierarchical internetwork topologies.

Là giao thức định tuyến dạng clasless nên hỗ trợ được VLSM và discontigous network.

OSPF sử dụng địa chỉ multicast 224.0.0.5 (all SPF router) 224.0.0.6 (DR và BDR router) để gửi các thông điệp Hello và Update.
OSPF còn có khả năng hỗ trợ chứng thực dạng plain text và dạng MD5.
Sử dụng route tagging để theo dõi các external route.
OSPF còn có khả năng hỗ trợ Type of Service.

1. Thuật ngữ

Router ID:

Chính là địa chỉ IP cập nhật của loopback interface.

Nếu không có loopback interface được cấu hình thì Router ID sẽ là địa chỉ cập nhật của physical interface.

Người ta sử dụng địa chỉ loopback vì 2 nguyên nhân sau:

Loopback interface ổn định hơn bất kỳ physical interface nào. Và nó luôn luôn active khi router hoạt động, chỉ fail khi toàn bộ router fail.

Người quản trị mạng điều khiển hoạt động của OSPF trong quá trình bình bầu DR và BDR.

Designated Router (DR): Để ngăn chặn tình trạng storm LSA trong multi-access network một DR được bầu ra trong multi-access network. DR có những nhiêm vụ sau:

Đại diện cho multi-access network và gắn bó với phần còn lại internetwork.

Để quản lý quá trình flood xử lý trên multi-access network.

Backup Designated Router (BDR): một vấn đề quan trọng với sự xắp xếp DR là khi DR bị fail, một new DR phải được xác định. Adjacency mới phải được thiết lập lại và tất cả Router trên mạng phải đồng bộ lại database của chúng với new DR. Trong suốt quá trình này thì mạng không gửi dữ liệu được.

Để ngăn chặn điều này người ta đưa ra khái niệm BDR. Tất cả các router không chỉ thiết lập adjacency với DR mà còn với BDR. Nếu DR bị fail thì BDR sẽ trở thành DR mới mà không ph3ai đồng bộ lại database của chúng.

2. Operation of OSPF

Hoạt động của OSPF có thể tóm tắt trong 7 bước sau:

Các OSPF-speaking router gửi các Hello packet ra tất cả các OSPF-enable interface. Nếu 2 router sau khi trao đổi Hello packet và thoả thuận một số thông số chúng sẽ trở thành neighbor.

Adjacency có thể được tạo qua virtual point-to-point link hay được tạo qua một vài

neighbor. OSPF định nghĩa ra một số loại network và một số loại router. Sự thiết lập một adjacency được xác định bởi loại router trao đổi Hello và loại network mà Hello trao đổi qua.

Mỗi router gửi các link state advertisement (LSA) qua tất c adjacency. LSA mô tả tất cả các interface của router (link) và trạng thái của link. Các link này có thể là stub network, tới OSPF router khác, tới network trong cùng một area, tới external network. Do có rất nhiều loại link state information cho nên OSPF định nghĩa ra đến 11 loại LSA.

Mỗi router nhận một LSA từ neighbor với link state database của neighbor đó và gửi một copy của LSA tới tất cả neighbor khác của nó.

Bằng cách flooding các LSA toàn bộ một area, tất cả router sẽ xây dựng chính xác link state database.

Khi database được hoàn tất, mỗi router sử dụng thuật toán SPF để xây dựng nên SPF tree.

Mỗi router sẽ xây dựng nên routing table từ SPF tree.

2.1. Neighbor và Adjacency

Trước khi bất kỳ LSA nào được gửi, OSPF router phải khám khám phá neighbor của chúng và thiết lập adjacency. Các neighbor sẽ được ghi lại vào trong neighbor table, cùng với link (interface) mà trên đó neighbor được định vị và thông tin cần thiết để duy trì neighbor.

a/ Hello protocol

Hello protocol có đặc trưng sau:

Nó là cách thức mà neighbor được khám phá.
Nó quảng bá một vài thông số mà qua đó 2 router phải đồng ý trước khi chúng trở thành neighbor.

Hello packet hoạt động giông như keepalive giữa các neighbor.
Đảm bảo thông tin 2 chiều giữa các neighbor.
Bình bầu DR và DBR đối với môi trường multiaccess.

OSPF-speaking router đều đặn gửi Hello packet ra tất cả OSPF-enable interface. Khoảng thời gian này gọi là HelloInterval, mặc định khoảng thời gian này là 10 giây và ta có thể thay đổi nó. Nếu router không nhận được Hello từ neighbor sau khi hết thời gian RouterDeadInterval (gấp 4 lần HellInterval) nó sẽ công bố neighbor bị down.

b/ Network types

OSPF định nghĩa 5 loại network:

Point-to-point network: như là T1 hay subrate link kết nối một cặp router. Valid neighbor trên point-to-point network luôn luôn trở thành adjacency. The destination address của OSPF packet luôn luôn là địa chỉ 224.0.0.5.

Broadcast network: như là Ethernet, Token Ring và FDDI. Broadcast network là multi-access trong đó có khả năng kết nối nhiều hơn 2 thiết bị và chúng là broadcast có nghĩa là tất cả các thiết bị có thể nhận được gói tin khi chỉ có một gói được truyền một lần. OSPF router trên broadcast network sẽ bình bầu DR và BDR sẽ được đề cập trong phần sau.

NBMA network: như là X.25, Frame Relay và ATM. Chúng có khả năng kết nối nhiều hơn 2 router nhưng không có khả năng broadcast. Có nghĩa là một packet được gửi bởi một router sẽ không thể được nhận bởi tất cả các router khác. Các OSPF router trên mạng NBMA có bình bầu DR và BDR nhưng tất cả OSPF packet đều là unicast.

Point-to-multipoint network: nó là một trường hợp đặc biệt trong cấu hình của NBMA network. Router trên các mạng này không có quá trình bình bầu DR và BDR và các OSPF packet được gửi dưới dạng multicast.

Virtual link: là trường hợp đặc biệt trong cấu hình. OSPF packet được gửi dưới dạng unicast qua virtual link.

c/ Bình bầu DR và BDR

Quá trình bình bầu DR và BDR được kích hoạt bởi interface state machine, để quá trình bình bầu được thực hiện thì một số điều kiện sau phải tồn tại:

Mỗi interface của router mà nối vào multi-access network có một Router priority, là một số nguyên từ 0 đến 255. Đối với các Cisco router thông số này có giá trị mặc định là 1. Router với priority là 0 sẽ bị loại khỏi quá trình bình bầu DR và BDR.

Hello packet phải có trường để cho router gửi xác định Router priority và IP address của interface của router để bình bầu DR và BDR.

Khi một interface lần đầu trở thành active trên multi-access network, nó thiết lập trường DR và BDR có giá trị là 0.0.0.0. Và nó cũng thiết lập wait timer cùng với giá trị Router DeadInterval.

Tồn tại interface trên multi-access network ghi lại address của DR và BDR trong interface data structure.

Quá trình bình đầu DR và BDR diễn ra theo các trình tự sau:

Sau khi 2-Way state được thiết lập với một hay nhiều neighbor, trường Priority, DR và BDR sẽ được xem xét trong Hello của neighbor. Danh sách tất cả router đủ tư cách tham gia bình bầu được thiết lập .(router có priority lớn hơn 0 và neighbor của nó ở trạng thái 2-Way state); tất cả router công bố chúng là DR (interface addresss của chúng được lưu trong trường DR của Hello packet); và tất cả các router công bố chúng là BDR (interface address của chúng được lưu trong trường BDR của Hello packet).

Từ danh sách những router đủ tư cách, nó sẽ tạo một subset những router không đòi hỏi là DR.

Nếu một hoặc nhiều hơn neighbor trong subset này chứa interface address của nó trong trường BDR, neighbor với highest priority sẽ công bố là BDR. Nếu priority bằng nhau thì neighbor với highest router ID sẽ được chọn.

Nếu có một hoặc nhiều hơn eligible router có interface address của nó trong trường DR thì neighbor với highest priority sẽ công bố là DR. Nếu priority bằng nhau thì neighbor với highest Router ID sẽ được chọn là DR.

Nếu không có router công bố là DR thì BDR sẽ trở thành DR.

Nếu router thực hiện hiện tính toán là DR hay BDR mới được bầu chọn hay chưa bình bầu được DR, BDR thì thực hiện repeat từ bước 2 đến bước 6.

Chú ý: khi một OSPF router trở thành active và khám phá neighbor của

nó, nó sẽ kiểm tra hiệu lực của DR và BDR.

Nếu DR và BDR tồn tại thì router sẽ chấp nhận nó.

Nếu BDR không tồn tại, quá trình bình bầu BDR sẽ diễn ra và router với highest priority sẽ trở thành BDR. Nếu priority bằng nhau thì router có highest router ID sẽ trở thành BDR.

Nếu không có active DR thì BDR tăng cấp làm DR và quá trình bình bầu BDR mới bắt đầu.

d/ Neighbor States

Down: Không có Hello packet được nhận từ neighbor.
Attempt: Neighbor phải cấu hình bằng tay cho trạng thái này. Nó chỉ áp dụng chỉ cho NBMA network connection và cho biết rằng không có thông gần đây được nhận từ neighbor.

Init: Một Hello packet được nhận từ neighbor nhưng local router không nhìn thấy nó trong Hello packet. Bi-directional communication chưa được thiết lập.

2-Way: Hello packet được nhận từ neighbor và chứa đựng Router ID trong trường Neighbor. Bi-directional communication được thiết lập.

ExStart: Quan hệ Masterr/Slave được thiết lập bằng cách trao đổi Database Description (DD) packet. Router với highest Router ID sẽ trở thành Master.

Exchange: thông tin định tuyến được trao đổi thông qua DD và LSR packet.

Loading: Link-State Request packet được gửi tới neighbor để yêu cầu cho bất kỳ LSA mới được tìm thấy trong state Exchange.

Full: tất cả LSA được đồng bộ giữa các adjacency.

e/Xây dựng một Adjacency

Neighbor trên point-to-point, point-to-multipoint, và virtual link network luôn luôn trở thành adjacency trừ phải những thông số trong Hello packet không sao khớp. Trên Broadcast và NBMA network, thì DR và BDR sẽ trở thành adjacency với tất cả neighbor nhưng không có adjacency giữa cac Drother.

Quá trình xây dựng Adjacency sử dụng 3 loại OSPF packet:

Database Description packet (type 2)
Link State Request packet (type 3)
Link State Update packet (type 4)

Database Description packet có vai trò đặc biệt quan trọng trong quá trình xây dựng adjacency. Như tên gọi của mình, nó mang thông tin mô tả tóm tắt của mỗi LSA trong Link state database của router gửi. Những thông tin mô tả này không phải là các LSA trọn vẹn mà chỉ đơn thuần là header của chúng-trong DD packet có 3 flag để điều khiển quá trình xây dựng adjacency.

Bit I (Initial), nó được thiết lập để cho biết DD packet đầu tiên được gửi.
Bit M (More), nó được thiết lập để cho biết rằng đó không phi là DD packet cuối cùng được gửi.

Bit MS (Master/Slave), nó được thiết lập để cho biết DD packet được gửi bởi Master router.

Hình sau: sẽ mô tả tiến trình xây dựng một adjacency.

Error!

Bước 1: RT1 trở thành active trên multi-access network và gửi Hello packet. Do chưa nhận được bất kỳ Hello nào từ neighbor cho nên trong Hello packet trường Neighbor là empty và trường DR và BDR được thiết lập với giá trị là 0.0.0.0.

Bước 2: Sau khi nhận được Hello packet từ RT1, RT2 tạo một neighbor data structure cho RT1 và thiết lập trạng thái của RT1 là Init. RT2 gửi một Hello packet với router ID của RT1 trong trường Neighbor. Như DR, thông tin interface address của RT2 có trong trường DR của Hello packet.

Bước 3: Sau khi RT1 nhận được Hello packet từ RT2 và kiểm tra thấy Router ID của mình có trong đó, RT1 tạo một neighbor data structure cho RT2 và thiết lập trạng thái của RT2 là ExStart cho sự tho thuận master/slave. Sau đó RT1 gửi một empty DD packet (no LSA summary), trong đó DD sequence number được gán là x, bit I = 1 cho biết đây là DD packet đầu tiên được trao đổi, bit M = 1 cho biết đây không phi là DD packet cuối cùng, bit MS = 1 cho biết RT1 xác nhận là master.

Bước 4: RT2 chuyển trạng thái của RT1 sang trạng thái Exstart dựa trên DD packet mà nó nhận được từ RT1. Sau đó nó cũng trả lời RT1 bằng một DD packet với DD sequence number là y; RT2 có higher router ID hơn RT1 cho nên nó thiết lập bit MS = 1.Giống DD packet đầu tiên, nó chỉ sử dụng để thoả thuận ra master/slave do đó nó là một empty DD packet.

Bước 5: RT1 đồng ý là RT2 là master và chuyển trạng thái của RT2 sang Exchange. RT1 gửi một DD packet với DD sequence number là y, MS = 0 cho biết nó là slave. Đây là một packet có chứa LSA header từ Link State Summary list của RT1.

Bước 6: RT2 chuyển trạng thái của neighbor của nó sang Exchange dựa trên DD packet mà nó nhận được từ RT1. Nó sẽ gửi một DD packet bao gồm LSA header từ Link State Summary list và tăng giá trị DD sequênc number lên là y +1.

Bước 7: RT1 gửi một ACK packet bao gồm giá trị DD sequence number giống DD sequence number của DD packet gửi từ RT2. Quá trình tiếp tục, RT2 gửi một DD packet và đợi cho một ACK packet từ RT1 trước khi gửi một một DD packet kế tiếp. Khi RT2 gửi DD packet với LSA summary cuối cùng thì nó thiết lập bit M = 0.

Bước 8: Sau khi nhận các DD packet và ACK packet sẽ gửi chứa đựng LSA summary cuối cùng của nó cho neighbor từ Link State Summary list, RT1 biết rằng quá trình Exchange đã xong. Tuy nhiên nó có mục nhập trong Link State Request list của nó, do đó nó chuyển sang trạng thái Loading.

Bước 9: Khi RT2 nhận DD packet cuối cùng của RT1, RT2 chuyển trạng thái của RT1 sang full bởi vì RT1 không có mục nhập trong Link State Request list của nó.

Bước 10: RT1 gửi các Link State Request packet và RT2 gửi trả lời bằng các LSA trong các Link State Update packet. Đến khi Link State Request list của RT1 là empty thì RT1 sẽ chuyển trạng thái của RT2 sang full.

2.2 LSA Flooding

Để mỗi node đưa các route một cách thích hợp chính xác qua mang, liên mạng thì mỗi node phải có một topology database của toàn mạng.

Database này bao gồm tất cả các LSA mà router nhận được. Bất cứ một sự thay đổi mạng nào đều được thể hiện trong các LSA. Flooding là quá trình khi một sự thay đổi suy ra thì các LSA mới được gửi qua mạng để đảm bảo rằng database của mỗi node được update và giống y hệt các database của node còn lại khác.

Quá trình flooding được tạo bởi 2 loại gói sau:

Link State Update packets (type 4)

Link State Acknowledgment packets (type 5)

Trên point-to-point network, Link State Update packet được gửi bằng địa chỉ multicast là 224.0.0.5.

Trên point-to-multipoint network và virtual link network, Link State Update packet được gửi dưới dạng unicast tới interface address của adjiaceny của nó.

Trên broadcast network, Drother chỉ là adjacency với DR và BDR. Do đó update packet được tới DR và BDR với địa chỉ là 224.0.0.6. Sau đó chỉ có DR router gửi update dưới dạng multicast với địa chỉ 224.0.0.5 tới tất cả các DRother router. Tiếp đó các DR, BDR router, DRother router flood LSA ra tất cả các interface còn lại.

Trên mạng NBMA network (full), quá trình trên cũng tương tự như vậy trừ điểm sau là các LSA được gửi dưới dạng unicast.

Mỗi một LSA riêng lẻ được truyền đều phải được báo nhận. Điều này được thực hiện bằng một trong các cách sau:

Implicit acknowledgment: neighbor thực hiện báo nhận cho một LSA bằng cách gửi lại một Link State Acknowledgement về nơi gửi.

Implicit acknowledgement: neighbor thực hiện báo nhận cho một lSA bằng cách gửi một copy của LSA về cho nơi gửi.

2.3. Tính toán SPF tree

Shortest Path First (SPF) là những tuyến đường qua mạng tới bất kỳ destination nào. Có 2 loại destination được thừa nhận trong OSPF:

Network
Router: là các area border router (ABR) và autonomous system boundary router (ASBR).

Chỉ một lần sau khi tất cả các OSPF router đồng bộ được link state database, mỗi router sẽ tính toán SPF tree cho mỗi destination mà nó biết. Sự tính toán này được thực hiện bởi thuật toán Dijkstra.

Error!

Metric của OSPF

OSPF đề cập đến metric là cost. Cost của toàn tuyến là tổng của cost của các outgoing interface dọc theo tuyến đường đó. Cách tính cost được IETF đưa ra trong RFC 2328. Cisco đã thực thi cách tính cost của riêng mình như sau: 108/bandwidth với giá trị bandwidth được cấu hình cho mỗi interface.

3. OSPF với Multi-Area

Như ta đã biết khi kích thước mạng càng lớn thì số lượng các LSA càng lớn, kich thước database sẽ rất lớn…Chính những điều đó sẽ làm tăng yêu cầu về CPU cũng như memory của OSPF router. Để giải quyết vấn đề trên OSPF đã đưa ra kỹ thuật Multi-Area.

3.1. Ưu điểm của Multi-Area

Mỗi router phải chia sẻ một link state database giống hệt nhau chỉ với router trong cùng area với chính nó chứ không phải là toàn mạng. Do đó giảm được kích thước của database dẫn tới giảm yêu cầu tới phần cứng của router như: memory.

Giảm kích thước link state database có nghĩa là giảm số lượng LSA phải xử và do đó giảm tác động trên CPU.

Bởi vì link state database chỉ phải duy trì database trong một area cho nên hầu hết flooding chỉ giới hạn trong một area.

3.2. Mộ số khái niệm

Intra-area traffic: bao gồm những packet mà trao đổi giữa các router trong cùng một area.

Inter-area traffic: bao gồm những packet mà trao đổi giữa các router thuộc các area khác nhau.

External traffic: bao gồm những packet mà trao đổi giữa một router trong một OSPF domain và một router thuộc một Autonomous system khác.

Internal Router: là những router mà tất cả các interface của nó đều thuộc cùng một area. Những router này chỉ có một link state database.

Area Border Routers (ABR): kết nối một hay nhiều area với backbone và đóng vai trò như là một gateway cho Intra-area traffic. Một ABR luôn luôn có ít nhất một interface thuộc vào backbone và phải duy trì nhiều link state database tách biệt, mỗi database cho một area. Do đó ABR thường có memory và processor cao hơn internal router. Một ABR sẽ summarize topology information của area không phải là area 0 mà nó kết nối vào backbone, backbone sẽ nhân bản summary information tới area khác.

Backbone Router: là những router mà ít nhất nó gắn với backbone. Do đó ABR cũng là Backbone Router. Và một Internal Router mà interface thuộc vào area 0 cũng là Backbone Router.

Autonomous System Boundary Routers (ASBR): là gateway cho external traffic đưa những route vào OSPF domain mà đã được học từ một số protocol khác như là: BGP và IEGRP. Một ASBR có thể được xác định ở bất cứ vị trí nào trong OSPF antonomous system; Nó có thể là Internal, Backbone hay ABR.

Virtual Link: là một link tới backbone xuyên qua một non-backbone area.

Link State Dabase: tất cả valid LSA mà rouer nhận được được lưu trong link state database của nó. Tuyển tập các LSA sẽ tạo ra topology của area.

3. 4. Các loại LSA.

Do có nhiều loại router được định bởi OSPF do đó cũng cần thiết phải định nghĩa ra các loại LSA. Cụ thể như sau:

Error!

3.5. Một số loại Area trong OSPF (OSPF Area Types)

a/ Stub Area

Một stub area là một area mà các External LSA không được flood vào trong area đó. Trong stub area sẽ không có LSA loại 4 và 5 hay những LSA đó bị block. ABR

tại cạnh của stub area sẽ sử dụng Network Summary để quảng bá một default route (destination là 0.0.0.0) vào trong area. Bất cứ destination của Internal Router không thể match tới một intra hay inter area, route đó sẽ được match với default route. Bởi vì default route được mang bởi LSA loại 3, nó sẽ không được quảng bá ra ngoài area.
Sự thực thi của router trong stub area được cải thiện, memory được bảo tồn và giảm kích thước database của chúng. Tất nhiên sự cải thiện này càng rõ ràng trong internetwork với rất nhiều LSA loại 5.

Bên cạnh đó nó vẫn mang những nhược điểm của mình:

Như bất kỳ area nào, tất cả router trong stub area phải có một link state database giống hệt nhau. Để đảm bảo điều kiện này, tất cả các stub router sẽ thiết lập một flag (bit_E) trong Hello packet là 0. Chúng sẽ không chấp nhận bất cứ Hello packet nào có bit_E là 1, kết quả là adjacency không được thiết lập với bất cứ router nào không được cấu hình là stub router.

Virtual link không được cấu hình trong stub area.

Không có router nào trong stub area có thể là ASBR. Vì trong stub area không có LSA loại 5.

Một stub area có thể có hơn một ABR nhưng bởi vì sử dụng defaul route, Internal router không thể xác định được router nào sẽ là gateway tối ưu tới ASBR.

b/ Totally Stubby Areas

Totally stubby area: sử dụng default không chỉ cho destination external tới autonomous system mà còn cho destination external tới area. ABR của totally stubby area sẽ không chỉ block AS External LSA mà còn block tất c Summary LSA trừ LSA loại 3 nào để quảng bá default route.

c/ Not-So-Stubby Area

Not-so-stubby areas(NSSA): cho phép external route được quảng bá vào trong OSPF autonomous system trong khi dữ lại những đặc tính còn lại của stub area. Cụ thể là ASBR trong một NSSA sẽ sinh ra LSA loại 7 để quảng bá external destination. Những External LSA được flood khắp NSSA area nhưng chúng sẽ bị block tại ABR.

Error!

Tóm lại ta có bảng tổng kết sau:

Error!

4. Định dạng gói tin OSPF
OSPF packet được đóng gói trong IP packet tương ứng với trường Protocol number là 89, do vậy maximum của OSPF packet là 1500 octet. OSPF packet header là giống đối với các loại OSPF packet khác nhau nhưng OSPF packet data thì biến đổi tuỳ theo loại OSPF packet.

Error!

Chú ý: IP packet với protocol number = 89 thì trường TTL luôn luôn bằng 1 để đảm bảo rằng packet không bao giờ đi quá một hop.

4.1. The Packet Header

Tất cả các OSPF packet đều có chung một dạng như sau:

Error!

Trong đó:
Version: là phiên bản OSPF, phiên bản gần đây nhất là 2.
Type: xác định ra loại OSPF packet. Có 5 loại OSPF packet như sau:

Error!

Packet length: là độ dài của OSPF packet gồm cả header (đơn vị là octet).
Router ID: là ID của router gửi.
Area ID: là area mà từ đó packet được gửi. Nếu packet được gửi qua virtual link, Area ID sẽ là 0.0.0.0 (backbone Area ID) bởi vì virtual link luôn được gắn với backbone.
Checksum: kiểm tra toàn bộ packet kể của header.
AuType: xác định loại nhận thực được sử dụng. Bảng sau là cấc loại nhận thực có thể:

Error!

a/ The Hello Packet
Hello packet được dùng để thiết lập và duy trì adjiacecy. Hello packet mang những thông số mà neighbor phải đồng ý để trở thành adjacency.

Error!

Network Mask: là address mask của interface mà packet được gửi từ đó. Nếu mask này không match với interface mà packet được nhận thì packet sẽ bị drop.

Hello Interval: là chu kỳ gửi bản tin Hello, được tính bằng giây. Nếu router gửi và nhận không có cùng thông số này nó sẽ không thiết lập quan hệ neighbor.

Options: trường này trong Hello packet đảm bảo ràng neighbor có khả năng tương thích. Router có thể từ chối một neighbor nếu khả năng này là không tương thích.

Router Priority: được sử dụng để bình bầu DR và BDR. Nếu nó được thiết lập giá trị là 0 thì sẽ loại khỏi quá trình bình bầu DR và BDR.

Router Dead Interval: là số giây mà router gửi đợi một Hello packet từ neighbor trước khi công bố neighbor dead. Nếu thông số này trong Hello đến không giống với thông số của nó thì packet sẽ bị drop.

Designated Route: là IP address của interface của DR trên mạng (không phải là Router ID của nó).

Backup DR: là IP address của interface của BDR trên mạng.

Neighbor: chứa danh sách tất cả neighbor trên mạng mà router gửi nhận từ các Hello hợp lệ.

b/ The Database Description Packet

Database Description packet: nó được sử dụng khi một adjacency được thiết lập. Mục đích chính của DD packet là mô tả một vài hay tất cả LSA trong database cho đến khi nào có thẻ xác định là match LSA trong database của nó.

Error!

Interface MTU: là kích thước lớn nhất của IP packet (đơn vị là octet) mà packet có thể được gửi đi mà không bị phân mảnh. Trường này được thiết lập là 0x0000 khi

packet được gửi qua virtual link.

Option: là trường tuỳ chọn, router sẽ không chuyển tiếp LSA nếu không thoả mãn điều kiện trong trường Option.

Có 5 bit không sử dụng và có giá trị là: 00000b.

Ba bit I, M và MS đã giới thiệu trong phần building adjacency.

DD Sequence Number: trường này để đảm bảo rằng DD packet được nhận đúng thứ tự trong quá trình đồng bộ database. Thông số này luôn luôn được thiết lập bởi master cho DD packet đầu tiên và tăng dần lên trong các DD packet gửi sau.

LSA Header: danh sách của một vài hay tất cả LSA header trong link state database của router gửi.

c/ The Link State Request Packet

Trong quá trình đồng bộ database khi router nhận các DD packet, router sẽ kiểm tra xem LSA header trong DD packet nếu không có trong database của nó thì những LSA này ghi lại vào Link State Request list. Router sẽ gửi một hay một vài Link State Request packet hỏi neighbor về LSA đó.

Định dạng của Link State Request packet như sau:

Error!

Link State Type: xác định loại LSA (router LSA, network LSA...).
Link State ID: xác định ra LSA header.\
Advertising Router: là router ID của router mà gửi LSA.

d/ The Link State Update Packet

Nó được sử dụng khi flood LSA và gửi LSA trả lời cho Link State Request packet.

Error!

Number of LSAs: xác định số LSA trong packet này.
LSAs: là full LSA (header + data). Mỗi update có thể mang nhiều LSA tới maximum kích thước của packet cho phép trên link.

f/ The Link State Acknowledgment Packet

Được sử dụng để tạo quá trình flood các LSA môt cách tin cậy (reliable).
Định dạng như sau:

Error!

OSPF Network type

OSPF chạy trên nhiều loại media khác nhau . Đối với OSPF , media có thể chia ra làm 4 loại sau :

- Multiaccess media
- Point-to-point media
- Nonbroadcast multi-access media
- Demand on Circuits

Multiacces media :

Multiaccess media bao gồm các loại sau : Ethernet ,Fast Ethernet , Gigabit Ethernet , FDDI , TokenRing , …. Đối với các media loại này , default OSPF sẽ gán network type là broadcast . Do vậy , ta không cần cấu hình gì thêm , ví dụ :

Error!

3 Router A , B , C chạy OSPF trên mạng multi-access , OSPF sẽ default gán default network là broadcast . Qua trình bầu chọn DR , BDR sẽ diễn ra . DR/BDR sẽ lắng nghe địa chỉ multicast 224.0.0.6 (all DR routers) , các router khác sẽ lắng nghe địa chỉ multicast 224.0.0.5 (all DR others) . Router A có priority cao nhất à DR . Router B, C có cùng priority nên sẽ xét tiếp highest ip address . Router B có ip address cao hơn à BDR .

Point-to-point media :

Bao gồm các loại sau : HDLC và PPP encapsultation links , FrameRelay/ATM point-to-point subinterfaces ,…Tương tự OSPF sẽ default gán cho các media loại này là point-to-point . Quá trinh bầu chọn DR/BDR sẽ không cần thiết nữa . Các router sẽ trao đổi thông tin qua địa chỉ multicast 224.0.0.5

Nonbroadcast Multiaccess media :

Bao gồm các loại sau : FrameRelay , X25 , ATM , SMDS . Default , OSPF sẽ gán media loại này là nonbroadcast . Đối với media loại này , tuy rằng hỗ trợ kết nối nhiều router lại với nhau nhưng không hỗ trợ broadcast . à OSPF không tự động detect ra được neighbors . è ta phải cấu hình làm sao đó cho OSPF mô phỏng NBMA thành các loại network model khác mà nó có thể hoạt động được như :

- Broadcast model
- Point-to-point model
- Point-to-multipoint model

Broadcast model : đối với model này môi trường broadcast được mô phỏng . DR và BDR được bầu chọn . Có 2 phương pháp để mô phỏng cho model này :

- Cấu hình bằng câu lệnh : ip ospf network-type broadcast
- Cấu hình chỉ ra neighbor cho các router bang câu lệnh : neighbor

Ex1 : ip ospf network-type broadcast .

Error!

Đây là một topology broadcast multi-access . Broadcast model chỉ làm việc khi các router đấu nối full-meshed với nhau . OSPF giả sử topology trên được đấu nối full-meshed . Và để thực hiện điều này , sử dụng câu lệnh :"ip ospf network-type broadcast". Câu lệnh này phải được thực hiện trên tất cả router's frame relay interfaces .

```
RouterA#
interface serial 0
encapsualtion frame-relay
ip ospf network-type broadcast
```

Đối với dạng network khong full-meshed trên , chạy broadcast model

là not recommened .

Ex2 : thực hiện câu lệnh neighbor command .

```
RouterA#
 interface serial 0
encapsulation frame-relay
ip address 141.108.1.1 255.255.255.0
ip ospf priority 10
 !
 router ospf 1
neighbor 141.108.1.2
neighbor 141.108.1.3
neighbor 141.108.1.4
 neighbor 141.108.1.5
```

Đối với dạng network khong full-meshed trên , chạy broadcast model là not recommened .

Ex2 : thực hiện câu lệnh neighbor command .

```
RouterA#

interface serial 0

encapsulation frame-relay

ip address 141.108.1.1 255.255.255.0

ip ospf priority 10

!

router ospf 1

neighbor 141.108.1.2

neighbor 141.108.1.3

neighbor 141.108.1.4

neighbor 141.108.1.5
```

Router A cấu hình với priority cao nhất để luôn là DR . HUB router nên làm DR .

Chú ý : trong trường hợp framerelay chạy full-meshed , nếu ta để inverse ARP chạy thì không cần cấu hình thêm câu lệnh nào cả . Tại sao ? vì inverse ARP sẽ học được tất cả các DLCI và đưa vào interface của mình nên OSPF lúc này hoạt động như là một mạng broadcast multi-access .

Nếu ta map static dlci bằng câu lênh frame-relay map thì lúc này ta phải chỉ ra neighbor cho routers vì lúc này OSPF hoạt động dưới dạng non-broadcast.

Point-to-point model :

Nếu model này được sử dụng , mỗi PVC sẽ là point-to-point subinterfaces , ứng với mỗi subinterfaces 1 subnet sẽ được dùng . Không cần cấu hình câu lệnh network type , OSPF sẽ default gán mỗi subinterface network type là point-to-point .

Cái lợi của model này là Virtual circuit cost có thể được config trên mỗi subinterface . Bất lợi ở chỗ tiêu tốn không gian địa chỉ trên mỗi point-to-point subinterface và kích thước của packet LSA gửi bởi router A trở nên khá lớn do phải mang theo Type 3 stublink cho mỗi subinterfaces .

RouterA#

Interface Serial 0.1 point-to-point

ip address 141.108.1.1 255.255.255.252

!

Interface Serial 0.2 point-to-point

ip address 141.108.1.5 255.255.255.252

Cấu hình tương tự cho các router khác .

Ex :

Error!

Router A
interface Loopback0

ip address 1.1.1.1 255.255.255.255
interface Serial0/0
bandwidth 64
no ip address
encapsulation frame-relay
!
interface Serial0/0.1 point-to-point
ip address 10.1.1.1 255.255.255.252
frame-relay interface-dlci 101
!
interface Serial0/0.2 point-to-point
ip address 10.1.1.5 255.255.255.252
frame-relay interface-dlci 102
!
router ospf 1
network 1.1.1.1 0.0.0.0 area 1
network 10.1.1.0 0.0.0.3 area 0
network 10.1.1.4 0.0.0.3 area 0
Router B
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
interface Serial0
ip address 10.1.1.2 255.255.255.252
encapsulation frame-relay
bandwidth 64
frame-relay map ip 10.1.1.1 110 broadcast
no frame-relay inverse-arp
frame-relay lmi-type ansi
!
router ospf 1
network 2.2.2.2 0.0.0.0 area 2
network 10.1.1.0 0.0.0.3 area 0
Router C
interface Loopback0
ip address 3.3.3.3 255.255.255.255
!
interface Serial0
bandwidth 64
no ip address

encapsulation frame-relay
no frame-relay inverse-arp
!
interface Serial0.1 point-to-point
ip address 10.1.1.6 255.255.255.252
frame-relay interface-dlci 120
!
router ospf 1
network 3.3.3.3 0.0.0.0 area 3
network 10.1.1.4 0.0.0.3 area 0
Neighbor relationship giữa A và C được thiết lập . Có gì bất ổn ở cấu hình này khiến B và A không thể trở thành neighbor . Ta nhận thấy trong cấu hình của router B không hề cấu hình ở dạng sub point-to-point interface à default OSPF sẽ cư xử như là dạng nonbroadcast à mismatch hello .
Ta phải chuyển câu hình của B sao cho OSPF cư xử với interface của Router B như là mạng point-to-point :
Router B
interface Serial0
ip address 10.1.1.2 255.255.255.252
encapsulation frame-relay
ip ospf network point-to-point
bandwidth 64
frame-relay map ip 10.1.1.1 110 broadcast
no frame-relay inverse-arp
frame-relay lmi-type ansi
Hoặc có thể cấu hình B với câu lênh neighbor
Router B
interface Serial0
ip address 10.1.1.2 255.255.255.252
encapsulation frame-relay
frame-relay map ip 10.1.1.1 110 broadcast
no frame-relay inverse-arp
frame-relay lmi-type ansi
!
router ospf 1
network 2.2.2.2 0.0.0.0 area 2
network 10.1.1.0 0.0.0.3 area 0
neighbor 10.1.1.1
Tuy đã chỉ ra cho router B biết neighbor của nó nhưng Router A cho rằng network type nối với routerB là point-to-point , trong khi đó RouterB lại cho rằng network

type nối với routerA lại là nonbroadcast à hello mismatch . Do đó ta phải cấu hình ip ospf hello interval sao cho match về mặt timer trong toàn area .

Point-to-multipoint model : được phân ra làm 2 dạng

- point-to-multipoint (broadcast)
- point-to-multipoint nonbroadcast

Point-to-multipoint (broadcast) :

Point-to-multipoint là một tập hợp gồm các point-to-point links , trong đó các router nhận ra được neighbors của nó nhưng không diễn ra quá trình bầu chọn DR/BDR . Điều lợi ở đây là nó không cần thêm các traffic dùng để lựa chọn DR/BDR , cũng như không cần thêm các virtual circuit cần được thiết lập . Point-to-multipoint commonly được sử dụng trong partial mesh hoặc star topology .

Error!

Error!

Error!

(HÌNH B)

RouterA#
interface serial 0
encapsulation frame-relay
ip address 172.16.0.129 255.255.255.128
ip ospf network-type point-to-multipoint

Cấu hình trên tất cả router B , C , D .

Chú ý nếu bạn cấu hình ở dạng mix (cả multipoint và point-to-point) Ví dụ :

Xem hình A .

Router A
interface Serial0/0
ip address 10.1.1.1 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-multipoint
Router B
interface Serial0
ip address 10.1.1.2 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-point
Router C

interface Serial0
ip address 10.1.1.3 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-point
Đối với router A , network type la multipoint nên hello interval=30s . Đối với B , C network type lại là point-to-point nên hello interval =10s . Do đó dẫn đến hello mismatch . à phải cấu hình lại hello interval sao cho match .
Router A
interface Serial0/0
ip address 10.1.1.1 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-multipoint
ip ospf hello-interval 30
Router B
interface Serial0
ip address 10.1.1.2 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-point
ip ospf hello-interval 30
Router C
interface Serial0
ip address 10.1.1.3 255.255.255.248
encapsulation frame-relay
ip ospf network point-to-point
ip ospf hello-interval 30
Còn nếu bạn cấu hình ở tất cả các router câu lệnh : “ip ospf network point-to-multipoint” (hình B) thì hello interval sẽ được tự động set là 30s .
Nêu media không hỗ trợ multicast/broadcast , do đó model point-to-multipoint không sử dụng được . à sử dụng câu lênh “ip ospf network-type point-to-multipoint non-broadcast “ . Lúc này không còn là dạng broadcast nữa nên ta phải manual cấu hình neighbor cho các router .

```
    RouterA#
  interface serial 0
 encapsulation frame-relay
 ip address 141.108.1.1 255.255.255.0
 ip ospf network-type point-to-multipoint non-broadcast
  !
  router ospf 1
 neighbor 141.108.1.2
 neighbor 141.108.1.3
```

neighbor 141.108.1.4
neighbor 141.108.1.5
Tóm tắt :

OSPF over NBMA	IP Subnets Needed	Description
NBMA	1 (same subnet number)	Fully meshed; manually configured adjacencies; DR/BDR elected; RFC2328-defined
Point-to-Multipoint	1 (same subnet number)	Partial mesh or star; automatic adjacency; no DR/BDR elected; RFC2328-defined
Point-to-Multipoint non-broadcast	1 (same subnet number)	Partial mesh or star; manually configured adjacencies; no DR/BDR elected; RFC2328-defined
Broadcast	1 (same subnet number)	Fully meshed; automatic adjacency; DR/BDR are elected; Cisco-defined
Point-to-Point	Separate subnet for each subinterface	Partial mesh or star; subinterfaces; automatic adjacency; no DR/BDR elected; Cisco-defined

OSPF LSA Details : Chúng ta sẽ khảo sát chi tiết từng loại LSA , và chủ yếu là 6 loại LSA sau đây :

1 . Type 1 : Router LSA : mô tả trạng thái , cost của link kết nối tới neighbor và ip prefix của link đó .

2 . Type 2 : Network LSA : mô tả số lượng router attach và segment cũng như là subnetmask của segment đó .

3 . Type 3 : Summary network : mô tả thông tin tóm tắt của một area cho các area khác trong cùng một OSPF domain và ngược lại .

4 . Type 4 : Summary ASBR : mô tả thông tin về ASBR . Trong một single area thì sẽ không tồn tại type 4 LSA . Chỉ khi nào OSPF domain gồm multiple area và có kết nối với AS khác thì lúc đó mới xuất hiện type 4 .

5 . Type 5 : External : mô tả thông tin về các route ở bên ngoài 1 ospf domain .

6. Type 7 : NSSA : cũng là external route nhưng có format gần giống với type 5 .

Mối LSA packet đều có 20 bytes LSA header có format như sau :

Error!

- LS Age : cho biết thời gian tạo ra LSA này . Max age của LSA là 3600s , refesh time là 1800s . Nếu LS age đạt tới 3000s thì LSA này mất giá trị và bị remove ra khỏi database .

- Options : tương tự như options field trong hello packets .

- LS type : chỉ ra đây là loại LSA nào (type 1 , type 2 or type 3 …)

- Link-State ID : chỉ ra phần network được mô tả bởi LSA . Field này thay đổi tùy theo loại LSA .

- Advertising router : Router ID của router tạo ra LSA .

- LS sequence number : dùng để phát hiện ra LSA đã cũ hoặc bị trùng lắp .

- LS checksum : kiểm lỗi cho LSA packet .

- Length : độ dài bao nhiêu bytes của LSA packet , bao gồm cả LSA header .

Type 1 – Router LSA

Router LSA được tạo ra bởi mỗi router cho mỗi area mà router thuộc về . Packet này mô tả trạng thái của các link kết nối trực tiếp với router và thông tin này được flood đi trong phạm vi một area . Tất cả các link kết nối trực tiếp với router sẽ được mô tả bằng một gói LSA duy nhất .

Error!

- Bit V : Bit này được dùng khi router là endpoint của virtual link .
- Bit E : Bit này được dùng khi router là ASBR .
- Bit B : Bit này được dùng khi router là ABR .
- Number of links : chỉ ra số lượng các links kết nối với router .
- Link ID , Link Data , Type :
    - Type : field này cho biết router link là loại gì (có 4 loại router links , phân biệt bằng type field)
    - Link ID và link Data : là giá trị 4 bytes ip address , tùy thuộc vào loại network type .

Type	**Description**	**Link ID**	**Link Data**
1	Point-to-point numbered	Neighbor's router ID	Interface IP address
1	Point-to-point unnumbered	Neighbor's router ID	MIBII IfIndex value
2	Transit	IP address of the DR	Interface IP address
3	Stub	IP network number	Subnet mask
4	Virtual link	Neighbor's router	Interface IP address

Type	Description	Link ID	Link Data
		ID	

- Tos & Tos metric : type of service . Thường được set là 0 .
- Metric : cho biết OSPF cost của một link . Cost=10^8/BW . Cost có thể được modified theo 2 cách , cách 1 dùng câu lệnh ip ospf cost (mode interface) , cách 2 dùng câu lệnh auto-cost reference-bandwidth [value] (router ospf mode) . reference bandwidth default là 10^8 .

Ví dụ :

Error!

RouterB#show ip ospf database router 141.108.1.21
LS age: 1362
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 141.108.1.21
Advertising Router: 141.108.1.21
LS Seq Number: 80000085
Checksum: 0xE914
Length: 60
Area Border Router
Number of Links: 3

Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 141.108.1.3
(Link Data) Router Interface address: 141.108.1.2
Number of TOS metrics: 0
TOS 0 Metrics: 64
Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 141.108.3.1
(Link Data) Router Interface address: 141.108.1.2
Number of TOS metrics: 0
TOS 0 Metrics: 64
Link connected to: a Stub Network
(Link ID) Network/subnet number: 141.108.1.2
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metrics: 0

Các output quan trọng được highlighted lên :

- Trong tình trạng bình thường , LS age < 1800
- Đối với trường hợp router LSA , Link-Stae ID và Advertising router có cùng giá trị .
- Router này là ABR và có 3 router links .

Stublink trong trường hợp này là gì ? Ứng với mỗi point-to-point link ,(hoặc point-to-multipoint) sẽ có 1 stub link cung cấp thông tin về subnetmask cho link đó.

Type 2 – Network LSA

DR tạo ra network LSA packet . Nếu không có DR (point-to-point or point-to-multipoint network) , thì sẽ không có type 2 LSA này . Network LSA mô tả tất cả những router attach vào network . Thông tin này được flood đi trong 1 area (giống router LSA) .

Error!

Network LSA có 2 thành phần quan trọng :

- network mask : Chỉ ra network mask của transit link .
- Attached router : chỉ ra router ID của các router attach vào transit link này . Trong danh sách này cũng có DR .

Error!

Transit link ở đây là gì ? Là network link mà trên đó các router có thiết lập quan hệ neighbor và bầu chọn ra DR/BDR .

RouterA#show ip ospf database network 141.108.1.1
Routing Bit Set on this LSA
LS age: 1169
Options: (No TOS-capability, DC)
LS Type: Network Links
Link State ID: 141.108.1.1 (address of Designated Router) à ip address của DR .
Advertising Router: 141.108.3.1 à RID của DR .
LS Seq Number: 80000002
Checksum: 0xC76E
Length: 36
Network Mask: /24
Attached Router: 141.108.3.1
Attached Router: 141.108.1.21
Attached Router: 141.108.1.3
Có 2 thông tin quan trọng cần lưu ý :

- Link state ID ở đây là ip address của DR
- Advertising router ở đây là Router ID của DR

Type 3 – Summary LSA
Summary LSA mô tả thông tin tóm tắt các route bên ngoài một area , nhưng vẫn thuộc một AS . Summary LSA được tạo ra khi có nhiều hơn 1 area kết nối vào Area 0 đã được configured . Type 3 packet được tạo ra với mục đích giảm một lượng thông tin khổng lồ trong nội bộ 1 area khi mang đi quảng bá với các area khác . Type 3 được tạo ra bởi ABR và mang theo ip prefix .

- Từ non-backbone to backbone area , summary LSA được tạo ra cho :
  - Connected routes
  - Intra-area routes
- Từ backbone to non-backbone area , summary LSA được tạo a cho :
  - Connected routes
  - Intra-area routes
  - Interarea routes

Intra-area routes là gì ? Là những routes được tạo ra nội bộ trong area đó mà thôi (ví dụ type 1 , type 2).
Interarea routes là gì ? là những routes liên area , area này thấy thông tin của area khác là nhờ những tuyên interarea routes .
Lưu ý : chỉ có intra-area route được quảng bá vào backbone area để chống loop . Nếu có bất kì một interarea nào được quảng bá từ non-backbone area vào backbone area thì có nghĩa rằng backbone area đã bị discontiguous . à không cho phép discontiguous backbone tồn tại .

Minh họa : Area 2 gủi intra-area chứa thông tin nội bộ của area 2 cho backbone Area 0 (2) . Tương tự Area 1 cũng gửi thông tin intra-area của area 1 cho area backbone (2) . Như vậy Area 1 đã thấy được thông tin interarea của area 2 nhờ area backbone (2) quảng bá . Area 1 lại mang thông tin này quảng bá cho area backbone (1) à discontiguous backbone .

Có 2 loại summary LSA :

- Type 3 : Lưu thông tin về network của area
- Type 4 : Lưu thông tin về ASBR

Format của một summary LSA :

Error!

- Network mask : Type 3 sẽ có network mask kèm theo , đối với type 4 field này là 0 .
- Metric : cost của network .
- ToS : set bằng 0 .

Type 3 , type 4 dùng chung một kiểu format . Những khác biệt sau đây cần nhớ về type 3 và type 4 :

- Network mask field trong type 3 chứa subnetmask của network .
- Network mask field trong type 4 là 0.0.0.0
- Type 3 LSAs , Link-State ID là network number.
- Type 4 LSAs , Link-State ID là RID của ASBR .
- Advertising roueter phải là router ID của ABR tạo ra summary LSA . Điều này đúng cho cả type 3 và type 4 .

Note : type 3 summary inf của routes trong area , bao gồm luôn cả thông tin cho ASBR (trường hợp có ASBR nằm trong area) . Để các area khác biết được thông tin của ASBR à type 4 được tạo ra để quảng bá thông tin cho biết ASBR nằm ở đâu .

Chỉ có 1 trường hợp đặc biệt của LSAs , đó là trường hợp stub-area ABR tạo ra summary default route . Trong trường hợp này Link-state ID field và networkmask field là 0.0.0.0 .

Ví dụ :

Error!

RouterB#show ip ospf database summary 9.9.9.0
LS age: 1261
Options: (No TOS-capability, DC)
LS Type: Summary Links(Network)

Link State ID: 9.9.9.0 (summary Network Number)
Advertising Router: 141.108.1.21
LS Seq Number: 80000001
Checksum: 0xC542
Length: 28
Network Mask: /24
TOS: 0 Metric: 10
Error!

RouterB#show ip ospf database asbr-summary 141.108.1.21
LS age: 1183
Options: (No TOS-capability, No DC)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 141.108.1.21 (AS Boundary Router address)
Advertising Router: 141.108.1.1
LS Seq Number: 80000001
Checksum: 0x57E4
Length: 28
Network Mask: /0
TOS: 0 Metric: 14
Error!

RouterB#show ip ospf database summary 0.0.0.0
LS age: 6
Options: (No TOS-capability, DC)
LS Type: Summary Links(Network)
Link State ID: 0.0.0.0 (summary Network Number)
Advertising Router: 141.108.1.21
LS Seq Number: 80000001
Checksum: 0xCE5F
Length: 28
Network Mask: /0
TOS: 0 Metric: 1

Type 5 – External LSA

External LSA cho biết thông tin về external route , outside AS . Type 5 được flood trong toàn bộ domain . Để LSA type 5 có mặt trong routing table , 2 điều quan trọng sau đây phải có :

- Router muốn install type 5 vào routing table phải thấy được ASBR thông qua *intra-area*hoặc *interarea route* .Có nghĩa là nó phải có Router LSA cho ASBR hoặc Type 4 LSA cho ASBR .

- Forwarding address phải được học thông qua intra hoặc interarea route .

Error!

- Network mask : network mask của external network .
- Bit E : chỉ ra external loại nào , loại 2 or loại 1 . Nếu bit E được set lên thì đó là loại 2 , nếu không set thì là loại 1 . Type 1 , external metric được cộng với internal metric . Type 2 , giữ nguyên trong toàn AS .
    - Forwarding address : chỉ ra địa chỉ mà data traffic phải forward tới . Nếu giá trị này là 0.0.0.0 có nghĩa là traffic phải được forward cho ASBR . Trong một vài tình huống , forwarding address là nonzero , nhằm tránh tình trạng định tuyến không tối ưu .

Error!

Router A , Router B , Router C đều là ASBR , trao đổi thông tin về external route chi xảy ra giữa RA và RX (external AS router) . RA quảng bá tuyến external này cho các router trong AS của nó . Lúc này RB và RC cũng biết được external route là phải thông qua RA , Như vậy , suboptimal routing đã xảy ra , RB và RC vô tình phải đi qua những hop không cần thiết để ra external route . Trong khi đó nêu RA chỉ ra next-hop là ip của RX thì RB và RC sẽ biết đường ra external một cách optimal hơn vì không phải qua RA .

Ví dụ :

Error!

RouterE#show ip ospf database external 10.10.10.0
LS age: 954
Options: (No TOS-capability, DC)
LS Type: AS External Link
Link State ID: 10.10.10.0 (External Network Number)
Advertising Router: 141.108.1.21

LS Seq Number: 80000003
Checksum: 0x97D8
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0

Những thông tin quan trọng sau cần nhớ :

- Link state ID : là external network number
- Advertising Router : Router ID của ASBR
- Metric type : 2 , nghĩa là metric của tuyến external không thay đổi trong toàn bộ 1 AS .
- Forwarding addess là 0.0.0.0 nghĩa là traffic phải forward trực tiếp cho ASBR .
- Route đến nonzero forwarding address phải được biết thông qua intra-area hoặc interarea route . Nếu không , external route sẽ không được đưa vào bảng routing table .

Type 7 – NSSA LSA

Format của packet type 7 và type 5 gần giống nhau . Chỉ có vài điểm khác biệt chính :

- Type field chỉ ra là loại type 7 LSA , không phải type 5 .
- Forwarding address được tính toán như sau :
  - Sử dụng một trong những loopback address trong area được quảng bá bởi LSAs .
  - Nếu không có loopback được configure , sử dụng address của interface đầu tiên trong area .

Ví dụ :

Error!

RouterI#show ip ospf database nssa-external 10.10.10.0
LS age: 36
Options: (No TOS-capability, **Type 7/5 translation**, DC)
LS Type: AS External Link
Link State ID: 10.10.10.0 (External Network Number)
Advertising Router: 141.108.1.21
LS Seq Number: 80000001

Checksum: 0x4309
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 141.108.1.21
External Route Tag: 0

Một vài điều cần lưu ý về P bit :

- P bit dùng để báo cho NSSA ABR biết có translate type 7 thành type 5 hay không .
- Bit P = 0 , không chuyển đổi type 7 thành type 5 . (NSSA ASBR = NSSA ABR).
- Bit P = 1 , có chuyển đổi type 7 thành type 5
- Bit P = 1 , co nhiều NSSA ABR tồn tại thì router nào có RID thấp nhất sẽ translate type 7 thành type 5

Mọi ý kiến đóng góp xin gửi về : hoanglenhan@vnpro.org
Xin cảm ơn !

password recovery)

Tác giả: Đặng Quang Minh

Tài liệu tham khảo cho học viên CCNA của VnPro

Qui trình khôi phục password (password recovery)

I. Đối với Cisco 1600, 1700 and 2600 Series Routers:

1. Establish a HyperTerminal (Private Edition 5.0 or higher) console connection with the router.
2. Tắt router, sau đó bật lại. Nhấn Ctrl-Break trong vòng 60 giây
monitor: command "boot" aborted due to user interrupt
rommon 1 >
3. Dùng lệnh confreg để đổi nội dung thanh ghi sang 2142.
rommon 1 >**confreg 0x2142**
4. Reboot the router with the **reset** command.
rommon 2 >**reset**
5. Sau khi reboot, dùng Ctrl-C để vào user mode:
router>

6.
router>**enable**

router#**copy startup-config running-config**
7.
router>**enable**
router#**show startup-config**
8. Đặt lại password mới:
router#**config term**
router(config)#**enable secret newpassword**
router(config)#**enable password newpassword**
router(config)#**line con 0**
router(config-line)#**login**
router(config-line)#**password newpassword**
router(config)#**line aux 0**
router(config-line)#**login**
router(config-line)#**password newpassword**
router(config)#**line vty 0 4**
router(config-line)#**login**
router(config-line)#**password newpassword**
9. #copy run start
10. Khôi phục giá trị thanh ghi về 0x2102
router#**config term**
router(config)#**config-register 0x2102**
router(config)#**exit**
router#**copy running-config startup-config**
11. Kiểm tra nội dung thanh ghi
router#**show version**
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DO3S-M), Version 12.0(5)T1, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 13:18 by cmong
Image text-base: 0x80008088, data-base: 0x80CB67B0
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
Configuration register is 0x2142 (will be 0x2102 at next reload)
Cisco 2500 Series Routers:

1. Thiết lập HyperTerminal (Private Edition 5.0 or higher) console connection with the router.
2. Tắt routers, sau đó bật lại. Nhấn CTRL-BREAK trong vòng 60 giây.
Abort at 0x10EA884 (PC)
>
3. Đổi nội dung thanh ghi thành 0x2142
>**o/r 0x2142** (lower case of the letter O for o/r and zero for 0x2142)
4. Reboot router
>**i**
5. Nhấn Ctrl-C để vào user mode khi router khởi động lại
router>
6. Vào enable mode
router>**enable**
router#**copy startup-config running-config**
7. Thực hiện các lệnh **show running-config** or **show startup-config**
router#**show startup-config**
8. Enter a new privileged password and change other lost passwords as may be necessary.
router#**config term**
router(config)#**enable secret newpassword**
router(config)#**enable password newpassword**
router(config)#**line con 0**
router(config-line)#**login**
router(config-line)#**password newpassword**
router(config)#**line aux 0**
router(config-line)#**login**
router(config-line)#**password newpassword**
router(config)#**line vty 0 4**
router(config-line)#**login**
router(config-line)#**password newpassword**
9. Copying the startup-configuration to running-configuration. Thực hiện lệnh **no shutdown** trên tất cả các interface được dùng.
10. Chuyển nội dung thanh ghi về giá trị ban đầu. Lưu cấu hình
router#**config term**
router(config)#**config-register 0x2102**
router#**copy running-config startup-config**
11. Kiểm tra thanh ghi có giá trị là 2102 bằng lệnh **show version**
router#**show version**
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4), RELEASE

SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE
SOFTWARE (fc1)
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2142 (will be 0x2102 at next reload)
12. Reboot the router.
router#**reload**

109011: Authen Session Start: user 'aaauser', sid 9
109005: Authentication succeeded for user 'aaauser' from 172.16.1.1/3719 to 209.162.1.2/23 on interface inside
109007: **Authorization permitted** for user 'aaauser' from 172.16.1.1/3791 to 209.162.1.2/23 on interface inside
302013: Built outbound TCP connection 27 for outside:209.162.1.2/23 (209.162.1.2/23) to inside:172.16.1.1/3791 (209.162.1.5/3791) (aaauser)
Kiểm tra ping :
Error!

Quan sát debug :
109001: Auth start for user 'aaauser' from 172.16.1.1/0 to 209.162.1.2/0
109011: Authen Session Start: user 'aaauser', sid 9
109007: **Authorization permitted** for user 'aaauser' from 172.16.1.1/0 to 209.162.1.2/0 on interface inside

Bài Viết Về PIX FIREWALL

Tác giả: Nguyễn Thị Băng Tâm

Chương 4 : **CẤU HÌNH AAA TRÊN PIX FIREWALL**

1. Tổng quan về AAA

Việc nhận thực quyết định việc nhận dạng một user và kiểm tra thông tin về user đó. Việc nhận thực truyền thống sử dụng tên và một password cố định . Khi truy nhập vào một thiết bị hay mạng với user ID thì sẽ biết được user đó là ai . Khi user đã được xác thực , authentication server sẽ cho phép user đó một quyền cụ thể (authorization) dựa trên thông tin về user ID và password đó . Authorization cho biết user có thể làm gì . Khi user đã vào được và đang sử dụng một dịch vụ , host hay một mạng nào đó , sẽ có một bản ghi lại những việc mà user đã làm . Accounting có nhiệm vụ thực hiện điều này . Accounting cũng có thể được sử dụng cho việc thanh toán hóa đơn , pháp lí hay một kế hoạch .

Authentication , Authorization và Accounting (AAA) được PIX firewall sử dụng kiểm tra xem user là ai , user có thể làm gì và user đã làm gì . Bản thân PIX firewall có thể điều khiển việc truy

nhập dựa trên port và địa chỉ IP , nhưng phương pháp này không cung cấp một cơ chế để xác định được bản thân mỗi user và điều khiển luồng traffic của user đó . Authentication có thể thực hiện được mà không cần có authorization , nhưng Authorization sẽ không bao giờ thực hiện được nếu không có Authentication .

Đặc điểm của AAA khi sử dụng với PIX firewall bao gồm :

- Client cần truy nhập đến một dịch vụ nào đó . PIX firewall , lúc này đóng vai trò là gateway giữa client và thiết bị , sẽ yêu cầu client gửi user ID và password .
- PIX nhận được thông tin đó và chuyển nó đến AAA server .AAA server được định nghĩa như là một thực thể logic dùng để cung cấp 3 chức năng AAA . Server sẽ tìm xem thông tin về user này có trong database của nó hay không ? Nếu có thì user sẽ được phép sử dụng dịch vụ đã yêu cầu . Nếu không , user bị từ chối sử dụng dịch vụ đó .

Với việc sử dụng AAA server riêng như vậy , giúp cho PIX giảm được tải (CPU) , cấu hình và quản lí đơn giản , làm tăng khả năng mở rộng .

Việc sử dụng AAA server cho phép chỉ có các user được xác thực mới được truy cập đến một mạng nào đó , ví dụ như các user có user ID và password hợp lệ mới được truy cập internet , hoặc là giới hạn quyền của user sau khi xác thực thành công sử dụng một dịch vụ nào đó . Bằng việc cấu hình trên PIX và AAA server , nhà quản trị mạng có thể giới hạn việc truy cập các dịch vụ như FTP , Telnet , HTTP , hay là các dịch vụ khác .

User có thể xác thực với PIX firewall sử dụng một trong 3 phương pháp sau :

- Telnet : dấu nhắc được phát ra bởi Pix , mỗi user có 4 lần log in . Nếu username hoặc password sai sau lần thứ tư , Pix sẽ làm rớt kết nối . Nếu xác thực và thẩm quyền thành công , user
- FTP : dấu nhắc được phát ra từ chương trình FTP . Nếu password không đúng , kết nối sẽ bị rớt ngay lập tức . Nếu username hoặc password trong authentication database khác với username và password của remote host mà ta cần truy nhập vào thông qua FTP , sử dụng username và password theo mẫu sau :
  - aaa_username@remote_username
  - aaa_password@remote_password

PIX firewall gửi aaa_username và aaa_password đến AAA server , nếu authentication và authorization thành công , remote_username và remote_password được gửi chuyến FTP server đích .

- HTTP : browser phát ra cửa sổ username , password . Nếu nhập vào không đúng password , user sẽ được nhắc nhập lại .

Nếu username hoặc password trong database authentication khác với username và password ở remote host , thì nhập username và password theo mẫu sau :

- aaa_username@remote_username
- aaa_password@remote_password

PIX firewall gửi aaa_username và aaa_password đến AAA server , nếu authentication và authorization thành công , remote_username và remote_password được gửi chuyến HTTP server đích .

2. Cut-through proxy

PIX firewall có thể configuration replication `ung cấp việc xác thực và thẩm quyền cho user để sử dụng dịch vụ nào đó thông qua Pix . Đặc biệt , pix cho phép ta thực hiện việc xác thực và thẩm quyền cho các phiên FTP , HTTP , và Telnet cho cả 2 hướng inbound và outbound . Chức năng này còn đươc gọi là cut-through proxy . Cut-through proxy cho phép ta điều khiển các dịch vụ thích hợp thông qua firewall bằng user chứ không phải địa chỉ IP . Khác với proxy server phải phân tích mỗi gói dữ liệu trong một phiên ở lớp application , điều này ảnh hưởng trực tiếp đến vấn đề thời gian và tốc độ xử lý , sử dụng Cut-through proxy , PIX firewall sẽ chỉ gửi query đầu tiên cho việc chứng thực tới một TACACS+ hoặc RADIUS database server . Khi một user được chứng thực thành công ứng với policy đã được thiết lập , thì pix sẽ chuyển session flow và traffic flow trực tiếp giữa 2 host trong khi vẫn duy trì thông tin trạng thái

Ví dụ sau đây sẽ giúp ta hiểu rõ hơn hoạt động của cut-through proxy :

Error!

Ứng dụng điển hình của công nghệ này là một user ở mạng bên ngoài (internet) truy cập vào HTTP server nằm trong vùng DMZ của mạng intranet như trong hình vẽ trên . User ở mạng ngoài truy cập vào XYZ web server , PIX yêu cầu user nhập thông tin username và password , thông tin này được pix chuyển đến AAA server . Nếu được xác thực , user được phép đến XYZ web server .

Nếu web server này cũng đòi xác thực , thì user sẽ gửi remote username và password đến server đó .

3. Cấu hình xác thực

Khi CSACS (Cisco Secure Access Control Server) được cấu hình (CSACS là một phần mềm được cài đặt trên server cung cấp đầy đủ 3 dịch vụ AAA) , một entry tương ứng với AAA server phải được cấu hình trên pix . Các bước cấu hình như sau:

- Tạo AAA group , chỉ ra giao thức dùng cho xác thực :

aaa-server *group_tag* **(if_name) host** *server_ip* **key timeout** *seconds*

- Tạo ra AAA server và đăng kí nó đến AAA group , nhiều AAA server có thể ở trong cùng một group :

aaa-server *group_tag* **protocol** *auth_protocol*

Group_tag : tên của server group

If_name : tên interface kết nối với server

Host server_ip : địa chỉ IP của TACACS+ server hoặc RADIUS server

Key : là từ khóa case-sensitive , có độ dài tối đa là 127 kí tự , từ khóa này phải giống với từ khóa của server . Key được sử dụng giữa client và server cho việc mã hóa dữ liệu giữa chúng . Nếu key không được chỉ ra , mã hóa sẽ không xảy ra . Không được sử dụng khoảng trắng giữa các kí tự trong key .

Timeout seconds : chỉ ra khoảng thời gian mà pix phải chờ để thử lại lần nữa , pix sẽ thử lại 4 lần trước khi chọn server kế tiếp cho việc xác thực . Giá trị mặc định của timeout là 30 giây .

Auth_protocol : là chỉ ra loại server nào được sử dụng , tacacs hay là radius .

?**Note** : Mặc định , PIX firewall giao tiếp với RADIUS server dùng port 1645 dành cho việc xác thực và port 1646 dành cho accounting . Các RADIUS đời mới hơn có thể sử dụng port 1812 và port 1813 . Nếu server sử dụng port khác 1645 và 1646 , ta cần phải định nghĩa lại giá trị port tương ứng trên Pix bằng câu lệnh *aaa-server radius-authport* và *aaa-server radius-acctport* trước khi cấu hình RADIUS server .

Với PIX firewall , nhà quản trị có thể định nghĩa từng group riêng cho các loại traffic khác nhau , ví dụ như một TÁCACS + server cho inbound traffic , một TACACS+ server khác cho outbound traffic . Ta có thể có đến 16 tag group và mỗi group có thể có đến 16 AAA server , tổng cộng có đến 256 server .

Cấu hình mặc định ở pix có hai giao thức AAA server là :

- aaa-server tacacs+ protocol tacacs+
- aaa-server radius protocol radius

Sau khi đã chỉ ra aaa-server , ta cần phải cấu hình xác

Tác giả: Nguyễn Thị Băng Tâm

Chương 1 : **GIỚI THIỆU VỀ PIX FIREWALL**

PIX (Private Internet Exchange) firewall là thành phần chính trong giải pháp bảo mật end-to-end của Cisco . PIX firewall là giải pháp bảo mật về phần cứng và phần mềm , đáp ứng bảo mật mạng mức độ cao mà không ảnh hưởng đến hoạt động của mạng . Pix là một thiết bị hybrid vì nó kết hợp các đặc điểm của công nghệ packet filtering và proxy server .

1. PIX hardware :

Pix có nhiều model khác nhau , thích hợp với nhiều môi trường mạng khác nhau , ví dụ như mạng SOHO thì khác với mạng của service provider .

PIX có các loại models sau : 501 , 506 , 506E , 515 , 515E , 520 , 525E , và 535 .

Theo hình sau :

Error!

Hình 1 : PIX firewall family

Đặc điểm của từng loại thiết bị PIX :

a. PIX 501 :

501 là model cơ bản của PIX và có cấu hình cố định . Nó có một switch 4 port cho kết nối bên trong và một interface 10Mbps cho kết nối đến thiết bị bên ngoài (như cable modem hay router DSL) . Pix 501 dành 3Mbps cho kết nối 3DES Ipsec (vượt quá cả yêu cầu của user trong mạng SOHO) .

Đặc điểm của PIX 501 là :

- bộ xử lí 133MHz AMD SC520
- RAM 16MB , flash 8MB
- 1 port console
- 1 port half-duplex RJ45 10BaseT cho outside
- 1 switch tích hợp , autosensing , auto-MDIX 4 port RJ45 10/100 cho inside

b. Pix 506

Error!

Pix 506 là thiết bị được thiết kế cho các công ty thuộc remote office/ branch office . Là thiết bị có :

- Một port console
- Hai port RJ45 10BaseT autonegotiate , một cho inside , một cho outside
- Hardware : 200MHz Intel Pentium MMX , trong đó RAM là 32Mbps , flash là 8Mbps
- Sử dụng TFTP cho download image và upgrade image .
- Pix 506 cung cấp VPN , có thể kết nối đến 4 VPN peer đồng thời .

PIX 506E là thiết bị được cải tiến từ PIX 506 , có CPU là 300MHz Intel Celeron . Clear-text throughput lên đến 20Mbps , 3DES throughput tăng lên 16Mbps .

c. PIX 515

Error!

PIX 515 thường được dùng trong các doanh nghiệp nhỏ , trung bình .

Pix có một slot để có thể gắn thêm một single-port , hoặc là four-port Fast Ethernet interface , cho phép inside , outside và có thể cung cấp thêm 4 mạng dịch vụ khác .

Pix 515 có RAM 32MB , Flash 8MB , licensing linh động do đó các doanh nghiệp có thể trả tiền những cái họ cần . Restricted license giới hạn 3 interface , nhưng unrestricted license cho phép tăng bộ nhớ RAM từ 32MB đến 64MB và tăng đến 6 interface cộng với failover .

d. PIX 520

Error!

PIX 520 được thiết kế dành cho các doanh nghiệp lớn và môi trường tốc

độ cao , phức tạp . Mặc dù các sản phẩm mới hơn có Flash đến 16MB
nhưng đối với PIX 520 đời cũ Flash chỉ có 2MB . Để chạy những software
có version từ 5.2 trở lên thì Flash cần phải được nâng cấp lên 16MB .
PIX 520 có kiểu thiết kế khung , là rack-mountable , sử dụng đĩa mềm
3.5inch để load và nâng cấp image .

e. PIX 525

Error!

PIX 525 được thiết kế dành cho các Enterprise và Service Provider sử dụng ,
đáp ứng môi trường bảo mật lí tưởng . **PIX 525** cung cấp một dãy nhiều
network interface card . Standard card bao gồm single-port hay four-port
10/100 Fast Ethernet , Gigabit Ethernet (với UR license) , 4/16 Token Ring
và dual-attached multimode FDDI card . Với restricted license , Pix 525 cung
cấp 6 interface . Với unrestricted license (UR) Pix 525 cung cấp đến 8 interface .

f. PIX 535

Error!

PIX 535 được thiết kế cho các Enterprise và Service Provider sử dụng .
Nó có công suất 1.0Gpbs với khả năng thực hiện cùng một lúc 500,000
kết nối . Đáp ứng cả site-to-site và remote access VPN với 56-bit DES
và 168-bit 3DES , chức năng tích hợp của PIX firewall 535 có thể thực hiện
với VPN Accelerator card để phân phối 10Mbps throughput và 2000 IPSEC
tunnel .
PIX firewall 535 cung cấp Fast Ethernet , Gigabit Ethernet và VPN Accelerator

interface . Flash là 16MB và sử dụng software có version từ 5.3 trở về sau .

2. Console port :

Cơ chế chính để giao tiếp với PIX là thông qua console port . Một vài thiết bị sử dụng DB9 connector , một vài thiết bị mới hơn sử dụng Cisco standard RJ45 connector . Nếu ta đang sử dụng Windows , thì dùng chương trình Hyperterm để giao tiếp với PIX . Giao diện phải tuân theo hình vẽ sau :

Error!

Và các tham số phải được thiết lập như sau :

Error!

Lúc này kết nối đến PIX đã thành công . Nếu cấp nguồn thì lúc này PIX sẽ diễn ra quá trình boot .

Đây là một đoạn ví dụ của quá trình boot :

Reading 1921536 bytes of image from flash.#########################
##
####
#########################
32MB RAM
mcwa i82559 Ethernet at irq 11 MAC: 000f.23ac.53f7
mcwa i82559 Ethernet at irq 10 MAC: 000f.23ac.53f6
System Flash=E28F640J3 @ 0xfff00000
BIOS Flash=am29f400b @ 0xd8000

..:||||||:..:||||||:..
c i s c o S y s t e m s
Private Internet eXchange

Cisco PIX Firewall
Cisco PIX Firewall Version 6.3(1)

Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
This PIX has a Restricted (R) license.
……
Cryptochecksum(changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Cannot select private key
Pre-configure PIX Firewall now through interactive prompts [yes]? n
=> sử dụng **n** để vào tiến vào CLI .

3. Software Licensing :

Để có được một sản phẩm linh động , PIX sử dụng software licensing để enable hay disable các đặc điểm trong PIX OS . Mặc dù hardware có thể giống nhau về platform giữa các thiết bị , nhưng sử dụng software nào cho PIX còn phụ thuộc vào RAM và Flash của PIX đó . Ví dụ như OS yêu cầu cho PIX model 506 là từ 5.1x trở lên , cho PIX model 525 là từ 5.2x trở lên … Các đặc điểm của software khác nhau còn phụ thuộc vào activation key .

Activation key là license key của PIX OS , cho phép ta upgrade các đặc điểm mới của OS mà không cần phải có software mới , mặc dù quá trình thực hiện là tương tự nhau . Activation key là do cisco đưa ra và

tính toán ,
phụ thuộc vào số serial mà ta có và phụ thuộc vào ta yêu cầu những gì .
Số serial đó có được là dựa vào Flash . Do đó nếu ta sử dụng Flash khác ,
ta phải thay đổi activation key . Khi ta muốn kích hoạt một chức năng nào
đó trong PIX , ta phải trả tiền để thực hiện điều này , để có key ta phải gửi
serial number của PIX đến Cisco , Cisco sẽ gửi lại cho ta key được tạo ra từ
serial number đó .

Có 3 lí do quan trọng để upgrade hay thay đổi activation key là :

- Cisco PIX firewall không kích hoạt failover
- Pix không kích hoạt VPN
- Khi ta cần nâng cấp từ connection-based license lên feature-based license .

Để có được thông tin về activation key , serial number , sử dụng **show version** command . Câu lệnh này cung cấp thông tin về code version , thông tin về phần cứng …

pixfirewall(config)# sh version
Cisco PIX Firewall Version 6.3(1)
Cisco PIX Device Manager Version 3.0(1)
Compiled on Wed 19-Mar-03 11:49 by morlee
pix up 27 mins 25 secs
Hardware: PIX-506E, 32 MB RAM, CPU Pentium II 300 MHz
Flash E28F640J3 @ 0x300, 8MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
0: ethernet0: address is 000f.23ac.53f6, irq 10
1: ethernet1: address is 000f.23ac.53f7, irq 11
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled

Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
This PIX has a Restricted (R) license.
Serial Number: 808036792 (0x3029a9b8)
Running Activation Key: 0x9a5c6f78 0x67304d0a 0xed4c2329 0x89dd199b
Configuration last modified by enable_15 at 23:52:55.403 UTC Sun Mar 6 2005

Licensing :

Về tổng quan , licensing được phân thành 3 loại đó là unrestricted , restricted , và failover . Việc dùng unrestricted hay restricted license là phụ thuộc vào số interface mà ta cần sử dụng ở PIX . Ví dụ đối với PIX 515 với unrestricted license cung cấp đến 6 interface . Quan sát lại những thông tin khi **show version** ở phía trên , ta thấy license là restricted cho phép tối đa cho pix là 2 interface (inside và outside) , đối với PIX 515 thì restricted cho phép tối đa là 3 interface (thêm một interface dmz nữa) . Do đó , muốn có unrestricted và failover license , ta phải nâng cấp activation key mới .

Đối với các PIX OS có version trước version 6.2 , activation key được thay đổi trong mode monitor . Từ version 6.2 trở về sau cho phép ta nâng cấp hay thay đổi license bằng cách thay đổi key ở CLI (command line interface) .

Thực hiện điều này bằng câu lệnh sau :

activation-key *license#*

license# : là key mà ta có được với license mới .

ví dụ : activation-key 0x9a5c6f78 0x67304d0a 0xed4c2329 0x89dd199b

Sau khi thay đổi activation key , ta phải reboot PIX firewall để kích hoạt license mới. Nếu PIX được nâng cấp đến một version mới hơn và thay đổi activation key , ta phải reboot PIX 2 lần -1 lần sau khi cài đặt

image mới ,
một lần sau khi activation key mới được cấu hình . Lưu ý là khi nâng cấp lên
version mới hơn , những chức năng đã được kích hoạt từ version cũ thì không
cần key .
Nếu ta thay đổi image của PIX với version cũ hơn , phải đảm bảo rằng
activation key đang chạy trong hệ thống không tác động đến các version cao
hơn trước khi cài đặt version thấp hơn . Nếu có thì ta cần phải thay đổi activation
key đó cho thích hợp với version thấp hơn trước khi cài đặt và reboot . Nếu không
hệ thống có thể không cho phép ta reload lại sau khi đã cài đặt software mới .

4. Password recovery :

Để vào chế độ enable trong PIX , cần phải biết password . Password được lưu
trong PIX sử dụng mã hóa MD5 , không phải ở dạng clear-text . Trong trường
hợp quên hoặc mất password console hoặc telnet vào PIX , giống như hầu hết
các sản phẩm của Cisco , PIX cũng cung cấp các thủ tục để khôi phục
password . Không giống như Cisco router là khôi phục password bằng cách
thay đổi thanh ghi cấu hình , PIX sử dụng một phương pháp khác . Khôi
phục password có thể được thực hiện trên PIX firewall bằng cách sử dụng
một file khôi phục password đặc biệt . Thực hiện khôi phục password
a trên PIX không có xóa cấu hình , chỉ có xóa password . Phụ thuộc vào |
các dòng sản phẩm của PIX mà ta có các phương pháp khôi phục password khác nhau . Thủ tục khôi phục pasword trong PIX bằng
đĩa mềm khác với khôi phục password ở các thiết bị PIX không có đĩa .
Sự khác nhau ở đây là PIX sẽ boot như thế nào với file mà ta sử

dụng
trong quá trình đó . Đối với PIX có đĩa mềm sẽ boot từ đĩa , còn những
PIX không có đĩa (diskless) sẽ boot từ TFTP server .
Bên cạnh binary file cần cho khôi phục password , ta còn cần các thành phần sau :

- Laptop hoặc là PC
- Terminal-emulating software
- TFTP software (cần cho các pix boot từ tftp)
- Công cụ rawrite.exe (cần cho các pix có đĩa mềm để tạo đĩa boot)

a. Khôi phục password cho các PIX 506 , 515 , 525 , 535 bằng TFTP

Khôi phục password cho các model này (các model không có đĩa mềm)
cần phải có TFTP server . Quá trình khôi phục như sau :
Bước 1 : download file npxx.bin với xx là version OS đang chạy trong
PIX . Ví dụ PIX đang chạy version 5.3(1) (biết được bằng cách show
version) thì file cần down là np53.bin
?Note : file np53.bin làm việc với tất cả các PIX OS 5.3(x) .
Bước 2 : chép file đó vào máy có cài TFTP server
Bước 3 : reboot PIX firewall , sau khoảng 10giây trong quá trình reboot .
Nhấn nút Escape hoặc Ctrl – Break để ngắt quá trình reboot , đưa Pix
vào chế độ *monitor*
monitor>
Bước 4 : chỉ ra interface của PIX firewall dùng cho TFTP . Để sử dụng
interface inside , dùng câu lệnh sau :
monitor > interface 1
Bước 5 : chỉ ra địa chỉ của interface PIX firewall
monitor> address ip_address
Bước 6 : chỉ ra default gateway (điều này chỉ cần thiết trong trường hợp
có mô hình là pix-router-TFTP server)
monitor> gateway ip_address
Bước 7 : chỉ ra địa chỉ của TFTP server

monitor>server ip_address_server

Bước 8 : kiểm tra kết nối đến TFTP server bằng cách ping đến TFTP server

monitor> ping ip_address_server

Bước 9 : chỉ ra filename của file dùng để khôi phuc password mà ta đã download trước đó

monitor> file npxx.bin

Bước 10 : khởi động chương trình TFTP .

monitor> tftp

b. khôi phục password cho các pix 510 , 520 bằng đĩa mềm :

Bước 1 : Download file npxx.bin (với xx là version của OS đang chạy trong PIX) .

Bước 2 : Chép file rawrite.exe vào cùng đường dẫn với OS version password mà ta đã download trước đó .

Bước 3 : Sau khi đã có được 2 file này , mở MS-DOS Window :

C :\> rawrite

Bước 4 : Reboot PIX firewall với đĩa mềm mà ta vừa tạo ra . Khi có dấu nhắc xuất hiện , sử dụng y để xóa password :

Do you wish to erase the passwords? [yn] y

Hệ thống sẽ tự động xóa password và bắt đầu reboot .

5. Nâng cấp Cisco PIX OS :

Có 3 thủ tục để nâng cấp PIX OS , và việc sử dụng thủ tục nào là do PIX OS đang chạy trong PIX và PIX model quyết định .

- Có thể sử dụng **copy tftp flash** command (đối với các PIX sử dụng software version 5.1 trở về sau thực hiện command này ở mode privileged)
- Nâng cấp OS ở monitor mode . Thủ tục này giống như thủ tục trên nhưng chỉ khác ở mode mà ta sử dụng khi copy file từ tftp server . Đối với các thiết bị PIX không có đĩa mềm bên trong (501 ,506 , 515 , 525 , 535) sẽ thực hiện nâng cấp image từ monitor mode . Đối với các PIX sử dụng version 5.0 trở về trước cần có một đĩa boothelper để tạo ra boothelper mode ,

tương tự như ROM monitor mode

- PIX firewall version 6.2 dùng HTTP client cho phép ta sử dụng
  câu lệnh **copy** để lấy thông tin cấu hình , software image , hay là
  Cisco PDM software từ HTTP server .

a. Nâng cấp OS sử dụng **copy tftp flash** command

Bước 1 : Download file pixnnx.bin (file binary software image , với
nn là version number , x là release number . Và chép file này vào tftp server
Bước 2 : sử dụng **copy tftp flash** command
Bước 3 : nhập địa chỉ IP của tftp server
Bước 4 : nhập source filename (file ta vừa download)
Bước 5 : nhập **Yes** để tiếp tục

b. Nâng cấp OS sử dụng monitor mode

Nếu PIX được nâng cấp từ version 5.0x hoặc trước đó lên version 5.1x trở về sau , cần sử dụng phương pháp boothelper mode hoặc là monitor mode . Bởi vì các version trước 5.1 , PIX firewall software
không có hỗ trợ **copy tftp flash** command
Các bước để nâng cấp PIX firewall sử dụng monitor mode :
Bước 1 : download binary software image file pixnnx.bin và chép file
này vào tftp server .
Bước 2 : reload lại PIX , nhấn Esc key (hoặc là nhấn Break) để vào
monitor mode . Đối với PIX firewall chạy version 5.0 trở về trước thì
sử dụng boothelper mode
Bước 3 : sử dụng **interface** command để chỉ ra PIX interface nào mà
TFTP server kết nối đến . Mặc định là interface 1 (inside)
monitor> **interface** *num*
Bước 4 : chỉ ra địa chỉ của interface
monitor> **address** *ip_address*
Bước 5 : chỉ ra default gateway (nếu cần)
monitor> **gateway** *ip_address*
Bước 6 : chỉ ra địa chỉ tftp server
monitor> **server** *ip_address*

Bước 7 : kiểm tra kết nối đến tftp server
monitor>**ping** *server_address*
Bước 8 : chỉ ra image filename :
monitor> **file** *name_file*
Bước 9 : bắt đầu quá trình tftp
monitor> tftp
Bước 10 : Khi xuất hiện prompt , gõ **y** để cài đặt image mới đến Flash .
Bước 11 : PIX firewall reboot và bắt đầu install image mới
?**Note** : Từ monitor hay boothelper mode , pix không sử dụng với Gigabit Ethernet

6. LAB :

Scenario :

Error!

Bài 1 : Upgrade image từ monitor mode
Trong bài này ta sẽ thực hiện nâng cấp image từ monitor mode theo
thứ tự các bước đã đưa ra ở phần trước .
Trước khi nâng cấp image , sử dụng **show version** command để xem version mà pix đang chạy , xem serial number và activation key .
?**Note** : Để bảo đảm an toàn , ta sẽ sử dụng lại image mà PIX đang chạy để thực hiện bài lab này

pixfirewall# sh version
Cisco PIX Firewall **Version 6.3(1)**
Cisco PIX Device Manager Version 3.0(1)
Compiled on Wed 19-Mar-03 11:49 by morlee
pix up 27 mins 25 secs
Hardware: PIX-506E, 32 MB RAM, CPU Pentium II 300 MHz
Flash E28F640J3 @ 0x300, 8MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
0: ethernet0: address is 000f.23ac.53f6, irq 10
1: ethernet1: address is 000f.23ac.53f7, irq 11
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled

Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
This PIX has a Restricted (R) license.
Serial Number: 808036792 (0x3029a9b8)
Running Activation Key: 0x9a5c6f78 0x67304d0a 0xed4c2329 0x89dd199b
Configuration last modified by enable_15 at 23:52:55.403 UTC Sun Mar 6 2005
Các bước thực hiện như sau :
pixfirewall>reload
Rebooting….
Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-506E
System Flash=E28F640J3 @ 0xfff00000
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Flash boot in 10 seconds.

Flash boot interrupted. ß Nhấn Esc hoặc Break
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 000f.23ac.53f7
Use ? for help.
monitor> ?
? this help message
address [addr] set IP address of the PIX interface on which
the TFTP server resides
file [name] set boot file name
gateway [addr] set IP gateway
help this help message
interface [num] select TFTP interface
ping <addr> send ICMP echo
reload halt and reload system
server [addr] set server IP address
tftp TFTP download

timeout TFTP timeout
trace toggle packet tracing
monitor> interface 1
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 000f.23ac.53f7
monitor> address 10.10.10.100
address 10.10.10.100
monitor> server 10.10.10.10
server 10.10.10.10
monitor> ping 10.10.10.10
Sending 5, 100-byte 0x13d ICMP Echoes to 10.10.10.10, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> file pix631.bin
file pix631.bin
monitor> tftp
tftp
pix631.bin@10.10.10.10 ……
……
……
…….
Received 656235 bytes
Cisco Secure PIX Firewall admin loader (3.0) #0: Thu Jul 17 08:01:09 PDT 2003
Flash =E28F640J3 @ 0xfff00000
BIOS Flash =AM29F400B @ 0xd8000
Flash version 6.3.1, Install version 6.3.1
Installing to flash
Serial Number: 808036792 (0x3029a9b8)
Activation Key: 0x9a5c6f78 0x67304d0a 0xed4c2329 0x89dd199b
Do you want to enter a new activation key ? **n**
Pix sẽ reboot và install image mới .
Bài 2 : Password recovery
Sau đây là bài password recovery được thực hiện trên PIX 506 .

Trước khi tiến hành khôi phục password , show version để kiểm tra pix đang chạy OS nào :

pixfirewall> sh version

Cisco PIX Firewall **Version 6.3(1)**
Cisco PIX Device Manager Version 3.0(1)
Compiled on Wed 19-Mar-03 11:49 by morlee
pix up 27 mins 25 secs
Hardware: PIX-506E, 32 MB RAM, CPU Pentium II 300 MHz
Flash E28F640J3 @ 0x300, 8MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
0: ethernet0: address is 000f.23ac.53f6, irq 10
1: ethernet1: address is 000f.23ac.53f7, irq 11
< -- omitted-- >

Quan sát thông tin từ show version ở trên , ta thấy pix hiện tại đang chạy OS version 6.3(1) . Do đó , để khôi phục password cho pix , ta cần phải có file np63.bin trong tftp server .

Bài làm được thực hiện dựa trên các bước khôi phục password đã nêu ở trên .

pixfirewall>en
password:

pixfirewall#enable password cisco

=>đặt password ở mode enable là cisco .

pixfirewall# write memory

Building configuration...
Cryptochecksum: 93bc4b61 43237b6a 67fe6565 ad91568d
[OK]

pixfirewall#reload

rebooting….
Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-506E
System Flash=E28F640J3 @ 0xfff00000
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Flash boot in 10 seconds.

Flash boot interrupted. ß Nhấn Esc hoặc Break

0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 000f.23ac.53f7
Use ? for help.
monitor> ?
? this help message
address [addr] set IP address of the PIX interface on which the TFTP
server resides
file [name] set boot file name
gateway [addr] set IP gateway
help this help message
interface [num] select TFTP interface
ping <addr> send ICMP echo
reload halt and reload system
server [addr] set server IP address
tftp TFTP download
timeout TFTP timeout
trace toggle packet tracing
monitor> interface ethernet1
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 000f.23ac.53f7
monitor> address 10.10.10.100
address 10.10.10.100
monitor> server 10.10.10.10
server 10.10.10.10
monitor> ping 10.10.10.10
Sending 5, 100-byte 0x9fd7 ICMP Echoes to 10.10.10.10, timeout is 4
seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> file np63.bin
file np63.bin
monitor> tftp

tftp np63.bin@10.10.10.10.....
.....
.....
Received 92160 bytes
Cisco Secure PIX Firewall password tool (3.0) #0: Thu Jul 17 08:01:09
PDT 2003
System Flash=E28F640J3 @ 0xfff00000
BIOS Flash=am29f400b @ 0xd8000
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
enable password qktPUfU6etg/RRvG encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration? [yn] y
Passwords and aaa commands have been erased.
Rebooting..

=> Hệ thống sẽ tự động xóa password và bắt đầu reboot .

Bài Viết Về PIX FIREWALL

Tác giả: Nguyễn Thị Băng Tâm

Chương 2: CẤU HÌNH CƠ BẢN CỦA PIX

1. ASA Security levels

Khi cấu hình PIX firewall , một điều quan trọng cần lưu ý là cấu hình pix có 2 interface cũng giống như cấu hình cho pix có 6 interface . Đó là vì PIX firewall hoạt động dựa trên cơ chế ASA (Adaptive Security Algorithm) sử dụng Security levels . Giữa 2 interface thì một sẽ có Security level cao hơn , một có Security level thấp hơn .

ASA Security levels :

Security level thiết kế cho interface là inside (trusted) hoặc interface outside (untrusted) quan hệ với các interface khác . Một interface được xem là inside trong mối quan hệ với các interface khác nếu nó có Security level cao hơn các interface khác , một interface được xem là outside nếu nó có Security level thấp hơn Security level của các interface khác .

Quy tắc cơ bản cho Security level là :

Khi PIX firewall được cấu hình với 6 command cơ bản , dữ liệu có thể đi vào pix thông qua một interface với Security level cao hơn , đi qua pix và đi ra ngoài thông qua interface có Security level thấp hơn . Ngược lại , dữ liệu đi vào interface có Security level thấp hơn không thể đi qua pix và đi ra ngoài thông qua interface có Security level cao hơn nếu trên pix không có cấu hình **conduit** hoặc **access-list** để cho phép nó thực hiện điều này .

Security level xắp xếp từ 0 đến 100 , cụ thể :

- Security level 100 : đây là Security level cao nhất cho một interface . Nó được sử dụng cho inside interface của PIX firewall , là cấu hình mặc định cho Pix và không thể thay đổi . Vì 100 là Security level trusted nhất cho interface , mạng của tổ chức thường ở sau interface này , không ai có thể truy nhập vào mạng này trừ khi được phép thực hiện điều đó . Việc cho phép đó phải được cấu hình trên pix , các thiết bị bên trong mạng này có thể truy cập ra mạng outside .
- Security level 0 : đây là Security level thấp nhất . Security level này được sử dụng cho outside interface . Đây là cấu hình mặc định cho Pix và không thể thay đổi . Vì 0 là Security level ít trusted nhất cho một interface , các untrusted network thường ở sau interface này . Các thiết bị ở outside chỉ được phép truy cập vào pix khi nó được cấu hình để làm điều đó . Interface này thường được dùng cho việc kết nối internet .
- Security level 1-99 : Các Security level này có thể được đăng kí cho perimeter interface kết nối đến PIX , mà thông thường là những kết nối đến một mạng hoạt động như là demilitarized zone (DMZ) . DMZ là một thiết bị hay là một mạng thường được sử dụng cho phép user từ untrusted network truy cập vào . DMZ là vùng được cách ly với môi trường internal , trusted .

Ví dụ về ASA với pix có 3 interface , Security level trong ví dụ này cụ thể như sau :

Error!

- Outside security 0 đến DMZ security 50 thì DMZ này được coi là inside . Do đó cần phải có **static translation** với **conduit** cấu hình cho phép các session được khởi tạo từ outside đến DMZ .
- Inside security 100 đến DMZ security 50 thì DMZ này được coi là outside . Do đó **global** và **nat** thường được cấu hình để

cho phép các session khởi tạo từ inside interface đến DMZ interface .

?**Note** : Một PIX firewall có thể có đến 4 perimeter network do đó nó có tối đa tổng cộng là 6 interfaces .

Khi có nhiều kết nối giữa PIX firewall và các perimeter device thì :

- Dữ liệu đi từ interface có Security level cao hơn đến interface có Security level thấp hơn : Cần phải có một translation (static hay dynamic) để cho phép traffic từ interface có Security level cao hơn đi đến interface có Security level thấp hơn . Khi đã có translation này , traffic bắt đầu từ inside interface đến outside interface sẽ được phép , trừ khi nó bị chặn bởi access-list , authentication hoặc là authorization .
- Dữ liệu đi từ interface có Security level thấp hơn đến interface có Security level cao hơn : 2 điều quan trọng cần thiết phải được cấu hình để cho traffic từ interface có security thấp hơn đến interface security cao hơn là static translation và conduit hoặc access-list . Nếu conduit được cấu hình , user cũng có thể chặn traffic nếu cấu hình thêm authentication hoặc là authorization .
- Dữ liệu đi qua 2 interface có Security level như nhau : Không có traffic đi giữa 2 interface có level như nhau .

2. Cấu hình cơ bản của PIX firewall

Phần này sẽ mô tả cấu hình cơ bản cần thiết để sử dụng PIX firewall và cách thiết lập kết nối cơ bản từ internal network đến public Internet .

a. **Các mode truy nhập** :

Cũng giống như các thiết bị của Cisco , pix cũng có các mode sau :

- Unprivileged mode : là mode được sử dụng khi ta truy nhập vào pix lần đầu tiên thông qua cổng console hoặc telnet . Mode này cho phép ta xem tập hợp các lệnh có trong pix . User không thể thay đổi cấu hình tại mode này .
- Privileged mode : tại mode này user có thể thay đổi một vài cấu hình hiện tại và xem cấu hình trong pix . Các câu lệnh ở mode unprivileged đều hoạt động tốt ở mode này . Khi ta đã vào được mode privileged , thì ta có thể vào được configuration mode .

- Configuration mode : Tại mode này ta có thể thay đổi cấu hình của hệ thống . Tất cả các lệnh unprivileged , privileged , configuration đều làm việc ở mode này .
- Monitor mode : Tại mode này cho phép ta thao tác một số cấu hình đặc biệt như là update image hay password recovery .

Dấu hiệu để nhận biết đang ở trong mode nào :

Mode	dấu hiệu
Unprivileged mode	Pixfirewall>
Privileged mode	Pixfirewall#
Configuration mode	Pixfirewall(config)#
Monitor mode	Monitor>

b. Các lệnh dùng để duy trì và kiểm tra PIX firewall

- Enable command : lệnh enable cho phép ta tiến vào mode privileged . Để thoát ra và trở về mode trước đó , sử dụng disable command .
- Enable password : tham số cấu hình này thiết lập password cho việc truy nhập vào mode enable . Không có password mặc định . Khi truy cập vào mode này lần đầu tiên (trước khi enable command được tạo ra) , pix đưa ra dấu nhắc cần nhập password . Bởi vì password chưa được cấu hình nên chỉ đơn giản là nhấn Enter . Password là case-sensitive và có thể dài đến 16 chữ cái . Ta có thể sử dụng bất kì kí tự nào ngoài khoảng trắng , dấu hỏi , và dấu hai chấm . Password ở dạng mã hóa .
- Passwd : password này được thiết lập cho inbound traffic telnet đến pix . Password mặc định là **cisco .**
- Hostname : câu lệnh hostname cho phép ta thay đổi tên của Pix , mặc định pix có tên là pixfirewall .
- Ping : lệnh ping quyết định PIX firewall có kết nối đến một đích cụ thể nào đó hay không . Khi ping command được sử dụng , pix sẽ gửi ra ngoài *echo-request.* Đích sẽ đáp lại bằng một *echo-reply.* nếu *echo-reply* được nhận thì host có tồn tại . Nếu không được nhận , ngõ ra sẽ xuất hiện “no response received” . Ping command truyền đi 3 echo-request để tìm địa

chỉ . Nếu ta muốn internal host có thể ping được external host , ta phải tạo một **ICMP conduit** hoặc là **access-list** để cho phép echo-reply .

?**Note**: Sau khi pix được cấu hình và hoạt động , user sẽ không thể từ outside interface ping được inside interface và ngược lại . Nếu từ inside interface ping thấy được inside network , và outside interface ping thấy outside network thì pix hoạt động đúng và bìng thường .

- Telnet : lệnh telnet cho phép ta chỉ ra host nào có thể truy cập cổng console PIX firewall thông qua telnet . Với các version 5.0 trở về trứơc , chỉ có các internal host mới có thể truy cập vào PIX firewall thông qua telnet , nhưng các version sau này , user có thể telnet vào PIX firewall qua tất cả các interface . Tuy nhiên , PIX firewall khuyến cáo rằng , tất cả telnet traffic đến outside interface phải được bảo vệ bởi IPSEC . Do đó , để khởi động một telnet session đến PIX , user cần cấu hình pix để thiết lập IPSEC tunnel hoặc là với một pix khác , hoặc là router , hay là VPN Client . Tunnel đó phải được mã hóa cho các traffic đặc biệt trong đó có telnet đến một host nào đó được định nghĩa trong câu lệnh telnet . Có đến 16 host hoặc mạng được phép telnet đến Pix , nhưng trong một lúc chỉ có 5 mà thôi .

  telnet ip_address [netmask] [if_name]
  clear telnet [ip_address] [netmask] [if_name]
  no telnet ip_address [netmask] [if_name]
  telnet timeout minutes
  show telnet
  show telnet timeout

- write terminal : cho xem cấu hình đang chạy trên pix , câu lệnh này có ý nghĩa như câu lệnh show running-config . Cấu hình này được lưu trong RAM
- write net : dùng để lưu running configuration vào TFTP server .
- write erase : xóa tập tin cấu hình trong Flash memory
- write memory : lưu tập tin running configuration vào Flash .
- write floppy : lưu cấu hình hiện tại vào đĩa mềm .
- write standby : ghi lại cấu hình được lưu trong RAM của active failover PIX , đến RAM của standby PIX firewall . Khi active PIX firewall boot , nó tự động ghi cấu hình này đến standby PIX firewall .

c. Sáu câu lệnh cơ bản cho cấu hình PIX firewall :

· Nameif command :

nameif *hardware_id if_name security_level*

câu lệnh nameif dùng để đăng kí 1 tên cho mỗi interface của Pix và chỉ ra mức security của nó (ngoại trừ outside và inside interface , chúng có tên mặc định)

Với cấu hình mặc định , e0 có tên là outside với mức security là 0 , e1 có tên là inside với mức security là 100 .

· Interface command :

interface *hardware_id hardware_speed [shutdown]*

- hardware_id : chỉ ra interface và vị trí vật lí của nó trên pix .

- hardware_speed : chỉ ra tốc độ kết nối . Sử dụng **auto** để pix tự động điều chỉnh tốc độ với thiết b

ị mà nó kết nối .

- shutdown : administratively shut down interface

?**Note**: tránh sử dụng từ khóa auto trên bất kì interface Ethernet nào . Duplex mismatch có thể xảy ra và làm giảm hoạt động của Pix .

· ip address command :

Mỗi interface trên pix phải được cấu hình với 1 địa chỉ .

ip address *if_name ip_address [netmask]*

· nat command :

Network address translation (NAT) giúp cho user dấu được địa chỉ internal khi đi ra mạng ngoài .

nat *(if_name) nat_id local_ip [netmask]*

- if_name : tên của internal interface sẽ sử dụng địa chỉ global . Dữ liệu sẽ đi ra khỏi pix thông qua interface được chỉ ra trong global command .
- nat_id : chỉ ra global pool , id này phải giống với id trong global commad
- local_ip : địa chỉ IP được đăng kí đến thiết bị của inside netword .0.0.0.0 (có thể viết tắt là 0) được sử dụng để cho phép tất cả các kết nối outbound được nat ra ngoài với địa chỉ trong global command .
- netmask : mặt nạ mạng cho local ip address

Khi bắt đầu cấu hình pix , tất cả các host có thể truy cập các kết nối outbound với **nat 1 0.0.0.0 0.0.0.0** command . Câu lệnh này có ý nghĩa cho phép tất cả các inside host được phép nat ra ngoài tương ứng với địa chỉ trong global command . 0 có thể được sử dụng để thay thế 0.0.0.0

· global command :

Khi dữ liệu được gửi đi từ một trusted network đến untrusted network, địa chỉ source ip thường được chuyển đổi . Pix thực hiện điều này bằng 2 câu lệnh , câu lệnh thứ nhất là **nat –** định nghĩa địa chỉ trusted source sẽ được chuyển đổi , câu lệnh thứ hai là global command - định nghĩa tầm địa chỉ mà source address sẽ chuyển đổi thành .

global *(if_name) nat_id* **interface** | *global_ip [- global_ip] netmask [global_mask]*

<u>Ví dụ về NAT :</u>

Khi gói dữ liệu outbound được gửi từ một thiết bị thuộc mạng inside đến pix , địa chỉ source được extract ra và so sánh với bảng chuyển đổi internal . Nếu địa chỉ của thiết bị không có trong bảng ,

nó sẽ được chuyển đổi thành . Một entry mới được tạo ra cho thiết bị đó , sau đó nó được đăng kí một địa chỉ global ip từ pool địa chỉ global . Đây được gọi là translation slot . Sau khi translation xảy ra , bảng được update và gói ip được chuyển đổi đó được gửi ra ngoài . Sau khoảng thời gian timeout (mặc định là 3 giờ) , sẽ không có gói tin được translate nào dành cho địa chỉ global đó , entry của nó ở trong bảng translation sẽ bị loại bỏ và địa chỉ global được sử dụng bởi bất kì host nào trong mạng inside .

Quá trình được miêu tả như hình vẽ sau :

Error!

?**NOTE** : PIX firewall đăng kí địa chỉ từ global pool bắt đầu từ thấp cho đến cao . Sau khi thay đổi , thêm vào , hay loại bỏ một global statement , sử dụng *clear xlate* để xóa tất cả các translation slot .

· Route command : định nghĩa một static route cho một interface .

route *if_name ip_address netmask gateway_ip [metric]*

3. PIX firewall translation

PIX firewall có thể được sử dụng để translate tất cả địa chỉ bên trong , khi dữ liệu đi từ inside ra outside hay đi đến một mạng có mức security thấp hơn . Nếu user ở mạng outside cố gắng thực hiện kết nối đến inside , user đó sẽ không thành công . Một session không thể được tạo ra từ Internet với địa chỉ đích là địa chỉ private trừ khi nó được cấu hình cho phép thực hiện điều đó .

Có hai cách để một mạng ít tin cậy hơn đi vào một mạng có độ tin cậy cao hơn là :

- *Response to Valid Request* : Khi user ở inside thành lập một kết nối đến thiết bị ở outside , mặc định response cho request đó được phép qua pix . Tất cả kết nối từ inside đến outside sẽ được update trong bảng translation . Khi một thiết bị outside đáp ứng cho request đó , PIX firewall sẽ kiểm tra bảng translation để xem thử có translation slot nào tồn tại cho request đó hay không ? Nếu nó tồn tại, PIX firewall cho phép response tiếp tục . Sau khi session được tạo ra , idle timer sẽ bắt đầu khởi động , mặc định là 3 giờ .
- *Cấu hình Conduit* : Được sử dụng cho việc liên lạc từ outside đến inside . Static translation hoặc là global và nat được cấu hình trước , sau đó cấu hình conduit để định nghĩa địa chỉ ,

hay là một nhóm địa chỉ , source port hay là destination port được phép đi qua pix .

a. **Static address translation** :

Static address translation được sử dụng nếu một host được translate đến cùng một địa chỉ khi mỗi outbound session được tạo ra qua pix . Tức là nó được dùng để tạo ra một ánh xạ cố định (static translation slot) giữa một địa chỉ local và một địa chỉ global . Khi kết nối đến internet , địa chỉ global phải được phải là địa chỉ thực (địa chỉ được đăng kí)

Static address translation được sử dụng bằng câu lệnh sau :

Static [*(internal_if_name , external_if_name)*] *global_ip local_ip* [**netmask** *network_mask] [max_conns [em_limit]] [norandomseq]*

Đối với outbound connection , sử dụng static để chỉ ra một địa chỉ global luôn được sử dụng cho việc translation giữa local host và global host đó . Đối với inbound connection , mặc định là các host ở untrusted network sẽ không được vào trusted network , do đó muốn cho các mạng outside vào inside , ta sẽ phải sử dụng kết hợp cả static command và conduit command để định nghĩa các địa chỉ trong mạng outside .

Một chú ý quan trọng là :

- **Conduit** command cho phép kết nối từ interface có mức bảo mật thấp hơn đến interface có mức bảo mật cao hơn .
- **Static** command được sử dụng để tạo ra ánh xạ cố định giữa local host và global ip address .

Conduit command :

conduit permit | deny *protocol global_ip global_mask [operator port [port]] foreign_ip foreign_mask [operator port [port]]*

Một ví dụ khi sử dụng conduit command là kiểm tra kết nối thông qua pix với các message ICMP . Để cho phép một gói tin echo-request từ outside qua pix , conduit phải được cấu hình . Ngoài ra , user outside cũng cần phải có một địa chỉ đích để sử dụng , thông tin này có thể được map vào pix sử dụng static command .

b. **Dynamic address translation** : đây chính là sử dụng nat và global command mà ta đã nhắc đến phía trước .

Ngoài ra thay vì nat các địa chỉ inside ra outside trong một pool địa chỉ , ta cũng có thể nat bằng một địa chỉ global bằng cách sử dụng PAT (port address translation) . PAT là sự kết hợp một địa chỉ và một source port number để tạo ra một session duy nhất . Pix

sẽ translate mỗi địa chỉ local đến cùng một địa chỉ global nhưng đăng kí giá trị port khác nhau và lớn hơn 1024. Câu lệnh cấu hình PAT giống như Nat , nhưng trong global command , thay vì sử dụng một pool địa chỉ ,ta chỉ sử dụng 1 địa chỉ .

c. Cấu hình NAT 0

Đây là chức năng phổ biến khi kết nối đến internet để cho phép truy cập từ outside đến HTTP server hoặc là SMTP server . Các server này phải có địa chỉ thực để còn liên lạc với các thiết bị khác trong mạng internet . Do đó có thể cấu hình pix để địa chỉ private của thiết bị đó trong inside network được phép đi ra ngoài mạng mà không có quá trình translation .

Sử dụng nat 0 command phụ thuộc vào chính sách bảo mật mà nơi ta áp đặt nó vào . Nếu chính sách đó cho phép các internal client sử dụng địa chỉ private của chúng để đi ra ngoài internet , nat 0 sẽ đáp ứng dịch vụ đó . Sử dụng nat 0 một minh sẽ không cho phép truy cập từ outside đến inside . Nếu chính sách cho phép truy cập từ outside đến inside , ta phải cấu hình thêm conduit command .

4. **Truy nhập vào PIX firewall**

Pix có thể được truy nhập vào thông qua port console hoặc là truy cập từ xa qua các phương pháp sau :

- telnet
- Secure Shell (SSH)
- Browser sử dụng PIX device Manger (PDM)

a. Truy cập vào PIX bằng Telnet

Có thể quản lí PIX firewall thông qua Telnet từ các host thuộc internal interface . Nếu IPSEC được cấu hình thì ta có thể quản lí PIX từ các interface có security level thấp hơn

Để truy cập vào PIX thông qua kết nối Telnet , ta cấu hình như sau :

bước 1 : cho phép host hay mạng được phép telnet :

telnet *local_ip [mask] [if_name]*

bước 2 : đặt password cho Telnet :

passwd *telnetpasswd*

bước 3 : Nếu cần thiết thì thiết lập cho phép Telnet session được idle trong khoảng bao lâu trước khi Pix làm rớt kết nối . Mặc định là 5 phút .

telnet timeout *time*

b. Cấu hình truy cập PIX qua Secure Shell (SSH)

SSH là một chương trình ứng dụng chạy trên lớp transport , có khả năng xác thực và mã hóa mạnh do đó nó có độ bảo mật cao hơn

Telnet . 5 SSH client có thể được phép truy cập PIX console đồng thời . PIX firewall hỗ trợ SSH v1 .

Cấu hình PIX cho việc truy cập thông qua SSH có 2 bước :

- Cấu hình trên PIX để chấp nhận kết nối SSH
- Cấu hình SSH client để kết nối đến PIX

5. LAB

Bài 1 : Cấu hình translation

Scenario :

Error!

Địa chỉ của các interface như sau :

Device	Interface	Address
PIX	E0 E1 E2	209.162.1.1/24 10.10.10.1/24 172.16.1.1/24
Router 2530	E0	209.162.1.2/24
Router dmz	E0	172.16.1.2/24
PC		10.10.10.10/24

Cấu hình toàn bộ :

Pix# write terminal

Building configuration...

: Saved

:

PIX Version 6.2(2)

nameif ethernet0 outside security0

nameif ethernet1 inside security100

nameif ethernet2 dmz security50

```
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pix
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list aclout deny tcp any any eq www
access-list aclout permit tcp 10.10.10.0 255.255.255.0 host
209.162.1.2 eq telnet access-list aclout permit tcp host
10.10.10.10 host 172.16.1.2 eq www
access-list aclout permit ip any any
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 209.162.1.1 255.255.255.0
ip address inside 10.10.10.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
pdm history enable
```

arp timeout 14400
global (outside) 1 209.162.1.30
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 209.162.1.10 172.16.1.2 netmask 255.255.255.255 0 0
static (inside,outside) 209.162.1.9 10.10.10.10 netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.1.5 10.10.10.10 netmask 255.255.255.255 0 0
access-group aclout in interface inside
conduit permit tcp host 209.162.1.10 eq www any
conduit permit tcp host 209.162.1.9 eq www any
conduit permit tcp host 209.162.1.9 eq telnet any
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 209.162.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet timeout 2
ssh timeout 5
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
2503#sh run
Building configuration...
Current configuration : 569 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
!
hostname 2503
!
enable password cisco
!
!
!
!
!
ip subnet-zero
!
!
!
!
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0
ip address 209.162.1.2 255.255.255.0
!
interface Serial0
no ip address
shutdown
no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
ip classless
ip http server
!
!
line con 0
```

line aux 0
line vty 0 4
no login
!
end
dmz#sh run
Building configuration...
Current configuration : 569 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dmz
!
enable password cisco
!
!
!
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
ip address 172.16.1.2 255.255.255.0
!
interface Serial0
no ip address
shutdown
no fair-queue
!
interface Serial1
no ip address
shutdown
!

```
interface BRI0
no ip address
shutdown
!
ip classless
ip http server
!
!
line con 0
line aux 0
line vty 0 4
no login
!
end
```

Cấu hình từng bước :

1. Command-line interface ;

Khi truy cập vào Pix sẽ vào mode unprivileged , sử dụng enable command để vào mode privileged

pixfirewall>enable

password :

=> trước khi vào mode enable , pix sẽ yêu cầu nhập password , mặc định là không có password nào cả , chỉ cần nhấn enter

pixfirewall#disable

pixfirewall> ß sử dụng disable để đưa pix về mode unprivileged

pixfirewall> ?

ð để xem những lệnh nào có thể dùng được ở mode này .

pixfirewall#configure terminal

pixfirewall(config)#

ð Pix đang ở trong mode configuration , tại đây ta có thể cấu hình mọi thứ cho PIX .

ð Tất cả câu lệnh sử dụng ở hai mode unprivileged và privileged đều có thể được sử dụng ở mode này .

Trước khi vào cấu hình sử dụng **show run** command để xem cấu hình mặc định của PIX

pixfirewall# sh run => hoặc có thể sử dụng write terminal command để xem

```
: Saved
:
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
pager lines 24
interface ethernet0 auto shutdown
interface ethernet1 auto shutdown
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 127.0.0.1 255.255.255.255
ip address inside 127.0.0.1 255.255.255.255
ip address dmz 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
```

failover ip address dmz 0.0.0.0
pdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end

Error!

Cấu hình hostname cho Pix :

pixfirewall(config)#hostname Pix
Pix(config)#

Error!

Cấu hình cho các interface :

- Đặt tên và level security cho các interface

Pix(config)#nameif e0 outside sec0
Pix(config)#nameif e1 inside sec100
Pix(config)#nameif e2 dmz sec50

- Up các interface đó lên :

Pix(config)# interface et1 auto
Pix(config)# interface ethernet0 auto
Pix(config)# interface e2 auto

Để kiểm tra xem các interface đã up lên chưa , sử dụng câu lệnh **show interface**

PIX(config)# sh interface
interface ethernet0 "outside" is up, line protocol is up

Hardware is i82559 ethernet, address is 000d.bda1.831d

IP address 127.0.0.1, subnet mask 255.255.255.255

MTU 1500 bytes, BW 10000 Kbit half duplex

53 packets input, 9948 bytes, 0 no buffer

Received 53 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 babbles, 0 late collisions, 0 deferred

0 lost carrier, 0 no carrier

input queue (curr/max blocks): hardware (128/128) software (0/1)

output queue (curr/max blocks): hardware (0/0) software (0/0)

interface ethernet1 "inside" is up, line protocol is up

Hardware is i82559 ethernet, address is 000d.bda1.831e

IP address 127.0.0.1, subnet mask 255.255.255.255

MTU 1500 bytes, BW 100000 Kbit full duplex

133 packets input, 22702 bytes, 0 no buffer

Received 133 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 babbles, 0 late collisions, 0 deferred

0 lost carrier, 0 no carrier

input queue (curr/max blocks): hardware (128/128) software (0/1)

output queue (curr/max blocks): hardware (0/0) software (0/0)

interface ethernet2 "dmz" is up, line protocol is up

Hardware is i82559 ethernet, address is 0002.b3d5.285d

IP address 127.0.0.1, subnet mask 255.255.255.255

MTU 1500 bytes, BW 10000 Kbit half duplex

<omitted>

ð Câu lệnh show interface cho phép user xem thông tin về interface ethernet , Token Ring , FDDI . Thông tin về interface nào là phụ thuộc cái nào được cài đặt trong pix . Trong trường hợp này là Ethernet . Ta có thể xem một số thông tin sau :

- Ethernet , Token Ring , FDDI : cho ta biết user đã sử dụng interface command để cấu hình interface . Cho biết interface là inside hay là outside .
- Line protocol up : cho biết cable hoạt động tốt (layer 1 connectivity)
- Line protocol down : cho biết hoặc là cable cắm vào interface không đúng , hoặc là nó không được cắm vào interface connector .
- Network interface type : chỉ ra network interface
- Mac address : cho biết địa chỉ MAC
- IP address : chỉ ra địa chỉ Ip được đăng kí cho interface , địa chỉ mặc định là 127.0.0.1 với subnet mask là 255.255.255.255
- MTU : kích thước được tính bằng byte mà dữ liệu có thể được gửi đi tốt nhất qua mạng .
- Line speed : tốc độ của interface , 10BaseT là 10000Kbps , 100BaseT là 100000Kbps
- Line duplex status : chỉ ra rằng pix đang chạy full-duplex hay là half-duplex .

v.v....

· Đăng kí địa chỉ cho interface :

Pix(config)# ip address inside 10.10.10.1 255.255.255.0
Pix(config)# ip address outside 209.162.1.1 255.255.255.0
Pix(config)# ip address dmz 172.16.1.1 255.255.255.0

Xem thông tin về địa chỉ của các interface , sử dụng **show ip address** command :

Pix# sh ip add
System IP Addresses:
ip address outside 209.162.1.1 255.255.255.0
ip address inside 10.10.10.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
Current IP Addresses:
ip address outside 209.162.1.1 255.255.255.0
ip address inside 10.10.10.1 255.255.255.0

ip address dmz 172.16.1.1 255.255.255.0

Error!

Cấu hình cho router 2530 :

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname 2503

2503(config)#int e0

2503(config-if)#ip add 209.162.1.2 255.255.255.0

2503(config-if)#no shut

2503(config-if)#exit

2503(config)#ip http server

2503(config)#enable pass cisco

2503(config)#line vty 0 4

2503(config-line)#no login

2503(config-line)#exit

2503(config)#int loopback 0

2503(config-if)#ip add 192.168.1.1 255.255.255.0

2503(config-if)#exit

2503(config)#exit

Error!

Cấu hình cho router dmz :

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname dmz

dmz(config)#int e0

dmz(config-if)#ip add 172.16.1.2 255.255.255.0

dmz(config-if)#no shut

dmz(config-if)#exit

dmz(config)#line vty 0 4
dmz(config-line)#no login
dmz(config-line)#exit
dmz(config)#ip http server
dmz(config)#enable pass cisco
dmz(config)#exit

Error!

Kiểm tra kết nối

Như ta đã biết mặc định các host trong một mạng chỉ ping được interface của pix mà mạng đó kết nối tới .

Pix# ping inside 10.10.10.10
10.10.10.10 response received -- 0ms
10.10.10.10 response received -- 0ms
10.10.10.10 response received -- 0ms
2503#ping 209.162.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.162.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Pix(config)# ping 209.162.1.2
209.162.1.2 response received -- 0ms
209.162.1.2 response received -- 0ms
209.162.1.2 response received -- 0ms
dmz#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Pix# ping dmz 172.16.1.2
172.16.1.2 response received -- 0ms
172.16.1.2 response received -- 0ms
172.16.1.2 response received -- 0ms

Error!

Cấu hình translation :

Pix(config)# route outside 0.0.0.0 0.0.0.0 209.162.1.2 1
Pix(config)# nat (inside) 1 0 0 0

Pix(config)# global (outside) 1 209.162.1.30
Global 209.162.1.30 will be Port Address Translated
Pix(config)# static (dmz,outside) 209.162.1.10 172.16.1.2
Pix(config)# static (inside,outside) 209.162.1.9 10.10.10.10
Pix(config)# static (inside,dmz) 172.16.1.5 10.10.10.10
Kiểm tra cấu hình bằng các lệnh show :
Pix# sh static
static (dmz,outside) 209.162.1.10 172.16.1.2 netmask 255.255.255.255 0 0
static (inside,outside) 209.162.1.9 10.10.10.10 netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.1.5 10.10.10.10 netmask 255.255.255.255 0 0
Pix# sh nat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
Pix# sh global
global (outside) 1 209.162.1.30
Pix(config)# sh route
outside 0.0.0.0 0.0.0.0 209.162.1.2 1 OTHER static
inside 10.10.10.0 255.255.255.0 10.10.10.1 1 CONNECT static
dmz 172.16.1.0 255.255.255.0 172.16.1.1 1 CONNECT static
outside 209.162.1.0 255.255.255.0 209.162.1.1 1 CONNECT static

ðMặc định trong bảng định tuyến của pix có các route là **connect static** . Các route được cấu hình sẽ có prompt là **other static**

Để các host giữa các mạng có thể ping thấy nhau , ta phải dùng conduit command để thực hiện điều này :
Pix(config)# conduit permit icmp any any
Pix(config)# conduit permit tcp host 209.162.1.10 eq www any
Pix(config)# conduit permit tcp host 209.162.1.9 eq www any
Pix(config)# conduit permit tcp host 209.162.1.9 eq telnet any

ð Tạo conduit để cho phép tất cả các host ở mạng outside (any) có thể truy cập web vào web server ở dmz và inside , có thể telnet vào mạng inside .
Kiểm tra cấu hình conduit :
Pix# sh conduit
conduit permit tcp host 209.162.1.10 eq www any (hitcnt=0)
conduit permit tcp host 209.162.1.9 eq www any (hitcnt=0)

conduit permit tcp host 209.162.1.9 eq telnet any (hitcnt=1)
conduit permit icmp any any (hitcnt=42)
Pix(config)# ping 192.168.1.1
192.168.1.1 response received -- 0ms
192.168.1.1 response received -- 0ms
192.168.1.1 response received -- 0ms
Tại command-prompt của PC , thực hiện ping :
C:\> ping 209.162.1.2
Ping 209.162.1.2 with 32 bytes of data :
Reply from 209.162.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 209.162.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 209.162.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 209.162.1.2 : bytes = 32 time<10ms TTL = 128
Bật debug lên để quan sát :
Pix(config)#debug icmp trace
39: Outbound ICMP echo request (len 32 id 3 seq 12800) 10.10.10.10 > 209.162.1.9 > 209.162.1.2
40: Inbound ICMP echo reply (len 32 id 3 seq 12800) 209.162.1.2 > 209.162.1.9 > 10.10.10.10
41: Outbound ICMP echo request (len 32 id 3 seq 13056) 10.10.10.10 > 209.162.1.9 > 209.162.1.2
42: Inbound ICMP echo reply (len 32 id 3 seq 13056) 209.162.1.2 > 209.162.1.9 > 10.10.10.10
C:\> ping 172.16.1.2
Ping 172.16.1.2 with 32 bytes of data :
Reply from 172.16.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 172.16.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 172.16.1.2 : bytes = 32 time<10ms TTL = 128
Reply from 172.16.1.2 : bytes = 32 time<10ms TTL = 128
Pix# 43: Outbound ICMP echo request (len 32 id 3 seq 13312) 10.10.10.10 > 172.16.1.5 > 172.16.1.2
44: Inbound ICMP echo reply (len 32 id 3 seq 13312) 172.16.1.2 > 172.16.1.5 > 10.10.10.10
45: Outbound ICMP echo request (len 32 id 3 seq 13568) 10.10.10.10 > 172.16.1.5 > 172.16.1.2
46: Inbound ICMP echo reply (len 32 id 3 seq 13568) 172.16.1.2 > 172.16.1.5 > 10.10.10.10
47: Outbound ICMP echo request (len 32 id 3 seq 13824) 10.10.10.10 > 172.16.1.5 > 172.16.1.2

48: Inbound ICMP echo reply (len 32 id 3 seq 13824) 172.16.1.2 > 172.16.1.5 > 10.10.10.10
49: Outbound ICMP echo request (len 32 id 3 seq 14080) 10.10.10.10 > 172.16.1.5 > 172.16.1.2
50: Inbound ICMP echo reply (len 32 id 3 seq 14080) 172.16.1.2 > 172.16.1.5 > 10.10.10.10
Kiểm tra quá trình translation :
Pix(config)# show xlate
2 in use, 2 most used
Global 172.16.1.5 Local 10.10.10.10
Global 209.162.1.9 Local 10.10.10.10
dmz#ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/180/200 ms
2530#ping 209.162.1.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.162.1.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/180/200
Kiểm tra các host inside có thể truy cập internet (mạng outside)
Error!

Bây giờ ta tạo một access-list cho outbound traffic như sau :

- từ chối outbound web traffic
- cho phép outbound traffic còn lại

Cấu hình như sau :
Tạo một access-list có tên là aclout .
Pix(config)# access-list aclout deny tcp any any eq www
Pix(config)#access-list aclout permit tcp host 10.10.10.10 host 172.16.1.2 eq www
=>mặc dù không cần thiết nhưng ta vẫn cấu hình cho phép các host trong mạng inside được phép đi web đến dmz .
Pix(config)# access-list aclout permit ip any any
Pix# sh access-list aclout

access-list aclout; 3 elements
access-list aclout deny tcp any any eq www (hitcnt=6)
access-list aclout permit tcp host 10.10.10.10 host 172.16.1.2 eq www (hitcnt=0)
access-list aclout permit ip any any (hitcnt=45)
Áp access-list aclout vào interface inside bằng lệnh access-group
Pix(config)# access-group aclout in interface inside
Kiểm tra :

Error!

ð từ PC không thể đi web ra mạng ngoài được .

Sau khi hoàn tất , thực hiện lưu cấu hình vào flash :

Pix(config)# write memory

Bài Viết Về PIX FIREWALL

Tác giả: Nguyễn Thị Băng Tâm

Chương 3: CẤU HÌNH PIX VỚI SSH

Error!

1. Cấu hình hostname và domain name cho PIX để tạo ra RSA key .

pixfirewall(config)# hostname PIX
PIX(config)# domain-name cisco.com

2. Cấu hình cho interface e1 :

PIX(config)# int e1 auto
PIX(config)# ip address inside 192.168.1.1 255.255.255.0
PIX(config)# exit
PIX# ping inside 192.168.1.2
192.168.1.2 response received -- 0ms
192.168.1.2 response received -- 0ms
192.168.1.2 response received -- 0ms

Tạo ra cặp RSA key và lưu các key này vào Flash :

PIX(config)# ca generate rsa key 123456 2048
For <key_modulus_size> >= 1024, key generation could take up to several minutes. Please wait.

3. Kiểm tra RSA public key vừa tạo :

PIX(config)# sh ca mypubkey rsa
% Key pair was generated at: 21:36:01 UTC Mar 10 2005
Key name: **PIX.cisco.com**
Usage: General Purpose Key
Key Data:
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
00b164bb 78da41b9 9b785ef3 806869da 42ef8df9 2e07039b 2b0d97dd 2fea856f
3a7c69fb c6ca8053 e11d50be 77ef63a3 b3449f71 99e4626a 3b6d21a1 0ef4aa63
0f0be998 13554e86 99eaf444 993e3c7e 828b24bd f5364037 764b6eaa f2706c28
0f688057 7b1a7704 06aef687 9a799369 a9face11 dbd9c719 a494da4f 2e0adaa3

e648fa63 c8eec049 27523b78 85262db5 64c9efe5 16632db8 85811fac e6f1f971
e012c745 874dd6c6 437e01e2 4e8651e1 7926bdb4 95312e3c f6f2d167 b78ef8aa
d0cc548f bc88b236 62bd29f6 02b4d17c 28aeb44b 718e5a84 85d3bd76 563b676a
45b93eb8 6dd7d9db 6b688e9f a163357a 4913f2e8 7e07ba25 9b42bcd1 9a15b93e
7f020301 0001

4. Sau khi tạo được key cần phải lưu key vào Flash . nếu không thì có thể xóa key trong lần reload tới .

PIX(config)# ca save all

5. Chỉ ra host nào được phép đến SSH
   PIX(config)# ssh 192.168.1.1 255.255.255.255 inside
   PIX(config)# ssh timeout 60
6. Đặt password enable và password telnet

PIX(config)# passwd vnpro
PIX(config)# enable password cisco

7. Cấu hình SSH client để kết nối đến PIX

Bước 1 : cài đặt SSH client software vào PC

Bước 2 : chọn setting từ Edit menu :

Error!

Bước 3 : click vào Connection từ list dưới Profile setting . Trong **hostname field** nhập IP address của PIX , **username field** nhập PIX , trong authentication methods chọn **password**

Error!

Bước 4 : click vào Cipher List . Không đánh dấu tất cả các cipher ngoại trừ một cipher mà ta sẽ sử dụng . Khi cipher đã được chọn , sử dụng mũi tên UP để đưa cipher mà ta chọn lên đầu tiên .

Error!

Bước 5 : để tránh việc phải điền thông tin mỗi lần sử dụng SSH client , chọn Save Setting từ File menu .

Bước 6 : chọn Quick Connect để kết nôí , điền thông tin vào các field

Error!

Xuất hiện một bảng warning , chọn **Yes**

Error!

Nếu lần đầu tiên kết nối đến PIX với SSH , ta phải trao đổi Public Key cho nhau để mã hóa session . SSH client sẽ đưa ra dấu nhắc , click YES để lưu Public Key của PIX đến local database :

Error!

Bước 7 : Sau khi đã lưu xong key , SSH client yêu cầu nhập password telnet .

Sau khi nhập telnet password xong nếu thành công ta sẽ vào được PIX . Khi đó kết nối bảo mật đến pix đã được tạo ra , lúc này ta có thể quản lí pix qua SSH connection

Error!

Trong quá trình tạo SSH connection đến PIX , sử dụng **debug ssh command** để quan sát .

```
PIX# debug ssh
SSH debugging on
SSH: Device opened successfully.
SSH: host key initialised
SSH: license supports 3DES: 3
SSH: license supports DES: 3
SSH0: SSH client: IP = '192.168.1.2'  interface # = 1
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: send SSH message: outdata is NULL
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.5-3.2.9 (compat mode)
SSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 330 ms
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: send SSH message: SSH_SMSG_PUBLIC_KEY (2)
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: receive SSH message:
```

SSH_CMSG_SESSION_KEY (3)
SSH0: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 272
SSH0: client requests 3DES cipher: 3
SSH0: send SSH message: SSH_SMSG_SUCCESS (14)
SSH0: keys exchanged and encryption on
SSH: Installing crc compensation attack detector.
SSH0: receive SSH message: SSH_CMSG_USER (4)
SSH0: authentication request for userid PIX
SSH(PIX): user authen method is 'no AAA', aaa server group ID = 0
SSH0: authentication successful for PIX

Bài Viết Về PIX FIREWALL

Tác giả: Nguyễn Thị Băng Tâm

Chương 4 : **CẤU HÌNH AAA TRÊN PIX FIREWALL**

Bài Lab cấu hình AAA với PIX

Scenario :

Error!

Địa chỉ của các interface :

Device	Interface	Address
PIX	E0 E1	209.162.1.1/24 172.16.1.2/24
Router	E0	209.162.1.2/24
PC		172.16.1.1/24

Cấu hình toàn bộ :

Error!

Cấu hình của PIX :

Pix(config)# sh run
: Saved
:
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pix
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
pager lines 24
logging console debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 209.162.1.1 255.255.255.0
ip address inside 172.16.1.2 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
global (outside) 1 209.162.1.30
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 209.162.1.2 1
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
timeout xlate 3:00:00

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server ccsp protocol tacacs+
aaa-server ccsp (inside) host 172.16.1.1 pixfirewall timeout 10
aaa authentication telnet console ccsp
aaa authentication http console ccsp

- bằng enable console :

Pix(config)# aaa authentication enable console ccsp

Để xác thực user bằng enable console , trên CSACS ta cấu hình thêm như sau :

- Tại interface configuration , chọn **TACACS + (cisco IOS)** .
- tại cửa sổ TACACS + (cisco IOS) , chọn advanced configuration options , tại đây chọn **Advanced TACACS+ features .** Sau khi thao tác xong , click **Submit** để bật tính năng advanced features .
- tại cửa sổ user setup => Advanced TACACS+ setting => TACACS +enable Control => **max privileged for any AAA client ,** tại đây chọn **level 15 .** Sau đó đến TACACS +enable password , nhập password mà ta muốn xác thực enable console , trong bài này password được nhập vào là **cisco .** Sau khi hoàn tất , click **Submit** .

Tại PIX , ta thoát ra ngoài mode unprivileged ,

Pix#exit

Pix> 611103: User logged out: Uname: enable_15

Để vào lại mode privileged , xuất hiện dấu nhắc đòi nhập username và password

Pix>en

Username: aaauser

Password: *******

Username:

Access denied.

=> bị deny là do ta nhập password *aaapass*

Pix> 308001: PIX console enable password incorrect for 3 tries (from PIX console)

Pix> en

Username: aaauser

Password: *****

Pix# 502103: User priv level changed: Uname: enable_1 From: 1 To: 15

111008: User 'enable_1' executed the 'enable' command.

ð Vào được mode enable là do nhập password enable mà ta đã cấu hình phía trước trong ACS server .

15. Cấu hình xác thực traffic đi qua PIX :

Pix(config)# aaa authentication include http outbound 0 0 0 0 ccsp

Pix(config)# aaa authentication include telnet outbound 0 0 0 0 ccsp

ð Cấu hình xác thực cho các traffic đi từ inside đến outside với group tag là ccsp .

Kiểm tra cấu hình :

Pix(config)# sh aaa authentication

aaa authentication telnet console ccsp

aaa authentication http console ccsp

aaa authentication enable console ccsp

aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

aaa authentication include telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

Tại PC command-prompt , telnet vào router 2530 :

Error!

Quan sát debug :

Pix# 305011: Built dynamic TCP translation from inside:172.16.1.1/2522 to outside:209.162.1.30/1056

109001: Auth start for user '???' from 172.16.1.1/2522 to 209.162.1.2/23

109011: **Authen Session Start: user 'aaauser', sid 3**

109005: **Authentication succeeded for user 'aaauser' from 172.16.1.1/2522 to 209.162.1.2/23 on interface inside** => */23 cho biết ta đang telnet* .

302013: Built outbound TCP connection 16 for outside:209.162.1.2/23 (209.162.1.2/23) to inside:172.16.1.1/2522 (209.162.1.30/1056) (aaauser)

Sau khi xác thực thành công , sử dụng command **show uauth** để xem thống kê của quá trình này :

Pix(config)# sh aaa uauth

Current Most Seen

Authenticated Users 1 1

Authen In Progress 0 1

user 'aaauser' at 172.16.1.1, authenticated

absolute timeout: 0:05:00

inactivity timeout: 0:00:00

Muốn xác thực lại ta cần phải refresh lại quá trình này :

Pix(config)# clear uauth

?**NOTE** : Đối với inbound traffic ta cũng thực hiện tương tự .

Như ta đã biết sử dụng virtual telnet để xác thực các traffic không hỗ trợ quá trình này . Trong bài này giả sử user muốn truy cập đến dịch vụ có port 49 .

- **Đối với inbound traffic** , địa chỉ virtual telnet phải là địa chỉ được định tuyến đến pix . Trong bài này , PIX được cấu hình để yêu cầu xác thực cho việc outbound access đến TCP port 49 . Client inside muốn sử dụng dịch vụ này , sẽ telnet đến địa chỉ virtual telnet 209.162.1.4

Pix(config)# virtual telnet 209.162.1.4
Pix(config)# aaa authenticaton include tcp/49 outbound 0 0 0 0 ccsp
Kiểm tra tương tự như lần trước , nhưng ở command-prompt của PC , thay vì telnet đến địa chỉ 209.162.1.2 ta sẽ telnet đến địa chỉ 209.162.1.4 sẽ thành công .
Quan sát debug để kiểm tra kết quả :
Pix(config)# 305011: Built dynamic TCP translation from inside:172.16.1.1/2878 to outside:209.162.1.30/1065
109001: **Auth start for user '???' from 172.16.1.1/2878 to 209.162.1.4/23**
109011: Authen Session Start: user 'aaauser', sid 6
109005: Authentication succeeded for user 'aaauser' from 172.16.1.1/2878 to 209.162.1.4/23 on interface inside

- **Đối với inbound traffic** ta cũng tiến hành tương tự nhưng thông thường người ta thường không cấu hình cho các host outside được phép telnet đến các host inside .

Cấu hình virtual telnet inbound :
Pix(config)# aaa authentication include tcp/49 inbound 0 0 0 0 ccsp
Pix(config)#conduit permit tcp host 209.162.1.4 eq telnet any
Pix(config)#conduit permit tcp host 209.162.1.5 eq 49 any
PIX(config)# sh aaa authentication
aaa authentication telnet console ccsp
aaa authentication http console ccsp
aaa authentication enable console ccsp
aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp
aaa authentication include telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp
aaa authentication include tcp/49 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

aaa authentication include tcp/49 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

Error!

Cấu hình authorization :

Kiểm tra lại cấu hình :

Pix(config)# sh conduit

conduit permit tcp host 209.162.1.4 eq telnet any (hitcnt=0)

conduit permit tcp host 209.162.1.5 eq tacacs any (hitcnt=0)

conduit permit icmp any any (hitcnt=0)

Như ta đã thực hiện phía trước , các host inside và outside có thể ping thấy nhau , các host inside có thể telnet vào host ở outside . Sau đây ta bật tính năng authorization trên pix , thì ping và telnet sẽ không thành công .

Pix(config)# aaa authorization include telnet outbound 0 0 0 0 ccsp

Pix(config)# aaa authorization include icmp/8 outbound 0 0 0 0 ccsp

ð Cấu hình PIX yêu cầu cấp quyền cho tất cả các outbound traffic ICMP và telnet .

Kiểm tra lại cấu hình :

PIX(config)# sh aaa autho

aaa authorization include telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ccsp

Thực hiện Ping và telnet :

Từ PC telnet vào router 2530 , tại command-prompt ta thấy telnet không thành công:

Error!

Từ PC ping router 2530 cũng không thành công :

Error!

Quan sát debug :

PIX(config)# 109001: Auth start for user '???' from 172.16.1.1/3719 to 209.162.1.2/23

109011: Authen Session Start: user 'aaauser', sid 9

109005: Authentication succeeded for user 'aaauser' from 172.16.1.1/3719 to 209.162.1.2/23 on interface inside

109008: **Authorization denied for user 'aaauser' from 172.16.1.1/3719 to 209.162.1.2/23 on interface inside**

109001: Authen start for user 'aaauser' from 172.16.1.1/0 to 209.162.1.2/0

109008: **Authorization denied for user 'aaauser' from 172.16.1.1/0 to 209.162.1.2/0 on interface inside**

Authorization bị từ chối là vì trên CSACS server ta chưa có cấu hình cấp quyền cho user :

Trên CSACS :

- click vào **Group Setup** để mở Group Setup interface
- Chọn **Default Group** (1user) từ group drop-down menu
- Kiểm tra rằng user thuộc về group đã được chọn . Click vào **Users in Group** để kiểm tra thông tin về user như sau :

User : aaauser
Status : Enabled
Group : Default Group (1 user)

- Click vào **Edit Settings** , vào group setting , cấu hình như hình sau :

Error!

Sau khi cấu hình authorization cho telnet traffic xong , click Submit để cấp quyền cho các traffic khác , mà cụ thể là ICMP traffic .

Error!

- Click submit+restart để lưu cấu hình và restart lại CSACS .

Kiểm tra telnet và ping lại như sau :

Từ PC telnet vào router sẽ thành công . Quan sát debug :

PIX(config)# 109001: Auth start for user 'aaauser' from 172.16.1.1/3791 to 209.162.1.2/23

thực , sử dụng câu lệnh **aaa authentication** để bật hay tắt việc xác thực user . Có các loại xác thực sau :

a. **Xác thực khi user truy cập vào PIX** :

Câu lệnh : **aaa authentication [serial | enable | telnet | ssh | http] console <group_tag>**

Xác thực việc access vào pix console có nhiều loại khác nhau tùy thuộc vào option được chọn . Enable option cho phép 3 lần thử trước khi từ chối việc access . Serial và telnet cho phép user thử nhiều lần cho đến khi log in vào được thiết bị .

Telnet cho phép ta chỉ ra host nào có thể access vào pix . Đối với các OS version 5.0 trở về trước , telnet đến pix chỉ được thực hiện từ internal interface đi ra mạng ngoài, không cho phép outside interface . Nhưng các version OS sau này đều hỗ trợ tính năng này . Tuy nhiên, PIX firewall bắt buộc rằng tất cả telnet traffic đến outside interface phải được bảo vệ bởi IPSEC . Do đó , để khởi động một telnet session đến outside interface , cấu hình IPSEC ở outside interface bao gồm cả IP traffic do pix tạo ra . Chỉ có traffic trở về telnet client được gửi qua IPSEC tunnel , không phải là tất cả traffic được phát ra bởi outside interface .

b. **Xác thực cho traffic đi qua pix** :

Câu lệnh :

aaa authentication {include | exclude} <*authen_service*> **{inbound | outbound | <interface>}** <*local_ip*> <*local_mask*> <*foreign_ip*> <*foreign_mask*> <*group_tag*>

include : tạo ra một quy tắc mới cho dịch vụ cụ thể nào đó .

exclude : chỉ ra host nào đó được bỏ qua các quy tắc mà ta đã định nghĩa trước đó

authen_service : dịch vụ mà user muốn access vào . Tham số này có thể là ftp , telnet , http , hay là cả 3 dịch vụ trên (any) .

inbound : xác thực các kết nối inbound . Inbound có nghĩa là kết nối đó được khởi tạo từ interface outside đến interface inside .

outbound : xác thực các kết nối outbound . Outbound có nghĩa là kết nối được khởi tạo từ inside interface đến outside interface .

if_name : tên của interface mà ở đó user cần xác thực . Sử dụng if_name , cộng với local_ip và foreign_ip để biết được kết nối được khởi tạo từ đâu đến đâu .

local_ip : địa chỉ IP của host hoặc mạng được xác thực . Địa chỉ này có thể được set đến 0 , có nghĩa là tất cả các host được xác thực . Local_ip luôn luôn nằm ở interface có mức bảo mật cao nhất .

local_mask : network mask của local_ip . Sử dụng 0 nếu địa chỉ IP là 0 . Sử dụng 255.255.255.255 nếu IP là dành cho một host .
foreign_ip : là địa chỉ IP của các host mà local_ip có khả năng truy cập đến . Sử dụng 0 cho tất cả các host .
foreign_mask : giống local_mask
group_tag : là tag group trong lệnh aaa-server
PIX firewall chỉ cho phép chỉ một giao thức authentication cho một mạng . Ví dụ , nếu một mạng kết nối inbound thông qua PIX firewall sử dụng TACACS + , thì cùng mạng đó không thể kết nối inbound thông qua PIX sử dụng RADIUS . Tuy nhiên , nếu một mạng kết nối inbound thông qua pix sử dụng TACACS+ , một mạng khác có thể kết nối inbound qua PIX sử dụng RADIUS .

c. **Xác thực cho các dịch vụ khác**

PIX firewall xác thực user thông qua Telnet , FTP , HTTP . Nhưng nó cũng có thể xác thực các loại dịch vụ khác . Ví dụ , PIX có thể được cấu hình để xác thực user khi user cần sử dụng dịch vụ Microsoft file server ở port 139 . Khi user được yêu cầu xác thử để access vào các dịch vụ khác ngoài Telnet , FTP , HTTP , họ cần thực hiện một trong các bước sau :

- Option 1 : xác thực đầu tiên bằng việc truy cập vào Telnet , FTP , hay HTTP server trước khi truy cập các dịch vụ khác .
- Option 2 : xác thực đến PIX virtual telnet trước khi truy cập vào các dịch vụ khác.

Khi không có các telnet , FTP , hay HTTP server để xác thức , hay chỉ làm đơn giản xác thực người dùng , PIX firewall cho phép sử dụng một virtual telnet hay http . Điều này cho phép user xác thực trực tiếp với pix qua địa chỉ IP của virtual telnet hay http .

Error!

Virtual telnet :

Virtual telnet cho phép các user cần có các kết nối thông qua pix sử dụng các dịch vụ hoặc các giao thức không hỗ trợ xác thực . User chỉ đơn giản telnet đến địa chỉ IP virtual , sử dụng AAA username , password của user . AAA server sẽ xác thực điều này . khi user đã được xác thực , pix đóng kết nối telnet đó lại , cất giữ thông tin xác thực trong suốt khoảng thời gian **uauth .**

Câu lệnh tạo ra virtual telnet server :

Virtual telnet <*ip_address*>

Ip_address phải là địa chỉ được định tuyến đến PIX .

Sử dụng virtual telnet không chỉ cho việc *log in* mà còn dành cho việc *log out* . Sau khi xác thực thành công thông qua virtual telnet

, user sẽ không phải xác thực trở lại cho đến khi hết thời gian *uauth* . Nếu ta không muốn sử dụng dịch vụ nữa , và muốn chặn không cho các traffic qua firewall sử dụng thông tin xác thực của mình , ta có thể telnet đến virtual telnet lại một lần nữa . Điều này sẽ kết thúc phiên làm việc và log out .

Error!

Virtual http :

Nếu xác thực được yêu cầu trong các site ngoài cũng như trong bản thân PIX , vì các browser có lưu username và password nên có thể việc xác thực sẽ không xảy ra đối với các browser mà pix không hiểu . Để tránh điều này , ta có thể sử dụng virtual http . PIX firewall giả sử rằng AAA server và web server chia sẽ cùng database , và pix tự động cung cấp cho 2 server này thông tin giống nhau . Virtual http sử dụng trong PIX dùng để xác thực user , tách thông tin AAA server từ request URL của web client , chuyển web client đến web server. Virtual http lại chuyển tiếp kết nối khởi tạo của web browser đến một địa chỉ IP thuộc về PIX firewall , xác thực user , sau đó chuyển browser về lại URL mà user đã yêu cầu .

Virtual http đặc biệt hữu dụng cho pix khi thao tác với Microsoft IIS (Internet Information Server) . Khi dùng xác thực HTTP đến các site chạy Microsoft ÍIS có "Basic text authentication" hoặc là "NT Challenge" , user có thể bị Microsoft từ chối truy cập vì browser thêm vào trong các lệnh HTTP GET dòng chữ sau : "Authorization : Basic = Uuhjksdkfhk==" . Dòng chữ này bao gồm các yếu tố xác thực trong PIX mà không có trong Microsoft IIS . Nhờ vào đặc điểm của Virtual http , kết nối khởi tạo của Web browser được chuyển trực tiếp đến địa chỉ IP của virtual http trong PIX , xác thực user , và browser được chuyển đến URL mà user đã yêu cầu . Virtual http trong suốt với người dùng .

Để định nghĩa Virtual http server , sử dụng command sau :

Virtual http <ip_address>

Tham số ip_address giống trong virtual telnet

Ta có thể mô tả tiến trình khi sử dụng virtual http như sau :

Error!

1. web browser gửi HTTP request đến web server
2. PIX firewall chặn connection này lại và reply bằng một message " HTTP 401 Authorization Required "

3. Web browser nhận response từ firewall và sử dụng username , password cho user chứng thực .
4. web browser gửi lại HTTP request này với username , password đã được mã hóa đến PIX .
5. PIX firewall nhận HTTP request , tách nó ra làm 2 phần : phần request AAA authentication bao gồm username , password và phần khởi tạo HTTP request không có username , password .
6. pix gửi AAA authentication request đến cho AAA server
7. AAA server xác thực user , sau đó gửi lại message là accept hay reject
8. Giả sử rằng user xác thực thành công , pix sẽ chuyển http request ban đầu (không có username , password) đến web server . Nếu web server yêu cầu xác thực , nó sẽ gửi challenge lại cho user .

Với vitural http , khi user đã xác thực xong , user sẽ không bao giờ phải xác thực trở lại ngay khi browser đã active . **Uauth** timer sẽ không bao giờ hết vì mỗi subsequent web request đều có username và password được mã hóa .

?**NOTE** : Không nên set uauth timer về 0 khi đã bật vitural http vì điều này sẽ chặn các kết nối đến web server được yêu cầu .

4. Một số cấu hình thêm

a. **Thay đổi thời gian uauth**

Mặc dù không cần thiết phải cấu hình nhưng uauth timer là một đặc điểm quan trọng để đảm bảo rằng các chức năng xác thực proxy đang thực hiện đúng . uauth timer điều khiển bao lâu user cần xác thực lại một lần . Khi user được xác thực thông qua cut-through proxy , PIX firewall cất giữ phiên xác thực thành công trong khoảng thời gian được quyết định bởi bộ định thời này . Khi khoảng thời gian đó qua đi , user cần phải xác thực lại bằng cách cung cấp lại thông tin về username và password. PIX firewall không ra dấu nhắc cho việc xác thực ngay lập tức sau khi uauth timer qua đi , nó chỉ ra dấu nhắc cho user khi có một kết nối được thực hiện sau khoảng thời gian timeout của uauth timer .

Uauth timer có hai đại lượng mà ta có thể cấu hình riêng biệt nhau để điều khiển reauthentication là : inactivity và absolute .

Câu lệnh như sau :

timeout uauth [hh:mm:ss] [absolute | inactivity]

- inactivity : bắt đầu sau khi kết nối trở nên idle . Nếu user thiết lập một kết nối mới trước khoảng thời gian inactivity ,

user không cần phải xác thực trở lại . Nếu user thiết lập kết nối sau khi thời gian inactivity qua đi , user phải xác thực lại .

- absolute : absolute timer chạy liên tục , nhưng chờ để ra dấu nhắc lại cho user khi user bắt đầu một kết nối mới , ví dụ như click vào một link sau khi absolute timer qua đi . Nếu timer qua đi và user click vào link mới , user sẽ phải xác thực lại . Absolute timer phải ngắn hơn xlate timer để mỗi khi phiên làm việc của họ kết thúc , họ phải xác thực trở lại .

Một số lưu ý khi sử dụng hai timer này :

- inactivity timer cho user truy cập internet tốt nhất bởi vì user không phải xác thực lại trong khoảng thời gian cách đều nhau . Absolute timer làm tăng độ bảo

mật và quản lí kết nối PIX firewall tốt hơn . Bằng việc xác thực lại trong khoảng thời gian đều nhau , user có thể quản lí việc sử dụng tài nguyên hiệu quả hơn .

- thiết lập cả hai timer về 0 , user phải xác thực lại trong mỗi kết nối mới .
- Không nên thiết lập cả hai timer về 0 nếu passive FTP được sử dụng thông qua PIX firewall .
- Không thiết lập cả hai timer về 0 nếu virtual command được sử dụng cho web authentication , vì điều này sẽ chặn các kết nối HTTP đến web server đích .
- Cả hai timer có thể hoạt động cùng một thời điểm . Absolute timer nên được thiết lập dài hơn inactivity timer . Nếu absolute timer ngắn hơn , inactivity timer sẽ không bao giờ xảy ra .
- để xác thực user sau khoảng thời gian inactivity , thiết lập inactivity timer đến một khoảng thời gian mong muốn và thiết lập absolute timer về 0 .

?**NOTE** : Hacker có thể tạo ra DoS attack trong Pix bằng cách khởi động nhiều lần login trong cơ chế xác thực AAA mà không cần cung cấp thông tin xác thực . Mỗi lần login tạo ra một kết nối , kết nối đó sẽ được duy trì cho đến khi thời gian timeout qua đi . Bằng cách tạo ra nhiều lần login như vậy , hacker có thể làm tiêu tốn nguồn tài nguyên AAA , vì vậy không có lần login nào được phục vụ .

b. **Thay đổi authentication prompt**

Cấu trúc :

auth-prompt accept | reject | prompt *string*

accept : Nếu xác thực user qua Telnet được chấp nhận , thì sẽ xuất hiện prompt *string*

reject : Nếu xác thực user qua Telnet bị loại bỏ , thì sẽ xuất hiện prompt *string*

prompt : Là chuỗi prompt thách thức AAA theo sau từ khóa prompt .

5. Cấu hình authorization

Khi đã cấu hình xác thực cho traffic thông qua firewall sử dụng cut-through proxy , ta có thể cấu hình authorization cho traffic thông qua firewall . Authentication là một yêu cầu cho authorization , tức là authorization sẽ quyết định

dịch vụ nào mà user sau khi được chứng thực có thể truy cập vào .

Để thực hiện authorization , đầu tiên cần cấu hình cho TACACS server . Sau đó ta cần phải cấu hình AAA authorization cho PIX sử dụng câu lệnh sau :

aaa authorization {include | exclude} *<author_service>* **{inbound | outbound}** *<if_name> <local_ip> <local_mask> <foreign_ip> <foreign_mask> <group_tag>*

Cấu trúc của câu lệnh trên tương tự trong authentication . Tất cả các tham số đều giống ngoại trừ *author_service* . Các giá trị có thể cho *author_service* là any , ftp , telnet , http , hay là <protocol/port> (ví dụ như TCP là 6 , UDP là 17 , ICMP là 1) . Thiết lập giá trị port về 0 chỉ ra tất cả các port .

?**NOTE** : RADIUS và local database trong PIX firewall không được cung cấp authorization cho traffic .

6. **Cấu hình accounting**

Sau khi cấu hình authentication và authorization , thông thường cũng cần phải cấu hình accounting . Thông tin accounting có thể được sử dụng để theo dõi user đã làm gì khi truy cập vào một dịch vụ nào đó . Các bản ghi accounting có thể chỉ ra số lượng thời gian user login vào , hoặc là chỉ ra số lượng thông tin được truyền và nhận . Thông tin này có thể dành cho mục đích thanh toán hóa đơn .

Cấu trúc của câu lệnh aaa accounting như sau :

aaa accounting {include | exclude} *<acctg_service>* **{inbound | outbound}** *if_name<local_ip> <local_mask> <foreign_ip> <foreign_mask> <group_tag>*

Chương 5: **MỘT SỐ CHỨC NĂNG KHÁC CỦA PIXFIREWALL**

1. Attack Guard

a. DNS guard

Giả sử để phân giải một tên đến một địa chỉ , một host có thể truy vấn (query) cùng DNS server nhiều lần . Đặc điểm DNS guard của

PIX firewall là nhận biết được một truy vấn outbound DNS và chỉ cho phép lần reply đầu tiên từ server được qua PIX firewall . Tất cả các lần replies khác sẽ bị loại bỏ . Sau lần DNS reply đầu tiên đó , DNS guard sẽ đóng tất cả các phiên UDP được mở bởi DNS request mà không cần chờ đến khoảng thời gian timeout của UDP . Một host cũng có thể truy vấn nhiều DNS server khác nhau . Ví dụ , nếu DNS resolver gửi ba query cụ thể đến 3 server khác nhau, PIX firewall sẽ tạo ra 3 kết nối khác nhau. Kết nối đến mỗi server được thực hiện riêng biệt vì request được gửi một cách riêng biệt , mỗi request được đặc trưng bởi một ID . Reply cho request này bao gồm cùng một ID và IP address giống nó . Từ đó , ta kết luận DNS Guard có những đặc điểm sau :

- Chỉ chấp nhận các replies nào đúng địa chỉ IP
- Chỉ chấp nhận một reply . Trong trường hợp có nhiều replies , ngoại trừ reply đầu tiên , tất cả các replies sẽ bị loại bỏ .
- Kết nối UDP tương ứng với kết nối DNS sẽ bị loại bỏ ngay khi nhận được DNS reply mà không đợi đến khi hết thời gian timeout .
- Bảo vệ được các phiên làm việc UDP từ các hình thức tấn công như DoS hay hijacking.

Để hiểu rõ hơn hoạt động của DNS Guard , ta xem xét ví dụ sau :

Error!

Client (có địa chỉ 192.168.0.1) và Web server (web.company.com , có địa chỉ 192.168.0.5) nằm trong inside interface của PIX và các địa chỉ private . DNS server nằm ở outside interface . PIX được cấu hình để chuyển địa chỉ của client và server khi đi ra mạng ngoài thành địa chỉ 1.2.3.4 thông qua PAT . Địa chỉ này được DNS server ghi lại là địa chỉ cho web.company.com. Khi client yêu cầu địa chỉ IP của server , PIX sẽ chuyển yêu cầu đó đến DNS

server, đổi địa chỉ source từ 192.168.0.1 thành 1.2.3.4 (PIX thực hiện NAT) . Khi PIX nhận được reply từ DNS server , ngoài việc pix đổi địa chỉ đích của gói tin (từ 1.2.3.4 đến 192.168.0.1) , nó còn thay đổi địa chỉ của Web server có trong reply đó (đó là 1.2.3.4 chuyển thành 192.168.0.5) .

? **NOTE :** không thể tắt tính năng DNS Guard cũng như thay đổi giá trị mặc định là port 53 của DNS trong PIX .

b. Mail Guard

Mail Guard được thiết kế để bảo đảm độ an toàn cho các kết nối SMTP từ outside đến email server inside , nó sẽ hạn chế server và client có thể được phép làm và xem gì ?

SMPT là một giao thức dựa trên telnet , được thiết kế cho việc truyền thư điện tử giữa các server . Client gửi các command đến server , server trả lời lại bằng các status messages và một số thông tin phụ thêm . Các command được phép đến mail server đó là : HELLO , MAIL , RCPT , DATA , RSET , NOOP , và QUIT .

Mặc định PIX sẽ kiểm tra các kết nối port 25 cho lưu lượng SMTP .

Nếu các SMTP server sử dụng nhiều port khác ngoài port 25 , ta phải sử dụng câu lệnh

[no] fixup protocol smtp [<port> [-<port>]]

Mục tiêu chính của Mail Guard là hạn chế các command mà client sử dụng đến mức thấp nhất (minimal set), trong khi vẫn quản lí toàn bộ command , cụ thể :

- Mail Guard quản lí các command được gửi bởi client , nếu command này không thuộc về minimal set , nó sẽ thay thể bằng NOOP command .
- Nếu Mail Guard gặp một command không biết , toàn bộ phần dữ liệu trong gói tin sẽ được đánh dấu bằng kí tự X , với kí tự này khi server nhận được sẽ phát ra một error .

c. SYN flood Guard

Để bảo vệ các host bên trong tránh khỏi các cuộc tấn công DoS , sử dụng câu lệnh **static** để giới hạn số lượng các kết nối embryonic được phép đến server .

Cấu trúc của câu lệnh như sau :

Static(internal_if_name , external_if_name) global_ip local_ip [netmask network_mask] [max_conns[em_limit]]

- Internal_if_name : tên của interface mạng bên trong
- External_if_name : tên của interface mạng bên ngoài
- Global_ip : địa chỉ global ip cho interface bên ngoài . Địa chỉ này không được là địa chỉ PAT
- Local_ip : địa chỉ local ip của mạng bên trong
- Netmask network_mask : là mask của địa chỉ global và local
- Max_conns : số lượng kết nối tối đa được phép đến local_ip . Mặc định là 0 , tức là unlimited
- Em_limit : được sử dụng để giới hạn số lượng kết nối embryonic
  được phép đến server .

è Nếu ta thiết lập mức ngưỡng quá cao , có nguy cơ sẽ làm quá tải IP stack và dễ bị DoS attack . Nếu thiết lập mức ngưỡng quá thấp,
dễ dẫn đến tình trạng từ chối dịch vụ của các user hợp lệ . Thông thường chọn giá trị em_limit thấp hơn giá trị max_conns.

Nếu trong câu lệnh static có cấu hình mức ngưỡng em_limit để giới hạn
kết nối embryonic , và khi các kết nối đó đạt được giá trị ngưỡng thì
PIX firewall chỉ đơn giản đánh rớt các kết nối mới . điều này cho phép kết thúc việc tổ chức lưu lượng từ các cuộc tấn công , ngay cả với các attack đơn giản nhất . Nếu trong câu lệnh static không có
cấu hình ngưỡng em_limit , PIX firewall sẽ cho tất cả traffic đi qua ,
điều này sẽ dẫn đến bảng kết nối embryonic bị quá tải và tất cả traffic
bị dừng lại khi có attack .

Trong các version từ 5.2 trở lên , đã đưa ra một đặc điểm mới là TCP Intercept . TCP Intercept là phương pháp cải tiến việc đáp ứng
một kết nối embryonic của PIX firewall . Khi số lượng kết nối này
vượt quá giá trị ngưỡng được cấu hình , PIX firewall sẽ chặn đứng và
chuyển sang kết nối mới . Các version trước 5.2 , pix không cho phép
các kết nối mới sau khi đạt được giá trị ngưỡng . Điều này vẫn gây ra DoS vì các TCP connection slot vẫn được làm đầy .

Hoạt động của TCP Intercept cũng đơn giản , đối với mỗi SYN , PIX firewall đáp ứng về cho server một SYN/ACK segment rỗng ,
PIX firewall giữ lại thông tin trạng thái SYN đó , đánh rớt các gói tin ,
và chờ ACK từ client . Nếu nhận được ACK , pix sẽ gửi bản copy SYN segment của client đến server , khi đó TCP three-way handshake được thực hiện giữa PIX firewall và server . Chỉ khi nào three-way handshake hoàn tất , kết nối đó mới được đưa về trạng thái bình thường .

Để bảo vệ các host bên ngoài từ các cuộc tấn công DoS và để giới hạn số lượng kết nối embryonic đến server , sử dụng lệnh **nat**

Cấu trúc câu lệnh như sau :

nat [(if_name)] nat_id local_ip {netmask [max_conns [em_limit]]}

Sử dụng lệnh **show local-host** để xem số lượng các kết nối hiện tại và các kết nối embryonic .

d. AAA Floodguard

Khi sử dụng AAA với PIX để nhận diện , thẩm quyền và quản lí user để làm giảm các vấn đề như truy cập không có thẩm quyền

đến nguồn tài nguyên thông tin , điều này cũng tạo cho hacker có hội trong việc attack . Nếu tất cả các connection đều phải được chứng thực thì khi có quá nhiều authentication request làm cho nguồn tài nguyên của AAA quá tải dẫn đến dịch vụ bị từ chối – DoS .

Floodguard command cho phép ta tự động bảo vệ nguồn tài nguyên cho PIX firewall nếu hệ thống xác thực user bị quá tải . Nếu kết nối uauth inbond hoặc outbound bị tấn công hoặc bị sử dụng quá nhiều , PIX tự động bảo vệ TCP user resource . Khi các nguồn tài nguyên bị cạn kiệt , PIX firewall sẽ đưa ra nhiều messages chỉ thị rằng nó đã hết tài nguyên (out of resource) . Nếu hệ thống uauth bị cạn kiệt , TCP user resource ở trạng thái khác sẽ được dùng phụ thuộc vào mức độ cảnh báo theo thứ tự sau :

- Timewait
- Finwait
- Embryonic
- Idle

Floodguard command mặc định đã được bật lên và có cấu trúc như sau :

floodguard enable | disable

e. Fragmentation Guard

Đặc điểm Fragmentation Guard đưa ra 2 security check ngoài các security check được đề nghị bởi RFC 1858 cho gói tin IP trong việc

bảo vệ cho gói tin khỏi bị phân mảnh từ các cuộc tấn công như teardrop , land …

Security check đầu tiên yêu cầu mỗi gói tin non-initial IP fragment phải liên kết với gói tin already-seen valid initial IP fragment . Vì các fragment này có thể đến không theo thứ tự .

Security check thứ hai là IP fragment phải có tốc độ là 100 gói tin IP fragment hoàn chỉnh trên 1 giây cho mỗi host internal . Điều này

có nghĩa là Pix có thể xử lý 1200 packet fragment trong vòng 1 giây . FragGuard hoạt động ở tất cả các interface của PIX firewall .

Để enable tính năng này lên , sử dụng câu lệnh **sysopt security fragguard**

2. syslog

Việc kiểm tra các cấu hình của thiết bị để bảo đảm nó hoạt động tốt là vấn đề quan trọng trong việc bảo mật mạng . Có rất nhiều cách để thực hiện điều này , nhưng cách chủ yếu vẫn là giám sát (monitor) và ghi lại (log) các sự kiện trong mạng . Việc ghi lại các sự kiện rất quan trọng trong quá trình theo dõi nhiều thông tin trong hệ thống .Thao tác này sẽ đưa ra tại ngõ ra của hệ thống các message báo lỗi như ai đang làm gì , ai đang đi đâu , hoặc là các loại tấn công có thể có vào mạng . Trong PIX firewall có hai cách để ghi lại thông tin , đó là local và remote . Local logging là việc bản thân Pix có thể ghi lại các sự kiện , nhưng hạn chế của phương pháp này là chỉ ghi được một vài sự kiện . Remote logging là phương pháp cho phép ta lưu các bản tin và sử dụng các scripts để kiểm tra các bản tin đó một cách chi tiết , điều khiển được dữ liệu và phát ra các bản báo cáo chi tiết . Remote logging cũng cho phép ta lưu tạm các sự kiện . Để thực hiện được phương pháp này , PIX firewall sử dụng cơ chế syslog , đó là một trong các phương pháp phổ biến nhất để lưu và giữ lại các log messages , trong đó có một host sẽ gửi các syslog messages và một server quản lí syslog , server này có thể là máy chủ sử dụng hệ điều hành Window , Linux / UNIX . PIX firewall sẽ đóng vai trò như là một host gửi các syslog messages đến syslog server , syslog server quyết định sẽ đặt các bản tin này ở đâu còn tùy thuộc vào các software sử dụng cho server . Syslog server có thể viết các bản tin này thành một file hoặc là gửi thông báo khẩn (alert) đến một người nào đó bằng email hay tin nhắn .

Mặc định PIX firewall sẽ tắt chức năng logging , để bật nó lên ta sử dụng câu lênh sau :

Pix (config)# logging on

Câu lệnh này cần thiết để bắt đầu logging tất cả các sự kiện ở ngõ ra như ở buffer , terminal , hay là ở syslog server . Tuy nhiên sau khi sử dụng lệnh này , ta vẫn phải chỉ ra hình thức logging cụ thể . Để tắt logging , sử dụng **no logging on**

a. Local logging

Có 3 loại local logging là : buffered logging (logging từ bộ đệm) , console logging (logging từ cổng console) , và terminal logging (logging từ thiết bị đầu cuối) .

- *Buffered logging* : Khi sử dụng phương pháp này , tất cả các log messages được gửi đến một bộ đệm bên trong PIX firewall .

Để bật tính năng này lên , sử dụng câu lệnh sau :

Pix(config)# logging buffered <level>

Tham số **level** chỉ ra mức độ chi tiết mà ta muốn xem trong các bản tin , các bản tin này sẽ xuất hiện ở cổng console của pix , tham số này được dùng để giới hạn số lượng bản tin được log .

Để xem các bản tin được giữ trong bộ đệm , sử dụng câu lệnh **show logging** , câu lệnh này chỉ cấu hình logging cũng như các bản tin được giữ trong bộ đệm . Lệnh **clear logging** cho phép ta làm sạch bộ đệm . Hai lệnh trên được sử dụng ở enable mode .

Ví dụ của lệnh show logging :

Pix # show logging

Syslog logging : enabled
Facility : 20
Timestamp logging : disabled
Standby logging : disabled
Console logging : level debugging , 37 messages logged
Monitor logging : disabled
Buffer logging : level debugging , 8 messages logged
Trap logging : disabled
History logging : disabled

? **NOTE** : Cisco đề nghị không nên bật tính năng buffered logging vì sẽ làm giảm hoạt động của PIX .

- *Console logging* : gửi các log messages đến console (cổng nối tiếp) của PIX firewall . Để bật tính năng này lên , sử dụng :

pix(config) # logging console <level>

Tham số level sử dụng giống như trong buffer logging .

- *Terminal logging* : gửi các log messages đến một phiên telnet hoặc SSH . Để bật terminal logging , sử dụng :

pix(config) # logging monitor <level>

Bên cạnh bật chức năng này ở mode global , logging output cùng phải được bật trên mỗi phiên làm việc telnet hoặc SSH hiện tại bằng cách sử dụng câu lệnh **terminal monitor .** Để tắt nó , sử dụng **terminal no monitor .**

b. Remote logging : syslog

Như đã nói ở trước , logging trong pix mặc định là bị tắt đi , ta cần phải bật nó trên trước khi cấu hình logging cho pix .

Pix(config) # logging on

- Để cấu hình syslog trên pix , đầu tiên cần phải xác định host nào sẽ gửi syslog messages đến bằng cách sử dụng câu lệnh :

logging host [<interface>] <ip_address>

- Tham số *interface* chỉ ra interface mà ta muốn gửi các bản tin ra ngoài ,
- Tham số *ip_address* chỉ ra địa chỉ của syslog server trên interface đó . Nếu không chỉ ra interface nào cụ thể , mặc định là lấy inside interface .

- Sẽ không có log messages nào được gửi đến syslog cho đến khi ta cấu hình mức độ logging sử dụng câu lệnh sau :

logging trap <level>

- Khi được cấu hình để sử dụng syslog , PIX firewall sẽ gửi log messages đến syslog server mặc định sử dụng UDP port 514 . Ta có thể thay đổi mặc định này như sau :

logging host [<interface>] <ip_address> [tcp | udp / <port_number>]

Có thể cấu hình UDP hay là TCP cho syslog , tham số port _number là giá trị nằm trong khoảng 1025 đến 65535 . TCP không phải là phương pháp chuẩn cho việc cấu hình syslog vì hầu hết các syslog server không hỗ trợ . Nếu sử dụng kết nối TCP cho syslog server , cần lưu ý là nếu syslog server bị down thì tất cả lưu lượng trong mạng qua pix sẽ bị khóa . Một lưu ý khác là khi cấu hình TCP syslog thì kết nối syslog sẽ chậm hơn UDP vì TCP phụ thuộc vào quá trình bắt tay 3 bước . Điều này sẽ dẫn đến thêm overhead của kết nối và làm chậm việc gửi syslog messages đến server .

- Đối với những pix có hỗ trợ tính năng failover , lệnh **logging standby** cho phép failover PIX gửi syslog messages cho các log files được đồng bộ trong trường hợp stateful failover xảy ra .

c. logging level

Mặc dù lệnh logging có 8 level khác nhau được sử dụng trong pix (theo bảng) , logging level 0 không được sử dụng . Khi cấu hình logging , ta phải chỉ ra mức level có thể bằng số hay bằng từ khóa . Khi đó , PIX firewall ghi lại tất cả các sự kiện như nhau cho mức level được chỉ ra cũng như các level thấp hơn nó . Ví dụ , level mặc định cho pix là

level 3 (error) , thì pix cũng sẽ log các sự kiện ở level 2 , level 1 , và level 0 .

Error!

Ví dụ về các level được ghi lại :

Error!

Error!

Error!

d. **Logging facility**

Mỗi syslog message có một số tiện ích (facility number) . Có 24 facility khác nhau được xếp từ 0 đến 23 . 8 facility được sử dụng phổ biến cho syslog là local0 đến local7 . Facility có vai trò giống như những ống dẫn dẫn dắt tiến trình syslog . Tiến trình syslog sẽ đặt các messages vào đúng log file dựa trên facility . Cấu hinh tính năng này như sau :

logging facility <facility_code>

Các facility_code được sắp xếp theo bảng sau :

Error!

3. Content Filtering

a. Filtering URL với Websense

Có thể sử dụng access-list để cho phép hoặc từ chối truy cập web , nhưng nếu list các site ngày càng dài hơn , thì giải pháp này sẽ ảnh hưởng đến hoạt động của firewall . Ngoài ra , access-list không đưa ra được sự tiện lợi trong việc điều khiển truy cập trong trường hợp này . Ví dụ như nó không thể cho phép hoặc từ chối truy cập đến các trang cụ thể trong website , mà là toàn bộ website được chỉ ra trong câu lệnh của nó . Access-list cũng không có tác dụng đối với những website là những host ảo . Ví dụ như có nhiều website thuộc về cùng một server và tất của các website đó phải có địa chỉ IP , do đó chỉ có thể cho phép hoặc từ chối truy cập đến tất cả các website đó trong cùng một lúc .

Pix đã đưa ra một giải pháp điều khiển truy cập web tốt hơn và hiệu quả hơn đó là sử filtering URL thông qua một filtering server . Cụ thể như trong hình sau :

Error!

- khi một client thiết lập kết nối TCP đến Web server

- Client gửi HTTP request cho một trang trong server này
- Pix chặn request này và chuyển nó đến filtering server

- Filtering server sẽ quyết định xem client có được phép truy cập đến trang đã yêu cầu hay không ?
- Nếu được , PIX sẽ chuyển request đến server và client nhận được nội dung đã request
- Nếu không , request của client bị đánh rớt .

Websense là một phần mềm cung cấp chức năng filtering cho PIX firewall , giúp cho nhà quản trị mạng giám sát và điều khiển lưu lượng mạng . Websense được sử dụng để khóa các URL mà PIX không thể khóa . Websense quyết định là khóa hay cho phép một URL nào đó dựa trên thông tin cấu hình của nó và Master Database . Cấu hình Websense là đưa ra các quy tắc filtering mà ta đã thiết lập trong Websense. Master Database là database của URL bị khóa . Database này được duy trì và cập nhập hằng ngày bởi Websense corporate office .

Câu lệnh chỉ ra filtering server cho Websense là :

url-server <*if_name*> **host** <*local_ip*> [**timeout** <*seconds*>] [*protocol <tcp> | <udp>] [version 1 | 4]*

Cấu hình Pix để làm việc với Websense :

Filter url http [*local_ip local_mask foreign_ip foreign_mask] [allow]*

b. Active Code Filtering

Active content trong các trang web có thể được xem là vấn đề không mong muốn trong việc bảo mật . PIX firewall có thể lọc các active code , các active code này có thể được sử dụng trong các ứng dụng như Java hay ActiveX .

PIX firewall hỗ trợ Java applet filer có thể dừng các ứng dụng Java nguy hiểm dựa trên user hay địa chỉ IP .

Câu lệnh để filter java là :

Filter java port *[- port] local_ip mask foreign_ip mask*

ActiveX controls có thể gây ra các vấn đề bảo mật bởi vì chúng có thể đưa một cách nào đó cho hacker tấn công server . PIX firewall có hỗ trợ tính năng khóa tất cả các activeX controls .

filter activex *port local_ip mask foreign_ip mask*

4. Intruction Detection

PIX Firewall software version 5.2 trở về sau có khả năng phát hiện xâm nhập (IDS). Phát hiện xâm nhập là khả năng phát hiện sự tấn công mạng. Có 3 loại tấn công vào mạng :

- Reconnaissance attack - Kẻ xâm nhập cố gắng phát hiện và sắp xếp hệ thống, dịch vụ hoặc các cho yếu điểm
- Access attack - Kẻ xâm nhập tấn công mạng hoặc hệ thống để lấy dữ liệu, tăng tốc độ truy cập và nâng cao đặc quyền truy cập
- DoS attack -Kẻ xâm nhâ tấn công vào hệ thống mạng bằng cách ga6 nguy hiểm hoặc làm hỏng các hệ thống máy tính hoặc từ chối iệc truy cấp vào mạng, các dịch vụ hoặc các hệ thống

PIX Firewall phát hiện xâm nhập bằng cách sử dụng signature phát hiện xâm nhập. Một signature là một tập các nguyên tắc gắn liền với các hoạt động xâ nhập. Với việc cho phép phát hiện xâm nhập, PIX Firewall có thể phát hiện signature và truyền đáp ứng khi một tập các nguyên tắc được so sánh với hoạt động của mạng. Nó có thể giám sát các gói của 53 signature phat hiện xâm nhập và được cấu hình để gởi cảnh báo đến một Syslog server, drop packet hoặc reset lại kết nối. 53 signature làmột tập con của các signature được hỗ trợ bởi Cisco Intrusion Detection System (CIDS)

PIX Firewall có thể phát hiện hai loại signature khác nhau: informational signature và attack signature. Information class signature là các signature mà được gây ra bởi hoạt động thông thường của mạng mà bản thân nó xem như

vô hại nhưng có thể được dùng để xác định tính hiệu lực của việc tấn công. Attack class signature là những signature mà được gây ra bởi một hoạt độg được biết, hoặc có thể dẫn đến, lấy lại dữ liệu không có thẩm quyền

a. Phát hiện xâm nhập trong PIX Firewall

Phát hiện xâm nhập được cho phép bởi lệnh **ip audit**. Sử dụng lệnh **ip audit** kiểm tra các policy có thể được tạo để xác định traffic mà được kiểm tra hoặc phân công các hoạt động khi một signature bị phát hiện. Sau khi một policy được tạo ra, nó có thể được đưa vào bất cứ interface nào

Mỗi interface có hai policy: một cho informational signature và một cho attack signature. Mỗi lần một policy của một class signature được tạo ra và đưa vào interface, tất cả các signature được hỗ trợ của class đó được giám sát trừ khi disable chúng với lệnh **ip audit signature disbale**

PIX Firewall hỗ trợ cả inbound và outbound auditing. Auditing thự hiện bằng cách nhìn vào các gói IP đến tại một input interface. Ví dụ, nếu một attack policy được đưa vào một outside interface, attack signature được gây ra khi attack traffic đến tại outside interface ở hướng vào, kể cả inbound traffic hoặc return traffic từmột kết nối outbound

b. Cấu hình IDS

Dùng lệnh **ip audit** để cấu hình IDS signature. Đầu tiên tạo ra một policy với lệnh **ip audit name** và sau đó đưa policy này đến một interface với lệnh **ip audit interface**

Có hai lệnh **ip auit name** khác nhau: **ip audit name info** và **ip audit name attack**. Lệnh ip audit name info được dùng để tạo ra các policy của các signature được phân loại như thông tin. Tất cả informational signature, trừ những cái bị loại bỏ bởi lệnh ip audit signature, trở thành một phần của policy. Lệnh ip audit name attack thực hiện cùng chức năng với signature được phân loại như attack signature

Lệnh **ip audit name** cũng cho phép chỉ rõ các hoạt động khi signature được gây ra. nếu một policy được định nghĩa mà không có các hoạt động, hoạt động mặc định có hiệu quả

Lệnh **no ip audit name** được dùng để bỏ một audit policy. Lệnh **sh ip audit name** miêu tả các audit policy. Để bỏ một policy từ một interface, sử dụng lệnh **no ip audit interface.** Để miêu tả cấu hình inteface, sử dụng lệnh **sh ip audit interface**

5. Failover

Chức năng failover của PIX firewall cung cấp độ dự phòng trong trường hợp một PIX bị hư , pix kia ngay lập tức đóng vai trò của Pix bị hư đó .

Failover làm việc với 2 , và chính xác là chỉ 2 , firewall . Hai firewall này phải :

- có model giống nhau (ví dụ pix 515 không thể sử dụng cùng với pix 515E)
- dung lượng Flash và RAM phải giống nhau
- có cùng số lượng interface và các loại interface
- Cùng loại activation key
- Primary firewall phải chạy unrestricted license
- Secondary firewall phải chạy hoặc là unrestricted hoặc là failover license .

Failover chỉ hỗ trợ trong các model high-end như PIX 515, 515E , 520 , 525 và 535.

?**Note** : Đặc điểm failover của PIX firewall chỉ hỗ trợ chức năng redundancy . Một PIX sẽ hoạt động như là active firewall , một PIX khác hoạt động ở chế độ standby mode . Không thể sử dụng cả hai firewall cùng vai trò active cùng một lúc tức là PIX firewall không hỗ trợ tính năng load balancing .

Khi cấu hình failover , 1 firewall có vai trò là primary , một firewall có vai trò là secondary . Ở trạng thái hoạt động bình thường , primary firewall là active và nắm giữ tất cả các traffic mạng . Secondary firewall ở chế độ standby và sẽ active khi primary firewall bị hư , lúc đó primary firewall lại ở chế độ standby . Standby firewall có thể cũng bị hư nhưng lần này failover sẽ không xảy ra . Mặc dù firewall có thể chuyển đổi các vai trò cho nhau nhưng primary và secondary không bao giờ thay

đổi . Nghĩa là khi có failover xảy ra , primary ở chế độ standby , còn secondary ở chế độ active .

Các trường hợp sau được xem là firewall bị hư :

- Bộ nhớ bị cạn kiệt trong vòng từ 15 giây trở lên trong PIX firewall active
- trạng thái liên kết của các interface mạng ở active PIX firewall bị down hơn 2 lần trong khoảng thời gian poll . Điều này không phải là interface bị administratively down
- Không có sự trao đổi Hello packets giữa primary và secondary qua tất cả các interface mạng (các gói hello này được gửi đi mặc định là 15 giây một lần , nhưng chu kì này có thể thay đổi được) . Nếu không có hello message nào được nhận trong khoảng chu kì 2 poll , interface không response đó sẽ được đặt vào trạng thái testing . Nếu interface không qua được

trong quá trình kiểm tra này , nó cũng được xem như là firewall bị hư .

- Các hello packets cũng được trao đổi giữa primary và secondary qua failover serial cable . Nếu standby firewall không có nghe thông tin gì từ active firewall trong khoảng 2 poll , trạng thái failover cable vẫn tốt , standby firewall sẽ xem như active firewall bị hư và đóng lấy vai trò của active firewall . Ngoài ra , active không có nghe thông tin gì từ standby trong khoảng 2 poll , nó xem như standby bị hư .
- Nếu standby firewall phát hiện rằng active firewall bị tắt nguồn hoặc là reboot , standby sẽ trở nên active . Nếu failover cable bị unplugged , failover không xảy ra .

Có hai loại failover là standard failover và LAN-based failover , chức năng của hai loại này là như nhau . Sự khác biệt lớn nhất giữa hai loại này là cách mà chúng sử dụng để trao đổi thông tin failover giữa primary và secondary firewall . Ở standard failover , một loại serial cable đặc biệt được sử dụng để kết nối 2 firewall lại với nhau . Cable này được gọi là failover cable . Failover cable là loại cable do Cisco đưa ra dựa trên chuẩn tín hiệu RS-232 . Đối với LAN-based failover , thay vì sử dụng serial cable , một link Ethenet dành riêng được sử dụng để trao đổi thông tin failover .

Thông tin được trao đổi giữa hai loại failover là như nhau và bao gồm :

- Địa chỉ MAC của firewall
- Các gói tin Hello
- Thông tin trạng thái (active hay là standby)
- Trạng thái liên kết network interface
- bản sao cấu hình (configuration replication)

Failover cable

Failover cable được sử dụng để kết nối primary và secondary firewall . Một đầu của failover cable được đánh dấu là primary được nối đến primary firewall , đầu kia được đánh dấu là secondary được nối đến secondary firewall . Cable chỉ nên nối đến firewall khi tắt secondary firewall đi .

Failover cable trao đổi trạng thái dữ liệu giữa 2 firewall ở 115Kbps . Đối với PIX OS có version trước 5.2 thì failover cable hoạt động ở tốc độ 9600bps . Không nên nối ngược failover cable vì làm như vậy replication sẽ xảy ra từ secondary firewall đến primary firewall và xóa toàn bộ cấu hình .

Việc liên lạc qua failover cable được thực hiện bằng cách sử dụng các messages , và mỗi message phải được ACK . Nếu một message không được ACK từ firewall khác trong vòng 3 giây , nó được truyền lại . Sau 5 lần truyền lại mà vẫn không có ACK , firewall không có ACK messages đó được xem như là bị hư .

Configuration replication

Configuration replication là chức năng đồng bộ cấu hình của primary với secondary. Khi configuration replication thành công , cả primary và secondary phải giống nhau về hardware và software , chạy cùng OS và có cùng số interface .

tiến trình replication xảy ra tại RAM , không được lưu vào trong Flash , do đó , sau khi replication hoàn tất , cần phải lưu cấu hình lại .

Configuration replication tự động xảy ra khi :

- standby PIX hoàn tất quá trình boot . Primary firewall sao chép toàn bộ cấu hình của nó đến secondary firewall .
- Khi các command được gõ trong active PIX firewall . Mỗi command được nhập vào thì nó sẽ được gửi đến standby qua failover connection .
- Khi write standby command được sử dụng ở active PIX firewall . Điều này sẽ làm cho toàn bộ cấu hình của active được tái bản ở secondary .

Bất kì sự thay đổi về cấu hình ở standby firewall sẽ không được sao lại ở primary .

Địa chỉ IP và MAC sử dụng cho failover

Mỗi network interface mà tại đó ta cấu hình failover , ta cần phải có hai địa chỉ . Một địa chỉ IP dành cho primary firewall , và một địa chỉ Ip dành cho failover . Khi hoạt động , primary sử dụng địa chỉ IP và địa chỉ MAC hệ thống của nó , secondary firewall sẽ sử dụng địa chỉ IP và địa chỉ MAC failover . Khi failover xảy ra , primary firewall bị hư , secondary sẽ active , địa chỉ IP và địa chỉ MAC sẽ được chuyển đổi . Nói cách khác , secondary firewall (bây giờ đã active) sẽ lấy địa chỉ IP và MAC của primary firewall . Primary firewall (bây giờ đang ở standby) sẽ lấy địa chỉ IP và MAC failover của secondary firewall .

Mặc định địa chỉ MAC của active firewall là các địa chỉ được tạo thành từ NICs của primary firewall và địa chỉ MAC của standby firewall là các địa chỉ được tạo thành từ NICs của secondary firewall . Thay vì sử dụng các địa chỉ này , ta có thể sử dụng địa

chỉ MAC ảo . Mỗi interface có thể đăng kí các địa chỉ MAC ảo sử dụng command sau :

failover mac address <*if_name*> <*active_mac*> <*standby_mac*>

Phát hiện lỗi (failure detection)

Primary và secondary firewall trao đổi gói tin hello cho nhau thông qua failover cable cũng như qua tất cả các network interface . Các gói hello này mặc định trao đổi 15giây 1 lần . Để thay đổi khoảng thời gian này , sử dụng command sau :

failover poll <*seconds*>

Giá trị nhỏ nhất cho seconds là 3 giây , giá trị lớn nhất là 15 giây . Nếu khoảng thời gian hello thấp hơn , lỗi sẽ được phát hiện nhanh hơn , nhưng cũng dễ tạo ra failover không cần thiết khi mạng bị nghẽn vì có quá nhiều gói hello .

Đặc điểm failover của PIX firewall giám sát việc trao đổi các gói hello cũng như trạng thái nguồn của firewall khác . Nếu lỗi được phát hiện và không phải là do mất nguồn hoặc là do secondary firewall reboot , PIX firewall (primary và secondary , cái nào phát hiện lỗi) sẽ thực hiện hàng loạt kiểm tra (theo một series) để quyết định xem firewall có bị hỏng hay không . Việc kiểm tra bắt đầu khi không có nghe các bản tin hello trong khoảng thời gian 2 poll . Đối với mỗi quá trình kiểm tra , nếu một firewall nhận được network traffic trong suốt quá trình kiểm tra , firewall kia không nhận được , thì firewall không nhận được traffic đó được xem là bị hỏng . Nếu cả hai firewall không nhận được traffic nào thì việc kiểm tra tiếp theo trong series đó sẽ được thực hiện . Có 4 quá trình kiểm tra thường được sử dụng :

- link up /down : firewall kiểm tra trạng thái liên kết mạng để đảm bảo rằng nó up . Quá trình kiểm tra này sẽ tìm ra được các vấn đề lỗi vật lí như cable unplugged , port của hub/switch trong tình trạng xấu , hay là hub / switch bị lỗi . Nếu interface không có lỗi gì hết , PIX firewall bắt đầu kiểm tra hoạt động mạng . Ngược lại , interface tương ứng với firewall được xem như bị hư .
- network activity : firewall lắng nghe network activity khoảng 5 giây . Nếu có gói tin được nhận trong suốt quá trình kiểm tra này , interface được xem là hoạt động và PIX kết thúc việc kiểm tra , ngược lại , nếu không nhận được gói tin nào , pix chuyển đến kiểm tra ARP .

- ARP : Pix lấy khoảng 10 entry gần nhất trong bảng ARP của nó và gửi ARP request cho mỗi entry đó để kích thích network traffic . Sau khi gửi mỗi request , PIX firewall giám sát tất cả các traffic được nhận trong khoảng 5 giây . Nếu không có traffic nào được nhận , PIX sẽ chuyển đến entry kế tiếp trong list đó . Nếu có traffic trong suốt quá trình kiểm tra đó , interface được xem là hoạt động và quá trình test kết thúc . Nếu đã kiểm tra hết entry trong list mà vẫn không nhận được traffic nào , PIX bắt đầu kiểm tra broadcast ping
- Broadcast ping : firewall gửi ra ngoài broadcast ping ở interface và quan sát có nhận được gói tin trong vòng 5 giây sau khi ping được gửi đi . Nếu nhận được bất kì gói tin nào , pix coi như interface hoạt động và ngừng kiểm tra . Nếu không nhận được , nó sẽ quay lại quá trình kiểm tra ARP .

?**Note** : Tất cả các interface (không phải administratively down) của cả hai firewall phải giao tiếp được với nhau , ngay cả nếu chúng không được sử dụng . Ví dụ như các interface đó có thể nối với nhau bằng cáp chéo , hoặc là được cắm vào cùng một switch . Nếu không quá trình test sẽ hỏng .

Stateful failover

Có hai loại failover là failover và stateful failover (có trong PIX OS version5.1 trở về sau) . Đối với failover , khi primary firewall bị hư , secondary trở nên active , tất cả các kết nối active qua firewall bị rớt , các ứng dụng phải khởi tạo kết nối mới để khởi động lại việc liên lạc qua pix . Nhưng stateful failover giải quyết được vấn đề này . Đối với stateful failover , khi active pix bị hư , secondary trở nên active , thì các kết nối active đó vẫn được duy trì ở PIX mới active . Các ứng dụng client vẫn tiếp tục hoạt động .

Khi sử dụng stateful failover , bên cạnh thông tin cấu hình , các thông tin sau phải được gửi cho standby PIX firewall :

- bảng translation (xlate) với static và dynamic translation
- bảng TCP connection (bao gồm thông tin timeout cho mỗi kết nối)
- đồng hồ hệ thống và thông tin về uptime

hầu hết các kết nối UDP không được sao lại cho standby ngoại trừ giao thức H.232, các thành phần sau không được sao bản lại là :

- thông tin trạng thái ISAKMP và IPSEC , điều này có nghĩa là ISAKMP và IPSEC SA không bị mất khi có failover xảy ra .

- DHCP
- bảng user authentication , khi failover xảy ra thì các user đã được chứng thực phải chứng thực lại .
- bảng định tuyến , nghĩa là tất cả các route động (thông qua RIP) phải được học lại .
- bảng ARP .

?**Note**: Mặc định thông tin về session HTTP sẽ không được sao lại nhưng trong các version 6.2 trở về sau , thì pix có hỗ trợ đặc điểm này bằng cách sử dụng câu lệnh sau :

failover replicate http

Để stateful failover làm việc , interface Fast Ethernet hoặc là Gigabit Ethernet trong mỗi pix phải được dành riêng cho các thông tin trạng thái đi qua (các interface này được gọi là stateful failover interface) . Interface này phải cung cấp kết nối giữa primary và secondary firewall thông qua các phương pháp sau :

- crossover Ethernet cable
- hub hoặc switch dành riêng
- VLAN dành riêng trong switch chỉ có 2 port kết nối đến firewall active trong VLAN

?Note : Stateful failover interface ít nhất là interface nhanh bằng interface nhanh nhất trong firewall . Token Ring và FDDI không hỗ trợ stateful failover .

Cấu hình failover

- để kích hoạt tính năng failover trong Pix , sử dụng **failover** command :

pix(config)# failover

- để cấu hình địa chỉ ip failover , sử dụng command sau :

failover ip address *ip_name ip_address*

- để bật tính năng stateful failover , sử dụng :

failover link *stateful_if_name*

stateful_if_name : chỉ ra interface dành riêng cho stateful failover . Mặc định là port LAN cao nhất có cấu hình failover .

- để PIX đóng vai trò active , sử dụng :

failover *active*

- Kiểm tra failover :

Show failover

LAN-based failover

Các PIX OS version 6.2 có hỗ trợ tính năng LAN-based failover . Trong LAN-based failover , thay vì sử dụng serial failover cable , Ethernet link được sử dụng để giám sát trạng thái failover và trao

đổi thông tin failover . Ưu điểm lớn nhất khi sử dụng LAN-based failover là giải quyết được vấn đề giới hạn về khoảng cách mà standard failover gặp phải (serial failover cable dài tối đa chỉ 6 feet) . Ethernet link phải là interface LAN dành riêng . Tuy nhiên , nếu sử dụng stateful failover , thì cùng interface đó có thể được sử dụng để trao đổi thông tin trạng thái . Một hub hay switch dành riêng hoặc là VLAN dành riêng trong switch có thể được sử dụng để kết nối 2 PIX firewall cho LAN-based failover , nhưng crossover Ethernet cable không dùng được . Nhược điểm khi sử dụng LAN-based failover là mất nguồn thì firewall khác không phát hiện được .

Port Security

Tác giả Lê Quảng Hà

I. Mục đích của bài lab

Giúp người thực hành hiểu được chức năng của port security

II. Sơ đồ và yêu cầu cấu hình

Yêu cầu : Bạn cần có 1 Switch 2950, 2 host

Sơ đồ:

Error!

III. Cấu hình

1. Cấu hình port security

Bước 1: Tiến hành nối dây như sơ đồ .Khởi động Switch.

Bước 2:

Bước 2-1:

```
Switch>enable
Switch#conf t
Switch(config)#interface f0/1
```

Bước 2-2: Đưa port vào chế độ access, đây là chế độ bắt buộc cho port khi cấu hình port security

```
Switch(config-if)#switchport mode access
```

Bước 2-3: Khởi động port security

```
Switch(config-if)#switchport port-security
```

Bước 2-4: Chỉ định số lần địa chỉ MAC được thay đổi.

Đây là thông số chỉ định số lần tối đa mà port vẫn còn chấp nhận sự thay đổi địa chỉ MAC. "Thay đổi địa chỉ MAC" có nghĩa là bạn đã thay đổi một host khác trong kết nối với Switch. Gọi số lần được phép thay đổi này là k, gọi số lần bạn đã thay đổi địa chỉ MAC là n. Port sẽ vẫn cho phép hoạt động nếu như $n \leq k$ và một điều quan trọng nữa là phải kết nối địa chỉ MAC ban đầu vào lại port. Số lần được thay đổi tối thiểu là 1 và tối đa là 1024, và mặc định là 1.

Ví dụ nếu chỉ định số lần là 3:

Switch(config-if)#switchport port-security maximum *maximum*

Bạn được phép thay đổi địa chỉ MAC tối đa là 3 lần. Cần chú ý là mặc dù cho phép thay đổi nhưng không có nghĩa là port vẫn hoạt động bình thường khi địa chỉ MAC bị sai. Khi địa chỉ MAC không đúng port sẽ chuyển sang trạng thái lỗi. Tuy nhiên nếu bạn kết nối địa chỉ MAC ban đầu vào lại trong lúc này thi port sẽ hoạt động bình thường trở lại.

Trở lại với bài cấu hình, ta sẽ cấu hình số lần được phép thay đổi là 1, đây là thông số mặc định và do đó không cần phải cấu hình lệnh này cho switch

Bước 2-5: Chỉ định địa chỉ MAC cần được bảo mật trên interface. Với động tác này khi host có địa chỉ MAC tương ứng sẽ được hoạt động bình thường khi kết nối vào switch trên interface này. Nếu địa chỉ MAC của host khác với địa chỉ được chỉ định trên interface thì port sẽ vào trạng thái lỗi và hiển nhiên là sẽ không có sự chuyển tiếp gói tin trên port này.

Switch(config-if)#switchport port-security mac-address *mac-address*

Chú ý :

Định dạng về địa chỉ MAC trong câu lệnh trên là: ***AAAA.BBBB.CCCC***

Địa chỉ này phải giống với địa chỉ của host cần được bảo mật.

Đối với host là PC, để tìm địa chỉ MAC này làm như sau:

- *Mở DOS command bằng cách vào Start\Run rồi gõ lệnh cmd*
- *Trong giao diện DOS này gõ lệnh C:\>ipconfig /all. Màn hình sẽ hiện ra các thông số về địa chỉ MAC của card mạng.*

Error!

Đối với host là Router, để tìm địa chỉ host:

- *Kết nối cổng console máy tính với router*
- *Dùng lênh show version để tìm địa chỉ MAC*

Cấu hình cho Switch:

Switch(config-if)#switchport port-security mac-address 00e0.4d01.2978

Bước 2-6: Chỉ định trạng thái của port sẽ thay đổi khi địa chỉ MAC kết nối bị sai:

Cấu trúc lệnh :

Switch(config-if)#switchport port-security violation [shutdown | restrict protect]

- *shutdown: port sẽ được đưa vào trạng thái lỗi và bị shutdown*
- *restrict: port sẽ vẫn ở trạng thái up mặc dù địa chỉ MAC kết nối bị sai. Tuy nhiên các gói tin đến port này đều bị hủy, và sẽ có một bản thông báo về số lượng gói tin bị hủy.*
- *protect: port vẫn up như restrict, các gói tin đến port bị hủy và không có thông báo về việc hủy bỏ gói tin này*

Trong bài lab này sẽ chỉ định trạng thái port là shut down.

Switch(config-if)#switchport port-security violation shutdown

Đến đây bạn đã hoàn tất phần cấu hình port security. Bước tiếp theo sẽ là thử nghiệm.

Bước 3: Cấu hình lệnh debug để quan sát sự thay đổi:

Switch#debug port-security

Bước 4: Sử dụng một host khác để thay thế cho host ban đầu. Kiểm tra địa chỉ MAC của host mới :

Error!

Host mới có địa chỉ MAC là 0006.7b08.cab5

Bước 4: Tiến hành rút cáp ra khỏi host và cắm vào host đã chuẩn bị ở bước 3. Quan sát:

+ Đèn trên port f0/1 sẽ bị tắt

+ Thông báo trên giao diện

00:22:24: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state

00:22:24: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0006.7b08.cab5 on port FastEthernet0/1.

00:22:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

00:22:26: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

Bước 5: Dùng lệnh show để xem trạng thái của port f0/1

Switch#show interface f0/1

FastEthernet0/1 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 000f.239d.c641 (bia 000f.239d.c641)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 10Mb/s

Lúc này mọi nỗ lực để tiến hành gửi thông tin trên port 1 đều vô ích!!!

1. Khôi phục port về trạng thái bình thường

Để khôi phục lại port thì bạn phải can thiệp vào switch.

Bước 1: Nối cổng console vào switch

Switch>enable
Switch#conf t

Bước 2: Có hai cách để khôi phục port

Cách 1: khôi phục nhân công, bạn sẽ thực hiện trực tiếp quá trình khôi phục này.

Switch(config)#interface f0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown

Thông báo trên màn hình khi thực hiện xong lệnh

00:17:58: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
00:18:00: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:18:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Quá trình trên giống như bạn cho phép port hoạt động lại bình thường, tuy nhiên cần chú ý rằng các cấu hình trước đó cho port này vẫn không thay đổi, kể cả port-security.

Cách 2: khôi phục tự động, thiết lập lệnh để switch tự động dò tìm lỗi và khôi phục.

Với cách này giả sử như bạn không hề biết nguyên nhân vì sao port bị down.

Bước 2-1: Tiến hành tìm lỗi trên port

Cấu trúc lệnh:

Switch(config)#errdisable detect cause [all | cause-name]

+ all có nghĩa là tìm tất cả các lỗi xảy ra

+ cause-name : chỉ tìm lỗi có tên là cause-name, gồm có:

all Enable error detection on all cases

dhcp-rate-limit Enable error detection on dhcp-rate-limit

dtp-flap Enable error detection on dtp-flapping

(Cấu trúc lệnh - tiếp theo)

gbic-invalid Enable error detection on gbic-invalid

link-flap Enable error detection on linkstate-flapping

loopback Enable error detection on loopback

pagp-flap Enable error detection on pagp-flapping

Trong bài lab này sẽ cho switch tìm tất cả các lỗi:

Switch(config)#errdisable detect cause all

Bước 2-2: cho switch khôi phục trạng thái

Switch(config)#errdisable recorvery cause all

Bước 2-3: cài đặt thông số thời gian cho quá trình khôi phục. Mặc định port sẽ được khôi phục sau 300 giây khi bạn đã thực hiện lệnh ở bước 2-2. Tuy nhiên bạn có thể can thiệp vào thông số thời gian này bằng cách dùng lệnh:

Switch(config-if)#errdisable recorvery *second*

Thông số thời gian *second* có đơn vị là giây bạn cần phải chú ý điều này để tránh nhầm lẫn.

Bây giờ bạn cài đặt thông số thời gian khôi phục cho switch là 30 giây

Switch(config-if)#errdisable recorvery 30

Switch(config-if)#^Z

Bước 2-4: Quan sát

+ Quan sát đèn trên port f0/1 của switch : sau 30 giây sẽ sáng lại

+ Quan sát trên giao diện:

- Quan sát thông số thời gian do lệnh debug tạo ra.

```
00:55:54: %PM-4-ERR_RECOVER: Attempting to recover
from psecure-violation err-disable state on Fa0/1
00:55:55: PSECURE: psecure_linkchange: Fa0/1
hwidb=0x807D6C98
00:55:55: PSECURE: Link is coming up
00:55:55: PSECURE: psecure_linkup_init_internal:
```

Fa0/1 hwidb = 0x807D6C98
00:55:55: PSECURE: No change in violation_mode
00:55:55: PSECURE: psecure_vlan_linkchange invoked: Vlan 1
00:55:55: PSECURE: Activating port-security feature
00:55:55: PSECURE: port_activate: status is 1
(Tiếp theo)
00:55:55: PSECURE:
PSECURE: Deleting all dynamic addresses from h/w tables.
00:55:55: PSECURE: psecure_platform_delete_all_addrs:
deleting all addresses on vlan 1
00:55:55: PSECURE: psecure_delete_address_not_ok
address <1,00e0.4d01.2978> allowed
00:55:55: PSECURE: skipping Fa0/1 while searching
<1,00e0.4d01.2978>
00:55:55: PSECURE: Adding entry to HA table from
port-security sub block
00:55:55: PSECURE: psecure_platform_add_mac_addrs:
Do nothing, called to add <1,00e0.4d01.2978>
to FastEthernet0/1
00:55:57: %LINK-3-UPDOWN: Interface FastEthernet0/1,
changed state to up
00:55:58: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet0/1, changed state to up
- Dùng lệnh :

Switch#show interface f0/1

FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 000f.239d.c641
(bia 000f.239d.c641)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
…

IV. Cấu hình toàn bộ

Cấu hình của switch:

Current configuration : 1727 bytes

!

version 12.1

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause psecure-violation
errdisable recovery cause gbic-invalid
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause unicast-flood
errdisable recovery cause vmps
errdisable recovery cause loopback
errdisable recovery interval 30
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security mac-address 00e0.4d01.2978
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23

!
interface FastEthernet0/24
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
!
ip http server
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
!
end

V. Đánh giá

Đến đây bạn đã có một khái niệm cơ bản và thao tác cấu hình tương đối về port security. Bạn có thể thay đổi các thông số trong các câu lệnh để tìm hiểu rõ các đặc tính của chúng

PPP over Ethernet

Tác giả Lê Anh Đức

Mô tả:
Error!

Ở topo trên, ta có, R3 sẽ làm PPPoE client, còn R1 sẽ làm PPPoE server, thực hiện kết nối với các mạng trong Internet với ISP làm router giả lập ISP. Router R2 là router ở chi nhánh, thực hiện NAT để cho mang private ra internet. Chú ý: Các router R3, R1 là các route 2600, chạy IOS version 12.2 trở lên.

Cấu hình:

R1

Building configuration...

*

!

hostname R1
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
vpdn enable ßbật vpdn
!
vpdn-group 1 ßtạo vpdn group để trao đổi với client
accept-dialin ß xác định đây là PPPoE server
protocol pppoe
virtual-template 1
!
interface Loopback1
ip address 203.162.3.2 255.255.255.255
!
interface Ethernet0/0
no ip address
half-duplex
pppoe enable
!
interface Serial0/0
ip address 203.20.20.2 255.255.255.252
no fair-queue
!
interface Virtual-Template1
ip unnumbered Loopback1
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
!
end
R2
Building configuration...
!
hostname R2
!
interface Ethernet0/0

ip address 10.10.2.1 255.255.255.0
ip nat inside
half-duplex
!
interface Serial0/0
ip address 203.30.30.2 255.255.255.252
ip nat outside
no fair-queue
!
ip nat inside source list 1 interface Serial0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 203.30.30.1
ip http server
!
!
access-list 1 permit 10.10.2.0 0.0.0.255
!
end
R3
Building configuration...
!
hostname R3
!

vpdn enable
!
vpdn-group 1
request-dialin ßđây là PPPoE client
protocol pppoe
!
interface Loopback0
ip address 10.10.1.1 255.255.255.0
ip nat inside
!
interface Ethernet0/0
no ip address
half-duplex
pppoe enable
pppoe-client dial-pool-number 1 ßsử dụng dialer 1 để giao tiếp với PPPoE server
!
interface Dialer1
mtu 1492
ip address 203.162.3.1 255.255.255.0
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
!
ip nat inside source list 1 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 203.162.3.2
ip http server
!
!
access-list 1 permit 10.10.1.0 0.0.0.255
dialer-list 1 protocol ip permit
!
end
ISP
!
hostname ISP
!
!

```
ip subnet-zero
!
interface Serial0
ip address 203.20.20.1 255.255.255.252
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 64000
!
interface Serial1
ip address 203.30.30.1 255.255.255.252
no ip directed-broadcast
clockrate 64000
!
ip classless
ip route 203.162.0.0 255.255.0.0 203.20.20.2
!
end
```

Thực hiện:

PPP over Ethernet là một sự phát triển dựa trên kỹ thuật PPP truyền thống. PPPoE cung cấp khả năng kết nối nhiều host trong mạng qua một thiết bị chuyển mạch vào một DSLAM, để cung cấp một kết nối PPPoE, mỗi phiên PPP phải học địa chỉ Ethernet của remote peer và thiết lập một danh định duy nhất. PPPoE gồm 2 pha: Discovery và Session:

- Discovery: khi một router muốn khởi tạo 1 phiên PPPoE, nó phải xác định địa chỉ MAC của thiết bị bên kia (Lát nửa debug sẽ cho thấy điều này) và thiết lập một PPPoE Session-ID. Trong quá trình này, CPE sẽ tìm các DSLAM và chọn một cái để sử dụng. Khi quá trình này chấm dứt, cả CPE và DSLAM đều sẽ có thông tin mà nó sử dụng để xây dựng kết nối PPPoE. Khi PPPsession được thiết lập thì cả CPE và DSLAM sẽ phải phân phát tài nguyên của mình cho một PPP virtual interface.
- Session: khi được thiết lập thì dữ liệu sẽ được gửi.

Để cấu hình, ta thực hiện các bước sau:

PPPoE server(R1):

R1(config)#vpdn enable ßbật PPPoE

R1(config)#vpdn-group 1

R1(config-vpdn)#accept-dialin ßxác định đây là PPPoE server

R1(config-vpdn-acc-in)#protocol pppoe

R1(config-vpdn-acc-in)#virtual-template 1 ßsử dụng virtual để giao tiếp với client

R1(config-vpdn-acc-in)#exit
R1(config)#int lo1
R1(config-if)#ip add 203.162.3.2 255.255.255.255
R1(config-if)#int e0/0
R1(config-if)#pppoe enable ßbật PPPoE trên interface kết nối với client
R1(config)#int virtual-template 1 ßtạo virtual template
R1(config-if)#ip unnumbered lo1
PPPoE client(R3):
R3(config)#vpdn enable
R3(config)#vpdn-group 1
R3(config-vpdn)#request-dialin ßxác định PPPoE client
R3(config-vpdn-req-in)#protocol pppoe
R3(config)#int e0/0
R3(config-if)#pppoe enable ßbật PPPoE trên interface nối với server
R3(config-if)#pppoe-client dial-pool-number 1 ßsử dụng dialer 1 để giao tiếp với server
R3(config-if)#exit
R3(config)#int dialer 1
R3(config-if)#mtu 1492
R3(config-if)#ip add 203.162.3.1 255.255.255.0
R3(config-if)#ip nat outside
R3(config-if)#encapsulation ppp
R3(config-if)#dialer pool 1
R3(config-if)#dialer-group 1
R3(config-if)#exit
R3(config)#dialer-list 1 protocol ip permit
Kiểm tra:
Ta sử dụng các lệnh show và debug để xem quá trình tạo kết nối và trao đổi dữ liệu như thế nào giữa client và server:
R3#sh int
Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0005.5e96.2cc0 (bia 0005.5e96.2cc0)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 192/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:41, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
47 packets input, 4752 bytes, 0 no buffer
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
317 packets output, 21918 bytes, 0 underruns
251 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
251 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
MTU 1492 bytes, BW 56 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 5 seconds on reset
Interface is bound to Di1 (Encapsulation PPP)
LCP Open
Listen: CDPCP
Open: IPCP
Last input 00:00:09, output never, output hang never
Last clearing of "show interface" counters 00:02:56
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
39 packets input, 544 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
39 packets output, 616 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Dialer1 is up, line protocol is up (spoofing)
Hardware is Unknown
Internet address is 203.162.3.1/24

MTU 1492 bytes, BW 56 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 1 seconds on reset
Interface is bound to Vi1
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:34:56
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 42 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
36 packets input, 504 bytes
36 packets output, 576 bytes
Bound to:
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
MTU 1492 bytes, BW 56 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 5 seconds on reset
Interface is bound to Di1 (Encapsulation PPP)
LCP Open
Listen: CDPCP
Open: IPCP
Last input 00:00:04, output never, output hang never
Last clearing of "show interface" counters 00:03:01
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
41 packets input, 572 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
41 packets output, 648 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Loopback0 is up, line protocol is up
Hardware is Loopback
Internet address is 10.10.1.1/24
MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation LOOPBACK, loopback not set
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
R3#sh vpdn
%No active L2TP tunnels
%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
VPDN group: 1
Session count: 1
PPPoE Session Information
SID RemMAC LocMAC Intf VASt OIntf VLAN/ VP/VC
1 0004.c052.7ce0 0005.5e96.2cc0 Vi1 UP Et0/0
R3#debug vpdn pppoe-data ßbật debug PPPoE
PPPoE data packets debugging is on
R3#debug ip nat ßvà NAT
IP NAT debugging is on

R3#ping ßthực hiện ping mở rộng với source là Private LAN
Protocol [ip]:
Target IP address: 203.30.30.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.10.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.30.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/64 ms
R3#
***Mar 1 00:47:59.363: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [34**]
*Mar 1 00:47:59.363: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 22 00 00 FF 01
03 B3 CB A2 03 01 CB 1E 1E 02 08 00 62 E7 0F ...
***Mar 1 00:47:59.423: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [34]**
*Mar 1 00:47:59.423: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 22 00 00 FC 01 CA 4B CB 1E
1E 02 0A 0A 01 01 00 00 6A E7 0F 88 1C 2B 00 00
00 00 00 2B EF 84 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.427: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [35]**
*Mar 1 00:47:59.427: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 23 00 00 FF 01
03 B2 CB A2 03 01 CB 1E 1E 02 08 00 62 A6 0F ...
***Mar 1 00:47:59.487: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [35]**
*Mar 1 00:47:59.487: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 23 00 00 FC 01 CA 4A CB 1E
1E 02 0A 0A 01 01 00 00 6A A6 0F 89 1C 2B 00 00
00 00 00 2B EF C4 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.491: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [36]**

*Mar 1 00:47:59.491: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 24 00 00 FF 01
   03 B1 CB A2 03 01 CB 1E 1E 02 08 00 62 65 0F ...
***Mar 1 00:47:59.551: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [36]**
*Mar 1 00:47:59.551: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 21 45 00 00 64 00 24 00 00 FC 01 CA 49 CB 1E
   1E 02 0A 0A 01 01 00 00 6A 65 0F 8A 1C 2B 00 00
   00 00 00 2B F0 04 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.555: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [37]**
*Mar 1 00:47:59.559: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 25 00 00 FF 01
   03 B0 CB A2 03 01 CB 1E 1E 02 08 00 62 24 0F ...
***Mar 1 00:47:59.615: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [37]**
*Mar 1 00:47:59.615: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 21 45 00 00 64 00 25 00 00 FC 01 CA 48 CB 1E
   1E 02 0A 0A 01 01 00 00 6A 24 0F 8B 1C 2B 00 00
   00 00 00 2B F0 44 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.619: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [38]**
*Mar 1 00:47:59.623: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 26 00 00 FF 01
   03 AF CB A2 03 01 CB 1E 1E 02 08 00 61 E3 0F ...
***Mar 1 00:47:59.679: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [38]**
*Mar 1 00:47:59.683: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
   00 21 45 00 00 64 00 26 00 00 FC 01 CA 47 CB 1E
   1E 02 0A 0A 01 01 00 00 69 E3 0F 8C 1C 2B 00 00
   00 00 00 2B F0 84 AB CD AB CD AB CD AB CD AB ...

Dựa vào debug trên, ta thấy quá trình discovery và session diễn ra như trên debug.

Tương tự như trên PPPoE server, ta cũng test y như trên client:

R1#sh vpdn

%No active L2TP tunnels

%No active L2F tunnels

%No active PPTP tunnels

PPPoE Tunnel and Session Information Total tunnels 1 sessions 1

PPPoE Tunnel Information

VPDN group: 1

Session count: 1

PPPoE Session Information

SID RemMAC LocMAC Intf VASt OIntf VLAN/ VP/VC

1 0005.5e96.2cc0 0004.c052.7ce0 Vi1 UP Et0/0

R1#debug vpdn pppoe-data

PPPoE data packets debugging is on

R1# **ßkhi client ping ra ngoài, ta sẽ thấy trên server xuất hiện debug sau:**

*Mar 1 00:56:26.538: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
FF 03 C0 21 09 6C 00 0C 04 E2 EC A9 00 00 00 CD
*Mar 1 00:56:26.538: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
C0 21 0A 6C 00 0C 05 82 38 4E 00 00 00 CD
*Mar 1 00:56:27.027: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
C0 21 09 6C 00 0C 05 82 38 4E 00 00 00 00
*Mar 1 00:56:27.027: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
FF 03 C0 21 0A 6C 00 0C 04 E2 EC A9 00 00 00 00
*Mar 1 00:56:27.223: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2C 00 00 FE 01 0E B3 CB A2
03 01 CB 14 14 02 08 00 A8 FA 10 25 0F D8 00 00
00 00 00 34 B5 1E AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.223: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2C 00 00 FF 01
0D B3 CB 14 14 02 CB A2 03 01 00 00 B0 FA 10 ...
*Mar 1 00:56:27.231: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2D 00 00 FE 01 0E B2 CB A2
03 01 CB 14 14 02 08 00 A8 F1 10 26 0F D8 00 00
00 00 00 34 B5 26 AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.231: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2D 00 00 FF 01
0D B2 CB 14 14 02 CB A2 03 01 00 00 B0 F1 10 ...
*Mar 1 00:56:27.239: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2E 00 00 FE 01 0E B1 CB A2
03 01 CB 14 14 02 08 00 A8 E8 10 27 0F D8 00 00
00 00 00 34 B5 2E AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.239: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2E 00 00 FF 01
0D B1 CB 14 14 02 CB A2 03 01 00 00 B0 E8 10 ...
*Mar 1 00:56:27.247: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0

00 21 45 00 00 64 00 2F 00 00 FE 01 0E B0 CB A2
03 01 CB 14 14 02 08 00 A8 DF 10 28 0F D8 00 00
00 00 00 34 B5 36 AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.247: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2F 00 00 FF 01
0D B0 CB 14 14 02 CB A2 03 01 00 00 B0 DF 10 ...
*Mar 1 00:56:27.255: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 30 00 00 FE 01 0E AF CB A2
03 01 CB 14 14 02 08 00 A8 D6 10 29 0F D8 00 00
00 00 00 34 B5 3E AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.255: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 30 00 00 FF 01
0D AF CB 14 14 02 CB A2 03 01 00 00 B0 D6 10 ...

PPP over Ethernet with VPN

Tác giả Lê Anh Đức

PPP over Ethernet kết hợp với VPN

Mô tả:

Error!

Ở topo trên, ta có, R3 sẽ làm PPPoE client, còn R1 sẽ làm PPPoE server, thực hiện kết nối với các mạng trong Internet với ISP làm router giả lập ISP. Router R2 là router ở chi nhánh, thực hiện NAT để cho mang private ra internet. Chú ý: Các router R3, R1 là các route 2600, chạy IOS version 12.2 trở lên. Kết hợp với đó, ta sẽ tạo một tunnel private giữa R3 và R2, để các traffic từ các mạng LAN trong nội bộ giữa 2 chi nhánh sẽ sử dụng để liên lạc với nhau qua môi trường Internet.

Cấu hình:

R1

```
!
version 12.2
!
hostname R1
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
```

```
!
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Loopback1
ip address 203.162.3.2 255.255.255.255
!
interface Ethernet0/0
no ip address
half-duplex
pppoe enable
!
interface Serial0/0
ip address 203.20.20.2 255.255.255.252
no fair-queue
!
interface Virtual-Template1
ip unnumbered Loopback1
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip http server
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
```

line con 0
line aux 0
line vty 0 4
!
!
end
R2
Building configuration...
Current configuration : 1290 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 10 ßtạo các chính sách xác minh cho VPN (phải đồng bộ)
hash md5
authentication pre-share
crypto isakmp key cisco address 203.162.3.1 ßtạo key để xác minh
!
!
crypto ipsec transform-set vnpro esp-des ßtạo chính sách mã hoá cho luống traffic trong tunnel
!
crypto map lee 10 ipsec-isakmp ßtạo crypto map để match traffic
set peer 203.162.3.1
set transform-set vnpro
match address 120
!
!

!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
ip address 10.10.2.1 255.255.255.0
ip nat inside
half-duplex
!
interface Serial0/0
ip address 203.30.30.2 255.255.255.252
ip nat outside
no fair-queue
crypto map lee ßáp crypto map vào interface S0/0
!
interface Serial0/1
no ip address
shutdown
!
ip nat inside source route-map nonat interface Serial0/0 overloadßtạo NAT
ip classless
ip route 0.0.0.0 0.0.0.0 203.30.30.1
ip http server
!
!
access-list 120 permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255ßxác định traffic được mã hoá

access-list 130 deny ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255ßmiễn NAT cho traffic trong tunnel
access-list 130 permit ip any any
!
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
R3
Building configuration...
*Mar 1 01:25:49.913: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 1523 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
!
memory-size iomem 10
ip subnet-zero
!

!
!

vpdn enable ßbật PPPoE
!
vpdn-group 1 ßtạo vpdn group để giao tiếp với server
request-dialin ßxác định đây là PPPoE client
protocol pppoe
!
!
crypto isakmp policy 10 ßtạo chính sách xác minh
hash md5
authentication pre-share
crypto isakmp key cisco address 203.30.30.2 ßtạo key để xác minh
!
!
crypto ipsec transform-set vnpro esp-des ßxác định giải thuật mã hoá cho traffic trong tunnel
!
crypto map lee 10 ipsec-isakmp ßtạo crypto map để xác định traffci được mã hoá
set peer 203.30.30.2
set transform-set vnpro
match address 120
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Loopback0

ip address 10.10.1.1 255.255.255.0
ip nat inside
!
interface Ethernet0/0
no ip address
half-duplex
pppoe enable ßbật PPPoE trên interface nối với server
pppoe-client dial-pool-number 1 ßsử dụng Dieler để giao tiếp với PPPoE server
!
interface Serial0/0
no ip address
shutdown
no fair-queue
!
interface Dialer1 ßxây dựng interface Dialer
mtu 1492
ip address 203.162.3.1 255.255.255.0
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
crypto map lee ßgán crypto map vào interface này
!
ip nat inside source route-map nonat interface Dialer1 overload ßsử dụng PAT
ip classless
ip route 0.0.0.0 0.0.0.0 203.162.3.2
ip http server
!
!
access-list 120 permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255 ßxác định traffic được bảo vệ
access-list 130 deny ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255 ßmiễn NAT cho traffic trong tunnel
access-list 130 permit ip any any
dialer-list 1 protocol ip permit
!
route-map nonat permit 10
match ip address 130

!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

ISP

Building configuration...
01:17:31: %SYS-5-CONFIG_I: Configured from console by console
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ISP
!
!
ip subnet-zero
!
!
!
interface Ethernet0
no ip address
no ip directed-broadcast
shutdown
!

```
interface Serial0
ip address 203.20.20.1 255.255.255.252
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 64000
!
interface Serial1
ip address 203.30.30.1 255.255.255.252
no ip directed-broadcast
clockrate 64000
!
ip classless
ip route 10.10.1.0 255.255.255.0 203.20.20.2 ßISP sử dụng static routing
ip route 10.10.2.0 255.255.255.0 203.30.30.2
ip route 203.162.0.0 255.255.0.0 203.20.20.2
!
!
line con 0
transport input none
line aux 0
line vty 0 4
!
end
```

Thực hiện:

1. **Cấu hình PPPoE:**

PPP over Ethernet là một sự phát triển dựa trên kỹ thuật PPP truyền thống. PPPoE cung cấp khả năng kết nối nhiều host trong mạng qua một thiết bị chuyển mạch vào một DSLAM, để cung cấp một kết nối PPPoE, mỗi phiên PPP phải học địa chỉ Ethernet của remote peer và thiết lập một danh định duy nhất. PPPoE gồm 2 pha: Discovery và Session:

- Discovery: khi một router muốn khởi tạo 1 phiên PPPoE, nó phải xác định địa chỉ MAC của thiết bị bên kia (Lát nửa debug sẽ cho thấy điều này) và thiết lập một PPPoE Session-ID. Trong quá trình này, CPE sẽ tìm các DSLAM và chọn một cái để sử dụng. Khi quá trình này chấm dứt, cả CPE và DSLAM đều sẽ có thông tin mà nó sử dụng để xây dựng kết nối PPPoE. Khi PPPsession được thiết lập thì cả CPE và DSLAM sẽ phải phân phát tài nguyên của mình cho một PPP virtual interface.
- Session: khi được thiết lập thì dữ liệu sẽ được gửi.

Để cấu hình, ta thực hiện các bước sau:

PPPoE server(R1):
R1(config)#vpdn enable ßbật PPPoE
R1(config)#vpdn-group 1
R1(config-vpdn)#accept-dialin ßxác định đây là PPPoE server
R1(config-vpdn-acc-in)#protocol pppoe
R1(config-vpdn-acc-in)#virtual-template 1 ßsử dụng virtual để giao tiếp với client
R1(config-vpdn-acc-in)#exit
R1(config)#int lo1
R1(config-if)#ip add 203.162.3.2 255.255.255.255
R1(config-if)#int e0/0
R1(config-if)#pppoe enable ßbật PPPoE trên interface kết nối với client
R1(config)#int virtual-template 1 ßtạo virtual template
R1(config-if)#ip unnumbered lo1
PPPoE client(R3):
R3(config)#vpdn enable
R3(config)#vpdn-group 1
R3(config-vpdn)#request-dialin ßxác định PPPoE client
R3(config-vpdn-req-in)#protocol pppoe
R3(config)#int e0/0
R3(config-if)#pppoe enable ßbật PPPoE trên interface nối với server
R3(config-if)#pppoe-client dial-pool-number 1 ßsử dụng dialer 1 để giao tiếp với server
R3(config-if)#exit
R3(config)#int dialer 1
R3(config-if)#mtu 1492
R3(config-if)#ip add 203.162.3.1 255.255.255.0
R3(config-if)#ip nat outside
R3(config-if)#encapsulation ppp
R3(config-if)#dialer pool 1
R3(config-if)#dialer-group 1
R3(config-if)#exit
R3(config)#dialer-list 1 protocol ip permit

2. Cấu hình VPN:

Để thực hiện cấu hình VPN giữa 2 chi nhánh qua môi trường DSL, ta cũng thực hiện tương tự như các bài lab VPN trước:
R2:
R2(config)#crypto isakmp policy 10

R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#exit
R2(config)#crypto isakmp key cisco address 203.162.3.1
R2(config)#crypto ipsec transform-set vnpro esp-des
R2(cfg-crypto-trans)#exit
R2(config)#crypto map lee 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R2(config-crypto-map)#set peer 203.162.3.1
R2(config-crypto-map)#set transform-set vnpro
R2(config-crypto-map)#match address 120
R2(config-crypto-map)#exit
R2(config)#int s0/0
R2(config-if)#crypto map lee
R2(config)#ip nat inside source route-map nonat interface s0/0 overload
R2(config)#access-list 120 permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
R2(config)#access-list 130 deny ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
R2(config)#access-list 130 permit ip any any
R2(config)#route-map nonat
R2(config-route-map)#match ip address 130
R3:
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#hash md5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 203.30.30.2
R3(config)#crypto ipsec transform-set vnpro esp-des
R3(cfg-crypto-trans)#exit
R3(config)#crypto map lee 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)#set peer 203.30.30.2
R3(config-crypto-map)#set transform-set vnpro
R3(config-crypto-map)#match address 120
R3(config-crypto-map)#exit
R3(config)#int dialer 1
R3(config-if)#crypto map lee
R3(config)#ip nat inside source route-map nonat interface dialer 1 overload

R3(config)#access-list 120 permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
R3(config)#access-list 130 deny ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
R3(config)#access-list 130 permit ip any any
R3(config)#route-map nonat
R3(config-route-map)#match ip address 130
Kiểm tra:

1. Kiểm tra VPN:

Ta sử dụng các lệnh show để xem thông tin về VPN:

R3:

R3#sh crypto map

```
Crypto Map "lee" 10 ipsec-isakmp
  Peer = 203.30.30.2
  Extended IP access list 120
     access-list 120 permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
  Current peer: 203.30.30.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={ vnpro, }
  Interfaces using crypto map lee:
            Virtual-Access1
            Dialer1
```

R3#sh crypto isakmp policy

```
Protection suite of priority 10
  encryption algorithm:        DES - Data Encryption Standard (56 bit keys).
  hash algorithm:               Message Digest 5
  authentication method:       Pre-Shared Key
  Diffie-Hellman group:         #1 (768 bit)
  lifetime:             86400 seconds, no volume limit
Default protection suite
  encryption algorithm:        DES - Data Encryption Standard (56 bit keys).
  hash algorithm:               Secure Hash Standard
  authentication method:       Rivest-Shamir-Adleman Signature
  Diffie-Hellman group:         #1 (768 bit)
  lifetime:             86400 seconds, no volume limit
```

R3#sh crypto ipsec transform-set

```
Transform set vnpro: { esp-des  }
will negotiate = { Tunnel,  },
```

R2:

R2#sh crypto isakmp policy

```
Protection suite of priority 10
```

encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit

R2#sh crypto ipsec transform-set

Transform set vnpro: { esp-des }
will negotiate = { Tunnel, },

R2#sh crypto map

Crypto Map "lee" 10 ipsec-isakmp
Peer = 203.162.3.1
Extended IP access list 120
access-list 120 permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
Current peer: 203.162.3.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ vnpro, }
Interfaces using crypto map lee:
Serial0/0
Tunnel0

2. <u>Kiểm tra PPPoE</u>:

Ta sử dụng các lệnh show và debug để xem quá trình tạo kết nối và trao đổi dữ liệu như thế nào giữa client và server:

R3#sh int

Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0005.5e96.2cc0 (bia 0005.5e96.2cc0)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 192/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:41, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
47 packets input, 4752 bytes, 0 no buffer
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
317 packets output, 21918 bytes, 0 underruns
251 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
251 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
MTU 1492 bytes, BW 56 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 5 seconds on reset
Interface is bound to Di1 (Encapsulation PPP)
LCP Open
Listen: CDPCP
Open: IPCP
Last input 00:00:09, output never, output hang never
Last clearing of "show interface" counters 00:02:56
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
39 packets input, 544 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
39 packets output, 616 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Dialer1 is up, line protocol is up (spoofing)
Hardware is Unknown
Internet address is 203.162.3.1/24

MTU 1492 bytes, BW 56 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 1 seconds on reset
Interface is bound to Vi1
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:34:56
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/16 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 42 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
36 packets input, 504 bytes
36 packets output, 576 bytes
Bound to:
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
MTU 1492 bytes, BW 56 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 5 seconds on reset
Interface is bound to Di1 (Encapsulation PPP)
LCP Open
Listen: CDPCP
Open: IPCP
Last input 00:00:04, output never, output hang never
Last clearing of "show interface" counters 00:03:01
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
41 packets input, 572 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
41 packets output, 648 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Loopback0 is up, line protocol is up
Hardware is Loopback
Internet address is 10.10.1.1/24
MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation LOOPBACK, loopback not set
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
R3#sh vpdn
%No active L2TP tunnels
%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
VPDN group: 1
Session count: 1
PPPoE Session Information
SID RemMAC LocMAC Intf VASt OIntf VLAN/

VP/VC

1 0004.c052.7ce0 0005.5e96.2cc0 Vi1 UP Et0/0

R3#debug vpdn pppoe-data ßbật debug PPPoE

PPPoE data packets debugging is on

R3#debug ip nat ßvà NAT

IP NAT debugging is on

R3#ping ßthực hiện ping mở rộng với source là Private LAN

Protocol [ip]:

Target IP address: 203.30.30.2

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 10.10.1.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 203.30.30.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/64 ms

R3#

***Mar 1 00:47:59.363: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [34**]

*Mar 1 00:47:59.363: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0

00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00

00 01 00 66 00 21 45 00 00 64 00 22 00 00 FF 01

03 B3 CB A2 03 01 CB 1E 1E 02 08 00 62 E7 0F ...

***Mar 1 00:47:59.423: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [34]**

*Mar 1 00:47:59.423: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0

00 21 45 00 00 64 00 22 00 00 FC 01 CA 4B CB 1E

1E 02 0A 0A 01 01 00 00 6A E7 0F 88 1C 2B 00 00

00 00 00 2B EF 84 AB CD AB CD AB CD AB CD AB ...

***Mar 1 00:47:59.427: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [35]**

*Mar 1 00:47:59.427: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0

00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00

00 01 00 66 00 21 45 00 00 64 00 23 00 00 FF 01

03 B2 CB A2 03 01 CB 1E 1E 02 08 00 62 A6 0F ...

***Mar 1 00:47:59.487: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [35]**
*Mar 1 00:47:59.487: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 23 00 00 FC 01 CA 4A CB 1E
1E 02 0A 0A 01 01 00 00 6A A6 0F 89 1C 2B 00 00
00 00 00 2B EF C4 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.491: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [36]**
*Mar 1 00:47:59.491: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 24 00 00 FF 01
03 B1 CB A2 03 01 CB 1E 1E 02 08 00 62 65 0F ...
***Mar 1 00:47:59.551: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [36]**
*Mar 1 00:47:59.551: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 24 00 00 FC 01 CA 49 CB 1E
1E 02 0A 0A 01 01 00 00 6A 65 0F 8A 1C 2B 00 00
00 00 00 2B F0 04 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.555: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [37]**
*Mar 1 00:47:59.559: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 25 00 00 FF 01
03 B0 CB A2 03 01 CB 1E 1E 02 08 00 62 24 0F ...
***Mar 1 00:47:59.615: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [37]**
*Mar 1 00:47:59.615: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 25 00 00 FC 01 CA 48 CB 1E
1E 02 0A 0A 01 01 00 00 6A 24 0F 8B 1C 2B 00 00
00 00 00 2B F0 44 AB CD AB CD AB CD AB CD AB ...
***Mar 1 00:47:59.619: NAT: s=10.10.1.1->203.162.3.1, d=203.30.30.2 [38]**
*Mar 1 00:47:59.623: PPPoE 1: O L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 04 C0 52 7C E0 00 05 5E 96 2C C0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 26 00 00 FF 01
03 AF CB A2 03 01 CB 1E 1E 02 08 00 61 E3 0F ...
***Mar 1 00:47:59.679: NAT*: s=203.30.30.2, d=203.162.3.1->10.10.1.1 [38]**
*Mar 1 00:47:59.683: PPPoE 1: I L:0005.5e96.2cc0 R:0004.c052.7ce0 Et0/0
00 21 45 00 00 64 00 26 00 00 FC 01 CA 47 CB 1E
1E 02 0A 0A 01 01 00 00 69 E3 0F 8C 1C 2B 00 00
00 00 00 2B F0 84 AB CD AB CD AB CD AB CD AB ...

Dựa vào debug trên, ta thấy quá trình discovery và session diễn ra như trên debug.

Tương tự như trên PPPoE server, ta cũng test y như trên client:

R1#sh vpdn
%No active L2TP tunnels

%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
VPDN group: 1
Session count: 1
PPPoE Session Information
SID RemMAC LocMAC Intf VASt OIntf VLAN/ VP/VC
1 0005.5e96.2cc0 0004.c052.7ce0 Vi1 UP Et0/0
R1#debug vpdn pppoe-data
PPPoE data packets debugging is on
R1# **ßkhi client ping ra ngoài, ta sẽ thấy trên server xuất hiện debug sau:**
*Mar 1 00:56:26.538: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
FF 03 C0 21 09 6C 00 0C 04 E2 EC A9 00 00 00 CD
*Mar 1 00:56:26.538: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
C0 21 0A 6C 00 0C 05 82 38 4E 00 00 00 CD
*Mar 1 00:56:27.027: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
C0 21 09 6C 00 0C 05 82 38 4E 00 00 00 00
*Mar 1 00:56:27.027: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
FF 03 C0 21 0A 6C 00 0C 04 E2 EC A9 00 00 00 00
*Mar 1 00:56:27.223: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2C 00 00 FE 01 0E B3 CB A2
03 01 CB 14 14 02 08 00 A8 FA 10 25 0F D8 00 00
00 00 00 34 B5 1E AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.223: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2C 00 00 FF 01
0D B3 CB 14 14 02 CB A2 03 01 00 00 B0 FA 10 ...
*Mar 1 00:56:27.231: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2D 00 00 FE 01 0E B2 CB A2
03 01 CB 14 14 02 08 00 A8 F1 10 26 0F D8 00 00
00 00 00 34 B5 26 AB CD AB CD AB CD AB CD AB ...
*Mar 1 00:56:27.231: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
00 01 00 66 00 21 45 00 00 64 00 2D 00 00 FF 01
0D B2 CB 14 14 02 CB A2 03 01 00 00 B0 F1 10 ...
*Mar 1 00:56:27.239: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
00 21 45 00 00 64 00 2E 00 00 FE 01 0E B1 CB A2
03 01 CB 14 14 02 08 00 A8 E8 10 27 0F D8 00 00

```
   00 00 00 34 B5 2E AB CD AB CD AB CD AB CD AB ...
*Mar  1 00:56:27.239: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
   00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 2E 00 00 FF 01
   0D B1 CB 14 14 02 CB A2 03 01 00 00 B0 E8 10 ...
*Mar  1 00:56:27.247: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
   00 21 45 00 00 64 00 2F 00 00 FE 01 0E B0 CB A2
   03 01 CB 14 14 02 08 00 A8 DF 10 28 0F D8 00 00
   00 00 00 34 B5 36 AB CD AB CD AB CD AB CD AB ...
*Mar  1 00:56:27.247: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
   00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 2F 00 00 FF 01
   0D B0 CB 14 14 02 CB A2 03 01 00 00 B0 DF 10 ...
*Mar  1 00:56:27.255: PPPoE 1: I L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
   00 21 45 00 00 64 00 30 00 00 FE 01 0E AF CB A2
   03 01 CB 14 14 02 08 00 A8 D6 10 29 0F D8 00 00
   00 00 00 34 B5 3E AB CD AB CD AB CD AB CD AB ...
*Mar  1 00:56:27.255: PPPoE 1: O L:0004.c052.7ce0 R:0005.5e96.2cc0 Et0/0
   00 05 5E 96 2C C0 00 04 C0 52 7C E0 88 64 11 00
   00 01 00 66 00 21 45 00 00 64 00 30 00 00 FF 01
   0D AF CB 14 14 02 CB A2 03 01 00 00 B0 D6 10 ...
```

Chú ý: nhớ phải test VPN trước (Nếu muốn debug) vì nếu không Tunnel sẽ được tạo và ta sẽ không xem được các sự kiện xảy ra.

Quá trình trao đổi dữ liệu giữa hai máy

Tác giả: Đặng Quang Minh
Tài liệu tham khảo cho học viên CCNA của VnPro

Máy A muốn liên lạc với máy X,phải biết IP address của nó (hoặc hostname/domainname).Máy A dò trong ARP cache để tìm địa chỉ MAC đích có chưa,nếu chưa sẽ dùng ARP gửi thông điệp (broadcast) đến tòan mạng .
Có 2 trường hợp:

1/ Host X cùng segment với nó :
Host A gửi thông điệp với địa chỉ IP đích (đã biết) và MAC đích là FF-FF-FF-FF-FF-FF để hỏi xem MAC của địa chỉ này là gì.Các host trên segment đều nhận và xử lý gói này ,host nào có địa chỉ IP trùng với yêu cầu sẽ gửi lại thông tin cho host A là "IP này có MAC là : .....".Host A nhập thông tin vào ARP cache (RAM).Khi muốn liên lạc với X thì lại tra trong ARP cache để biết địa chỉ MAC cần đến.

ARP là gì?
Trong protocol TCP/IP có ARP protocol. ARP tự động cập nhật các MAC tương ứng với các IP và xây dựng một bảng ARP table trong máy tính trong cùng mạng subnet.

Khi này , nếu A và X ở trong cùng LAN, thì khi A muốn gửi packet cho X, no' sẽ match IP của X với MAC tương ứng trong bang ARP của no'. Nếu A biết IP của X , nhưng không match được MAC tương ứng trong bang ARP của no' , thì khi này nó sẽ gửi một packet , gọi là ARP request, với địa chỉ MAC broadcast FFFFFFFFFF . Khi này tất cả máy tính trên cùng một mạng sẽ nhận được gói này và chuyển lên lớp Network; nhưng chỉ có máy có IP match với IP destination address trong ARP request mới gửi trả lại gói tin có chứa dia chỉ MAC tương ứng mà máy A muộn tìm . Gói tin này là ARP reply.

Khi đó gói tin ARP request sẽ có MAC nguồn là MAC của A, MAC đích là FF-FF-FF-FF-FF-FF.

Nếu Host X available trên Segment thì nó sẽ biết là gói tin này gửi cho nó nhờ vào địa chỉ IP mà Host A ghi trong gói tin ARP request và nó sẽ trả lời bằng 1 gói tin ARP reply. Gói tin ARP reply sẽ có MAC nguồn là MAC của Host X, MAC đích là MAC của Host A, khi Host A nhận được gói tin này tự nhiên sẽ biết được MAC của X.

Sau khi A nhận được ARP reply , nó sẽ mở gói và update bảng ARP table của nó: IP và MAC của máy X.

2/ Host X không cùng segment với host A :
lúc đó phải nhờ đến router để forward yêu cầu này đến các segment khác. Trong trường hợp này, router sẽ gửi địa chỉ MAC của interface mà nhận gói ARP request trên Router cho máy gửi (máy A).

Một cách khác để liên lạc với một máy tính khác không cùng nằm trên 1 segment là "default gateway". Default Gateway là một phần của một host (máy tính). Nó là một địa chỉ IP của một interface trên router, và được cấu hình cho host. Địa chỉ IP của host và của Default Gateway phải cùng segment mạng. Khì này, máy gửi (A) sẽ kiểm tra xem nó và máy nhận (B) có cùng nằm trên một subnet hay không. Nếu không, nó sẽ đóng gói packet gửi với IP destination address là của máy nhận và MAC address destinaiton là của Router nối với subnet của nó.

Nếu Proxy ARP hay default gateway không được cấu hình, thì không có "traffic" nào có thê rời khỏi một subnet (một mạng cục bộ). Phải có một trong hai cái được cấu hình (hay cho phép) để có thể giao tiếp với các segment mạng khac được.

"IP source và dest không bao giờ thay đổi, chỉ có MAC source và dest là thay đổi thôi".

Proxy ARP: Theo cách thức hoạt động của proxy ARP, ta có thể thấy rằng client khi muốn biết MAC của một host nào đó, nó chỉ đơn giản là broadcast ARP-Request lên mạng. Router sẽ có trách nhiệm đáp trả lại bằng ARP-Reply nếu nó nhận thấy IP-destination là thuộnc mạng khác. Như vậy, cấu hình IP cho client cực kỳ đơn giản, nhưng gánh nặng lại đè lên router. Thử tưởng tượng cứ sau 1p', ARP-entry bị hủy bỏ, thế là các client thi nhau broadcast lên mạng thì router "tiêu" như chơi. Ngoài ra,

proxy ARP còn gặp một bất lợi nếu trong segment có tới hơn 1 router. Chọn router nào, nếu như các router đều có route đến mạng đích?

Default-Gateway: Nếu client biết rằng IP-dest không thuộc mạng của nó, nó dùng MAC của default-gateway để gửi gói tin, router default-gateway nhận lấy gói tin sẽ biết phải xử lý tiếp theo như thế nào (dựa trên IP source/destination). Cách này giảm tải cho router, giải quyết được trường hợp có nhiều router nối vào cùng segment, và đỡ gây nhầm lẫn.

Nếu Host A có cấu hình sử dụng Defaul gateway trong TCP/IP protocol thì gói tin ARP request sẽ không phải dạng Broadcast mà được gửi thẳng đến cho Router (TCP/IP stack quy định như vậy). Tất nhiên để gửi được gói tin này đến cho Router thì nó cũng phải request MAC của defaul gateway trên Router trước, sau đó khi có MAC của default gateway thì Host A sẽ tạo 1 gói tin ARP request MAC của Host X với IP đích là IP Host X, MAC đích là MAC của default gateway.
Khi Router gateway nhận được gói tin này thì nó sẽ Forward qua interface trên segment thích hợp, tại đây phần Datalink header sẽ được lấy ra (Pull out) và phần Datalink header mới sẽ được gắn vào với mục đích để truyền trên Segment của Host B. Khi Host B nhận được gói tin ARP request thì cũng sẽ trả lời lại bằng gói tin ARP reply được gửi đến DF gateway trên Segment của nó. Khi Router nhận được gói tin này cũng làm việc tương tự như khi gửi đi từ Host A (pull out Datalink header, gắn datalink header mới v.v....)

Nếu Host A không có cấu hình default gateway (tất nhiên sẽ broadcast gói tin ARP request) nhưng nếu Router trên Segment của host A có chức năng ARP Proxy thì căn cứ trên IP mà gói tin ARP request yêu cầu ROUTER sẽ so sánh với Routing Table của nó và nhận gói tin này nếu Match trong Routing table, sau đó sẽ forward qua Segment thích hợp. Quá trình tiếp theo tương tự như trường hợp A.

Như vậy : nếu 1 trong 2 default gateway của 2 segment cấu hình sai thì sẽ dẫn đến việc Host A không thể liên lạc được với Host X và ngược lại. Ngoài ra nếu thời gian tồn tại của ARP cache trong memory quá lâu công với việc có thay đổi MAC của DF gateway sẽ dẫn đến việc tạm thời không thể thực hiện ARP request.

Ví dụ minh họa cho các lý thuyết nêu trên:

xin lưu ý các IP của source và destination là không thay đổi chỉ có mac là thay đổi thôi. các bạn xem một ví dụ sau để dễ hiểu hơn nhé

máy A-------Router1--------router2--------router3------máy B

đầu tiên máy A đóng gói gói tin như sau

IP nguồn là IP của máy A. IP đích là IP của máy B xuống đến tầng datalink máy A sẽ xem máy B có trong cùng subnet với mình không, trong trường hợp này là không.

lúc này máy A sẽ dùng :

MAC nguồn là của máy A. MAC đích là mác của interface trên router1 nối với subnet A.

Router1 sẽ xem IP đích có nằm trong subnet của mình hay không trong trường hợp này là không, lúc này router sẽ dóng gói địa chỉ MAC nguồn là mác cùa interface mà router này nối với router2, mác đích sẻ là mác trên interface của router2, router2 cũng xử lý giống router 1 và chuyển đến router3.

Router3 sẽ xem IP này có nằm trong subnet của mình không, nếu có thì nó sẽ xem xét địa chỉ mac tương ứng với IP này (router3 biết được vì nó tra trong bảng ARP của nó có chứa máy B vì B cùng subnet) ư1ng với IP này router3 xác định được MAC là máy B lúc này máy B nhưng nó vẫn gửi Brodcast đến tất cả các máy trong subnet có máy B nhưng chỉ máy B nhận gói tin vì nó có MAC trùng với MAC đích trong gói tin.

A sẽ gửi 1 gói tin gọi là ARP request (ARP = Address Resolution Protocol) bằng cơ chế broadcast để tất cả các máy đều có thể nhận được gói tin này

Redistribute giữa OSPF và IGRP

Tác giả: Nguyễn Thị Băng Tâm

Trong bài này sẽ thực hiện redistribute giữa hai giao thức classless là OSPF và ISIS với nhau .

Mục tiêu bài làm :

Thực hiện multiple redistribute points (redistribute tại nhiều điểm)

Chỉ ra vấn đề gặp phải khi redistribute và cách giải quyết vấn đề đó .

Từ một router ping thấy tất cả các địa chỉ trong mạng .
Mô hình mạng như sau : router R3 và R4 sẽ chạy giao thức OSPF , R5 chạy giao thức ISIS. Router R4 và R1 sẽ là các router thực hiện redistribute .
Error!

Địa chỉ trên các interface của các router :

Router	Interface	địa chỉ
Router R1	E0/0 S0/0	172.16.1.1/24 172.16.2.2 /30
Router R2	S0/0 E0/0	172.16.2.1/30 192.168.4.2/24
Router R3	E0/0 S0/0	192.168.4.1/24 192.168.1.1/24
Router R4	S0/1 S0/0	192.168.1.2/24 192.168.2.1/30
Router R5	S0/0 E0/0 Loopback 0	192.168.2.2/30 172.16.1.2/24 10.1.1.1/24

Cấu hình ban đầu :
R1
!
hostname R1
!
enable password cisco
!
interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0

```
!
interface Serial0/0
ip address 172.16.2.2 255.255.255.252
!
end
R2
!
hostname R2
!
interface Ethernet0/0
ip address 192.168.4.2 255.255.255.0
!
interface Serial0/0
ip address 172.16.2.1 255.255.255.252
clockrate 64000
!
ip classless
!
end
R3
!
hostname R3
!
interface Ethernet0/0
ip address 192.168.4.1 255.255.255.0
half-duplex
!
interface Serial0/0
ip address 192.168.1.1 255.255.255.0
no fair-queue
!
end
R4
!
hostname R4
!
interface Ethernet0/0
ip address 192.168.100.1 255.255.255.0
!
interface Serial0/0
```

```
ip address 192.168.2.1 255.255.255.0
clockrate 64000
no fair-queue
!
interface Serial0/1
ip address 192.168.1.2 255.255.255.0
clockrate 64000
!
ip http server
ip classless
!
end
```

R5

```
!
hostname R5
!
interface Loopback0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/0
ip address 172.16.1.2 255.255.255.0
no ip directed-broadcast
!
interface Serial0/0
ip address 192.168.2.2 255.255.255.252
!
ip classless
end
```

Cấu hình ban đầu cho các router :

R1

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname  R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
```

R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable password cisco
R1(config)#interface s0/0
R1(config-if)#ip address 172.16.2.2 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#int e0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
cấu hình cho router R2 :
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#line vty 0 4
R2(config-line)#no login
R2(config-line)#exit
R2(config)#interface e0/0
R2(config-if)#ip address 192.168.4.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface s0/0
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#^Z
R2#
cấu hình cho router R3 :
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#line console 0
R3(config-line)#password cisco

R3(config-line)#line vty 0 4
R3(config-line)#no login
R3(config-line)#exit
R3(config)#interface s0/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#interface e0/0
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#^Z
R3#
cấu hình cho router R4 :
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#line console 0
R4(config-line)#password cisco
R4(config-line)#line vty 0 4
R4(config-line)#no login
R4(config-line)#exit
R4(config)#interface s0/1
R4(config-if)#ip address 192.168.1.2 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#interface s0/0
R4(config-if)#ip address 192.168.2.1 255.255.255.252
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#exit
cấu hình cho router R5 :
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R5
R5(config)#line console 0
R5(config-line)#password cisco
R5(config-line)#line vty 0 4
R5(config-line)#no login
R5(config-line)#exit

R5(config)#interface s0/0
R5(config-if)#ip address 192.168.2.2 255.255.255.252
R5(config-if)#clock rate 64000
R5(config-if)#no shutdown
R5(config-if)#interface e0/0
R5(config-if)#ip address 172.16.1.2 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#interface loopback 0
R5(config-if)#ip address 10.1.1.1 255.255.255.0
R5(config-if)#^Z
R5#
kiểm tra bảng định tuyến :
R1#show ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
R2#show ip route
Gateway of last resort is not set
172.16.0.0/30 is subnetted, 1 subnets
C 172.16.2.0 is directly connected, Serial0/0
C 192.168.4.0/24 is directly connected, Ethernet0/0
R3#show ip route
Gateway of last resort is not set
C 192.168.4.0/24 is directly connected, Ethernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0
R4#show ip route
Gateway of last resort is not set
C 192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0/30 is directly connected, Serial0/0
R5#show ip route
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0

Cấu hình định tuyến cho các router .Router R2,R3, interface s0/0 của R1 và interface s0/1 của R4 chạy OSPF process 1 ,còn lại là chạy ISIS .
Ta biết cấu hình ISIS đòi hỏi cần phải có địa chỉ NET ,mỗi system-ID đại diện cho mỗi node, ta có thể gắn nó một cách tùy ý nhưng để đảm bảo system-ID là duy nhất của mỗi router trong một area ta sẽ sử dụng địa chỉ Mac .
Ta kiểm tra địa chỉ Mac của thiết bị bằng cách show arp hoặc show interface .

```
R1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.1.1             -   0004.c052.7ce0  ARPA   Ethernet0/0
R4#show interface e0/0
Ethernet0/0 is administratively down, line protocol is down
Hardware is AmdP2, address is 0002.4b79.9ca0 (bia 0002.4b79.9ca0)
Internet address is 192.168.100.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 252/255, txload 1/255, rxload 1/255
    <omitted>
R5#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.1.2             -   00d0.ba1a.f080  ARPA   Ethernet0/0
```

Cấu hình như sau :

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.2.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#clns routing
R1(config)#router isis
R1(config-router)#net 01.0001.0004.c052.7ce0.00
R1(config-router)#exit
R1(config)#interface e0/0
R1(config-if)#ip router isis
R1(config-if)#^Z
R1#
R2(config)#router ospf 1
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#exit
R2(config)#^Z
R3(config)#router ospf 1
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.1.0 0.0.0.255 area 0
R3(config-router)#exit
```

```
R3(config)#^Z
R4(config)#router ospf 1
R4(config-router)#network 192.168.1.0 0.0.0.255 area 0
R4(config-router)#exit
R4(config)#clns routing
R4(config)#router isis
R4(config-router)#net 01.0001.0002.4b79.9ca0.00
R4(config-router)#exit
R4(config)#int s0/0
R4(config-if)#ip router isis
R4(config-if)#^Z
R5(config)#clns routing
R5(config)#router isis
R5(config-router)#net 01.0001.00d0.ba1a.f080.00
R5(config-router)#int s0/0
R5(config-if)#ip router isis
R5(config-if)#int e0/0
R5(config-if)#ip router isis
R5(config-if)#exit
R5(config)#int loopback 0
R5(config-if)#ip router isis
R5(config)#^Z
```

kiểm tra lại bảng định tuyến :

```
R1#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
C       172.16.2.0/30 is directly connected, Serial0/0
O    192.168.4.0/24 [110/74] via 172.16.2.1, 00:03:18, Serial0/0
10.0.0.0/24 is subnetted, 1 subnets
i L1    10.1.1.0 [115/20] via 172.16.1.2, Ethernet0/0
O    192.168.1.0/24 [110/138] via 172.16.2.1, 00:03:18, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
i L1    192.168.2.0 [115/20] via 172.16.1.2, Ethernet0/0
```

Những route nào học từ ISIS sẽ bắt đầu bằng i. Trong bài này các router chạy ISIS để mặc định là L1/L2 router và các router đang chạy level – 1 routing nên có kí hiệu là L1 .Đối với metric của ISIS thì loại metric có chiều dài là 1 byte. Bit 8 chỉ ra sự hiện diện của loại metric trong TLV.Bit 7 được dùng để phân loại metric là internal hay là external .Internal metric đề cập đến các route được tạo ra trong miền ISIS , trong khi đó external route đề cập đến các route bên ngoài miền ISIS

hoặc là từ các giao thức định tuyến khác. 6 bit còn lại dành cho việc tính toán thực sự giá trị của metric. Do đó ta có giá trị cost cực đại của default metric là 63 trên một link . Đối với Cisco router cost của một link được quyết định bởi giá trị được đăng kí đến interface ngõ ra . Cisco đăng kí default metric là 10 cho mỗi interface mà không quan tâm interface đó thuộc loại nào. Lúc này mỗi subnetwork được xem là bằng nhau và ISIS metric được tính toán đơn giản bằng cách tính tổng các hop-count nó phải đi qua để đến đích , mỗi hop có cost là 10. Ví dụ trong bảng định tuyến của R1 ta thấy ,route 192.168.2.0 có metric là 20 vì nó đi qua R5,R1. Cost của các route học được từ OSPF được tính tương tự như bài redistribute giữa classfull và classless. Cost của 192.168.1.0/24 là 138 vì nó phải đi qua 2 serial interface (mỗi interface có cost là 64) và một ethernet interface (có cost là 10). Cách tính cost của OSPF là không đổi khi thực hiện redistribute ,do đó trong bài này ta sẽ không xét kĩ về nó .

```
R2#show ip route
Gateway of last resort is not set
172.16.0.0/30 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0
C    192.168.4.0/24 is directly connected, Ethernet0/0
O    192.168.1.0/24 [110/74] via 192.168.4.1, 00:00:05, Ethernet0/0
R3#sh ip route
Gateway of last resort is not set
172.16.0.0/30 is subnetted, 1 subnets
O       172.16.2.0 [110/74] via 192.168.4.2, 00:01:07, Ethernet0/0
C    192.168.4.0/24 is directly connected, Ethernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0
R4#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
i L1    172.16.1.0/24 [115/20] via 192.168.2.2, Serial0/0
O       172.16.2.0/30 [110/138] via 192.168.1.1, 00:01:51, Serial0/1
O    192.168.4.0/24 [110/74] via 192.168.1.1, 00:01:51, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
i L1    10.1.1.0 [115/20] via 192.168.2.2, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Serial0/0
R5#show ip route
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Ethernet0/0
```

10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
Kiểm tra bằng lệnh ping :
R4#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/40 ms
R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R4#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R4#ping 192.168.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
R2#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2 không thể ping 192.168.2.1 được vì R2 chạy giao thức OSPF còn mạng 192.168.2.0/24 sử dụng ISIS .Muốn thực hiện ping thành công ta phải redistribute giữa hai giao thức . cấu hình redistribute được thực hiện trên cả hai routert R1 và R4 được gọi là multiple redistribute points Cấu hình như sau :
R4(config)#router ospf 1
R4(config-router)#redistribute isis level-1 metric 20
% Only classful networks will be redistributed
R4(config-router)#router isis
R4(config-router)#redistribute ospf 1 metric 10 level-1-2
R4(config-router)#exit

R1(config)#router ospf 1
R1(config-router)#redistribute isis level-1 metric 20
% Only classful networks will be redistributed
à redistribute các route ISIS vào OSPF với metric là 20 và các route này đóng vai trò là
level-1.
R1(config-router)#router isis
R1(config-router)#redistribute ospf 1 metric 10 level-1-2
à redistribute những route OSPF vào ISIS với metric là 10 và các route có vai trò level-1-2 route .
Kiểm tra bảng định tuyến :
R2#show ip route
Gateway of last resort is not set
172.16.0.0/30 is subnetted, 1 subnets
C   172.16.2.0 is directly connected, Serial0/0
C   192.168.4.0/24 is directly connected, Ethernet0/0
O   192.168.1.0/24 [110/74] via 192.168.4.1, 00:11:09

, Ethernet0/0
à trên bảng định tuyến của R2 không học được route nào từ ISIS lí do là vì chỉ có những classfull networks mới được đi vào OSPF .
R5#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
i L1 172.16.2.0/30 [115/20] via 192.168.2.1, Serial0/0
[115/20] via 172.16.1.1, Ethernet0/0
i L1 192.168.4.0/24 [115/20] via 192.168.2.1, Serial0/0
[115/20] via 172.16.1.1, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback0
i L1 192.168.1.0/24 [115/20] via 192.168.2.1, Serial0/0
[115/20] via 172.16.1.1, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
Để R2,R3 thấy được các route trong ISIS ta thêm vào trong câu lệnh redistribute một subnets.
R4(config)#router ospf 1
R4(config-router)#no redistribute isis level-1 metric 20
R4(config-router)#redistribute isis level-1 metric 20 subnets
R4(config-router)#router isis
R4(config-router)#no redistribute ospf 1 metric 10 level-1-2
R4(config-router)#redistribute ospf 1 metric 10 metric-type external
à các route được redistribute vào ISIS có thể là internal route hoặc external route (internal là default) hoặc là level 1 ,hoặc là level 2 (level 2 là default). Trong cấu hình trên các OSPF route được redistribute như là external route với default metric là 10 .
R1(config)#router ospf 1
R1(config-router)#no redistribute isis level-1 metric 20
R1(config-router)#redistribute isis level-1 metric 20 subnets
R1(config-router)#router isis
R1(config-router)#no redistribute ospf 1 metric 10 level-1-2
R1(config-router)#redistribute ospf 1 metric 10 metric-type external
Kiểm tra bảng định tuyến:
R4#show ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
i L1 172.16.1.0/24 [115/20] via 192.168.2.2, Serial0/0

O 172.16.2.0/30 [110/138] via 192.168.1.1, 00:23:26, Serial0/1
O 192.168.4.0/24 [110/74] via 192.168.1.1, 00:23:26, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
i L1 10.1.1.0 [115/20] via 192.168.2.2, Serial0/0
C 192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
à bảng định tuyến của R4 không có gì thay đổi .
R1#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
O 192.168.4.0/24 [110/74] via 172.16.2.1, 00:23:14, Serial0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 172.16.2.1, 00:10:32, Serial0/0
O 192.168.1.0/24 [110/138] via 172.16.2.1, 00:23:14, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
i L1 192.168.2.0 [115/20] via 172.16.1.2, Ethernet0/0
à bảng định tuyến đã khác trước ,có sự xuất hiện một external route .Đó là route 10.1.1.0 được học thông qua OSPF qua interface 172.16.2.1 thay vì học trực tiếp từ router R5 .Ở đây ta gặp phải một vấn đề ,cả R1 và R4 đều đang redistribute các route được học bởi ISIS vào OSPF.R4 học mạng 10.1.1.0 thông qua ISIS và quảng bá vào OSPF domain .Kết quả là R1 học mạng 10.1.1.0 không phải từ R5 mà từ R2 thông qua OSPF .
R1#traceroute 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.1.1.1
1 172.16.2.1 16 msec 16 msec 12 msec
2 192.168.4.1 16 msec 16 msec 16 msec
3 192.168.1.2 28 msec 28 msec 28 msec
4 192.168.2.2 44 msec 16 msec *
R4#traceroute 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.1.1.1
1 192.168.2.2 20 msec 24 msec *
Ta reload lại router R4 ,quan sát bảng định tuyến của cả 2 router R1 và R4 :
R1#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.0/24 is directly connected, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
i L2 192.168.4.0/24 [115/94] via 172.16.1.2, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
i L1 10.1.1.0 [115/20] via 172.16.1.2, Ethernet0/0
i L2 192.168.1.0/24 [115/94] via 172.16.1.2, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
i L1 192.168.2.0 [115/20] via 172.16.1.2, Ethernet0/0
à R1 xem R5 như là next hop để đi đến route 10.1.1.0 ,do đó có kí hiệu L1 .Bảng định tuyến cũng cho thấy R1 xem route 192.168.1.0 là level-2 , metric 94 cho thấy đây là external route.
Trong khi đó thì R4 lại xem 10.1.1.0 như là một route bên ngoài mà nó học được thông qua R3.
R4#show ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
i L1 172.16.1.0/24 [115/20] via 192.168.2.2, Serial0/0
O 172.16.2.0/30 [110/138] via 192.168.1.1, 00:00:18, Serial0/1
O 192.168.4.0/24 [110/74] via 192.168.1.1, 00:00:18, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 192.168.1.1, 00:00:00, Serial0/1
C 192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
Sự hội tụ trong một mạng : các router chia sẽ thông tin định tuyến với nhau , nhưng mỗi cá nhân router phải tự tính toán bảng định tuyến của chúng .Đối với mỗi bảng định tuyến cá nhân đó được chính xác , các router đã có một cái nhìn chung về topology mạng .Lúc này mạng được xem là hội tụ .Nếu mạng đang trong quá trình hội tụ ,sẽ dễ dàng xảy ra nhiều vấn đề định tuyến như router nghĩ rằng một link đang up trong khi thật sự là nó đang bị down dẫn đến bảng định tuyến sai và loop dễ dàng xảy ra .Mạng được xem là hội tụ nhanh khi khôi phục được sự cố (như lỗi liên kết hoặc sự thay đổi về mạng) một cách nhanh chóng .
Các giao thức link-state hội tụ mạng rất nhanh vì khi có sự thay đổi xảy ra trong mạng ,sự thay đổi này ngay lập tức được gửi đi bằng multicast tới các neighbor trong partial update (tức là update chỉ gồm có sự thay đổi này) điều này làm loop khó có thể xảy ra trong một mạng chạy toàn giao thức link- state .
Trở lại với bài trên ,ta thấy loop đã không xảy ra nhưng trong cả hai trường hợp ,router R1 và R4 đều chọn con đường đi không tối ưu đến mạng 10.1.1.0 .R1 thay vì xem R5 như là next hop để đến đích thì nó lại xem R2 như là next hop .R4 cũng

tương tự .Ta có thể giải thích điều này như sau : (xem bảng định tuyến trước khi R4 được reload)
giả sử cả hai router R1 và R4 thực hiện redistribute cùng một thời điểm .Cả hai router đều gửi OSPF update trong đó có mạng 10.1.1.0 ,R4 may mắn hơn ,nó gửi update nhanh hơn R1. R4 chỉ gửi những route mà nó học từ ISIS vào OSPF , đó là những route 172.16.1.0 và 10.1.1.0 , nó không gửi những route kết nối trực tiếp hoặc là những route nó đã được học thông qua OSPF.
R3 nhận update từ R4 , xem R4 như là next –hop router (quan sát bảng định tuyến của R3 ,những route học từ R4 được tô đậm) và gửi update đến R2 .

R3#show ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2 172.16.1.0/24 [110/20] via 192.168.1.2, 00:28:39, Serial0/0
O 172.16.2.0/30 [110/74] via 192.168.4.2, 00:41:20, Ethernet0/0
C 192.168.4.0/24 is directly connected, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 192.168.1.2, 00:28:39, Serial0/0
C 192.168.1.0/24 is directly connected, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
O E2 192.168.2.0 [110/20] via 192.168.4.2, 00:14:14, Ethernet0/0
R2 , nhận update từ R3 ,xem R3 là next-hop router .

R2#show ip route

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2 172.16.1.0/24 [110/20] via 192.168.4.1, 00:00:40, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
C 192.168.4.0/24 is directly connected, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 192.168.4.1, 00:00:40, Ethernet0/0
O 192.168.1.0/24 [110/74] via 192.168.4.1, 00:00:40, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
O E2 192.168.2.0 [110/20] via 172.16.2.2, 00:00:40, Serial0/0
R1 và R2 gửi update cho nhau . Khi nhận được update của R2 về mạng 10.1.1.0 , router R1 nghĩ rằng đường đi đến mạng 10.1.1.0 qua R2 tốt hơn vì có AD nhỏ hơn

, dẫn đến R1 cập nhập bảng định tuyến và xem R2 như là next-hop. R1 không cập nhập những route còn lại từ R2 vì bản thân trong bảng định tuyến của nó đã tồn tại những route đó với AD tốt hơn . Khi R2 nhận update từ R1 , nó chỉ cập nhập route 192.168.2.0 . Lúc này R2 xem R1 như là next-hop để đi đến mạng 192.168.2.0 , R2 lại gửi update về mạng 192.168.2.0 cho R3 ,R3 xem R2 là next –hop để đến mạng 192.168.2.0 (xem bảng định tuyến).

Bảng định tuyến của R5 ,R5 cân bằng tải giữa hai đường :

```
R5#show ip route
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
i L2    172.16.2.0/30 [115/84] via 192.168.2.1, Serial0/0
                      [115/84] via 172.16.1.1, Ethernet0/0
i L2 192.168.4.0/24 [115/84] via 192.168.2.1, Serial0/0
                    [115/84] via 172.16.1.1, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
i L2 192.168.1.0/24 [115/84] via 192.168.2.1, Serial0/0
                    [115/84] via 172.16.1.1, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Serial0/0
```

Khi ra reload lai router R4 , quá trình học route của các router diễn ra như sau :

R5 ,R3 nhận ra sự thay đổi trong mạng ,ngay lập tức chúng gửi update chỉ bao gồm thông tin về sự thay đổi đó cho các router chạy

cùng giao thức với chúng ,trong trường hợp này R5 gửi update cho R1 , R3 gửi update cho R2 . R1 cũng có thể nhận update cho biết về sự thay đổi trong mạng từ R2 nhưng vì ISIS hội tụ nhanh hơn OSPF nên R1 sẽ update thông tin từ R5. R1 xem R5 là next-hop để đi đến các route còn lại trong mạng .

```
R1#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
C       172.16.2.0/30 is directly connected, Serial0/0
i L2 192.168.4.0/24 [115/94] via 172.16.1.2, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
i L1    10.1.1.0 [115/20] via 172.16.1.2, Ethernet0/0
i L2 192.168.1.0/24 [115/94] via 172.16.1.2, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
i L1    192.168.2.0 [115/20] via 172.16.1.2, Ethernet0/0
```

Khi R1 đã có đầy đủ thông tin về mạng của nó , là khi các mạng trong ISIS đã hội tụ xong , R1 liền gửi ngay update đến cho R2 ,trong update chỉ bao gồm những route bên trong nó học được từ ISIS (những route có kí tự L1 phía trước), R2 cập nhập update và gửi cho R3 ,R3 lại gửi cho R4 .R4 xem R3 như là next-hop .Do đó khi R4 cập nhập update nó sẽ chọn đường đi đến mạng 10.1.1.0 qua R3 vì nó thấy đường đi qua R3 có AD nhỏ hơn .

```
R4#show ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
i L1    172.16.1.0/24 [115/20] via 192.168.2.2, Serial0/0
O       172.16.2.0/30 [110/138] via 192.168.1.1, 00:00:18, Serial0/1
O    192.168.4.0/24 [110/74] via 192.168.1.1, 00:00:18, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
O E2    10.1.1.0 [110/20] via 192.168.1.1, 00:00:00, Serial0/1
C    192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Serial0/0
```

Qua phân tích trên ta thấy administrative distance có thể gây việc chọn đường đi không tối ưu mà trong một vài giao thức khác như RIP ,IGRP có thể gây loop , làm chậm lại quá trình hội tụ. có nhiều cách giải quyết vấn đề này như là sử dụng route filtering , thay đổi administrative distance bằng phương pháp thủ công , hay là sử dụng route map .Trong bài này ta sẽ thay đổi AD bằng cách dùng thêm câu lệnh distance để giải quyết vấn đề sub-optimal route , mà trong một vài trường hợp loop và black-hole có thể xảy ra .

Thay đổi AD sao cho R1 muốn đi đến mạng 10.1.1.0 và 192.168.1.0 phải coi router R5 là next-hop .R4 muốn đi đến mạng 10.1.1.0 và 172.16.1.0 phải coi R5 là next-hop. R2,R3 có thể tùy ý chọn lựa đường .
cấu hình như sau :

```
R4(config)#router ospf 1
R4(config-router)#distance 130
R4(config-router)#distance 110 0.0.0.0 255.255.255.255 1
R4(config-router)#router isis
R4(config-router)#distance 130
R4(config-router)#distance 115 192.168.2.2 0.0.0.0 2
R4(config-router)#exit
R4(config)#access-list 1 permit 192.168.4.0
R4(config)#access-list 1 permit 172.16.2.0 0.0.0.3
R4(config)#access-list 2 permit 10.1.1.0 0.0.0.255
R4(config)#access-list 2 permit 172.16.1.0 0.0.0.255
R1(config)#router ospf 1
R1(config-router)#distance 130
R1(config-router)#distance 110 0.0.0.0 255.255.255.255 1
R1(config-router)#router isis
R1(config-router)#distance 130
R1(config-router)#distance 115 172.16.1.2 0.0.0.0 2
R1(config-router)#exit
R1(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 2 permit 10.1.1.0 0.0.0.255
R1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
R1#sh run
!
router ospf 1
log-adjacency-changes
redistribute isis level-1 metric 20 subnets
network 172.16.2.0 0.0.0.3 area 0
distance 130
distance 110 0.0.0.0 255.255.255.255 1
!
router isis
net 01.0001.0004.c052.7ce0.00
redistribute ospf 1 metric 10 metric-type external
distance 130 clns
distance 115 172.16.1.2 0.0.0.0 2
```

```
!
!
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 2 permit 10.1.1.0 0.0.0.255
access-list 2 permit 192.168.2.0 0.0.0.255
!
R4#sh run
!
router ospf 1
log-adjacency-changes
redistribute isis level-1 metric 20 subnets
network 192.168.1.0 0.0.0.255 area 0
distance 130
distance 110 0.0.0.0 255.255.255.255 1
!
router isis
net 01.0001.0002.4b79.9ca0.00
redistribute ospf 1 metric 10 metric-type external
distance 130 clns
distance 115 192.168.2.2 0.0.0.0 2
!
access-list 1 permit 192.168.4.0
access-list 1 permit 172.16.2.0 0.0.0.3
access-list 2 permit 10.1.1.0 0.0.0.255
access-list 2 permit 172.16.1.0 0.0.0.255
!
```

Câu lệnh distance đầu tiên trong hai cấu hình thiết lập distance mặc định cho các route của OSPF và ISIS là 130 . Câu lệnh distance thứ hai thiết lập một distance khác tùy theo router quảng bá nào được chỉ định và có tham chiếu đến access-list .Chẳng hạn trên router R1 , tiến trình ISIS của R1 đăng kí distance là 115 cho các route được quảng bá bởi R5 và được cho phép bởi access-list 2 .Tất cả các route còn lại được gán distance bằng 130 . Inverse mask được sử dụng trong địa chỉ của router quảng bá (cụ thể là R5) chỉ ra chính xác interface nào mà R1 cần đi đến .Đối với OSPF , địa chỉ và inverse mask trong câu lệnh distance là 0.0.0.0 255.255.255.255 chỉ định bất kì router nào .Các route OSPF từ tất cả các router được cho phép bởi access- list 1 được đăng kí một distance là 110 , tất cả các route còn lại khác có distance là 130 .

Câu lệnh distance trong R4 được giải thích tương tự .

Kết quả là ta có bảng định tuyến sau :

R4#sh ip route
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
i L1 172.16.1.0/24 [115/20] via 192.168.2.2, Serial0/0
O 172.16.2.0/30 [110/138] via 192.168.1.1, 00:57:37, Serial0/1
O 192.168.4.0/24 [110/74] via 192.168.1.1, 00:57:37, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
i L1 10.1.1.0 [115/20] via 192.168.2.2, Serial0/0
C 192.168.1.0/24 is directly connected, Serial0/1
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
R1#sh ip route
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
O 192.168.4.0/24 [110/74] via 172.16.2.1, 00:00:53, Serial0/0
10.0.0.0/24 is subnetted, 1 subnets
i L1 10.1.1.0 [115/20] via 172.16.1.2, Ethernet0/0
O 192.168.1.0/24 [110/138] via 172.16.2.1, 00:00:53, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
i L1 192.168.2.0 [115/20] via 172.16.1.2, Ethernet0/0
Trong bảng định tuyến của R4 ta thấy rằng , R4 đang định tuyến đến tất cả các mạng trong miền OSPF thông qua R3 và đến tất cả các mạng trong miền ISIS thông qua R5 . Distance của OSPF và ISIS được gắn cho các route .Bảng định tuyến của R1 tương tự .
Để thấy rõ hơn ý nghĩa của câu lệnh distance 130 ,ta giả sử interface giữa R5 và R4 down .
R4(config)#int s0/0
R4(config-if)#shutdown
*Mar 1 01:44:29.056: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
*Mar 1 01:44:30.058: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
kiểm tra lại bảng định tuyến của R4 :
R4#sh ip route
Gateway of last resort is not set
172.16.0.0/30 is subnetted, 1 subnets
O 172.16.2.0 [110/138] via 192.168.1.1, 00:37:45, Serial0/1
O 192.168.4.0/24 [110/74] via 192.168.1.1, 00:37:45, Serial0/1
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [130/20] via 192.168.1.1, 00:00:22, Serial0/1

C 192.168.1.0/24 is directly connected, Serial0/1
Bảng định tuyến cho thấy tất cả các route bây giờ đi đến R4 thông qua R3 .Các route đến các mạng trong miền ISIS có distance là 130 , đây là route mà R4 học được thông qua OSPF có metric là 20 vì là external route .Khi kết nối trên interface của R4 và R5 được khôi phục trở lại, các bản tin quảng bá ISIS từ R5 với distance 115 sẽ thay thế các bản tin quảng bá OSPF với distance 130 .
Tương tự ,giả sử khi kết nối giữa R5 và R1 bị down thì R1 cũng học các route trong miền ISIS thông qua OSPF với distance là 130 .
R1#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2 172.16.1.0/24 [130/20] via 172.16.2.1, 00:00:03, Serial0/0
C 172.16.2.0/30 is directly connected, Serial0/0
O 192.168.4.0/24 [110/74] via 172.16.2.1, 00:00:03, Serial0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [130/20] via 172.16.2.1, 00:00:03, Serial0/0
O 192.168.1.0/24 [110/138] via 172.16.2.1, 00:00:03, Serial0/0
Bảng định tuyến của các router còn lại khi tất cả các interface đều up là :
R2#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2 172.16.1.0/24 [110/20] via 192.168.4.1, 00:00:45, Ethernet0/0
C 172.16.2.0/30 is directly connected, Serial0/0
C 192.168.4.0/24 is directly connected, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 172.16.2.2, 00:00:45, Serial0/0
O 192.168.1.0/24 [110/74] via 192.168.4.1, 01:32:57, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
O E2 192.168.2.0 [110/20] via 172.16.2.2, 00:00:50, Serial0/0

R3#sh ip route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2 172.16.1.0/24 [110/20] via 192.168.1.2, 00:01:49, Serial0/0
O 172.16.2.0/30 [110/74] via 192.168.4.2, 01:34:01, Ethernet0/0
C 192.168.4.0/24 is directly connected, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
O E2 10.1.1.0 [110/20] via 192.168.1.2, 00:01:49, Serial0/0
C 192.168.1.0/24 is directly connected, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
O E2 192.168.2.0 [110/20] via 192.168.4.2, 00:01:54, Ethernet0/0
R5#sh ip route
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
i L2 172.16.2.0/30 [115/84] via 192.168.2.1, Serial0/0
  [115/84] via 172.16.1.1, Ethernet0/0
i L2 192.168.4.0/24 [115/84] via 192.168.2.1, Serial0/0
  [115/84] via 172.16.1.1, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback0
i L2 192.168.1.0/24 [115/84] via 192.168.2.1, Serial0/0
  [115/84] via 172.16.1.1, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
Hiện tại R5 đang thực hiện cân bằng tải với chi phí bằng nhau trên cả hai router R1 và R4 để đi đến các route trong miền OSPF .Ta xây dựng chính sách trên R5 sao cho R5 sử dụng R1 như là gateway chính để đi đến miền OSPF , các route chỉ đi qua R4 khi R1 không còn thích hợp .Tức là sử dụng R1 như là primary gateway còn R4 là backup gateway .Sử dụng câu lệnh distance để thực hiện điều này :
R5(config)#router isis
R5(config-router)#distance 100 172.16.1.1 0.0.0.0
R5# clear ip route *
R5#sh ip route
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0
i L2 172.16.2.0/30 [100/84] via 172.16.1.1, Ethernet0/0
i L2 192.168.4.0/24 [100/84] via 172.16.1.1, Ethernet0/0
10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, Loopback0
i L2 192.168.1.0/24 [100/84] via 172.16.1.1, Ethernet0/0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
à R5 xem R1 như là next-hop .
giả sử R1 không còn chạy nữa .
R5(config)#int e0/0
R5(config-if)#shutdown
R5#debug ip packet
IP packet debugging is on
03:27:42: IP: s=172.16.1.2 (local), d=172.16.1.1, len 56, unroutable
03:28:02: IP: s=172.16.1.2 (local), d=172.16.1.1, len 56, unroutable
03:28:21: IP: s=172.16.1.2 (local), d=172.16.1.1, len 56, unroutable
R5#sh ip route
172.16.0.0/30 is subnetted, 1 subnets
i L2 172.16.2.0 [115/84] via 192.168.2.1, Serial0/0
i L2 192.168.4.0/24 [115/84] via 192.168.2.1, Serial0/0
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback0
i L2 192.168.1.0/24 [115/84] via 192.168.2.1, Serial0/0
192.168.2.0/30 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, Serial0/0
à R5 bây giờ chuyển sang xem R4 như là next-hop

Phân phối lại (Redistribution)

Tác giả: Trần Văn Thành

Phân phối lại (Redistribution)

1. Định nghĩa

Thực tế rất hiếm khi chỉ có một giao thức định tuyến được cài chạy trong một tổ chức. Và trường hợp nếu công ty chạy nhiều giao thức định tuyến thì cần phải có một phương thức để chia sẻ thông tin định tuyến giữa các giao thức khác nhau đó. Quá trình đó gọi là redistribution.

Chú ý là trong trường hợp tồn tại nhiều giao thức định tuyến trên cùng một router không có nghĩa là redistribution tự xảy ra. Mà để quá trình redistribution xảy ra thì ta phải cấu hình chúng. Trường hợp có nhiều giao thức định tuyến tồn tại trên cùng một router mà không được cấu hình redistribution được gọi là ships in the night

(SIN) routing. Có nghĩa là router chỉ trao đổi thông tin định tuyến với neighbor của nó trong cùng process domain. Mặc dù SIN routing thường được để cập tới trường hợp nhiều giao thức định tuyến trên cùng một router (như là OSPF của giao thức IP và NLSP của giao thức IPX).

Một chú ý nữa là redistribution chỉ có thể xy ra giữa các giao thức định tuyến tương ứng với cùng một giao thức lớp 3 (IP, IPX hay Apple Talk). Một vài giao thức định tuyến thì tự động redistribution mà không cần phải cấu hình, tuy nhiên thường là ta phải cấu hình thì quá trình redistribution mới diễn ra.

Hình 3.1 dưới đây sẽ miêu tả chính sách redistribution của từng giao thức định tuyến.

Routing Protocol Chính sách redistribution (Redistribution Policy)
Static Phải cấu hình bằng tay vào các giao thức định tuyến khác.
Connected Trừ phi có câu lệnh Network cho quá trình định tuyến, phải yêu cầu cấu hình redistribution bằng tay vào các giao thức định tuyến khác.

RIP Yêu cầu cấu hình redistribution bằng tay.

IGRP Nó sẽ tự động diễn ra giữa IGRP và EIGRP nếu giá trị autonomous system của chúng giống nhau. Trường hợp còn lại yêu cầu phải cấu hình bằng tay.

EIGRP Nó sẽ tự động diễn ra giữa IGRP và EIGRP nếu giá trị autonomous system của chúng giống nhau. EIGRP cho giao thức Apple Talk sẽ tự động redistribution giữa EIGRP và RTMP. EIGRP cho IPX sẽ tự động redistribution giữa EIGRP và IPX RIP/SAP. Trường hợp còn lại yêu cầu phải cấu hình bằng tay. Trong các phiên bản sau, NLSP có thể redistribution bằng tay.

OSPF Yêu cầu phải cấu hình redistribution giữa các OSPF process khác nhau và với giao thức định tuyến khác

IS-IS Yêu cầu phải cấu hình bằng tay giữa các giao thức định tuyến khác nhau.

BGP Yêu cầu phải cấu hình bằng tay giữa các giao thức định tuyến khác nhau.

Trong hình 3.2, trong routing table của router B có mục nhập cho những route từ RIP và OSPF domain. Không có mục nhập cho route đến từ EIGRP domain vì chỉ có một network nối trực tiếp vào router. Bạn có thể thấy rằng RIP update được gửi ra ngoài interface không bao gồm network từ OSPF domain. Hơn nữa, router C chỉ

có một kết nối trực tiếp trong routimg table. Lý do là vì mặc dù router C được cấu hình EIGRP nhưng router C là một stub router. Khi một interface khác được cấu hình địa chỉ và phần còn lại của EIGRP network kết nối vào router C, mạng sẽ được quảng bá với EIGRP route, nó sẽ phân bổ tới router B. Nếu redistribution được thực hiện thì toàn bộ mạng sẽ sẵn sàng cho mọi router.

Các trường hợp dẫn tới tồn tại nhiều giao thức định tuyến trong cùng một tổ chức:

Tổ chức chuyển từ một giao thức này sang một giao thức khác bởi vì họ cần một giao thức định tuyến phức tạp hơn.

Do yếu tố lịch sử, tổ chức có rất nhiều mạng con. Công ty cần được thiết kế để chuyển sang một giao thức duy nhất trong tương lai.

Một vài doanh nghiệp sử dụng giải pháp host-based yêu cầu nhiều giao thức định tuyến. Ví dụ, ví dụ một UNIX host sử dụng RIP để khám phá gateway.

Sau khi 2 công ty được hợp nhất.

Về mặt chính trị, có những tư tưởng khác nhau giữa các nhà quản trị mạng khác nhau.

Trong một môi trường rất lớn, những vùng khác nhau có những yêu cầu khác nhau, do đó một giải pháp đơn lẻ là không hiệu quả. Ví dụ: một mạng đa quốc gia, thì EIGRP là giao thức định tuyến được sử dụng ở access layer và distribution layer nhưng BGP là giao thức định tuyến được dùng kết nối với core layer.

2. Các vấn đề phát sinh và giải pháp khi thực hiện redistribution.

Khả năng của IP routing protocol thay đổi rộng rãi. Đặc trưng của các giao thức định tuyến mà hầu hết được mang trong redistribution là sự khác nhau trong metric và administrative distance, và khả năng classful hay classless của chúng. Sự thất bại trong sự đem lại của sự xem xét cẩn thận sự khác nhau khi redistribution có thể dẫn tới các vấn đề sau: sự thất bại trong sự trao đổi một vài hoặc tất cả các tuyến (route), routing loop và black hole.

a/ Metric

Các router của hình 3.1 được redistribution static route vào OSPF, chúng sẽ quảng bá những tuyến (route) tới các OSPF-speaker router khác. Static route không có metric đi kèm với chúng, nhưng mỗi OSPF route (tuyến OSPF) phải có một giá trị cost đi kèm. Một ví dụ khác liên quan đến metric nữa đó là redistribution của RIP route (tuyến RIP) vào IGRP. Metric của RIP là hop count, trong khi IGRP sử dụng bandwidth và delay. Metric của IGRP là một số 24 bit trong khi của RIP giá trị giới hạn là 15. Trong cả 2 trường hợp, yêu cầu đối với giao thức định tuyến tham gia redistribution là đối với những tuyến (route) được redistribution vào domain của nó thì nó phải kết hợp được metric của nó với metric của

những tuyến đó.

Do đó cần có một giải pháp đó là khi router thực hiện redistribution phải gán một giá trị metric cho những tuyến tham gia redistribution.

Error!

Trường hợp như Hình 3.2 đây là EIGRP được redistribution vào OSPF, và OSPF được redistribution vào EIGRP. OSPF không hiểu metric tổ hợp của EIGRP và EIGRP cũng không hiểu cost của OSPF. Kết quả là, các phần của quá trình redistribution là các router phải được giao một cost cho mỗi EIGRP route trước khi tuyến đó được quảng bá sang OSPF domain. Tương tự như vậy, router cũng phải gán một cặp giá trị sau: bandwidth, delay, reliability, load và MTU cho mỗi OSPF route trước khi nó được quảng bá sang EIGRP domain. Nếu quá trình gán metric là không đúng thì quá trình redistribution sẽ thất bại.

b. Khoảng cách quản lý (Administrative Distance)
Tính đa dạng của metric còn gây ra vấn đề sau: nếu một router chạy nhiều hơn một giao thức định tuyến và học một tuyến (route) tới cùng một đích từ mỗi giao thức tương ứng, thì tuyến nào sẽ được chọn? Mỗi giao thức định tuyến sử dụng metric của nó để xác định ra route tốt nhất theo cách của mình. So sánh tuyến (route) với metric khác nhau chẳng hạn: hop count và cost, chẳng khác nào so sánh táo và cam.

Có một giải pháp để giải quyết vấn đề này đó là administrative distance. Đúng như metric được gán cho mỗi tuyến (route) đến mức độ ưu tiên của mỗi route có thể được xác định, administrative distance được gán cho tuyến nguồn (route source) đến mức độ ưu tiên hơn của tuyến nguồn được xác định. Như trong phần hai đã giới thiệu administrative distance nó như là thước đo về độ tin cậy. Giá trị administrative distance càng nhỏ thì độ tin cậy của thông tin định tuyến trao đổi bởi giao thức tương ứng càng lớn.
Ví dụ, giả sử một router chạy 2 giao thức định tuyến là RIP và EIGRP. Khi router học một tuyến tới mạng 192.168.5.0 bằng cả 2 giao thức định tuyến thì nó sẽ nhận được thông tin về tuyến tới mạng 192.168.5.0 từ cả RIP

neighbor và EIGRP neighbor. Bởi vì EIGRP sử dụng metric tổ hợp cho nên những thông tin định tuyến học được từ EIGRP sẽ chính xác hơn là thông tin định tuyến học được từ RIP. Do đó, EIGRP tin cậy hơn RIP.

Bảng 3.3 cho biết các giá trị administrative distance mặc định của các giao thức định tuyến khác nhau. EIGRP có administrative distance là 90 trong khi RIP là 120. Điều đó chứng tỏ EIGRP tin cậy hơn RIP.

Error!

c. Redistributing từ Classless vào Classful Protocols

Sự suy xét thận trọng đã được nói rõ được nói rõ khi thực hiện redistribution từ một classless routing process domain vào một classful domain. Để hiểu được tại sao lại như vậy, đầu tiên cần hiểu một classful routing protocol phản ứng lại như thế nào với sự thay đổi của subnet. Như đã biết RIP là một classful routing protocol cho nên nó không gửi mask trong thông tin định tuyến. Đối với các route mà một classful router nhận được sẽ ra vào một trong 2 khả năng sau:

Router sẽ có một hay nhiều hơn interface gắn với mạng chính (major network).

Router sẽ không có interface gắn vào mạng chính.

Trong trường hợp thứ nhất, router phải sử dụng mặt nạ định hình của chính mình cho mạng chính để xác định một cách chính xác subnet của địa chỉ đích trong gói packet. Trong trường hợp thứ 2, chỉ địa chỉ của mạng chính mà nó có thể bao gồm trong thông tin quảng bá bởi vì nó không có cách nào để xác định subet mask để sử dụng.

Trong hình 3.6, subnet của OSPF domain biến đổi và Paige thực hiện redistribution OSPF-route vào IGRP domain.

Error!

Như trong hình 3.7, Paige biết về tất cả các subnet của cả OSPF domain và IGRP domain. Và bởi vì OSPF là một classless routing protocol, router biết mask nào được gắn kết với mỗi subnet mà kết nối trực tiếp với Gibson. Tiến trình IGRP (IGRP process) của Paige là sử dụng 24-bit mask; do đó 172.20.113.192/26 và 172.20.114.48/28 là không tương thích và không được quảng bá như trong hình 3.8. Chú ý rằng IGRP quảng bá 172.20.112.0/24 và 172.20.115.0/24. Kết quả là chỉ subnet trong OSPF domain mà Leonard biết là chúng có cùng chung subnet là 24-bit như hình 3.9.

Error!

Error!

Error!

Giải pháp thứ 1: cho việc redistribution giữa classful routing protocol và classless routing protocol là sử dụng định tuyến tĩnh để phân phối các route vào trong classful routing domain.

Giải pháp thư 2: thực hiện route summary để nhóm các subnet con thành một subnet to hơn mà classful routing domain hiểu được.

3. Các tình huống dẫn đến routing loop khi thực hiện redistribution

Mặc dù administrative distance đã giải quyết được vấn đề sự lộn xộn của sự thay đổi khác nhau của metric hay nói cách khác giải quyết được vấn đề nguồn gốc của thông tin định tuyến, nhưng chúng vẫn có thể gây lên một số vấn đề cho redistribution. Như ví dụ trong hình 3.10, cả Gehrig và Ruth

được redistribution RIP-route vào IGRP domain. Gehrig học về mạng 172.168.1.0 qua RIP và quảng bá network đó vào IGRP domain. Kết quả là Ruth học được về mạng 192.168.1.0 không chỉ từ Combs qua RIP-route mà còn từ Meusel qua IGRP route.

Error!

Hình 3.11 cho thấy routing table của Ruth. Chú ý rằng tuyến đường tới mạng 192.168.1.0 là một IGRP route. Ruth đã chọn IGRP route vì IGRP có administrative distance nhỏ hơn RIP. Ruth sẽ gửi dữ liệu tới mạng 192.168.1.0 với lộ trình qua Meusel thay vì phải gửi trực tiếp tới Combs.

Error!

Mặc dù Split horizon chặn routing loop trên internet như hình 3.10. C Gehrig và Ruth lúc đầu đều quảng bá mạng 192.168.1.0 vào IGRP domain, và cả 4 router đều hội tụ với chỉ có một đường đến đến mạng đó. Tuy nhiên, sự hội tụ là không thể đoán trước được. Cụ thể như trong trường hợp sau. C hai router Lazzeri và Meusel khởi động lại. Sau khi khởi động, bảng routing talble của Ruth cho biết tuyến đường đến mạng 12.168.1.0 sẽ sử dụng Combs làm next-hop (như hình 3.12).

Error!

Trạng thái hội tụ của mạng sau khi khởi động lại không chỉ không đoán trước được mà còn rất chậm. Như hình 3.13 cho biết routing table của Gehrig sau khong 3 phút sau khi khởi động lại. Nó sử dụng router Lazzeri là next-hop của tuyến đường tới mạng 192.168.1.0 nhưng khi ping tới địa chỉ trên mạng đó thì lại bị fail. Hình 3.14 là routing table của Lazzeri: Lazzeri

sử dụng router Gehrig là next-hop của tuyến tới mạng 192.168.1.0. Kết quả là tồn tại routing loop.

Error!

Sau đây là trình tự của các sự kiện dẫn đến routing loop:

1. Trong khi router Lazzeri và Meusel khởi động lại, cả Gehrig và Ruth đều có mục nhập trong routing table của tuyến đường tới mạng 192.168.1.0 với thông tin next-hop là router Combs.

2. Ngay sau khi Lazzeri và Meusel trở thành active, cả Gehrig và Ruth đều gửi thông tin update mà có chứa thông tin đến mạng 192.168.1.0. Giả sử trường hợp này, Ruth gửi thông tin update sớm hơn một chút so với Gahrig.

3. Meusel, nhận thông tin update của Ruth, và coi Ruth như là next-hop và gửi thông tin update tới Lazzeri.

4. Lazzeri, nhận thông tin update của Meusel, và coi Meusel như là next-hop.

5. Lazzeri và Gehrig đều gửi thông tin update tới nhau trong cùng một thời gian. Lazzeri coi Gehrig là next-hop của tuyến đường tới mạng 192.168.1.0 bởi vì theo tính chất của distance vector routing protocol nó sẽ coi router quảng bá tuyến đường đó tới nó sẽ là next-hop. Còn Gehrig coi Lazzeri là next-hop của tuyến đường cùng tới mạng 1923.168.1.0 bởi vì thông tin định tuyến của IGRP router quảng bá có độ tin cậy lớn là thông tin định tuyến do router RIP quảng bá (thực hiện điều này dựa vào administrative distance). Kết quả là loop xuất hiện.

Split horizon và thời gian không hợp lệ (invalid timer) rốt cuộc sẽ sắp xếp lại các thông tin định tuyến sai đó. Lazzeri quảng bá tuyến tới mạng tới Meusel, nhưng Meusel tiếp tục sử dụng metric tôt hơn cho tuyến đó qua Ruth. Và từ khi Ruth được coi là next-hop router, split horizin có tác dụng cho tuyến tới mạng 192.168.1.0 tại interface S1 của Meusel. Meusel cũng

gửi quảng bá tuyến tới mạng 192.168.1.0 tới Lazzeri, nhưng Lazzeri vẫn coi Gehrig là next-hop cho tuyến tới mạng 192.168.1.0 với metric tốt hơn. Lazzeri và Gehrig coi lẫn nhau là next hop cho tuyến tới mạng 192.168.1.0, cho nên chúng sẽ không quảng bá tuyến tới mạng đó cho nhau. Sau khoảng thời gian invalid timer hết hạn thì routing table của 2 router đó như hình 3.15.

Error!

Khi invalid timer của Lazzer hết hạn, tuyến tới mạng 192.168.1.0 sẽ khởi tạo giá trị holddown cho tuyến đó. Mặc dù Meusel được quảng bá một tuyến tới mạng đó, Lazzeri không thể đồng ý nó cho đến khi holddown timer hết hạn. Hình 3.16 cho biết rằng Lazzeri cuối cùng cũng đồng ý tuyến được qung bá từ Meusel và hình 3.17 cho biết Gehrig đã đến được mạng 192.168.1.0 thành công qua Lazzeri. Quá trình này mất khoảng hơn 9 phút cho 2 router hội tụ và những tuyến mà nó sử dụng không phải là tuyến tối ưu.

Error!

Error!

Administrative distances có thể gây lên vấn đề tệ hơn cả lựa chọn đường đi sai (sub-optimal route) như các tình huống không dự đoán trước được và thời gian hội tụ chậm như ví dụ trước đã phân tích. Như hình 3.18 các router trong IGRP domain được cấu hình trong môI trường Frame Relay. ở trạng thái mặc định split horizon được tắt trên các interface Frame Relay. Kết quả là routing loop vĩnh cửu xảy ra giữa Lazzeri và Gehrig và giữa Meusel và Ruth. Kết luận cuối cùng là mạng 192.168.1.0 không thể đến được trong IGRP domain..

REDISTRIBUTION VÀ POLICY BASED ROUTING

Tác giả: Đặng Quang Minh

REDISTRIBUTION VÀ POLICY BASED ROUTING

Nếu một hệ thống mạng chạy nhiều hơn một giao thức trong một công ty, người quản trị cần một vài phương thức để gửi các routes của một giao thức này vào một giao thức khác. Quá trình đó gọi là *redistribution.*

Quá trình redistribution được dùng khi một router nhận thông tin về một network ở xa thông qua các nguồn khác nhau. Mặc dù tất cả các network được đưa vào bảng định tuyến và các quyết định định tuyến được thực hiện trên bảng này, một giao thức chỉ truyền những network mà nó học từ chính bản thân nó. Nếu không có việc chia sẽ thông tin mạng giữa các quá trình định tuyến, người ta gọi đó là *ships in the nights* (SIN).

Redistribution thường cần thiết trong một network như một giải pháp tạm thời. Tuy nhiên, giải pháp này không phải là nhanh chóng và dễ dàng. Mặc dùng cách dùng route-redistribution là một giải pháp cứu cánh trong nhiều tình huống, nó khá phức tạp. Khi một giao thức chẳng hạn như EIGRP có routes được phân phối vào nó như một quá trình định tuyến, nó giả sử rằng tất cả các routes này từ các AS khác và là routes ngoại (external routes). Điều này ảnh hưởng đến quá trình chọn lựa đường đi vì EIGRP thường ưu tiên cho routes nội.

Trong hình vẽ dưới đây, bảng định tuyến của routerB các các entry từ RIP và OSPF, không có entry cho EIGRP bởi vì đây chỉ là một mạng riêng lẽ nối trực tiếp vào router. Hơn nữa, routerc chỉ có các routes kết nối trực tiếp trong bảng bảng định tuyến. Đây là vì, mặc dùng EIGRP đã được cấu hình, routerC vẫn chỉ là một stub router. Khi có những interface khác được cấu hình và toàn bộ các mạng EIGRP còn lại kết nốI vào routerC, các lớp mạng này sẽ được quảng bá.

Quá trình redistribution chỉ diễn ra ở các giao thức lớp 3. Vì vậy các giao thức OSPF, RIP, IGRP và EIGRP có thể phân phối các routing update giữa chính các giao thức này. Tuy nhiên sẽ không có quá trình redistribution giữa AppleTalk và IPX.

Bảng 6-1: Các chính sách redistribution

GIAO THứC ĐịNH TUYếN	CHÍNH SÁCH REDISTRIBUTION

Static	Phải cấu hình redistribution bằng tay vào các giao thức khác
Connected	Phải cấu hình redistribution bằng tay vào các giao thức khác
RIP	Cấu hình redistribution bằng tay
IGRP	Tự động redistribution giữa IGRP và EIGRP nếu giá trị AS là giống nhau. nếu giá trị AS là khác nhau, phải cấu hình redistribution bằng tay.
EIGRP	Sẽ tự động redistribution giữa IGRP và EIGRP nếu giá trị AS là giống nhau. nếu giá trị AS này là khác nhau, ta phải cấu hình redistribution bằng tay. EIGRP cho AppleTalk sẽ tự động redistribution giữa EIGRP và RTMP. EIGRP cho IPX sẽ tự động redistribute giữa EIGRP và IPX RIP/SAP. Trong các phiên bản sau, NLSP có thể redistribution bằng tay.
OSPF	Phải cấu hình redistribution bằng tay giữa các OSPF process
IS-IS	Phải cấu hình bằng tay giữa các giao thức khác nhau
BGP	Phải cấu hình băng tay giữa các giao thức khác nhau

Hình 6-1: Hình vẽ minh hoạ chính sách redistribution

Error!

Các nguyên nhân làm cho nhiều giao thức định tuyến tồn tại bên trong một tổ chức là:

- Hệ thống đang chuyển từ một giao thức này sang một giao thức khác bởi vì cần cài đặt một giao thức mới phức tạp hơn.
- Do lịch sử, hệ thống mạng gồm nhiều mạng nhỏ hơn. Công ty cần phải chuyển sang một giao thức duy nhất trong tương lai.

- Một vài phòng ban trong công ty có dùng các giải pháp host-based, ví dụ như dùng RIP trên máy Unix.
- Sau khi hay công ty sát nhập với nhau.

Hình 6-2: Quá trình phân phối route giữa các giao thức khác nhau

Error!

Khi cấu hình mạng mà một bên dùng routing là static, bên kia là dynamic, hoặc một bên là RIP, một bên dùng IGRP thì chúng ta phải dùng các lệnh redistribute ở các Router biên. Lệnh redistribute được dùng để chia sẽ thông tin định tuyến giữa các miền routing khác nhau. Một miền định tuyến (routing domain) có thể là RIP; bên còn lại có thể là IGRP; hoặc một miền là static và một bên còn lại là ospf....

- Những nguyên nhân mang tích chính trị, những quản trị mạng khác nhau có các tư tưởng khác nhau
- Trong một môi trường rất là lớn, trong đó các miền khác nhau có các yêu cầu khác nhau. Điều này làm cho một giải pháp đơn lẻ là không hiệu quả.

Routing Metrics và Redistribution

Có nhiều giao thức định tuyến cho IP. Mỗi giao thức định tuyến dùng các metric khác nhau. Nếu các giao thức khác nhau muốn chia sẽ thông tin thông qua quá trình redistribution, ta phải cấu hình để chuyển đổi metric. Các vấn đề sẽ nảy sinh khi các metric được redistribute mà không dùng thêm các lệnh cấu hình. Các metric không có thông tin gì để tham khảo trong giao thức mới. Ví dụ RIP sẽ không hiểu giá trị metric là 786 vì RIP mong đợi giá trị metric nằm trong khoảng từ 0-15. Khi chấp nhận những network mới, giao thức định tuyến phải có một điểm bắt đầu, gọi là seed metric. Giá trị seed metric sẽ tăng từ vị trí router đó khi các mạng được truyền trong routing domain mới.

Bảng 6-2: Các giá trị mặc định của metric khi được redistribute

IP	DEFAULT SEED	HÀNH ĐộNG

ROUTING	METRIC	
RIP	Gía trị là không xác định	Route không được đưa vào bảng định tuyến
IGRP	Không xác định	Route không được đưa vào bảng định tuyến
EIGRP	Không xác định	Route không được đưa vào bảng định tuyến
ISIS	0	Route được đưa vào bảng định tuyến
OSPF	20 (loại 2), nhưng các route từ BGP có metric là 1	Route được đưa vào bảng định tuyến
BGP	MED sẽ lấy giá trị metric từ các IGP	Route được đưa vào bảng định tuyến

Giá trị metric là phương thức chủ yếu của quá trình chọn lựa bên trong một giao thức định tuyến. Vì vậy cần thiết phải định nghĩa một seed metric cho những network được chấp nhận từ những giao thức định tuyến khác.

Chọn lựa đường đi giữa các giao thức định tuyến

Quá trình tìm đường bên trong một giao thức định tuyến đã được khảo sát trong các chương trước. Phần này sẽ khảo sát quá trình chọn lựa đường đi giữa các giao thức định tuyến khi có nhiều hơn một giao thức định tuyến chạy trên mạng.
Nếu một giao thức có nhiều đường đi đến cùng một mạng ở xa, quá trình định tuyến phải quyết định đưa đường đi nào vào bảng route. Vì các metric của các giao thức là khác nhau, quá trình chọn lựa đường đi dựa trên metric sẽ không được dùng. Thay vào đó, một cách thức khác được định nghĩa để giải quyết vấn đề, đó là giá trị AD. Sự khác nhau giữa hai quá trình chọn lựa là đơn giản: giá trị AD sẽ xác định giữa các giao thức định tuyến. Giá trị AD và metric giải quyết hầu hết vấn đề trong quá trình redistribution. Mọi việc bắt đầu phát sinh khi phải phân phối routes giữa các giao thức định tuyến và khi quá trình routing bắt đầu gặp khó khăn trong

khâu xác định về nguồn gốc của thông tin định tuyến. Khi đó, các vấn đề về định tuyến không tối ưu và routing loop có thể xảy ra.

Vì vậy cần phải xem xét các luật sau khi thực hiện redistribution giữa các giao thức:

- Nếu có nhiều hơn một giao thức định tuyến đang chạy trên một router, những routes nào có giá trị AD tốt nhất sẽ được đưa vào bảng route.
- Để được redistributed , route đó phải có trong bảng định tuyến. Ngoài ra, route đó phải được học từ giao thức định tuyến đang được redistribute. Như vậy, nếu RIP đang được redistribute vào EIGRP , bảng định tuyến phải có một entry cho mạng RIP.
- Khi một route được redistribute, nó sẽ thừa hưởng giá trị AD mặc định của giao thức mới.

Rõ ràng là quá trình redistribution không phải là một thiết kế mang tính tối ưu. Một thiết kế càng đơn giản và dễ dàng, mạng sẽ dễ quản trị và hội tụ nhanh. Vì vậy, một sơ đồ địa chỉ IP được thiết kế để cho phép mạng phát triển, kết hợp với một giao thức định tuyến IP sẽ dẫn đến một hệ thống mạng nhanh, mạnh và tin cậy.

Các vấn đề có thể phát sinh khi thực hiện redistribution có thể rất khó để khắc phục bởi vì vấn đề xuất hiện có thể nằm ở nơi khác. Các vấn đề có thể phát sinh bao gồm:

- Các quyết định định tuyến là sai, kém hiệu quả vì sự khác biệt về metric. Việc chọn lựa đường đi sai còn được gọi là sub-optimal path.
- Khi một routing loop xảy ra, data sẽ được chuyển bất tận mà không bao giờ đến đích. Điều này là do vấn đề route-feedback trong đó một router gửi thông tin update ra khỏi AS lại nhận được route đó gửi ngược lại vào AS.
- Khoảng thời gian hội tụ của mạng sẽ tăng bởi vì sự khác nhau của các công nghệ. Nếu các giao thức định tuyến hội tụ ở các khoảng thời gian khác nhau, điều này có thể dẫn đến vấn đề timeouts và mất các

network.

- Quá trình ra quyết định và thông tin được gửi bên trong một giao thức có thể không tương thích với nhau và không dễ dàng trao đổi. Điều này sẽ dẫn đến lỗi và các cấu hình phức tạp.

Tránh vòng lặp khi redistribution

Routing loop xảy ra khi một giao thức định tuyến nhận được các mạng của chính nó. Các giao thức định tuyến có thể thất một mạng trên một đường đi tốt mặc dù đường đi này chỉ về chiều ngược lại vào một giao thức định tuyến khác.

Hình 6-3: Tránh vòng lặp khi redistribution

Error!

Vấn đề này được giải quyết bằng các cấu hình như sau:

- Thay đổi metric.
- Thay đổi giá trị AD.
- Dùng default-route.
- Dùng passive interfaces với định tuyến tĩnh.
- Dùng distribute-list.

Để quản lý sự phức tạp của các hệ thống mạng này và giảm thiểu sự phức tạp của routing-loop, người quản trị nên giới hạn một vài thông tin được gửi trên các domain. Công việc này được thực hiện thông qua cách dùng access-list.

Hình 6-4: Thực hiện redistribution giữa RIP và EIGRP

Error!

Giả sử rằng ở thời điểm routerA đang chạy RIP và quảng bá mạng 190.10.10.0 đến các hai routerB và E. Khi routerB nhận cập nhật từ RIP, nó sẽ redistribute network 190.10.10.0 vào OSPF và quảng bá route đó đến routerC. RouterC sẽ quảng bá route đó đến D. Cuối cùng routerE nhận một OSPF update từ D, báo rằng network 190.10.10.0 thông qua đường đi D,C,B,A. Tuy nhiên, routerE có một đường đi trực tiếp đến A thông qua RIP. Đây mới là đường đi được đáng được ưu tiên hơn. Trong tình huống này, giá trị AD có tác dụng. Bởi vì OSPF có giá trị AD là 110 và RIP có giá trị AD là 120, đường đi được đặt trong bảng định tuyến là đường đi

được quảng bá bởI OSPF thông qua D,C, B và A. Trong tình huống này, ta nên cấu hình bằng tay giá trị AD trên routerB và E.
Nếu EIGRP chạy trên các router B,C,D và E sẽ không có vấn đề gì. Khi RIP redistribute vào EIGRP trên RouterB và update được truyền đến routerE, bảng định tuyến sẽ chọn lựa đường đi đến 190.10.10.0 thông qua routerA. Lý do là khi network 190.10.10.0 được phân phối vào EIGRP, nó sẽ được đánh dấu như external route. Như vậy, route đó sẽ có giá trị AD là 170 và sẽ bị bỏ qua nếu so với giá trị AD=120 của RIP. Bảng định tuyến chứa các đường đi qua ngõ RIP về network 190.10.10.0. Khi EIGRP redistribute lại vào RIP, bảng định tuyến không có route của EIGRP nào đến network 190.10.10.0 và không thể redistribute route này ngược vào RIP. Về phương diện lý thuyết, một routing-loop đã được tránh. Tuy nhiên thực tế không phải là như vậy. Bạn phải tránh quá trình redistribution hai chiều. Bạn cũng nên đặt các filter khi thực hiện redistribution để ngăn ngừa routing-loop.

Cú pháp tổng quát của lệnh redistribute như sau:

Router(config-router)#

Cú pháp:

redistribute protocol [process-id] [metric metric-value] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [weight weight] [subnets]

Để xóa lệnh này, bạn có thể dùng:

no redistribute protocol [process-id] [metric metric-value] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [weight weight] [subnets]

Mô tả cú pháp:

protocol: Giao thức định tuyến đang được "đẩy vào"/đang được phân phối vào một giao thức định tuyến khác.

Ví dụ 1: đưa rip routes vào ospf:

```
Router(config)#router ospf 1
Router(config-router)#redistribute rip
```

Các từ khóa có thể dùng với lệnh redistribute là: bgp, egp, eigrp, igrp, iso-igrp, isis, odr, ospf, mobile, static, connected, và rip. Từ khóa static được dùng với tuyến đường tĩnhs. Từ khóa connected được dùng để chỉ ra những route được kết nối trực tiếp. Đối với những giao thức định tuyến như ospf, các route được phân phối vào sẽ là loại ngoại lai (external).

process-id: Mục chọn này được dùng cho các giao thức định tuyến có dùng AS number. Giá trị này sẽ chỉ ra process-id hoặc routing process. Đối với RIP thì không cần dùng.

metric *metric-value*
Metric được dùng cho những route được phân phối vào. Nếu giá trị này không được chỉ ra, và nếu không có giá trị mặc định nào được chỉ ra trong lệnh default-metric, giá trị mặc định được dùng là 0 (chính xác hơn là tùy thuộc vào giao thức định tuyến). Bạn nên dùng một giá trị nhất quán cho giá trị metric này.

Lệnh trên sẽ phân phối các igrp route vào ospf domain. các routes ngoại lai sẽ có metric là 100.

```
Router(config)#router ospf 109
Router(config-router)#redistribute igrp 108 metric 100 subnets
Router(config-router)#redistribute rip metric 200 subnets
```

Giá trị metric được chỉ ra trong redistribute command sẽ có độ ưu tiên cao hơn giá trị metric được chỉ ra bởi lệnh default-metric. Khi phân phối một giao thức định tuyến vào một giao thức định tuyến khác, bạn cần phải gán các metric phù hợp cho các routes mới này. Các giao thức định tuyến khác nhau dùng các metric rất khác nhau. Các giá trị thích hợp phụ thuộc vào giao thức định tuyến trong từng trường hợp cụ thể. Để tránh hiện tượng route lại nhiều lần, ta có thể dùng các cơ chế route-filtering như distribute-list, route-map, distance, prefix-list. Trong thực tế thì

có một số trường hợp thường dùng redistribution là giữa các nhà cung cấp dịch vụ Internet. Các ISP dùng IGP cho mạng của mình và dùng BGP để kết nối với các ISP khác. Thường thì các internal routers sẽ có default gateway là các bgp routers và trên bgp routers sẽ phân phối các prefixes được học từ IGP để đẩy ra các bgp routers của ISP khác. Một trường hợp khác có thể cần đến route redistribution đó là việc sát nhập các công ty. Công ty A (đang dùng EIGRP) mua lại công ty B (đang dùng OSPF), khi kết nối mạng lại với nhau mà chưa kịp thay đổi toàn bộ hệ thống mạng thì họ sẽ dùng redistribution trên một router nào đó, còn gọi là mutual redistribution.

Tránh vấn đề định tuyến không tối ưu khi thực hiện redistribution

Như đã đề cập trong các mục trước, vấn đề suboptimal thỉng thoảng sẽ bị tạo ra bởi các quá trình redistribution. Ví dụ giá trị AD sẽ chọn lựa đường đi kém tối ưu khi một đường đi kết nối trực tiếp lại được dùng như một đường đi dự phòng.
Hãy tuân theo các nguyên tắc sau đây khi thiết kế mạng để tránh routing-loop:

- Có một kiến thức tốt về sơ đồ mạng, Routing domain, dòng traffic
- Không cho các giao thức chạy chất chồng lên nhau. Mọi việc sẽ dễ dàng hơn nếu các giao thức khác nhau có thể được phân chia rõ ràng vào các domain riêng lẽ trong đó router hoạt động như các router ở ranh giới. Đây còn được gọi là core và edge protocol.
- Chỉ ra các router ở ranh giới mà trên đó phải cấu hình redistribution
- Xác định giao thức nào là core, giao thức nào là edge
- Xác định chiều của quá trình redistribution, trong đó giao thức nào sẽ được redistribute. Lấy ví dụ, RIP sẽ redistribute vào EIGRP như EIGRP sẽ không redistribute vào RIP. Điều này nhằm tránh các mạng sẽ bị phản hồi ngược lại vào domain ban đầu. Hãy dùng default-route hoặc quá trình redistribution một chiều nếu cần thiết.
- Nếu quá trình redistribution hai chiều là không thể tránh khỏi, hãy dùng cơ chế sau: cấu hình metric bằng tay, cấu hình giá trị AD bằng tay, dùng distribution access-list.

Tránh các vấn đề với hội tụ mạng khi redistribution

Để duy trì tính nhất quán giữa các giao thức định tuyến khác nhau, ta phải xem xét nhiều công nghệ. Một mối quan tâm lớn là quá trình tính toán của bảng định tuyến và khoảng thời gian hội tụ trong bao lâu. EIGRP có tốc độ hội tụ khá nhanh trong khi RIP thì hội tu chậm hơn. Việc chia sẽ thông tin giữa hai công nghệ có thể gây ra vài vấn đề. Ví dụ mạng sẽ hội tụ ở tốc độ của giao thức chậm hơn. Ở một vài

thời điểm, điều này sẽ tạo ra timeout và khả năng routing loops. Điều chỉnh timers sẽ giải quyết vấn đề nhưng bất cứ một giao thức nào cũng phải được cấu hình với một kiến thức vững chắc về toàn bộ hệ thống mạng. Các thông số thời gian timers thường yêu cầu là cấu hình giống nhau trong tất cả các routers sao cho timer có cùng giá trị.

Kiểm soát routing update khi redistribution

Kiểm soát routing update thì hữu ích trong nhiều trường hợp. Các lý do để kiểm soát các routing update gồm:

- Che dấu một vài network nào đó ra khỏi phần còn lại.
- Ngăn ngừa routing loop.
- Kiểm soát phí tốn của traffic trên mạng, cho phép mạng có khả năng mở rộng.
- Vì các lý do bảo mật

Các phương thức khác nhau để kiểm soát bao gồm các phương thức sau:

- Dùng passive interface.
- Dùng định tuyến tĩnhs.
- Dùng default routes.
- Dùng null interface.
- Dùng distribute-lists.
- Dùng route-map.

Cổng giao tiếp bị động trong quá trình định tuyến (Passive Interfaces)

Một cổng bị động sẽ không tham gia vào quá trình định tuyến. Trong RIP và IGRP, quá trình này sẽ lắng nghe các cập nhật mà không gửi các thông tin cập nhật định tuyến. Trong OSPF và EIGRP, các quá trình này sẽ không lắng nghe hay gửi các cập nhật vì các router không gửi đi các gói hello và vì vậy các quan hệ láng giềng giữa các router không thể hình thành. Các cổng giao tiếp của router tham gia vào các quá trình định tuyến được kiểm soát bởi cấu hình. Trong khi cấu hình, quá trình định tuyến sẽ dùng lệnh network đề chỉ ra cổng giao tiếp nào của router tham gia vào quá trình định tuyến. Cấu hình passive-interface sẽ ngăn ngừa các cập nhật đi vào các miền định tuyến khác và có thể ngăn ngừa routing loop.

Định tuyến tĩnh

Định tuyến tĩnh là một route được cấu hình bằng tay. Định tuyến tĩnh có độ ưu tiên cao hơn các routes được học thông qua một giao thức động vì nó có giá trị AD thấp hơn. Nếu không có giao thức định tuyến nào được cấu hình, định tuyến tĩnh có thể được cấu hình. Cách dùng định tuyến tĩnh không phù hợp với các hệ thống mạng lớn trong thực tế bởi vì bảng định tuyến sẽ không cập nhật các thay đổi một cách tự động. Trong những môi trường nhỏ hơn hoặc những stub-network, cách dùng định tuyến tĩnh là một giải pháp hiệu quả. Đặc biệt trong tình huống có nhiều giao thức được cấu hình trên router, thay vì redistribution toàn bộ bảng định tuyến giữa các giao thức, định tuyến tĩnh sẽ được định nghĩa và redistribution. Điều này đặc biệt hữu ích nếu bạn cần cung cấp nhiều thông tin hơn là dùng default-route. Cách dùng định tuyến tĩnh trong redistribution là một cách dùng tiêu biểu.

Các lý do để dùng định tuyến tĩnh được tóm tắt như sau:

- Ngăn ngừa việc phải chạy một giao thức định tuyến động chạy trên một mạng, giảm chi phí mạng về zero.
- Nếu có hai AS không cần trao đổi toàn bộ bảng định tuyến mà chỉ cần biết về một vài routes
- Không có một giao thức định tuyến động nào được dùng, ví dụ mạng stub
- Để thay đổi giá trị netmask của mạng. Ví dụ như trong BGP, ta có thể định nghĩa một supernet và redistribution route vào BGP process. Tác vụ

này cũng được dùng khi redistribute một giao thức hỗ trợ cho VLSM vào một giao thức không hỗ trợ VLSM.

Default Routes

Một default route được dùng nếu không có một entry nào trong bảng định tuyến cho một mạng đích. Nếu quá trình tìm kiếm bảng định tuyến không tìm thấy entry nào trong bảng routing cho mạng đích và default-route không được cấu hình, gói dữ liệu về địa chỉ mạng đó sẽ bị loại bỏ. Nếu quá trình định tuyến bị từ chối quyền gửi các cập nhật, các router downstream sẽ có một kiến thức giới hạn về mạng do không nhận đủ thông tin. Để giải quyết vấn đề này, default route sẽ được dùng. Các default route sẽ giảm phí tổn cho hệ thống và đơn giản hóa công tác quản trị, đặc biệt là có thể xóa routing loop khi được dùng thay cho quá trình redistribution. Một giao thức định tuyến có thể dùng một default route đến những giao thức định tuyến khác. Một ví dụ tiêu biểu là một IGP sẽ chỉ một default route đến một router BGP nằm ở ranh giới của AS. Một trường hợp khác cần cấu hình default route là cho một mạng stub để kết nối đến một hệ thống mạng lớn hơn.

Hình 6-5: Cách dùng default-route

Error!

Error!

Null Interface

Null interface là một interface ảo được định nghĩa như là next hop trong một dòng định tuyến tĩnh. Tất cả các traffic đến một mạng ở xa sẽ được route vào một lỗ đen. Điều này có tác dụng rất tốt trong quá trình redistribution vì nó thường được dùng để loại bỏ route.

Distribute Lists

Distribute list là những access list áp dụng vào quá trình định tuyến, xác định network nào sẽ được chấp nhận vào quá trình routing. Khi giao tiếp với quá trình định tuyến khác thông qua quá trình redistribution, việc kiểm soát các thông tin gửi

đến các quá trình khác là quan trọng. Việc kiểm soát này là nhằm mục đích bảo mật. Access list là công cụ tốt để xác định traffic trên một network.

Route Maps

Route map là các access-list phức tạp cho phép lập trình thêm các tuỳ chọn. Nếu một gói hoặc một route match với tiêu chuẩn định nghĩa trong phát biểu match, các hành động hoặc thay đổi được định nghĩa trong lệnh set sẽ được thực hiện trên packet. Route map thì được dùng trong quá trình redistribution trong cùng một cách như distribute list nhưng cho phép kiểm soát nhiều hơn trong các tiêu chuẩn đưa ra.

Hình 6-6: Cách dùng route-map

Error!

Trong hình vẽ trên, router A có một distribute list trong đó từ chối quá trình truyền của mạng 140.100.32.0 đi ra khỏi E3. Network 140.100.32.0 có thể có vài nguyên nhân bảo mật nên không thể cho các router nối về routerB thấy network này. S0 và S1 có cấu hình định tuyến tĩnh. Trong trường hợp S0, đây là kết nối đi vào Internet và định tuyến tĩnh được cấu hình bởI ISP. Điều này cho phép hệ thống mạng trên kết nối đến ISP mà không nhận những routing update động từ ISP. Các routing update từ ISP chứa các bảng định tuyến rất lớn. Mạng có một default-route được thiết lập. Trên S1, các cổng giao tiếp của router được cấu hình dùng định tuyến tĩnh sao cho các router ở đầu kia không cần thiết chạy một giao thức động. Router ở đầu xa sẽ dùng một default route được cấu hình vì đây là mà stub network. Điều này đảm bảo rằng routerC có một cấu hình đơn giản với một vài yêu cầu đặt ra.

Cấu hình Redistribution

Cấu hình redistribution cho một giao thức sẽ tùy thuộc vào đặc điểm của từng giao thức. Tất cả các giao thức yêu cầu các bước sau khi thực hiện redistribution:
Bước 1: cấu hình redistribution

Bước 2: định nghĩa giá trị metric mặc định được gán vào bất cứ network nào đang được redistribute vào các quá trình định tuyến.

Các lệnh để cấu hình redistribution được cấu hình như là các lệnh con của quá trình routing. Lệnh redistribute có thể chỉ ra giao thức định tuyến mà từ đó các updates được chấp nhận. Nó sẽ chỉ ra nguồn của updates. Tùy thuộc vào thiết kế mạng, các cấu hình thêm vào là cần thiết.

Cấu hình Default Metric

Giá trị default metric có thể được cấu hình theo vài cách. Cách đầu tiên là bao gồm tùy chọn metric trong lênh redistribute, định nghĩa giá trị metric cho route đó. bạn cũng có thể cấu hình giá trị default metric với lệnh default-metric trong quá trình định tuyến. Dùng lệnh default-metric sẽ giảm số lệnh phải cấu hình vì khi này không cần phải cấu hình cho mỗi quá trình redistribution riêng lẽ.

Cấu hình giá trị metric mặc định cho OSPF, IS-IS, RIP, EGP, or BGP

Có thể cấu hình redistribution giao thức định tuyến, sau đó dùng lệnh riêng lẽ default-metric để chỉ ra giá trị default-metric. Điểm thuận lợi là đây là cấu hình đơn giản hơn, dễ troubleshooting hơn. Ngoài ra nếu có nhiều giao thức được redistribute vào, giá trị default-metric sẽ áp dụng cho tất cả các giao thức đang được redistribute. Riêng ISIS không thể định nghĩa giá trị default metric. Giá trị metric phải chỉ ra khi thực hiện redistribute. Nếu giá trị metric không được chỉ ra, giá trị mặc định (cost = 0) sẽ được dùng và route sẽ bị bỏ qua. Để cấu hình các giá trị mặc định cho ospf, rip, egp hoặc bgp, hãy dùng cú pháp sau:

Router(config-router)#default--metric number

Cấu hình giá trị AD

Bên cạnh việc chỉ ra giá trị metric cho các route trong quá trình redistribution, người quản trị mạng cũng cần kiểm soát quá trình chọn lựa giữa các giao thức định tuyến khác nhau. Trong trường hợp này thì chỉ dùng giá trị metric là không đủ vì có nhiều giao thức đang được redistribute. Việc thay đổi giá trị AD cho phép đường đi tốt nhất được thực hiện. Để đảm bảo đường đi tối ưu được chọn lựa, đôi khi cần phải thay đổi giá trị AD để làm cho một route là kém hơn so với các route khác. Cấu trúc lệnh là giống nhau cho các giao thức ngoại trừ EIGRP dùng kiểu lệnh khác. Cú pháp dưới đây là dành cho EIGRP:
Router(config)#distance eigrp internal-distance external-distance

Để cấu hình giá trị AD cho giao thức IP, dùng cú pháp lệnh sau:

Router(config-router)#distance weight [address mask] [access-list-number | name] [ip]

Cấu hình Passive Interface

Passive interface được dùng cho những giao thức định tuyến trong đó gửi update ra tất cả các interface có địa chỉ được chỉ ra trong lệnh network. Lệnh passive interface sẽ làm router không gửi ra cập nhật về hướng đo. Cú pháp như sau:
Router(config-router)#passive--interface type number

Cấu hình định tuyến tĩnh

Router(config)#ip route prefix mask { address | interface} [distance] [tag tag] [permanent]

Lệnh này sẽ định nghĩa bằng cách chỉ ra next-hop router để gửi traffic. Cấu hình này chỉ có thể dùng chỉ nếu địa chỉ phần mạng của next-hop router là có trong bảng định tuyến. Nếu định tuyến tĩnh cần phải được quảng bá đến các router khác, nó nên được redistribute. Trong một vài phiên bản IOS, route này sẽ tự động redistribute.

Cấu hình default route

Trong những hệ thống mạng lớn hơn, có thể cấu hình nhiều tuyến đường tĩnh. Nếu quá nhiều tuyến đường tĩnh được cấu hình, bạn có thể cấu hình một dạng tuyến đường tĩnh đặc biệt gọi là static default route.

Router(config)#ip route 0.0.0.0 0.0.0.0 s0

Khi thông tin định tuyến được truyền thông qua một giao thức định tuyến động, không cần yêu cầu một cấu hình gì thêm. Trong trường hợp của RIP, chỉ có thể có một default-route, network 0.0.0.0. Tuy nhiên trong trường hợp

của IGRP, vài network có thể làm default route mặc dù chỉ một default-route là được dùng.
Nếu một router không có một network kết nối trực tiếp nhưng có một route về nó, route đó có thể xem xét như candidate default-route. Để cấu hình một default-route, dùng lệnh sau:

Router(config)#ip default-network network-number

lệnh này sẽ tạo ra một default route được gửi trong các update. Nó sẽ không tạo ra một default route trên router được cấu hình và nó chỉ tạo ra một default route nếu route đó đang kết nối trực tiếp. Khi có nhiều default route trong bảng định tuyến, các default route này sẽ được kiểm tra. Đường đi mặc định tốt nhất sẽ được chọn lựa dựa trên giá trị AD và metric. Địa chỉ gateway của đường đi tốt nhất sẽ trở thành *gateway of last resort* của router. Thuật ngữ này còn có một tên gọi khác là default-router. Bạn có thể hiển thị gateway of last resort bằng lệnh:

Router#show ip route

Giá trị default route sẽ xuất hiện trong bảng định tuyến và được đánh dấu như một tuyến đường tĩnh vớI ký hiệu S*. Giá trị gateway of last resort sẽ được gán về network này.

Route Maps

Route map là các công cụ trong đó các logic "if/then" có thể được áp dụng cho một router. Các route-map là các công cụ lập trình được dùng để kiểm soát quá trình redistribution, để hiện thực PBR, để kiểm soát quá trình NAT hoặc để hiện thực BGP.

Bạn có thể dùng route-map cho các mục đích sau đây:

- Để kiểm soát quá trình redistribution: các route map cho phép kiểm soát một mức cao hơn so với cách dùng distribution list. Route-map không đơn thuần ngăn chặn hay cho phép một mạng giống như distribute list mà còn có khả năng gán metric cho những route bị match.
- Để kiểm soát và thay đổi thông tin định tuyến: các route map được dùng để thay đổi thông tin định tuyến bằng cách gán giá trị metric cho các route.

- Định nghĩa chính sách trong PBR: các route-map ra các quyết định dựa trên địa chỉ nguồn. Khi một match được tìm thấy trong access-list, sẽ có các hành động tương ứng.

- Để thêm vào mức độ tinh tế trong cấu hình NAT: các route map định nghĩa dãy của các địa chỉ public và địa chỉ private. Có các lệnh show để giám sát và kiểm tra hoạt động của NAT.

- Để hiện thực BGP: một trong những điểm mạnh của giao thức BGP là khả năng thực hiện policy based routing. Các thuộc tính trong BGP được dùng để ảnh hưởng đến đường đi cho traffic. Các thuộc tính này thường được hiện thực dùng route maps. *Nếu* có một match *thì* áp dụng thuộc tính này. Khi này dùng lệnh set để thực hiện. Route map là phương thức chủ yếu được dùng bởi BGP để định nghĩa chính sách định tuyến BGP.

Route map rất giống ACL. Cả hai thực hiện tác vụ if/then, trong đó các tiêu chí được dùng để xác định là packet có được cho phép hoặc từ chối hay không. Sự khác nhau cơ bản là route map có khả năng thực hiện hành động thay đổi thuộc tính đến các gói dữ liệu thõa điều kiện match. Trong một ACL, tiêu chí match là ngầm định, trong một route map, đó là một keyword. Điều này có nghĩa rằng, nếu một gói thõa với một tiêu chuẩn cho trong một route map, một vài hành động phải được thực hiện để thay đổi gói, trong khi accesslist chỉ đơn giản cho phép hoặc deny một gói.

Các đặc điểm của route map được tóm tắt trong danh sách sau:

- Một route map có một danh sách các tiêu chí và tiêu chuẩn chọn lựa, được liệt kê với phát biểu mạtch.

- Một route map có khả năng thay đổi các gói hoặc các route bị match bằng cách dùng lệnh set.

- Một tập hợp của các phát biểu mạch có cùng tên được xem là cùng một route map

- Route map sẽ ngừng xử lý ngay khi có một match được thực hiện, giống như một ACL.

- Trong một route map, mỗi phát biểu được đánh số thứ tự và có thể được soạn thảo riêng lẽ.
- Số thứ tự được dùng để chỉ ra thứ tự trong đó các điều kiện được kiểm tra. Như vậy nếu hai phát biểu trong route map có tên là BESTTEST, một phát biểu có chỉ số là 5, một phát biểu có chỉ số là 15 thì phát biểu có chỉ số là 5 sẽ được kiểm tra trước. Nếu không có một phát biểu match trong phát biểu 5 thì phát biểu thứ 15 sẽ được kiểm tra.
- Route map có thể dùng các IP access-list chuẩn hoặc mở rộng để thiết lập các chính sách định tuyến.
- Các access-list mở rộng có thể được dùng để chỉ ra tiêu chí match dựa trên phần địa chỉ nguồn và địa chỉ đích, ứng dụng, kiểu giao thức, kiểu dịch vụ ToS và độ ưu tiên.
- lệnh match trong các cấu hình route map được dùng để định nghĩa điều kiện phải kiểm tra.
- Lệnh set trong cấu hình route map được dùng để định nghĩa hành động theo sau một phát biểu match.
- Một route map có thể chứ các phép AND và OR. Giống như một access-list, có một phát biểu ngầm định DENY ở cuối một route map. Hành động theo sau của phát biểu deny này tùy thuộc route map được dùng như thế nào. Để hiểu điều này một cách chính xác, bạn cần hiểu chính xác route map hoạt động như thề nào.

Danh sách sau đây sẽ giải thích logic của hoạt động route-map:

- Phát biểu của route map dùng cho PBR có thể được đánh dấu như là permit hoặc deny
- Chỉ nếu phát biểu được đánh dấu như permit và packet bị match, lệnh set mới được áp dụng.
- Các phát biểu trong route-map sẽ tương ứng với các dòng của một access-list. Chỉ ra một điều kiện match trong route map thì cũng tương tự như chỉ ra nguồn và đích trong access list

- Các phát biểu trong route map được so sánh với đường đi của gói để xem có một match nào đó hay không. Các phát biểu này sẽ được lần lượt kiểm tra từ trên xuống dưới.
- Một phát biểu match có thể chứa nhiều điều kiện. Ít nhất một điều kiện trong phát biểu match phải là đúng. Đây là phép logic OR
- Mộ route-map có thể chứa nhiều phát biểu match. Tất cả các phát biểu match trong route map phải được xem xét là đúng để cho phát biểu của route map là match. Điều kiện này gọi là phép logic AND.

Định tuyến theo chính sách (Policy-Based Routing – PBR)

Các route map được dùng trong cấu hình PBR cho phép chọn lựa nhiều tiêu chuẩn như địa chỉ IP, các ứng dụng, giao thức, kích thước gói tin. Khi được chọn lựa, các lệnh của PBR sẽ hiện thực chính sách cho các route được chọn lựa.

Các routes được route theo policy và các tuyến đường tĩnh có rất nhiều điểm chung. Tuy nhiên định tuyến tĩnh sẽ chuyển các gói dựa trên địa chỉ đích, trong khi policy sẽ chuyển gói theo địa chỉ nguồn. Nếu các access-list được dùng với route-map, các thông số trong một access-list mở rộng có thể được dùng để route traffic dựa trên những tiêu chuẩn như địa chỉ đích, chiều dài, giao thức IP, độ ưu tiên hoặc port number. Khả năng này cho phép điều chỉnh tốt hơn nữa các tiêu chuẩn mà qua đó giá trị next-hop là được quyết định.

Các luật áp dụng để định nghĩa PBR là như sau:

- Traffic có thể được điều chuyển dựa trên địa chỉ nguồn và địa chỉ đích
- PBR chỉ ảnh hưởng đến quá trình định tuyến trong router mà nó được cấu hình
- PBR không có ảnh hưởng đến địa chỉ đích của gói tin nhưng nó có thể ảnh hưởng đến việc chọn lựa đường đi bằng cách thay đổi giá trị next-hop
- PBR không cho phép traffic gửi tới một AS khác thay đổi đường đi đã được chọn lựa bởi AS đó
- PBR chỉ có thể ảnh hưởng chỉ đến việc traffic sẽ đến router láng giềng nào

- Khi PBR kiểm tra địa chỉ source, nó được cấu hình trên inbound interface.
- Nếu không có match, gói tin sẽ không bị policy route và sẽ được route bình thường đến đích
- Cách sử dụng route map trong PBR thì hơi khác so với các cách dùng route-map khác. Khi được sử dụng cho PBR, nếu một gói không match với các tiêu chí được chỉ ra trong route-map thì gói tin sẽ không bị loại bỏ. Thay vào đó, gói tin sẽ được gửi đến quá trình định tuyến và được route bình thường dựa trên địa chỉ đích. Nếu bạn muốn loại bỏ packet, bạn nên dùng lệnh set để route packet đến null interface trong dòng cuối cùng của route-map
- PBR cũng cho phép một cơ chế để đánh dấu các packet với các giá trị ToS khác nhau. Đặc điểm này có thể được dùng kết hợp với các kỹ thuật hàng đợI sao cho một vài loại traffic nhận được các dịch vụ ưu tiên hơn.
- Thay vì định tuyến bằng cách dùng địa chỉ đích, PBR cho phép bạn xác định và cài đặt chính sách định tuyến bằng cách cho phép hoặc deny một gói tin dựa trên các thông số như địa chỉ của một thiết bị đầu cuối, ứng dụng đang chạy, giao thức đang dùng, kích thước của gói tin.

Các lợi ích của PBR

- Chọn lựa nhà cung cấp dịch vụ dựa trên nguồn gốc traffic: các nhà cung cấp dịch vụ thường dùng PBR để ra các quyết định định tuyến dựa trên địa chỉ nguồn. Các traffic của các khách hàng khác nhau sẽ được route đến các kết nối Internet khác nhau.

- Chất lượng dịch vụ: bằng cách thiết lập các kiểu chất lượng dịch vụ (ToS) trong gói IP, các tổ chức có thể cung cấp dịch vụ QoS. Theo cách này, các traffic có thể khác nhau và các cơ chế hàng đợi có thể được cài đặt để ưu tiên traffic dựa trên giá trị QoS trên lớp core và backbone của mạng.

- Tiết kiệm chi phí: các traffic được tạo ra bởi một hoạt động đặc biệt có thể được áp đặt cho một mức băng thông cao hơn trong một khoảng thời gian ngắn.

- Chia sẽ tải: PBR cho phép hiện thực các chính sách để phân phối traffic giữa các đường đi khác nhau dựa vào loại traffic. Tính năng này không giống với đặc tính chia sẽ tải động trong các giao thức định tuyến.

Các điểm bất lợi của PBR:

- Nên dùng thêm một đường đi dự phòng trong trường hợp router kế tiếp bị down. Nếu không có một giải pháp dự phòng, PBR dùng bảng định tuyến

- Phải dùng thêm nhiều chu kỳ CPU vì tất cả các địa chỉ source đều phải được kiểm tra

- Phải cấu hình thêm

- Sẽ tồn tại khả năng các loại traffic khác bị hủy

Hoạt động của route-map và của Policy based Routing (PBR)

PBR áp dụng vào các gói tin đi vào hoặc các gói tin được tạo ra bởi router. Khi một gói tin nhận được trên một interface có cấu hình PBR, gói tin sẽ trải qua một qui trình như sau:

- Nếu có một match xảy ra và hành động là cho phép, gói tin sẽ được route theo hành động được chỉ ra trong lệnh set
- Nếu có một match xảy ra và hành động là từ chối gói tin thì packet sẽ không được route theo chính sách nhưng sẽ được định tuyến như bình thường
- Nếu không có match nào và nếu không có thêm đoạn cấu hình nào chỉ ra phải làm gì trong tình huống này, mặc định gói tin sẽ bị deny, nghĩa là sẽ chuyển về định tuyến bình thường. Quá trình định tuyến bình thường sẽ có

thể bị loại bỏ nếu ta dùng thêm một phát biểu set để định tuyến packet về null0. Nói cách khác, đây là cách để loại bỏ gói tin.

Cấu hình Route Maps cho Policy-Based Routing

Cách cấu hình route map như sau:

Router(config)#route-map map-tag [{permit | deny} sequence-number]

Cấu hình Fast Switching với Policy-Based Routing

Tốc độ đi qua một hệ thống mạng bị ảnh hưởng bởi khả năng của các thiết bị mạng trong xử lý traffic. Cơ chế fast switching cho PBR bị tắt ở chế độ mặc định. Để cấu hình fast-switch cho PBR, thực hiện các bước sau:
bước 1: cấu hình PBR trước khi bạn có thể cấu hình fast-switch
bước 2: khi PBR được cấu hình, bật fast-switching với lệnh
Router(config-if)#**ip route-cache policy**

Cơ chế fast-switch PBR hỗ trợ tất cả các dạng của lệnh match và phần lớn các lệnh set ngoại trừ việc lệnh set ip default không được hỗ trợ

Lệnh set interface được hỗ trợ chỉ trên những kết nối point-to-point trừ phi có một entry đã được cache dùng cùng một interface trong lệnh set interface trong route map. Route cache là một phần của bộ nhớ được dành cho các quyết định định tuyến. Trong process switching, bảng định tuyến sẽ được tham khảo để tìm đường đi đến đích. Trong fast switching, hệ điều hành không kiểm tra bảng định tuyến bởi vì đã có thông tin được cache lại. Thay vào đó, nếu một gói là match, hệ điều hành sẽ nhanh chóng chuyển gói tin ra interface ngay lập tức.

Phân phối lại (Redistribution) các kỹ thuật chống loop và tối ưu

Tác giả: Trần Văn Thành

Phân phối lại (Redistribution) với các kỹ thuật liên quan để chống loop và tối ưu

1. Phân phối lại với tóm lược tuyến (Redistribution và RouteSummarization)

a. Tóm lược tuyến (Route Summarization)

Trong một routing domain, khi một topo mạng càng lớn thì kích thước routing table của các router trong domain đó không những có kích thước càng lớn mà còn rất khó khăn cho các nhà quản trị gỡ dối mạng cũng như yêu cầu rất cao về phần cứng của router. Có một giải pháp giải quyết vấn đề này đó là route summarization. Bằng cách nhóm các subet con thành một subnet đại to hơn.

Route summarization còn có một ứng dụng quan trọng khác nữa đó nó là giải pháp để thực hiện redistribution từ classless routing protocol vào classful routing protocol.

b. Phân phối lại và tóm lược tuyến (Redistribution and Route Summarization)

Các giao thức định tuyến EIGRP, OSPF và IS-IS có khả năng thực hiện tóm tắt những tuyến phân phối lại(summary redistribute route). Trong trường hợp như hình 3.19 sẽ nghiên cứu summary của EIGRP và OSPF. Điều đầu tiên cần ghi nhớ khi thực hiện summary đó là có chiến lược thiết kế subnet IP phù hợp cho summary. Chẳng hạn như hình 3.19, các subnet của mạng 192.168.3.0 trong OSPF domain có thể được nhóm vào một subnet đại diện đó là 192.168.3.0/25. Tương tự như vậy các subnet trong EIGRP 1 domain có thể nhóm lại thành một subnet đại diện là 192.168.3.128/25. Nếu subnet 192.168.3.0/27 được nối trực tiếp vào router Podres, thì subnet đó sẽ được quảng bá một cách riêng lẻ mà không thực hiện summary được. Tuy nhiên nếu các tuyến riêng lẻ không tham gia summary tồn tại càng nhiều thì hiệu quả của summary càng kém.

Error!

Thực hiện summary với OSPF
Câu lệnh summary-address xác định một địa chỉ và mask summary tới một OSPF domain. Bất cứ địa chỉ subnet ra vào đãI được xác định bởi địa chỉ summary sẽ bị khử (suppress). Chú ý khi thực hiện summary đối với OSPF là:
Khi summary các tuyến ngoại thì sẽ được thực hiện tại ASBR.

Khi summary các tuyến nội OSPF thì sẽ được thực hiện tại ABR với câu lệnh area range.

Tại Robinson trong hình 3.19, các subnet trong EIGRP domain được summary vào OSPF domain với địa chỉ summary là 192.168.3.128/25, và các subnet trong EIGRP domain được summary với địa chỉ summary 172.16.0.0/16.

```
Router eigrp 1
redistribute ospf 1 metric 1000 100 1 255 1500
redistribute eigrp 2
passive-interface Ethernet0
network 192.168.3.0
!
router eigrp 2
redistribute eigrp 1
network 192.168.4.0
network 172.16.0.0
!
router ospf 1
summary-address 192.168.3.128 255.255.255.128
summary-address 172.16.0.0 255.255.0.0
redistribute eigrp 1 metric 50 subnets
redistribute eigrp 2 metric 100 metric-type
1 subnets
network 192.168.3.33 0.0.0.0 area 0
```

Error!

Thực hiện summary với EIGRP

Summary cho EIGRP được thực hiện ở interface. Thay vì việc xác định địa chỉ summary (gồm địa chỉ và mask) trong một routing process như OSPF, đối với EIGRP chúng được xác định dưới các interface riêng rẽ. Hệ thống này cung cấp khả năng mềm dẻo trong việc quảng bá các summary route (tóm lược tuyến đường) khác nhau cho các interface khác nhau trong cùng một process (quá trình). Câu lệnh thực hiện là ip summary-address eigrp process-id xác định một địa chỉ summary (bao gồm cả địa chỉ và mask).

Để thực hiện 3 địa chỉ summary là 192.168.3.0/25; 172.16.0.0/16; 192.168.4.0/24

vào IEGRP 1 domain.

Cần thực hiên cấu hình tại Robinson như sau:

```
interface Ethernet0
ip address 192.168.3.33 255.255.255.224
!
interface Ethernet1
ip address 192.168.3.129 255.255.255.224
ip summary-address eigrp 1 192.168.3.0 255.255.255.128
ip summary-address eigrp 1 172.16.0.0 255.255.0.0
ip summary-address eigrp 1 192.168.4.0 255.255.255.0
!
interface Serial0
ip address 192.168.4.5 255.255.255.252
ip summary-address eigrp 2 192.168.3.0 255.255.255.0
!
interface Serial1
ip address 172.16.2.21 255.255.255.252
ip summary-address eigrp 2 192.168.0.0 255.255.0.0
!
router eigrp 1
redistribute ospf 1 metric 1000 100 1 255 1500
redistribute eigrp 2
passive-interface Ethernet0
network 192.168.3.0
!
router eigrp 2
redistribute eigrp 1
network 192.168.4.0
network 172.16.0.0
!
router ospf 1
summary-address 192.168.3.128 255.255.255.128
summary-address 172.16.0.0 255.255.0.0
redistribute eigrp 1 metric 50 subnets
redistribute eigrp 2 metric 100 metric-type 1 subnets
network 192.168.3.33 0.0.0.0 area 0
```

Hình 3.21 cho biết routing table của Podres. Cũng giống như OSPF

summarization, EIGRP summarization khử việc quảng bá những subnet mà thuộc miền (range) của địa chỉ summary. Điểm không giống với OSPF là routing table của Podres chỉ cho biết những route tóm lược được quảng bá vào EIGRP mà không đánh dấu đó là external route.

Error!

Error!

Error!

Một điều chú ý trong routing table của Snider là mục nhập cho 192.168.4.0/24. Là subnet này không được summary với địa chỉ summary 192.168.0.0/16 với lý do là summary chỉ áp dụng cho những route được redistribution vào process domain.

Xem lại mục nhập cho tuyến đường tóm lược (summary route) 192.168.3.128/25. Mục nhập này được redistribution vào OSPF domain và được đánh dấu là tuyến ngoại (external route), chính điều này khiến cho nó lại được redistribution ngược trở lại EIGRP domain. Chuyện gì sẽ xảy ra khi tuyến đường tóm lược đó được quảng bá vào OSPF và lại được quảng bá quay trở lại EIGRP domain. Dưới đây là một tình huống không mong muốn tại Podres:

Giả sử rằng subnet 192.168.3.1/27 trở thành không tới được. Podres có thể forward (chuyển tiếp) packet có địa chỉ đích thuộc subnet 192.168.3.128/125 một cách không rõ ràng. Packet được gửi vào OSPF domain nơi mà bạn mong muốn tuyến đường tóm lược sẽ mang packet trở lại Podres. Kết quả là xuất hiện routing loop.

Có một giải pháp để khắc phục tình huống trên đó là: sử dụng null interface để bảo vệ tình trạng routing loop gây lên bởi summarization. Null interface chỉ là một interface o (software-only) không tới nơi nào c-packet được định tuyến tới đó sẽ bị drop.

Với kỹ thuật này trong thực tế tình huống trên sẽ không xảy ra. Bất cứ khi nào một router tạo ra một địa chỉ summary thì router sẽ tạo ra một tuyến tới null interface. Quay trở lại tình huống trên nếu Robinson nhận được một packet với địa chỉ đích thuộc subnet 192.168.3.192/27 và subnet đó không đến được nữa thì router sẽ forward packet đó tới null interface. Routing loop đã được giải quyết.

2. Phân phối lại tuyến tĩnh (Redistributing Static Routes)

Hình 3.25 cho biết routing table của router Williams trong hình 3.24. Chú ý rằng tuyến tới subnet 10.1.2.160/28 và 10.1.2.224/28 không có trong routing table, do là subnetmask của chúng không nhất quán với 24-bit mask trên interface E1 của May dẫn tới những đó không có trong thông tin update vào RIP domain. Đây là tình huống thường gặp trong quá trình redistribution từ classless routing protocol vào classful routing protocol.

Error!

Có một giải pháp để giải quyết vấn đề này là summary 2 subnet 28-bit vào một subnet đại diện 24-bit là 10.1.2.0/24. Tuy nhiên là RIP không hỗ trợ lệnh summary vì nó là một classful routing protocol. Cần có một giải pháp khác đó là cấu hình static route để summary để chỉ và redistribution tuyến đó vào RIP domain. Cấu hình cụ thể như sau:

```
router isis
summary-address 10.2.0.0 255.255.0.0 level-1
redistribute rip metric 0 metric-type external level-1
net 01.0001.0000.0c76.5432.00
!
router rip
redistribute static metric 1
redistribute isis level-1-2 metric 1
passive-interface Ethernet0
network 10.0.0.0
!
ip route 10.1.2.0 255.255.255.0 10.1.4.1
```

3. Lọc tuyến và phân phối lại (Route Filtering and Redistribution)

a. Lọc tuyến (Route Filtering)

Như trong phần trước đã giới thiệu một số tình huống dẫn đến routing loop khi thực hiện redistribution. Chẳng hạn như ví dụ trong hình 3.19, tuyến tóm lược 192.168.3.128/25 được quảng bá vào OSPF domain nhưng lại được quảng bá lại vào trong EIGRP domain- nơi mà summary subnet tồn tại. Trong hiện tượng này có sự quảng bá sai hướng qua redistributing router và được gọi là route feedback.

Có một giải pháp để giải quyết vấn đề trên là sử dụng route filtering. Route filtering là một kỹ thuật để điều khiển thông tin định tuyến bằng cách sử dụng access-list. Bất cứ khi nào quá trình mutual redistribution diễn ra có sự chia sẻ hai chiều thông tin định tuyến giữa hai hay nhiều giao thức định tuyến chính những điều này có thể dẫn đến hiện tượng feedback- route filter có thể đảm bảo những tuyến đó sẽ chỉ được quảng bá theo một chiều.

Mục đích của việc sử dụng route filter là tạo ra một route firewall. Trong thực tế thường xuyên xảy ra hiện tượng một tập đoàn hay một tổ chức lớn có rất nhiều tổ chức con và phải liên hệ giữa chúng nhưng vẫn đảm bảo một vài tổ chức con hay một mạng con nào đó có sự riêng tư trong việc điều khiển thông tin update. Route filter được thực hiện tại interconnecting router sẽ đảm bảo rằng router đó chỉ đồng ý những route phù hợp với chính sách điều khiển định tuyến định tuyến của người quản trị.

Route filter làm việc bởi sự quy định những tuyến được tham dự vào hay quảng bá ra ngoài routing table. Route filter có tác dụng đối với link state routing protoco khác một chút so với distance vector routing protocol.

Đối với các router chạy distance vector routing protocol việc quảng bá tuyến dựa vào việc trao đổi routing table của nó đối với các router khác trong cùng domain dưới dạng broadcast. Kết quả là route filter có ảnh hưởng những route mà router quảng bá tới neighbor của nó.

Đối với các router chạy link state routing protocol thì bình thường nó chỉ trao đổi bản tin Hello để duy trì neighbor mà không trao đổi các tuyến với nhau. Và nó xây dựng lên các tuyến (route) dựa vào link state database của nó. Do đó route filter không có ảnh hưởng trong việc quảng bá thông tin trạng thái. Kết quả là route filter chỉ có ảnh hưởng đến routing table của router mà được cấu hình route filter mà không ảnh hưởng tới các mục nhập tuyến của router neighbor. Chính điều này dẫn tới route filter thường được sử dụng tại điểm redistribution vào link state domain chẳng hạn như tại ASBR đối với OSPF.

b. Lọc tuyến với phân phối lại (Route Filtering with redistribution)
Bất cứ khi nào một router thực hiện mutual redistribution, thì khả năng feedback luôn có khả năng xảy ra. Ví dụ như hình 3.26, tuyến từ RIP domain có thể được redistribution vào OSPF domain và từ đó chúng lại được redistribution vào RIP domain. Do đó sử dụng route filter để điều khiển hướng quảng bá tuyến một cách khôn ngoan nhất.

Error!

Cấu hình route filter tại Cruncher như sau:

```
router ospf 25
redistribute rip metric 100
network 172.16.1.254 0.0.0.0 area 25
network 172.16.8.254 0.0.0.0 area 25
network 172.16.50.254 0.0.0.0 area 25
distribute-list 3 in Ethernet0/0
distribute-list 3 in Ethernet0/1
distribute-list 3 in Ethernet0/2
!
router rip
redistribute ospf 25 metric 5
passive-interface Ethernet0/0
passive-interface Ethernet0/1
passive-interface Ethernet0/2
network 172.16.0.0
distribute-list 1 in Ethernet0/3
distribute-list 1 in Ethernet2/0
distribute-list 1 in Ethernet2/1
!
ip classless
access-list 1 permit 172.16.128.0 0.0.127.255
access-list 3 permit 172.16.0.0 0.0.127.255
```

Với cấu hình như trên, những tuyến có đích thuộc OSPF domain sẽ không quảng bá vào OSPF domain từ RIP domain và những tuyến có đích thuộc RIP domain sẽ không được quảng bá vào RIP domain từ OSPF domain.
Tuy nhiên với cách cấu hình như trên, trong những trường hợp có rất nhiều subnet con và chúng phân bố rất khó để thực hiện summary thì việc cấu hình access list sẽ rất khó. Có một giải pháp để giải quyết vấn đề trên đó là cấu hình route filter tại các điểm redistribution để lọc bởi quá trình định tuyến (route process) thay vì bởi interface. Cấu hình cụ thể như sau:

```
router ospf 25
redistribute rip metric 100
network 172.16.1.254 0.0.0.0 area 25
network 172.16.8.254 0.0.0.0 area 25
network 172.16.50.254 0.0.0.0 area 25
distribute-list 10 out rip
!
```

```
router rip
redistribute ospf 25 metric 5
passive-interface Ethernet0/3
passive-interface Ethernet2/0
passive-interface Ethernet2/1
network 172.16.0.0
distribute-list 20 out ospf 25
!
ip classless
access-list 10 permit 172.16.130.0
access-list 10 permit 172.16.145.0
access-list 10 permit 172.16.240.0
access-list 20 permit 172.16.23.0
access-list 20 permit 172.16.9.0
access-list 20 permit 172.16.75.0
```

Route filter cấu hình trong OSPF domain cho phép OSPF quảng bá những route do RIP domain gửi với điều kiện được cho phép trong access list 10. Tương tự như vậy, route filter cấu hình trong RIP domain chỉ cho phép RIP quảng bá những route do OSPF 25 khám phá với điều kiện những tuyến đó được cho phép trong access list 20.

Chú ý rằng mặc dù lọc (filter) bởi routing protocol là hữu ích cho việc xác định tuyến nào được redistribution nhưng nó cũng không phải phương pháp tốt để giải quyết tình trạng route feedback. Ví dụ với hình 3.26 có cấu hình như sau:

```
router ospf 25
redistribute rip metric 100
network 172.16.1.254 0.0.0.0 area 25
network 172.16.8.254 0.0.0.0 area 25
network 172.16.50.254 0.0.0.0 area 25
distribute-list 1 out rip
!
router rip
redistribute ospf 25 metric 5
passive-interface Ethernet0/3
passive-interface Ethernet2/0
passive-interface Ethernet2/1
network 172.16.0.0
distribute-list 3 out ospf 25
```

!
ip classless
access-list 1 permit 172.16.128.0 0.0.127.255
access-list 3 permit 172.16.0.0 0.0.127.255

Giả sử rằng một route từ RIP domain chẳng hạn 172.16.190.0/24, redistribution vào OSPF domain, lại được quảng bá lại Crucher. Mặc dù distribute list được cấu hình trong RIP domain sẽ chặn tuyến được quảng bá lại RIP domain, nhưng distribute lisr lại không chặn việc tuyến đó được quảng bá vào routing table của Cruncher cũng như được tạo ra trong OSPF domain. Sự thật filter cho rằng tuyến đó đã được đưa vào routing table của OSPF. Kết luận để ngăn chặn tình trạng feedback, tuyến phải được lọc từ khi tuyến đến một interface trước khi được đưa vào routing table.

4. Di chuyển một giao thức định tuyến (A protocol Migration)

a. Định nghĩa

Sự di chuyển một giao thức định tuyến là rất hay gặp trong thực tế. Khi một tổ chức đang chạy một giao thức định tuyến nào đó tuy nhiên nó mắc phải một số nhược điểm và họ muốn chuyển sang chạy một giao thức định tuyến khác tin cậy hơn. Quá trình này được gọi là a protocol migration.

Câu lệnh distance được sử dụng không với bất cứ thông số tuỳ chọn nào, để xác định administrative distance được gán cho các tuyến đường được học từ một giao thức định tuyến xác định. Khi router chạy nhiều giao thức định tuyến khác nhau, thì các tuyến đường được đồng ý hay từ chối căn cứ dựa trên administrative distance của chúng.

Ví dụ: topo mạng như hình 3.27 đang chạy RIP và người ta muốn thiết kế để chuyển sang chạy EIGRP.

Error!

b. Các phương pháp thực hiện

Để thực hiện a protocol migration có một vài phương pháp như sau:

Phương pháp thứ nhất: tắt giao thức cũ và bật giao thức mới tại mỗi router. Phương pháp này không khả thi khi giải quyết trong mô hình mạng cỡ lớn bởi vì thời gian chết (downtime) sẽ rất lớn.

Phương pháp thứ hai: cài đặt thêm giao thức định tuyến mới vào nhưng không xoá giao thức định tuyến cũ. Phương pháp này chỉ áp dụng cho trường hợp giá trị administrative distance của giao thức định tuyến mới nhỏ hơn giao thức cũ, mỗi router sẽ chọn các tuyến do giao thức mới quảng bá để đưa vào bảng định tuyến. Sau một thời gian toàn mạng sẽ hội tụ với giao thức định tuyến mới đồng nghĩa với quá trình a protocol migration đã hoàn tất lúc này ta có thể gỡ giao thức định tuyến cũ ra mà không ảnh hưởng đến mạng. Tuy nhiên khi thực hiện phương pháp thứ 2 thì khả năng routing loop và black hole vẫn tồn tại trong suốt quá trình hội tụ lại.
Phương pháp thứ ba: thay đổi administrative distance của một trong hai giao thức định tuyến đảm bảo sao cho những route mà được quảng bá bởi giao thức định tuyến mới sẽ không đưa vào routing table cho đến khi tất cả các router trên mạng đã sẵn sàng cho quá trình chuyển đổi. Cho đến khi tất cả các thiết bị trên mạng đều được cấu hình giao thức định tuyến mới khi ấy ta mới thay đổi giá trị administrative distance về giá trị ban đầu.

Ưu điểm 1: Mặc dù routing loop và black hole vẫn có thể xảy ra đối với phương pháp này nhưng quá trình chuyển đổi nhanh hơn và ít xảy ra lỗi hơn bởi vì chỉ cần một sự thay đổi administrative distance trên các thiết bị.

Ưu điểm 2: khi người quản trị có thể sử dụng lại giao thức định tuyến ban đầu bằng cách thay đổi giá trị administrative distance của các giao thức định tuyến nếu như giao thức định cũ chưa bị xoá.

Nhược điểm : khi thực hiên phưng pháp này router phải có khả năng chạy được hai quá trinh định tuyến cho nên yêu cầu về phần cứng phải cao hơn khi chỉ chạy một giao thức định tuyến. Do đó sau các thiết bị trên mạng nhận biết sự xuất hiện của giao thức định tuyến mới thì nên xoá giao thức định tuyến cũ đi.

5. Nhiều điểm phân phối lại (Multiple Redistribution Points)

Khi mutual redistribution được thực hiện ở nhiều hơn một điểm, như trong hình 3.28. Administrative distance có gây lựa chọn sai tuyến đường (sub-optimal routing), routing loop và black holes. Ví dụ như trong routing table của Bumble như trong hình 3.29, tuyến đến mạng 192.168.6.0 mà router Bumble sẽ đi qua Blather mà không đi qua router Monks.

Error!

Error!

Giải cho vấn đề này là sử dụng distribute-list để điều khiển nguồn gốc của các tuyến tại các redistribution point. Cấu hình tại Bumble và Grimwig cụ thể như sau:

```
Bumble
router ospf 1
redistribute rip metric 100
network 192.168.3.1 0.0.0.0 area 0
distribute-list 1 in
!
router rip
redistribute ospf 1 metric 2
network 192.168.2.0
distribute-list 2 in
!
ip classless
access-list 1 permit 192.168.4.0
access-list 1 permit 192.168.5.0
access-list 2 permit 192.168.1.0
```

```
access-list 2 permit 192.168.6.0
Grimwig
router ospf 1
redistribute rip metric 100
network 192.168.5.1 0.0.0.0 area 0
distribute-list 1 in
!
router rip
redistribute ospf 1 metric 2
network 192.168.6.0
distribute-list 2 in
!
no ip classless
access-list 1 permit 192.168.3.0
access-list 1 permit 192.168.4.0
access-list 2 permit 192.168.1.0
access-list 2 permit 192.168.2.0
```

Trong cấu hình trên, access list 1 chỉ cho phép network trong OSPF domain đồng ý bởi OSPF và access list 2 chỉ cho phép network trong RIP domain đồng ý bởi RIP. Hình 3.30 cho biết routing table của Bumble sau khi thực hiện distribute-list.

Error!

Vấn đề xảy ra ở đây đó là khi kết nối trên cổng Ethernet của Bumble bị fail. Thì khi ấy mạng 192.168.6.0 sẽ không đến được do phương pháp này không khả năng dự phòng. Cụ thể xem routing table của Bumble sau khi kết nối trên cổng Ethernet của Bumble bị fail như hình 3.31 sẽ chứng minh điều này.

Error!

Để khắc phục điều này chúng ta sử dụng hai câu lệnh command để thiết lập độ ưu tiên của các tuyến. Cấu hình cụ thể như sau:

Bumble
router ospf 1
redistribute rip metric 100
network 192.168.3.1 0.0.0.0 area 0
distance 130
distance 110 0.0.0.0 255.255.255.255 1
!
router rip
redistribute ospf 1 metric 2
network 192.168.2.0
distance 130
distance 120 192.168.2.1 0.0.0.0 2
!
ip classless
access-list 1 permit 192.168.4.0
access-list 1 permit 192.168.5.0
access-list 2 permit 192.168.1.0
access-list 2 permit 192.168.6.0
Grimwig
router ospf 1
redistribute rip metric 100
network 192.168.5.1 0.0.0.0 area 0
distance 130
distance 110 0.0.0.0 255.255.255.255 1
!
router rip
redistribute ospf 1 metric 2
network 192.168.6.0
distance 130
distance 120 192.168.6.1 0.0.0.0 2
!
ip classless
access-list 1 permit 192.168.3.0
access-list 1 permit 192.168.4.0

access-list 2 permit 192.168.1.0
access-list 2 permit 192.168.2.0

Câu lệch distance thứ nhất trong cấu hình của cả hai router đều thiết lập giá trị mặc định cho cả OSPF và RIP là 130.

Câu lệnh thứ hai thiết lập một giá trị distance khác cho các tuyến được xác định bởi access list tương ứng.

Như trong ví dụ cấu hình trên, RIP gán giá trị distance là 120 cho các tuyến quảng bá bởi Monks (192.168.6.1) mà được cho phép bởi access list 2. Tất cả các tuyến khác đều được gán giá trị distance là 130. Rõ ràng là với cấu hình trên là khi kết nối trên cổng Ethernet của Bumble bị fail thì sẽ tồn tại tuyến dự phòng qua Duff. Như vậy là tình huống trên đã được giải quyết.

6. Route Maps và Redistribution

a. Route map

Route map tương tự như access list, cả hai đều có tiêu chuẩn cho việc sao khớp (match) một packet nào đó và một hành động (action) cho phép hay từ chối nhữnh packet đó. Nhưng route map có điểm không giống so với access list là nó được chia thành các sequence. Và mỗi sequence có một giá trị để xác định nó là sequence number và một cặp tiêu chuẩn (match, set). Cặp tiêu chuẩn (match, set) được dùng để chay đổi một loại lưu lượng mạng xác định nào đó.

Hoạt động của route map nó sẽ hoạt động từ sequence có giá trị nhỏ nhất đến sequence có giá trị lớn nhất. Nếu điều kiện so khớp tại một sequence nào đó không khớp thì nó sẽ chuyển xuống sequence có giá trị lớn hơn. Những lưu lượng mà không so khớp với bất kỳ sequence nào thì nó sẽ tham gia định tuyến bình thường.

b. Route map với redistribution

Ngoài việc Route map với redistribution có tác dụng tương đương như route filtering với redistribution là nó có tác dụng lọc tuyến chỉ cho phép

những tuyến nào đó mới được tham gia quá trình redistribution nó còn làm thay đổi đặc tính của những tuyến đó bằng câu lệnh set. Nhưng nó có một điểm khác biệt so với route filtering với redistribution là nó rất cơ động trong việc thay đổi những tuyến bị lọc bằng cách chèn một sequence với cặp tiêu chuẩn (match, set) vào cấu hình.

Routing OSPF

Open Shortest Path First (OSPF) được phát triển bởi Internet Engineering Task Force (IETF) như một sự thay thế những hạn chế cũng như nhược điểm của RIP.

OSPF là một link state protocol, như tên gọi của mình nó sử dụng thuật toán Dijkstra'' Shortest Path First (SPF) để xây dựng routing table và open nói nên tính phổ biến của nó. OSPF đã được John Moy đưa ra thông qua một số RFC, gần đây nhất là RFC 2328.

Giống như các link state protocol, OSPF có ưu điểm là hội tụ nhanh, hỗ trợ được mạng có kích thước lớn và không xảy ra routing loop. Bên cạnh đó OSPF còn có những đặc trưng sau:

Sử dụng area để giảm yêu cầu về CPU, memory của OSPF router cũng như lưu lượng định tuyến và có thể xây dựng hierarchical internetwork topologies.

Là giao thức định tuyến dạng clasless nên hỗ trợ được VLSM và discontigous network.

OSPF sử dụng địa chỉ multicast 224.0.0.5 (all SPF router) 224.0.0.6 (DR và BDR router) để gửi các thông điệp Hello và Update.
OSPF còn có khả năng hỗ trợ chứng thực dạng plain text và dạng MD5.
Sử dụng route tagging để theo dõi các external route.
OSPF còn có khả năng hỗ trợ Type of Service.

1. Thuật ngữ

Router ID:

Chính là địa chỉ IP cập nhật của loopback interface.

Nếu không có loopback interface được cấu hình thì Router ID sẽ là địa chỉ cập nhật của physical interface.

Người ta sử dụng địa chỉ loopback vì 2 nguyên nhân sau:

Loopback interface ổn định hơn bất kỳ physical interface nào. Và nó luôn luôn active khi router hoạt động, chỉ fail khi toàn bộ router fail.

Người quản trị mạng điều khiển hoạt động của OSPF trong quá trình bình bầu DR và BDR.

Designated Router (DR): Để ngăn chặn tình trạng storm LSA trong multi-access network một DR được bầu ra trong multi-access network. DR có những nhiêm vụ sau:

Đại diện cho multi-access network và gắn bó với phần còn lại internetwork.

Để quản lý quá trình flood xử lý trên multi-access network.

Backup Designated Router (BDR): một vấn đề quan trọng với sự xắp xếp DR là khi DR bị fail, một new DR phải được xác định. Adjacency mới phải được thiết lập lại và tất cả Router trên mạng phải đồng bộ lại database của chúng với new DR. Trong suốt quá trình này thì mạng không gửi dữ liệu được.

Để ngăn chặn điều này người ta đưa ra khái niệm BDR. Tất cả các router không chỉ thiết lập adjacency với DR mà còn với BDR. Nếu DR bị fail thì BDR sẽ trở thành DR mới mà không ph3ai đồng bộ lại database của chúng.

2. Operation of OSPF

Hoạt động của OSPF có thể tóm tắt trong 7 bước sau:

Các OSPF-speaking router gửi các Hello packet ra tất cả các OSPF-enable interface. Nếu 2 router sau khi trao đổi Hello packet và thoả thuận một số thông số

chúng sẽ trở thành neighbor.

Adjacency có thể được tạo qua virtual point-to-point link hay được tạo qua một vài neighbor. OSPF định nghĩa ra một số loại network và một số loại router. Sự thiết lập một adjacency được xác định bởi loại router trao đổi Hello và loại network mà Hello trao đổi qua.

Mỗi router gửi các link state advertisement (LSA) qua tất c adjacency. LSA mô tả tất cả các interface của router (link) và trạng thái của link. Các link này có thể là stub network, tới OSPF router khác, tới network trong cùng một area, tới external network. Do có rất nhiều loại link state information cho nên OSPF định nghĩa ra đến 11 loại LSA.

Mỗi router nhận một LSA từ neighbor với link state database của neighbor đó và gửi một copy của LSA tới tất cả neighbor khác của nó.

Bằng cách flooding các LSA toàn bộ một area, tất cả router sẽ xây dựng chính xác link state database.

Khi database được hoàn tất, mỗi router sử dụng thuật toán SPF để xây dựng nên SPF tree.

Mỗi router sẽ xây dựng nên routing table từ SPF tree.

2.1. Neighbor và Adjacency

Trước khi bất kỳ LSA nào được gửi, OSPF router phải khám khám phá neighbor của chúng và thiết lập adjacency. Các neighbor sẽ được ghi lại vào trong neighbor table, cùng với link (interface) mà trên đó neighbor được định vị và thông tin cần thiết để duy trì neighbor.

a/ Hello protocol

Hello protocol có đặc trưng sau:

Nó là cách thức mà neighbor được khám phá.
Nó quảng bá một vài thông số mà qua đó 2 router phải đồng ý trước khi chúng trở thành neighbor.

Hello packet hoạt động giông như keepalive giữa các neighbor.
Đảm bảo thông tin 2 chiều giữa các neighbor.
Bình bầu DR và DBR đối với môi trường multiaccess.

OSPF-speaking router đều đặn gửi Hello packet ra tất cả OSPF-enable interface. Khoảng thời gian này gọi là HelloInterval, mặc định khoảng thời gian này là 10 giây và ta có thể thay đổi nó. Nếu router không nhận được Hello từ neighbor sau khi hết thời gian RouterDeadInterval (gấp 4 lần HellInterval) nó sẽ công bố neighbor bị down.

b/ Network types

OSPF định nghĩa 5 loại network:

Point-to-point network: như là T1 hay subrate link kết nối một cặp router. Valid neighbor trên point-to-point network luôn luôn trở thành adjacency. The destination address của OSPF packet luôn luôn là địa chỉ 224.0.0.5.

Broadcast network: như là Ethernet, Token Ring và FDDI. Broadcast network là multi-access trong đó có khả năng kết nối nhiều hơn 2 thiết bị và chúng là broadcast có nghĩa là tất cả các thiết bị có thể nhận được gói tin khi chỉ có một gói được truyền một lần. OSPF router trên broadcast network sẽ bình bầu DR và BDR sẽ được đề cập trong phần sau.

NBMA network: như là X.25, Frame Relay và ATM. Chúng có khả năng kết nối nhiều hơn 2 router nhưng không có khả năng broadcast. Có nghĩa là một packet được gửi bởi một router sẽ không thể được nhận bởi tất cả các router khác. Các OSPF router trên mạng NBMA có bình bầu DR và BDR nhưng tất cả OSPF packet đều là unicast.

Point-to-multipoint network: nó là một trường hợp đặc biệt trong cấu hình của

NBMA network. Router trên các mạng này không có quá trình bình bầu DR và BDR và các OSPF packet được gửi dưới dạng multicast.

Virtual link: là trường hợp đặc biệt trong cấu hình. OSPF packet được gửi dưới dạng unicast qua virtual link.

c/ Bình bầu DR và BDR

Quá trình bình bầu DR và BDR được kích hoạt bởi interface state machine, để quá trình bình bầu được thực hiện thì một số điều kiện sau phải tồn tại:

Mỗi interface của router mà nối vào multi-access network có một Router priority, là một số nguyên từ 0 đến 255. Đối với các Cisco router thông số này có giá trị mặc định là 1. Router với priority là 0 sẽ bị loại khỏi quá trình bình bầu DR và BDR.

Hello packet phải có trường để cho router gửi xác định Router priority và IP address của interface của router để bình bầu DR và BDR.

Khi một interface lần đầu trở thành active trên multi-access network, nó thiết lập trường DR và BDR có giá trị là 0.0.0.0. Và nó cũng thiết lập wait timer cùng với giá trị Router DeadInterval.

Tồn tại interface trên multi-access network ghi lại address của DR và BDR trong interface data structure.

Quá trình bình đầu DR và BDR diễn ra theo các trình tự sau:

Sau khi 2-Way state được thiết lập với một hay nhiều neighbor, trường Priority, DR và BDR sẽ được xem xét trong Hello của neighbor. Danh sách tất cả router đủ tư cách tham gia bình bầu được thiết lập .(router có priority lớn hơn 0 và neighbor của nó ở trạng thái 2-Way state); tất cả router công bố chúng là DR (interface addresss của chúng được lưu trong trường DR của Hello packet); và tất cả các router công bố chúng là BDR (interface address của chúng được lưu trong trường BDR của Hello packet).

Từ danh sách những router đủ tư cách, nó sẽ tạo một subset những router không đòi hỏi là DR.

Nếu một hoặc nhiều hơn neighbor trong subset này chứa interface address của nó trong trường BDR, neighbor với highest priority sẽ công bố là BDR. Nếu priority bằng nhau thì neighbor với highest router ID sẽ được chọn.

Nếu có một hoặc nhiều hơn eligible router có interface address của nó trong trường DR thì neighbor với highest priority sẽ công bố là DR. Nếu priority bằng nhau thì neighbor với highest Router ID sẽ được chọn là DR.

Nếu không có router công bố là DR thì BDR sẽ trở thành DR.

Nếu router thực hiện hiện tính toán là DR hay BDR mới được bầu chọn hay chưa bình bầu được DR, BDR thì thực hiện repeat từ bước 2 đến bước 6.

Chú ý: khi một OSPF router trở thành active và khám phá neighbor của nó, nó sẽ kiểm tra hiệu lực của DR và BDR.

Nếu DR và BDR tồn tại thì router sẽ chấp nhận nó.

Nếu BDR không tồn tại, quá trình bình bầu BDR sẽ diễn ra và router với highest priority sẽ trở thành BDR. Nếu priority bằng nhau thì router có highest router ID sẽ

trở thành BDR.

Nếu không có active DR thì BDR tăng cấp làm DR và quá trình bình bầu BDR mới bắt đầu.

d/ Neighbor States

Down: Không có Hello packet được nhận từ neighbor.
Attempt: Neighbor phải cấu hình bằng tay cho trạng thái này. Nó chỉ áp dụng chỉ cho NBMA network connection và cho biết rằng không có thông gần đây được nhận từ neighbor.

Init: Một Hello packet được nhận từ neighbor nhưng local router không nhìn thấy nó trong Hello packet. Bi-directional communication chưa được thiết lập.

2-Way: Hello packet được nhận từ neighbor và chứa đựng Router ID trong trường Neighbor. Bi-directional communication được thiết lập.

ExStart: Quan hệ Masterr/Slave được thiết lập bằng cách trao đổi Database Description (DD) packet. Router với highest Router ID sẽ trở thành Master.

Exchange: thông tin định tuyến được trao đổi thông qua DD và LSR packet.

Loading: Link-State Request packet được gửi tới neighbor để yêu cầu cho bất kỳ LSA mới được tìm thấy trong state Exchange.

Full: tất cả LSA được đồng bộ giữa các adjacency.

Error!

e/Xây dựng một Adjacency

Neighbor trên point-to-point, point-to-multipoint, và virtual link network luôn luôn trở thành adjacency trừ phải những thông số trong Hello packet không sao khớp. Trên Broadcast và NBMA network, thì DR và BDR sẽ trở thành adjacency với tất cả neighbor nhưng không có adjacency giữa cac Drother.

Quá trình xây dựng Adjacency sử dụng 3 loại OSPF packet:

Database Description packet (type 2)
Link State Request packet (type 3)
Link State Update packet (type 4)

Database Description packet có vai trò đặc biệt quan trọng trong quá trình xây dựng adjacency. Như tên gọi của mình, nó mang thông tin mô tả tóm tắt của mỗi LSA trong Link state database của router gửi. Những thông tin mô tả này không phải là các LSA trọn vẹn mà chỉ đơn thuần là header của chúng-trong DD packet có 3 flag để điều khiển quá trình xây dựng adjacency.

Bit I (Initial), nó được thiết lập để cho biết DD packet đầu tiên được gửi.
Bit M (More), nó được thiết lập để cho biết rằng đó không phi là DD packet cuối cùng được gửi.

Bit MS (Master/Slave), nó được thiết lập để cho biết DD packet được gửi bởi Master router.

Hình sau: sẽ mô tả tiến trình xây dựng một adjacency.

Error!

Bước 1: RT1 trở thành active trên multi-access network và gửi Hello packet. Do chưa nhận được bất kỳ Hello nào từ neighbor cho nên trong Hello packet trường Neighbor là empty và trường DR và BDR được thiết lập với giá trị là 0.0.0.0.

Bước 2: Sau khi nhận được Hello packet từ RT1, RT2 tạo một neighbor data structure cho RT1 và thiết lập trạng thái của RT1 là Init. RT2 gửi một Hello packet với router ID của RT1 trong trường Neighbor. Như DR, thông tin interface address của RT2 có trong trường DR của Hello packet.

Bước 3: Sau khi RT1 nhận được Hello packet từ RT2 và kiểm tra thấy Router ID của mình có trong đó, RT1 tạo một neighbor data structure cho RT2 và thiết lập trạng thái của RT2 là ExStart cho sự tho thuận master/slave. Sau đó RT1 gửi một empty DD packet (no LSA summary), trong đó DD sequence number được gán là x, bit I = 1 cho biết đây là DD packet đầu tiên được trao đổi, bit M = 1 cho biết đây không phi là DD packet cuối cùng, bit MS = 1 cho biết RT1 xác nhận là master.

Bước 4: RT2 chuyển trạng thái của RT1 sang trạng thái Exstart dựa trên DD packet mà nó nhận được từ RT1. Sau đó nó cũng trả lời RT1 bằng một DD packet với DD

sequence number là y; RT2 có higher router ID hơn RT1 cho nên nó thiết lập bit MS = 1.Giống DD packet đầu tiên, nó chỉ sử dụng để thoả thuận ra master/slave do đó nó là một empty DD packet.

Bước 5: RT1 đồng ý là RT2 là master và chuyển trạng thái của RT2 sang Exchange. RT1 gửi một DD packet với DD sequence number là y, MS = 0 cho biết nó là slave. Đây là một packet có chứa LSA header từ Link State Summary list của RT1.

Bước 6: RT2 chuyển trạng thái của neighbor của nó sang Exchange dựa trên DD packet mà nó nhận được từ RT1. Nó sẽ gửi một DD packet bao gồm LSA header từ Link State Summary list và tăng giá trị DD sequênc number lên là y +1.

Bước 7: RT1 gửi một ACK packet bao gồm giá trị DD sequence number giống DD sequence number của DD packet gửi từ RT2. Quá trình tiếp tục, RT2 gửi một DD packet và đợi cho một ACK packet từ RT1 trước khi gửi một một DD packet kế tiếp. Khi RT2 gửi DD packet với LSA summary cuối cùng thì nó thiết lập bit M = 0.

Bước 8: Sau khi nhận các DD packet và ACK packet sẽ gửi chứa đựng LSA summary cuối cùng của nó cho neighbor từ Link State Summary list, RT1 biết rằng quá trình Exchange đã xong. Tuy nhiên nó có mục nhập trong Link State Request list của nó, do đó nó chuyển sang trạng thái Loading.

Bước 9: Khi RT2 nhận DD packet cuối cùng của RT1, RT2 chuyển trạng thái của RT1 sang full bởi vì RT1 không có mục nhập trong Link State Request list của nó.

Bước 10: RT1 gửi các Link State Request packet và RT2 gửi trả lời bằng các LSA trong các Link State Update packet. Đến khi Link State Request list của RT1 là empty thì RT1 sẽ chuyển trạng thái của RT2 sang full.

2.2 LSA Flooding

Để mỗi node đưa các route một cách thích hợp chính xác qua mang, liên mạng thì mỗi node phải có một topology database của toàn mạng.

Database này bao gồm tất cả các LSA mà router nhận được. Bất cứ một sự thay đổi mạng nào đều được thể hiện trong các LSA. Flooding là quá trình khi một sự thay đổi suy ra thì các LSA mới được gửi qua mạng để đảm bảo rằng database của mỗi node được update và giống y hệt các database của node còn lại khác.

Quá trình flooding được tạo bởi 2 loại gói sau:

Link State Update packets (type 4)

Link State Acknowledgment packets (type 5)

Trên point-to-point network, Link State Update packet được gửi bằng địa chỉ multicast là 224.0.0.5.

Trên point-to-multipoint network và virtual link network, Link State Update packet được gửi dưới dạng unicast tới interface address của adjiaceny của nó.

Trên broadcast network, Drother chỉ là adjacency với DR và BDR. Do đó update packet được tới DR và BDR với địa chỉ là 224.0.0.6. Sau đó chỉ có DR router gửi update dưới dạng multicast với địa chỉ 224.0.0.5 tới tất cả các DRother router. Tiếp đó các DR, BDR router, DRother router flood LSA ra tất cả các interface còn lại.

Trên mạng NBMA network (full), quá trình trên cũng tương tự như vậy trừ điểm sau là các LSA được gửi dưới dạng unicast.

Mỗi một LSA riêng lẻ được truyền đều phải được báo nhận. Điều này được thực hiện bằng một trong các cách sau:

Implicit acknowledgment: neighbor thực hiện báo nhận cho một LSA bằng cách gửi lại một Link State Acknowledgement về nơi gửi.

Implicit acknowledgement: neighbor thực hiện báo nhận cho một lSA bằng cách gửi một copy của LSA về cho nơi gửi.

2.3. Tính toán SPF tree

Shortest Path First (SPF) là những tuyến đường qua mạng tới bất kỳ destination nào. Có 2 loại destination được thừa nhận trong OSPF:

Network
Router: là các area border router (ABR) và autonomous system boundary router (ASBR).

Chỉ một lần sau khi tất cả các OSPF router đồng bộ được link state database, mỗi

router sẽ tính toán SPF tree cho mỗi destination mà nó biết. Sự tính toán này được thực hiện bởi thuật toán Dijkstra.

Error!

Metric của OSPF

OSPF đề cập đến metric là cost. Cost của toàn tuyến là tổng của cost của các outgoing interface dọc theo tuyến đường đó. Cách tính cost được IETF đưa ra trong RFC 2328. Cisco đã thực thi cách tính cost của riêng mình như sau: 108/bandwidth với giá trị bandwidth được cấu hình cho mỗi interface.

3. OSPF với Multi-Area

Như ta đã biết khi kích thước mạng càng lớn thì số lượng các LSA càng lớn, kich thước database sẽ rất lớn…Chính những điều đó sẽ làm tăng yêu cầu về CPU cũng như memory của OSPF router. Để giải quyết vấn đề trên OSPF đã đưa ra kỹ thuật Multi-Area.

3.1. Ưu điểm của Multi-Area

Mỗi router phải chia sẻ một link state database giống hệt nhau chỉ với router trong cùng area với chính nó chứ không phải là toàn mạng. Do đó giảm được kích thước của database dẫn tới giảm yêu cầu tới phần cứng của router như: memory.

Giảm kích thước link state database có nghĩa là giảm số lượng LSA phải xử và do đó giảm tác động trên CPU.

Bởi vì link state database chỉ phải duy trì database trong một area cho nên hầu hết flooding chỉ giới hạn trong một area.

3.2. Mộ số khái niệm

Intra-area traffic: bao gồm những packet mà trao đổi giữa các router trong cùng

một area.

Inter-area traffic: bao gồm những packet mà trao đổi giữa các router thuộc các area khác nhau.

External traffic: bao gồm những packet mà trao đổi giữa một router trong một OSPF domain và một router thuộc một Autonomous system khác.

Internal Router: là những router mà tất cả các interface của nó đều thuộc cùng một area. Những router này chỉ có một link state database.

Area Border Routers (ABR): kết nối một hay nhiều area với backbone và đóng vai trò như là một gateway cho Intra-area traffic. Một ABR luôn luôn có ít nhất một interface thuộc vào backbone và phải duy trì nhiều link state database tách biệt, mỗi database cho một area. Do đó ABR thường có memory và processor cao hơn internal router. Một ABR sẽ summarize topology information của area không phải là area 0 mà nó kết nối vào backbone, backbone sẽ nhân bản summary information tới area khác.

Backbone Router: là những router mà ít nhất nó gắn với backbone. Do đó ABR cũng là Backbone Router. Và một Internal Router mà interface thuộc vào area 0 cũng là Backbone Router.

Autonomous System Boundary Routers (ASBR): là gateway cho external traffic đưa những route vào OSPF domain mà đã được học từ một số protocol khác như là: BGP và IEGRP. Một ASBR có thể được xác định ở bất cứ vị trí nào trong OSPF antonomous system; Nó có thể là Internal, Backbone hay ABR.

Virtual Link: là một link tới backbone xuyên qua một non-backbone area.

Link State Dabase: tất cả valid LSA mà rouer nhận được được lưu trong link state database của nó. Tuyển tập các LSA sẽ tạo ra topology của area.

3. 4. Các loại LSA.

Do có nhiều loại router được định bởi OSPF do đó cũng cần thiết phải định nghĩa ra các loại LSA. Cụ thể như sau:

Error!

3.5. Một số loại Area trong OSPF (OSPF Area Types)

a/ Stub Area

Một stub area là một area mà các External LSA không được flood vào trong area đó. Trong stub area sẽ không có LSA loại 4 và 5 hay những LSA đó bị block. ABR tại cạnh của stub area sẽ sử dụng Network Summary để quảng bá một default route (destination là 0.0.0.0) vào trong area. Bất cứ destination của Internal Router không thể match tới một intra hay inter area, route đó sẽ được match với default route. Bởi vì default route được mang bởi LSA loại 3, nó sẽ không được quảng bá ra ngoài area.
Sự thực thi của router trong stub area được cải thiện, memory được bảo tồn và giảm kích thước database của chúng. Tất nhiên sự cải thiện này càng rõ ràng trong internetwork với rất nhiều LSA loại 5.

Bên cạnh đó nó vẫn mang những nhược điểm của mình:

Như bất kỳ area nào, tất cả router trong stub area phải có một link state database giống hệt nhau. Để đảm bảo điều kiện này, tất cả các stub router sẽ thiết lập một flag (bit_E) trong Hello packet là 0. Chúng sẽ không chấp nhận bất cứ Hello packet nào có bit_E là 1, kết quả là adjacency không được thiết lập với bất cứ router nào không được cấu hình là stub router.

Virtual link không được cấu hình trong stub area.

Không có router nào trong stub area có thể là ASBR. Vì trong stub area không có LSA loại 5.

Một stub area có thể có hơn một ABR nhưng bởi vì sử dụng defaul route, Internal router không thể xác định được router nào sẽ là gateway tối ưu tới ASBR.

b/ Totally Stubby Areas

Totally stubby area: sử dụng default không chỉ cho destination external tới autonomous system mà còn cho destination external tới area. ABR của totally stubby area sẽ không chỉ block AS External LSA mà còn block tất c Summary LSA trừ LSA loại 3 nào để quảng bá default route.

c/ Not-So-Stubby Area

Not-so-stubby areas(NSSA): cho phép external route được quảng bá vào trong OSPF autonomous system trong khi dữ lại những đặc tính còn lại của stub area. Cụ thể là ASBR trong một NSSA sẽ sinh ra LSA loại 7 để quảng bá external

destination. Những External LSA được flood khắp NSSA area nhưng chúng sẽ bị block tại ABR.

Error!

Tóm lại ta có bảng tổng kết sau:

Error!

4. Định dạng gói tin OSPF
OSPF packet được đóng gói trong IP packet tương ứng với trường Protocol number là 89, do vậy maximum của OSPF packet là 1500 octet. OSPF packet header là giống đối với các loại OSPF packet khác nhau nhưng OSPF packet data thì biến đổi tuỳ theo loại OSPF packet.

Error!

Chú ý: IP packet với protocol number = 89 thì trường TTL luôn luôn bằng 1 để đảm bảo rằng packet không bao giờ đi quá một hop.

4.1. The Packet Header

Tất cả các OSPF packet đều có chung một dạng như sau:

Error!

Trong đó:
Version: là phiên bản OSPF, phiên bản gần đây nhất là 2.
Type: xác định ra loại OSPF packet. Có 5 loại OSPF packet như sau:

Error!

Packet length: là độ dài của OSPF packet gồm cả header (đơn vị là octet).
Router ID: là ID của router gửi.
Area ID: là area mà từ đó packet được gửi. Nếu packet được gửi qua virtual link, Area ID sẽ là 0.0.0.0 (backbone Area ID) bởi vì virtual link luôn được gắn với backbone.

Checksum: kiểm tra toàn bộ packet kể của header.
AuType: xác định loại nhận thực được sử dụng. Bảng sau là cấc loại nhận thực có thể:

Error!

a/ The Hello Packet
Hello packet được dùng để thiết lập và duy trì adjiacecy. Hello packet mang những thông số mà neighbor phải đồng ý để trở thành adjacency.

Error!

Network Mask: là address mask của interface mà packet được gửi từ đó. Nếu mask này không match với interface mà packet được nhận thì packet sẽ bị drop.

Hello Interval: là chu kỳ gửi bản tin Hello, được tính bằng giây. Nếu router gửi và nhận không có cùng thông số này nó sẽ không thiết lập quan hệ neighbor.

Options: trường này trong Hello packet đảm bảo ràng neighbor có khả năng tương thích. Router có thể từ chối một neighbor nếu khả năng này là không tương thích.

Router Priority: được sử dụng để bình bầu DR và BDR. Nếu nó được thiết lập giá trị là 0 thì sẽ loại khỏi quá trình bình bầu DR và BDR.

Router Dead Interval: là số giây mà router gửi đợi một Hello packet từ neighbor trước khi công bố neighbor dead. Nếu thông số này trong Hello đến không giống với thông số của nó thì packet sẽ bị drop.

Designated Route: là IP address của interface của DR trên mạng (không phải là Router ID của nó).

Backup DR: là IP address của interface của BDR trên mạng.

Neighbor: chứa danh sách tất cả neighbor trên mạng mà router gửi nhận từ các Hello hợp lệ.

b/ The Database Description Packet

Database Description packet: nó được sử dụng khi một adjacency được thiết lập. Mục đích chính của DD packet là mô tả một vài hay tất cả LSA trong database cho đến khi nào có thẻ xác định là match LSA trong database của nó.

Error!

Interface MTU: là kích thước lớn nhất của IP packet (đơn vị là octet) mà packet có thể được gửi đi mà không bị phân mảnh. Trường này được thiết lập là 0x0000 khi packet được gửi qua virtual link.

Option: là trường tuỳ chọn, router sẽ không chuyển tiếp LSA nếu không thoả mãn điều kiện trong trường Option.

Có 5 bit không sử dụng và có giá trị là: 00000b.

Ba bit I, M và MS đã giới thiệu trong phần building adjacency.

DD Sequence Number: trường này để đảm bảo rằng DD packet được nhận đúng thứ tự trong quá trình đồng bộ database. Thông số này luôn luôn được thiết lập bởi master cho DD packet đầu tiên và tăng dần lên trong các DD packet gửi sau.

LSA Header: danh sách của một vài hay tất cả LSA header trong link state database của router gửi.

c/ The Link State Request Packet

Trong quá trình đồng bộ database khi router nhận các DD packet, router sẽ kiểm tra xem LSA header trong DD packet nếu không có trong database của nó thì những LSA này ghi lại vào Link State Request list. Router sẽ gửi một hay một vài Link State Request packet hỏi neighbor về LSA đó.

Định dạng của Link State Request packet như sau:

Error!

Link State Type: xác định loại LSA (router LSA, network LSA...).
Link State ID: xác định ra LSA header.\

Advertising Router: là router ID của router mà gửi LSA.

d/ The Link State Update Packet

Nó được sử dụng khi flood LSA và gửi LSA trả lời cho Link State Request packet. **Error!**

Number of LSAs: xác định số LSA trong packet này.
LSAs: là full LSA (header + data). Mỗi update có thể mang nhiều LSA tới maximum kích thước của packet cho phép trên link.

f/ The Link State Acknowledgment Packet

Được sử dụng để tạo quá trình flood các LSA môt cách tin cậy (reliable).
Định dạng như sau:

(nguồn chuyenviet.com

MỤC LỤC

PHẦN I CÔNG NGHỆ MẠNG RIÊNG ẢO

Chương I. Giới thiệu chung về Mạng riêng ảo

Chương này, chúng ta bắt đầu bằng việc định nghĩa Mạng riêng ảo và những lợi ích cơ bản từ việc thực thi giải pháp Mạng riêng ảo. Chúng ta cũng xem xét các mô hình kết nối mạng riêng ảo thông dụng.

1.1. Các khái niệm cơ bản về mạng riêng ảo

1.1.1. Định nghĩa về Mạng riêng ảo

Mạng riêng ảo, có tên tiếng Anh là Virtual Private Network, viết tắt là VPN. Sau đây ta thường gọi ngắn gọn theo tên viết tắt.

Có nhiều định nghĩa khác nhau về Mạng riêng ảo.

Theo VPN Consortium, VPN là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập. Nói cách khác, VPN được định nghĩa là liên kết của khách hàng được triển khai trên một hạ tầng công cộng với các chính sách như là trong một mạng riêng. Hạ tầng công cộng này có thể là mạng IP, Frame Relay, ATM hay Internet.

Theo tài liệu của IBM. VPN là sự mở rộng một mạng Intranet riêng của một doanh nghiệp qua một mạng công cộng như Internet, tạo ra một kết nối an toàn, thực chất là qua một đường hầm riêng. VPN truyền thông tin một cách an toàn qua Internet kết nối người dùng từ xa, nhánh văn phòng và các đối tác thương mại thành một mạng Công ty mở rộng.

Theo cách nói đơn giản, VPN là một sự mở rộng của mạng Intranet qua một mạng công cộng (như Internet) mà đảm bảo sự bảo mật và hiệu quả kết nối giữa 2 điểm truyền thông cuối. Mạng Intranet riêng được mở rộng nhờ sự trợ giúp của các "đường hầm". Các đường hầm này cho phép các thực thể cuối trao đổi dữ liệu theo cách tương tự như truyền thông điểm - điểm.

Và như trong hình 1.2, mạng riêng của các Công ty loại trừ được các đường Lease-Line chi phí cao. Một báo cáo nghiên cứu về VPN cho thấy: Có thể tiết kiệm

từ 20% đến 47% chi phí mạng WAN khi thay thế các đường Lease-Line để truy cập mạng từ xa bằng VPN. Và với VPN truy cập từ xa có thể tiết kiệm từ 60% đến 80% chi phí khi sử dụng đường Dial-up để truy cập từ xa đến Công ty.

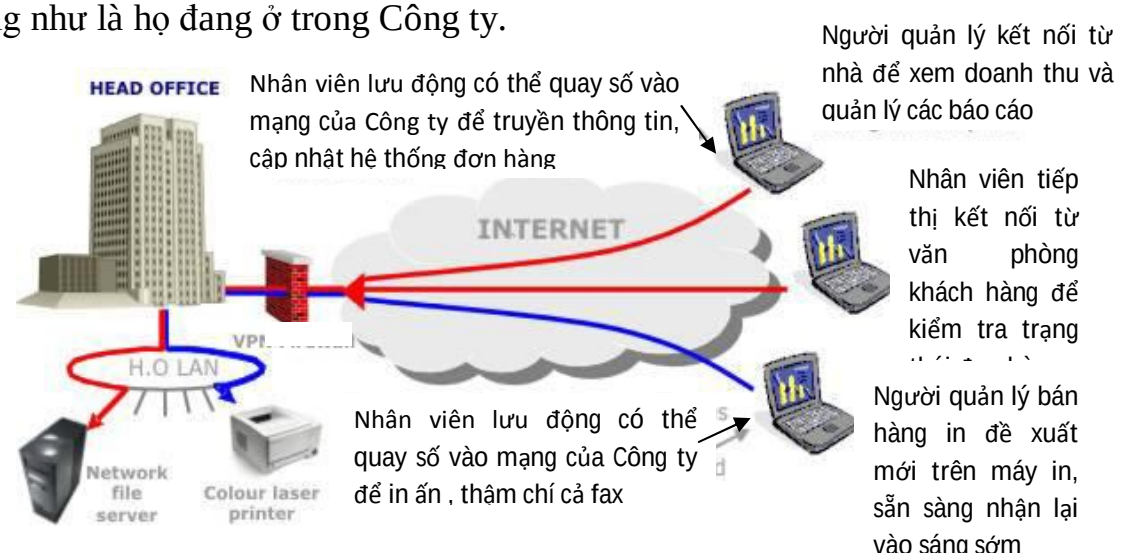
Mạng riêng ảo đã thực sự chinh phục cuộc sống. Việc kết nối các mạng máy tính của các doanh nghiệp lâu nay vẫn được thực hiện trên các đường truyền thuê riêng, cũng có thể là kết nối Frame Relay hay ATM. Nhưng, rào cản lớn nhất đến với các doanh nghiệp tổ chức đó là chi phí. Chi phí từ nhà cung cấp dịch vụ, chi phí từ việc duy trì, vận hành hạ tầng mạng, các thiết bị riêng của doanh nghiệp... rất lớn. Vì vậy, điều dễ hiểu là trong thời gian dài, chúng ta gần như không thấy được nhiều ứng dụng, giải pháp hữu ích trên mạng diện rộng WAN.

Rõ ràng, sự ra đời của công nghệ mạng riêng ảo đã cho phép các tổ chức, doanh nghiệp có thêm sự lựa chọn mới. Không phải vô cớ mà các chuyên gia viễn thông nhận định: "Mạng riêng ảo chính là công nghệ mạng WAN thế hệ mới".

1.1.2. Một số ví dụ về Mạng riêng ảo:

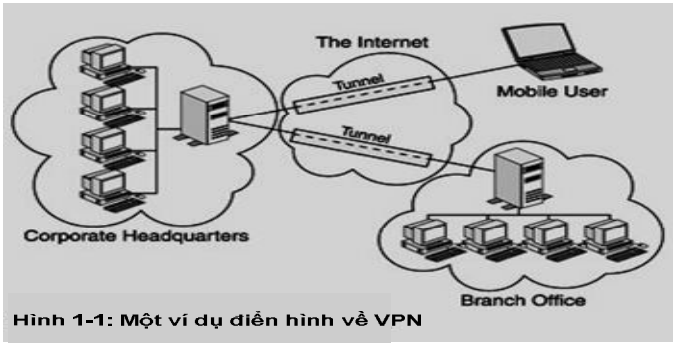
a) Ví dụ về các mô hình kết nối Mạng riêng ảo

Hình 1.1: Những người dùng di động, người dùng từ xa thiết lập kết nối VPN qua Internet đến mạng Công ty của họ để trao đổi dữ liệu, truy cập các tài nguyên giống như là họ đang ở trong Công ty.



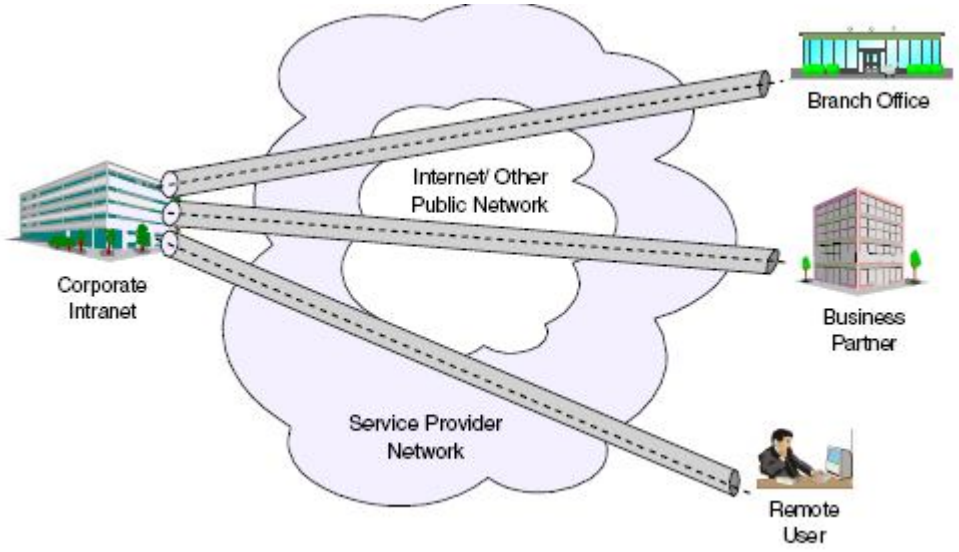
Hình 1.1

Hình 1.2: Là một ví dụ thiết lập VPN gồm một nhánh Văn phòng từ xa, một người dùng di động kết nối VPN đến mạng Văn phòng chính



Hình 1.2

Hình 1.3: Một ví dụ đầy đủ hơn



Hình 1.3

Một mạng VPN điển hình đầy đủ bao gồm mạng LAN chính tại trụ sở (Văn phòng chính), các mạng LAN khác tại những văn phòng từ xa, những đối tác kinh doanh, các điểm kết nối (như 'Văn phòng' tại gia) hoặc người sử dụng (Nhân viên di động) truy cập đến từ bên ngoài.

b) Ví dụ về ứng dụng Mạng riêng ảo

Mới đây, ngày 11/08/2005, bệnh viện Nhi trung ương đã thử nghiệm thành công dịch vụ Mạng riêng ảo.

Một ca chẩn đoán bệnh từ xa được thực hiện tại bệnh viên Nhi trung ương, đầu bên kia là bệnh viện Nghệ An và bệnh viện Hoà Bình. Thông qua dịch vụ truyền hình hội nghị "video conferencing" sử dụng công nghệ mạng riêng ảo, các chuyên gia y tế đầu ngành có thể cùng hội chẩn các ca bệnh "khó" tại bệnh viện tuyến dưới, từ đó đưa ra các chẩn đoán, phác đồ điều trị phù hợp cho người bệnh. Đây là một việc đã cũ với thế giới nhưng hoàn toàn mới với Việt Nam.

1.2. Những lợi ích cơ bản của Mạng riêng ảo

VPN mang lại nhiều lợi ích, những lợi ích này bao gồm:

- Giảm chi phí thực thi: Chi phí cho VPN ít hơn rất nhiều so với các giải pháp truyền thống dựa trên đường Lease-Line như Frame Relay, ATM hay ISDN. Bởi vì VPN loại trừ được những yếu tố cần thiết cho các kết nối đường dài bằng cách thay thế chúng bởi các kết nối cục bộ tới ISP hoặc điểm đại diện của ISP.

- Giảm được chi phí thuê nhân viên và quản trị: Vì giảm được chi phí truyền thông đường dài. VPN cũng làm giảm được chi phí hoạt động của mạng dựa vào WAN một cách đáng kể. Hơn nữa, một tổ chức sẽ giảm được toàn bộ chi phí mạng nếu các thiết bị dùng trong mạng VPN được quản trị bởi ISP. Vì lúc này, thực tế là Tổ chức không cần thuê nhiều nhân viên mạng cao cấp.

- Nâng cao khả năng kết nối: VPN tận dụng Internet để kết nối giữa các phần tử ở xa của một Intranet. Vì Internet có thể được truy cập toàn cầu, nên hầu hết các nhánh văn phòng, người dùng, người dùng di động từ xa đều có thể dễ dàng kết nối tới Intranet của Công ty mình.

- Bảo mật các giao dịch: Vì VPN dùng công nghệ đường hầm để truyền dữ liệu qua mạng công cộng không an toàn. Dữ liệu đang truyền được bảo mật ở một mức độ nhất định, Thêm vào đó, công nghệ đường hầm sử dụng các biện pháp bảo mật như: Mã hoá, xác thực và cấp quyền để bảo đảm an toàn, tính tin cậy, tính xác thực của dữ liệu được truyền, Kết quả là VPN mang lại mức độ bảo mật cao cho việc truyền tin.

- Sử dụng hiệu quả băng thông: Trong kết nối Internet dựa trên đường Lease-Line, băng thông hoàn toàn không được sử dụng trong một kết nối Internet

không hoạt động. Các VPN, chỉ tạo các đường hầm logic để truyền dữ liệu khi được yêu cầu, kết quả là băng thông mạng chỉ được sử dụng khi có một kết nối Internet hoạt động. Vì vậy làm giảm đáng kể nguy cơ lãng phí băng thông mạng.

- Nâng cao khả năng mở rộng: Vì VPN dựa trên Internet, nên cho phép Intranet của một công ty có thể mở rộng và phát triển khi công việc kinh doanh cần phải thay đổi với phí tổn tối thiểu cho việc thêm các phương tiện, thiết bị. Điều này làm cho Intranet dựa trên VPN có khả năng mở rộng cao và dễ dàng tương thích với sự phát triển trong tương lai.

Như chúng ta thấy, yêu cầu ứng dụng các công nghệ mới và mở rộng mạng đối với các mạng riêng ngày càng trở nên phức tạp và tốn kém. Với giải pháp mạng riêng ảo, chi phí này được tiết kiệm do sử dụng cơ sở hạ tầng là mạng truyền số liệu công cộng (*ở Việt Nam, thực tế chi phí tốn kém cho mạng riêng là chi phí cho các kênh thuê riêng đường dài, các mạng riêng cũng không quá lớn và phức tạp, giải pháp VPN sẽ là giải pháp giúp tiết kiệm chi phí cho kênh truyền riêng cũng như sử dụng hiệu quả hơn cơ sở hạ tầng mạng truyền số liệu công cộng*).

Trên đây là một số lợi ích cơ bản mà giải pháp VPN mang lại. Tuy nhiên bên cạnh đó, nó cũng không tránh khỏi một số bất lợi như: **Phụ thuộc nhiều vào Internet.** Sự thực thi của một mạng dựa trên VPN phụ thuộc nhiều vào sự thực thi của Internet. Các đường Lease-Line bảo đảm băng thông được xác định trong hợp đồng giữa nhà cung cấp và Công ty. Tuy nhiên không có một đảm bảo về sự thực thi của Internet. Một sự quá tải lưu lượng và tắc nghẽn mạng có thể ảnh hưởng và từ chối hoạt động của toàn bộ mạng dựa trên VPN.

1.3. Những yêu cầu đối với Mạng riêng ảo

Như ta đã biết trong phần trước, VPN là một phương pháp để kết nối mạng Intranet tương đối đơn giản và bảo mật qua mạng công cộng như Internet. Công nghệ VPN không chỉ làm giảm chi phí thực thi một môi trường mạng bảo mật cao mà còn giảm chi phí cho việc quản trị và tổ chức nhân viên. Hơn nữa, nó mang lại sự sẵn sàng, sự tin cậy và hiệu quả cao trong việc sử dụng băng thông mạng.

Làm thế nào để đưa ra giải pháp dựa trên VPN, các thành phần và yêu cầu của VPN là gì? Tất cả sẽ được xem xét trong phần này.

VPN như là một phiên bản sửa đổi của mạng riêng, cho phép chúng ta dễ dàng thiết lập mạng LAN hoặc Intranet cùng với Internet và các mạng công cộng khác để truyền thông một cách bảo mật và kinh tế. Và như vậy, hầu hết các yêu cầu của VPN và của mạng riêng truyền thống là rất giống nhau. Tuy nhiên, trong VPN có các yêu cầu nổi bật như sau:

Bảo mật, Chất lượng dịch vụ (QoS), Tính sẵn sàng, Tính tin cậy, Khả năng tương thích, Khả năng quản trị.

1.3.1. Bảo mật

Các mạng riêng và Intranet mang lại môi trường bảo mật cao vì các tài nguyên mạng không được truy cập bởi mạng công cộng. Vì vậy, xác suất truy cập trái phép đến Intranet và các tài nguyên của nó là rất thấp. Tuy nhiên, nhận định này rất có thể không đúng với VPN có sử dụng Internet và các mạng công cộng khác như mạng điện thoại chuyển mạch công cộng (Public Switched Telephone Networks - PSTNs) cho truyền thông. Thiết lập VPN mang lại cho các Hacker, Cracker cơ hội thuận lợi để truy cập tới mạng riêng và luồng dữ liệu của nó qua các mạng công cộng. Vì vậy, mức độ bảo mật cao và toàn diện cần phải được thực thi một cách chặt chẽ.

Dữ liệu và các tài nguyên cục bộ trong mạng có thể được bảo mật theo các cách như sau:

+ Thực thi các kỹ thuật phòng thủ vòng ngoài, chỉ cho phép các dòng lưu lượng đã cấp quyền từ các nguồn tin cậy vào mạng và từ chối tất cả các lưu lượng khác. Các Firewall và bộ dịch chuyển địa chỉ mạng(NAT) là các ví dụ về kỹ thuật phòng thủ. Firewall không chỉ kiểm tra kỹ lưu lượng vào mà còn cả với lưu lượng ra, vì vậy, đảm bảo một mức bảo mật cao. Bộ dịch chuyển địa chỉ là một ví dụ khác, nó không để lộ địa chỉ IP của nguồn tài nguyên cục bộ trong mạng. Và như vậy, kẻ tấn công không biết được đích của các tài nguyên đó trong mạng Intranet.

+ Xác thực(Authentication): Xác thực người dùng và các gói dữ liệu để thiết lập định danh của người dùng và quyết định anh ta có được phép truy cập tới các tài nguyên trong mạng hay không. Mô hình xác thực, cấp quyền, kiểm toán (AAA) là một ví dụ về hệ thống xác thực người dùng toàn diện. Đầu tiên hệ thống sẽ xác nhận người dùng truy cập vào mạng. Sau khi người dùng đã được xác thực thành công, họ chỉ có thể truy cập đến các tài nguyên đã được cấp quyền. Hơn nữa, một nhật ký chi tiết các hoạt động của tất cả các người dùng mạng cũng được duy trì, cho phép người quản trị mạng ghi lại những hoạt động trái phép, bất thường.

+ Mã hoá dữ liệu(Data Encryption): Thực thi các cơ chế mã hoá dữ liệu để đảm bảo tính xác thực, tính toàn vẹn và tính tin cậy của dữ liệu khi được truyền qua mạng không tin cậy. Bảo mật giao thức Internet(Internet Protocol Security - IPSec) nổi bật lên như một cơ chế mã hoá dữ liệu mạnh nhất. Nó không chỉ mã hoá dữ liệu đang được truyền mà còn cho phép xác thực mỗi người dùng và từng gói dữ liệu riêng biệt.

+ Quản lý khoá (Key Management): Để mã hoá dữ liệu, VPN cần cung cấp khoá mật mã để tạo ra các đường hầm phiên (session tunnull). Vì vậy, cần phải tạo ra các khoá, phân phối và cập nhật, làm tươi chúng.

1.3.2. Tính sẵn sàng và tin cậy

Tính sẵn sàng chỉ tổng thời gian mà người dùng truy cập được vào mạng (uptime). Trong các mạng riêng và mạng Intranet, thời gian này là tương đối cao vì toàn bộ cơ sở hạ tầng mạng thuộc quyền sở hữu riêng và được kiểm soát đầy đủ bởi tổ chức. Tuy nhiên, VPN sử dụng các mạng tương tác trung gian như Internet và PSTN vì vậy các thiết lập dựa trên VPN phụ thuộc nhiều vào mạng trung gian. Trong trường hợp này, nhân tố tính sẵn sàng phụ thuộc vào nhà cung cấp dịch vụ (ISP).

Thông thường, ISP đảm bảo tính sẵn sàng trong một bản "hợp đồng mức dịch vụ" (*Service Level Agreement* - SLA). SLA là bản hợp đồng được ký kết giữa ISP và người dùng (*một tổ chức hoặc một công ty*) để cam kết về thời gian truy cập mạng. Một số ISP đề xuất uptime rất cao, khoảng 99%. Nếu một tổ chức muốn

đảm bảo tính sẵn sàng rất cao, thì tìm một ISP có cơ sở hạ tầng chuyển mạch xương sống có khả năng phục hồi cao. Đó là:

+ Khả năng định tuyến mạnh, nó cho phép định tuyến lại qua một đường thay thế trong trường hợp đường chính bị lỗi hoặc bị tắc nghẽn. Để đảm bảo hiệu suất cực đại, khả năng định tuyến này cũng hỗ trợ nhiều lựa chọn ưu tiên định tuyến khi được yêu cầu.

+ Dư thừa các đường truy cập, thường được dùng để đáp ứng yêu cầu tăng giải thông mạng.

+ Các thiết bị dự phòng hoàn toàn tự động vượt qua lỗi, các thiết bị này không chỉ gồm các thiết bị thay thế nóng mà còn là nguồn cung cấp điện và hệ thống làm lạnh

Tính tin cậy cũng là một yêu cầu quan trọng nữa của VPN và nó liên quan mật thiết với nhân tố tính sẵn sàng. Tính tin cậy của giao dịch trong VPN đảm bảo rằng những người dùng cuối được phân phối dữ liệu trong mọi hoàn cảnh. Cũng như hầu hết các thiết lập mạng khác, tính tin cậy trong môi trường dựa trên VPN có thể đạt được bằng việc chuyển mạch các gói dữ liệu tới một đường dẫn khác nếu liên kết đã tạo hoặc thiết bị trong đường bị lỗi. Toàn bộ quá trình này là hoàn toàn trong suốt với người dùng cuối.

1.3.3. Chất lượng dịch vụ

Trong một mạng riêng ảo, cũng như trong một mạng thông thường. Đều có mong muốn là mang lại tính trong suốt cho các gói dữ liệu khi chúng được truyền từ nguồn đến đích cũng như đảm bảo chất lượng các dịch vụ khác.

Vấn đề với QoS là xác định như thế nào? có được đảm bảo hay không? là rất khó. Trừ khi có tắc nghẽn mạng, rất khó để chứng minh rằng QoS được đảm bảo.

Chất lượng dịch vụ là khả năng phản hồi trong các hoàn cảnh tới hạn bằng cách gán một tỷ lệ để xác định giới hạn lỗi trong việc sử dụng băng thông mạng và các tài nguyên cho các ứng dụng. Các ứng dụng như giao dịch tài chính, quá trình đặt hàng từ các đối tác thương mại là tương đối nhạy cảm với băng thông. Các ứng

dụng truyền video là rất nhạy cảm với độ trễ và đòi hỏi băng thông lớn để tránh hiện tượng chất lượng kém của giao dịch.

1.3.4. Khả năng quản trị

Việc kiểm soát hoàn toàn các hoạt động và tài nguyên trong mạng, cùng với việc quản trị thích hợp là rất quan trọng đặt ra với tất cả các đơn vị có mạng kết nối phạm vi toàn cầu. Hầu hết các đơn vị được kết nối với các nguồn tài nguyên của thế giới bằng sự trợ giúp của nhà cung cấp dịch vụ. Kết quả là không thể kiểm soát tại 2 đầu cuối trong mạng Intranet của một đơn vị vì phải qua mạng Intranet trung gian của nhà cung cấp dịch vụ. Trong hoàn cảnh này, một đơn vị phải quản trị được tài nguyên cho đến cả mạng kinh doanh của họ, trong khi nhà cung cấp dịch vụ quản trị các thiết lập mạng của họ. Với sự sẵn có các thiết bị VPN của các hãng sản xuất bên ngoài và hợp đồng giữa tổ chức với nhà cung cấp dịch vụ thì có thể loại trừ được ranh giới vốn có của việc quản trị tài nguyên và quản trị toàn bộ phần riêng và phần công cộng của các phần cuối VPN. Một Công ty có thể quản trị, giám sát, hỗ trợ và duy trì mạng của họ như trong mô hình truyền thống, có thể kiểm soát toàn bộ truy cập mạng và có quyền giám sát trạng thái thời gian thực, sự thực thi của VPN. Hơn nữa Công ty cũng có thể giám sát phần công cộng của VPN. Tương tự, các ISP quản trị và kiểm soát phần cơ sở hạ tầng thuộc quyền kiểm soát của họ. Tuy nhiên, nếu được yêu cầu, nhà cung cấp dịch vụ cũng có thể quản trị toàn bộ cơ sở hạ tầng, bao gồm cả cơ sở hạ tầng VPN của người dùng.

1.3.5. Khả năng tương thích

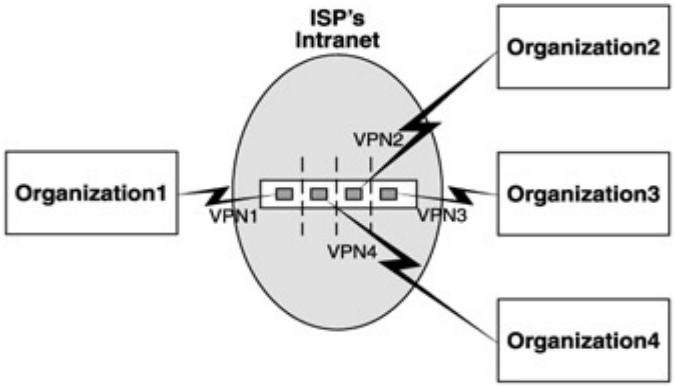
Như chúng ta đã biết VPN sử dụng mạng công cộng như là một kết nối đường dài, các mạng trung gian này có thể dựa trên IP như Internet hoặc cũng có thể dựa trên công nghệ mạng khác như Frame Relay (FR), Asynchronous Transfer Mode (ATM). Kết quả là VPN có thể sử dụng tất cả các kiểu công nghệ và giao thức cơ sở.

Trong trường hợp mạng tương tác trung gian dựa trên IP, VPN phải có khả năng dùng địa chỉ IP và các ứng dụng IP, để đảm bảo tương thích với một cơ sở hạ tầng dựa trên IP, các phương pháp sau có thể được tích hợp vào VPN.

Sử dụng Getway IP: Getway IP chuyển(hoặc dịch) các giao thức không dựa trên IP thành IP. Các thiết bị này có thể là các thiết bị mạng chuyên dụng hoặc cũng có thể là các giải pháp dựa trên phần mềm. Getway IP được cài đặt trên mọi Server và thường được dùng để chuyển đổi dòng lưu lượng.

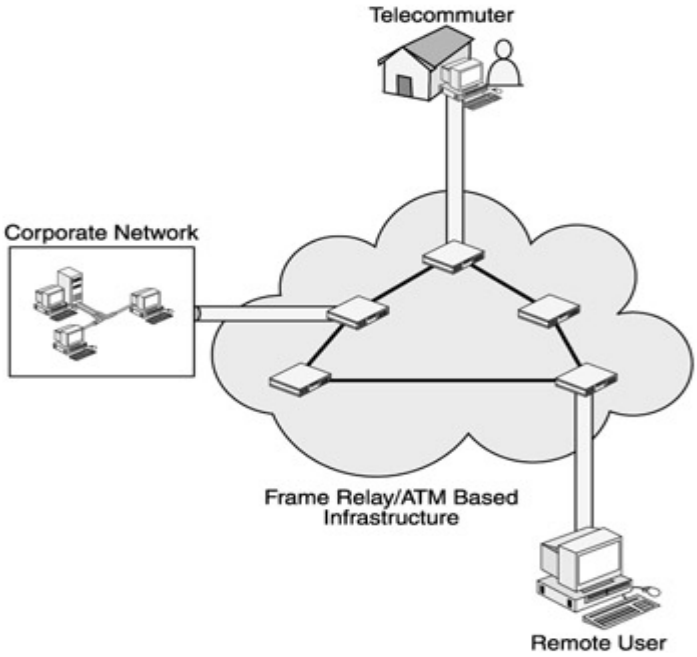
Sử dụng đường hầm: Đường hầm, như chúng ta đã biết, là kỹ thuật đóng gói các gói dữ liệu không IP thành các gói IP để truyền qua một cơ sở hạ tầng dựa trên IP. Các thiết bị cuối khác, khi nhận được các gói dữ liệu đã đóng gói này sẻ xử lý và loại bỏ phần tiêu đề IP để lấy lại dữ liệu gốc. "Đường hầm" bây giờ được xem như là một thiết bị tryền tải.

Sử dụng định tuyến IP ảo(Virtual IP Routing - VIPR): như trong hình vẽ 1.4, VIPR làm việc bằng cách phân vùng lôgic một Router vật lý tại vị trí nhà cung cấp dịch vụ sau cùng(như là một phần cơ sở hạ tầng của ISP). Mỗi một phân vùng được cấu hình và quản trị như một Router vật lý và có thể hỗ trợ một VPN. Theo cách gọi đơn giản, mỗi một phân vùng lôgic được xem như một Router với đầy đủ các chức năng của nó. Kết quả là, phân vùng Router lôgic có thể hỗ trợ nhiều giao thức và có khả năng chứa địa chỉ IP riêng.



Hình 1.4 Mô tả chung của VIPR

Với các công nghệ và giao thức không dựa trên IP như FR, ATM, công nghệ đường điện thoại riêng ảo(Virtual Private Trunking - VPT) được sử dụng. Công nghệ VPT được mô tả như trong hình 1.5.



Hình 1.5 Mô tả chung của VPT

VPT tương thích với nhiều giao thức và được dựa trên công nghệ chuyển mạch gói. Vì vậy nó sử dụng các kênh cố định ảo(Permanent Virtual Circuits - PVC) và kênh chuyển mạch ảo(Switched Virtual Circuit - SVC) cho việc truyền dữ liệu. Để truyền dữ liệu thành công, VPT yêu cầu một thiết bị WAN như một Router có khả năng hỗ trợ FR và ATM. Để chắc chắn rằng các giao dịch thương mại có lợi nhuận, các PVC thường được dùng cho việc liên kết các Site trong một mạng riêng hoặc một Intranet. SVC lại thường được dùng để liên kết các Site trong một Extranet

1.4. Cách tiếp cận cơ bản thiết kế và cài đặt VPN

Một ý tưởng và kế hoạch thiết kế tốt là yếu tố quan trọng khi thiết lập một mạng. Với bất kỳ VPN nào cũng vậy: Nếu sơ suất trong việc phân tích các yêu cầu của tổ chức sẽ kéo theo thiếu sót trong lập kế hoạch và ta sẽ thấy ảnh hưởng rất nhiều về sau.

Lúc thiết kế và thực thi mạng VPN, chúng ta cần phải tuân thủ theo ý tưởng tối ưu hoá mọi thứ.

Những vấn đề chính cần xem xét kỹ trong khi thiết kế và cài đặt VPN bao gồm:

+ Mô hình VPN nào được chọn để thực hiện?

+ Bảo mật

+ VPN sẽ được quản trị như thế nào?

+ Đánh địa chỉ và định tuyến

+ Các vấn đề liên quan đến DNS

+ Các vấn đề Router/Getway, firewall, NAT

+ Hiệu suất

+ Khả năng mở rộng và tương thích trong tương lai.

1.5. Các mô hình kết nối VPN thông dụng

Mục tiêu của công nghệ VPN là quan tâm đến ba yêu cầu cơ bản sau:

- Các nhân viên liên lạc từ xa, người dùng di động, người dùng từ xa của một Công ty có thể truy cập vào tài nguyên mạng của công ty họ bất cứ lúc nào

- Có khả năng kết nối từ xa giữa các nhánh văn phòng.

- Kiểm soát được truy cập của các khách hàng, nhà cung cấp là đối tác quan trọng đối với giao dịch thương mại của công ty.

Với các yêu cầu cơ bản như trên, ngày nay, VPN được phát triển và phân thành ba loại như sau: VPN Truy cập từ xa (Remote Access VPN), VPN Cục bộ (Intranet VPN), VPN mở rộng (Extranet VPN)

1.5.1.VPN Truy cập từ xa (Remote Access VPN):

Cung cấp các dịch vụ truy nhập VPN từ xa (remote access hay dial-up VPN) đến một mạng Intranet hay Extranet của một tổ chức trên nền hạ tầng mạng công cộng. Dịch vụ này cho phép người dùng truy xuất tài nguyên mạng của Công ty họ như là họ đang kết nối trực tiếp vào mạng đó.

Giống như tên gọi của nó, VPN truy cập từ xa cho phép người dùng từ xa, người dùng di động của một tổ chức có thể truy cập tới các tài nguyên mạng của tổng công ty. Điển hình, các yêu cầu truy cập từ xa này được đưa ra bởi người

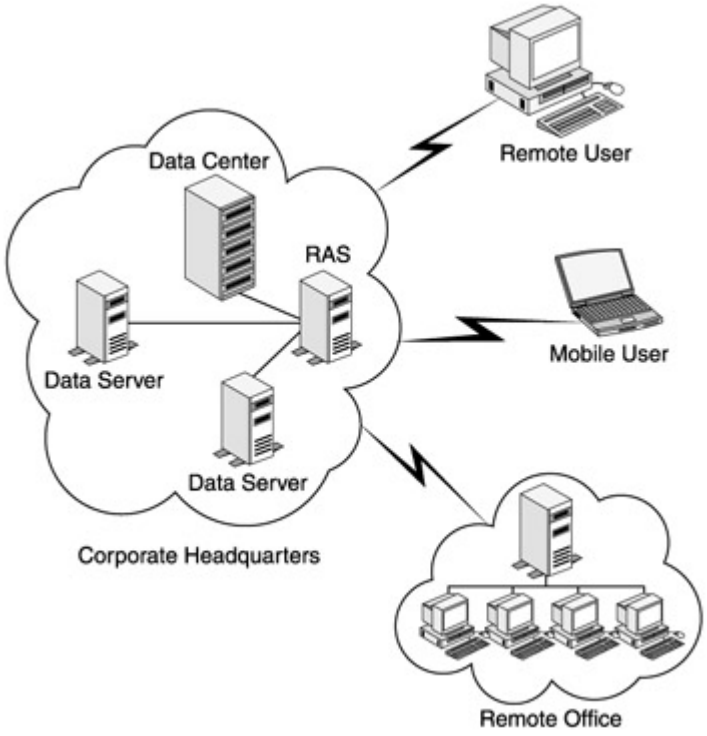
dùng đang di chuyển hoặc các nhánh văn phòng từ xa mà không có một kết nối cố định tới Intranet của tổng công ty.

Như trong hình 1.6, chuyển mạch truy cập từ xa thiết lập khi chưa có sự mở rộng của VPN bao gồm các thành phần chính như sau:

+ Một Remote Access Server: Nó được đặt tại mạng trung tâm để xác thực và cấp quyền cho các yêu cầu truy cập từ xa.

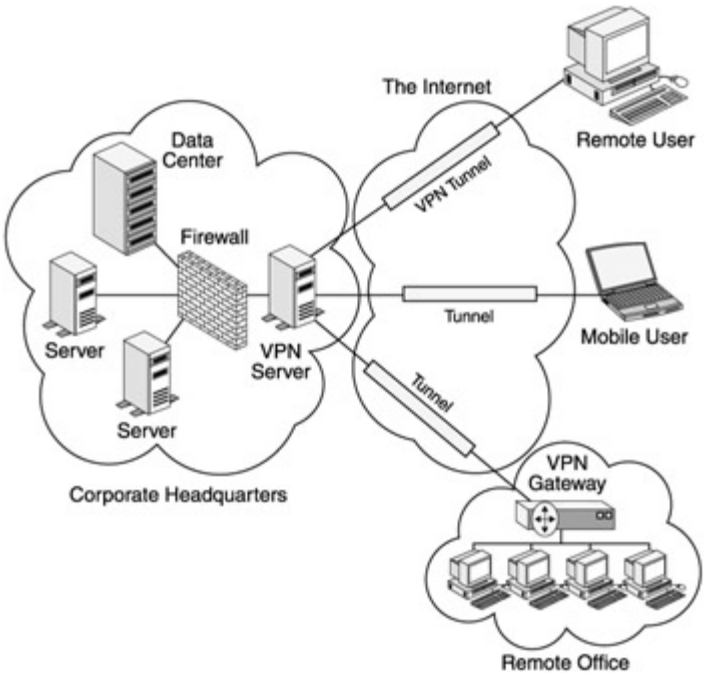
+ Kết nối Dialup tới mạng trung tâm

+ Người hỗ trợ chịu trách nhiệm cấu hình, duy trì và quản trị RAS và hỗ trợ người dùng từ xa



Hình 1.6 Thiết lập truy cập từ xa không có VPN

Bằng việc thực thi giải pháp VPN truy cập từ xa, các nhánh văn phòng và người dùng từ xa chỉ cần thiết lập kết nối Dial-up cục bộ tới ISP và thông qua đó để kết nối tới mạng của công ty qua Internet. Thiết lập VPN truy cập từ xa tương ứng được mô tả như trong hình 1.7.

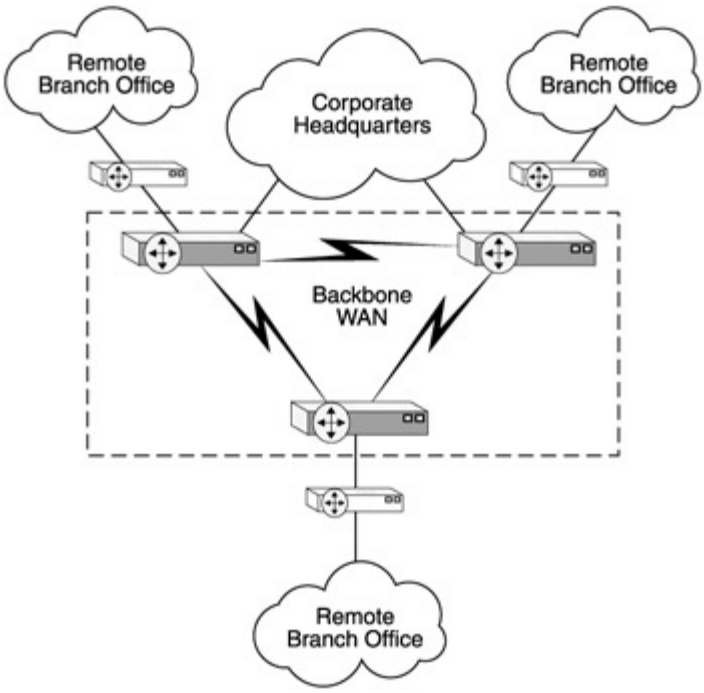


Hình 1.7 Thiết lập VPN truy cập từ xa

1.5.2. VPN Cục bộ (Intranet VPN)

Intranet VPN mở rộng các dịch vụ của mạng nội bộ tới các trụ sở ở xa, đây là một mô hình liên mạng hướng phi kết nối qua một mạng WAN dùng chung. Yêu cầu ở đây là phải thực hiện được tất cả các dịch vụ mạng đã được thực hiện ở mạng trung tâm, bao gồm các dịch vụ về an ninh, VoIP, chất lượng dịch vụ cũng như các dịch vụ đa phương tiện (Multimedia). Mục đích của Intranet VPN là giảm thời gian cũng như chi phí lắp đặt, hỗ trợ các đường dây thuê riêng theo các cách kết nối WAN truyền thống.

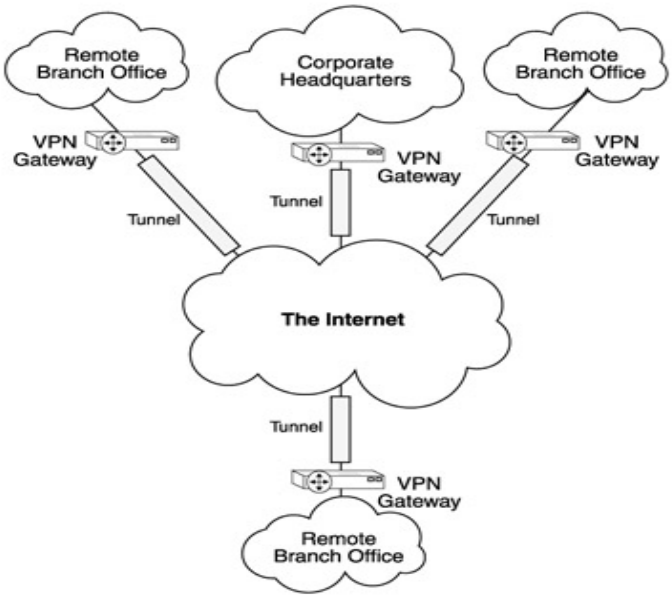
Intranet VPN thường được dùng để kết nối các nhánh Văn phòng từ xa của một tổ chức với Intranet trung tâm của tổ chức đó. Trong cách thiết lập Intranet không sử dụng công nghệ VPN, mỗi một mạng từ xa phải kết nối tới Intranet của tổ chức qua các Router trung gian. Thiết lập này được mô tả như trong hình 1.8.



Hình 1.8 Thiết lập Intranet sử dụng WAN

Thiết lập này mất chi phí rất cao vì cần ít nhất 2 Router để kết nối tới một Khu trung tâm từ xa để tới Intranet của tổ chức. Hơn nữa việc thực thi, duy trì và quản trị Intranet xương sống có thể là một việc cực kỳ tốn kém. Chẳng hạn, chi phí của Intranet toàn cầu có thể lên tới hàng ngàn USD/1 tháng. Phạm vi Intranet càng lớn thì chi phí càng cao.

Với việc thực thi giải pháp VPN, đường WAN xương sống được thay thế bằng kết nối Internet chi phí thấp nên có thể giảm được tổng chi phí của việc thực thi toàn bộ Intranet. Một giải pháp Intranet VPN điển hình được mô tả như trong hình 1.9.



Hình 1.9 Thiết lập VPN dựa trên VPN

Ưu điểm của việc thiếp lập dựa trên VPN như trong hình 1.9 là:

+ Loại trừ được các Router từ đường WAN xương sống.

+ Vì Internet hoạt động như một phương tiện kết nối, nó dễ dàng cung cấp các liên kết ngang hàng mới.

+ Vì kết nối tới các ISP cục bộ, khả năng truy cập nhanh hơn, tốt hơn. Cùng với việc loại trừ các dịch vụ đường dài giúp cho tổ chức giảm được chi phí của hoạt động Intranet.

Tuy nhiên cũng có một số nhược điểm:

+ Vì dữ liệu được định đường hầm qua một mạng chia sẽ công cộng nên các tấn công mạng như: từ chối dịch vụ vẫn đe doạ nghiêm trọng đến an ninh mạng.

+ Khả năng mất các gói dữ liệu khi truyền vẫn còn cao.

+ Đường truyền dữ liệu đầu trên như multimedia, độ trể truyền tin vẫn rất cao và thông lượng có thể bị giảm xuống rất thấp dưới sự hiện diện của Internet.

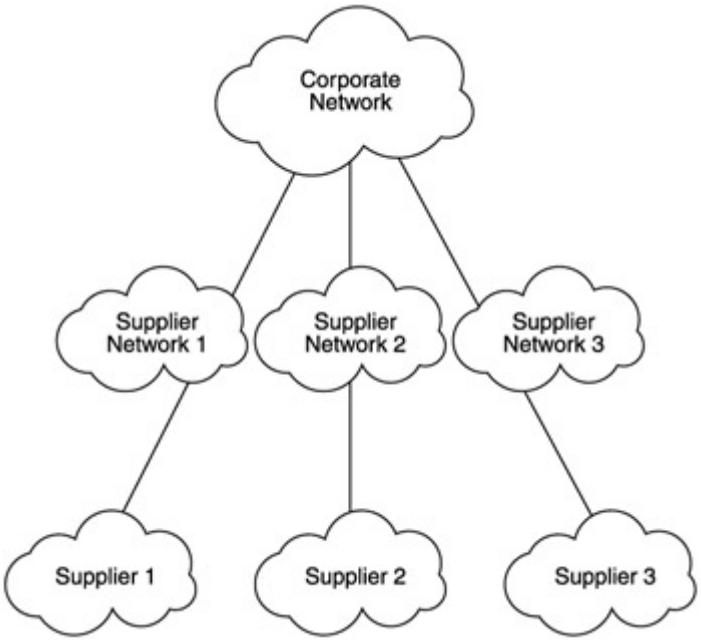
+ Vì sự hiện diện của kết nối Internet sự thực thi có thể bị gián đoạn và QoS có thể không được đảm bảo

1.5.3. Mạng riêng ảo mở rộng (Extranet VPN)

Liên kết các khách hàng, các nhà cung cấp, hay cộng đồng người sử dụng vào mạng Intranet của một tổ chức trên nền hạ tầng mạng công cộng sử dụng các đường truyền thuê bao. Giải pháp này cũng cung cấp các chính sách như trong mạng riêng của một tổ chức như đảm bảo tính bảo mật, tính ổn định. Tương tự như Intranet VPN, Extranet VPN cũng có kiến trúc tương tự, tuy nhiên điểm khác biệt giữa chúng là phạm vi các ứng dụng cho phép các đối tác Extranet VPN sử dụng. So với Intranet VPN thì vấn đề tiết kiệm chi phí không rõ bằng nhưng điều quan trọng là khả năng cộng tác với các đối tác, khách hàng hay các nhà cung cấp sản phẩm. Việc để cho khách hàng nhập trực tiếp dữ liệu về các hợp đồng vào hệ thống sẽ tiết kiệm được rất nhiều thời gian cũng như các lỗi không đáng có, tuy nhiên việc này rất khó thực hiện với công nghệ WAN truyền thống. Extranet VPN thường sử dụng các kết nối dành riêng và thêm vào các lớp bảo mật để xác thực và giới hạn truy nhập trên hệ thống.

Không giống như Intranet VPN và Remote Access VPN. Extranet VPN không hẳn có nghĩa là “Xa hơn ngoài phạm vi”. Thực tế, Extranet VPN cho phép kiểm soát truy cập các tài nguyên mạng cần thiết với toàn bộ giao dịch thương mại mở rộng như: đối tác, khách hàng, nhà cung cấp

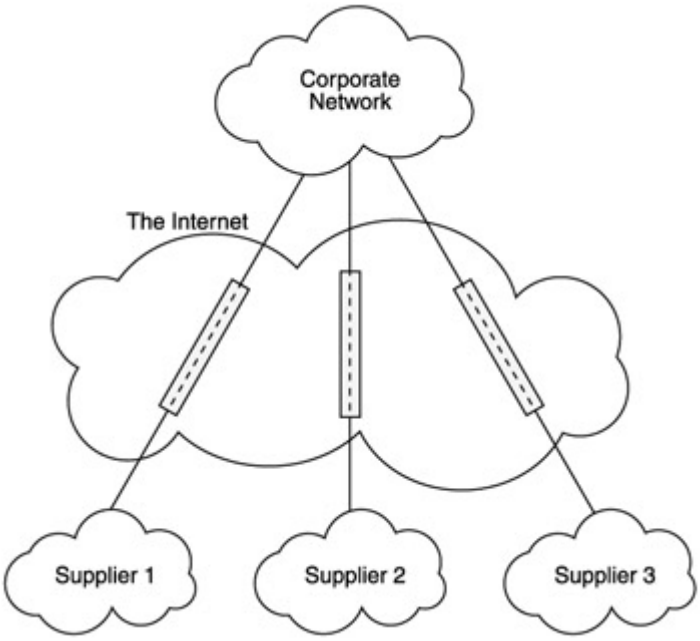
Theo cách thức truyền thống, kết nối Extranet được thể hiện như trong hình 1-10



Hình 1.10 Mạng Extranet truyền thống

Theo cách này chi phí cực đắt vì mỗi mạng riêng trong trong Intranet phải hoàn toàn thích hợp với mạng mở rộng. Đặc điểm này dẫn đến sự phức tạp trong việc quản trị và thực thi của các mạng khác nhau. Hơn nữa rất khó mở rộng vì làm như vậy có thể phải thay đổi toàn bộ mạng Intranet và có thể ảnh hưởng đến các mạng mở rộng đã kết nối khác và đây có thể là một cơn ác mộng đối với các nhà thực thi và quản trị mạng.

Thực thi giải pháp VPN làm cho công việc thiết lập một Extranet trở nên dễ dàng và giảm chi phí đáng kể.



Hình 1.11 Mạng Extranet dựa trên VPN

Ưu điểm chính của Extranet VPN là:

+ Chi phí rất nhỏ so với cách thức truyền thống.

+ Dễ thực thi, duy trì và dễ thay đổi

+ Dưới sự hiện diện của Internet, ta có thể chọn các đại lý lớn

+ Vì một phần kết nối Internet được duy trì bởi ISP nên số lượng nhân viên hỗ trợ có thể giảm xuống.

Tuy nhiên cũng có một số nhược điểm:

+ Các nguy cơ an ninh như tấn công DOS vẫn còn tồn tại

+ Tăng rủi ro vì các xâm nhập vào Intranet của tổ chức

+ Độ trễ truyền thông vẫn lớn và thông lượng bị giảm xuống rất thấp với các ứng dụng Multimedia.

+ Sự thực thi có thể bị gián đoạn và QoS cũng có thể không được bảo đảm

Tuy có một số nhược điểm như đã mô tả, nhưng các ưu điểm của giải pháp VPN vẫn vượt trội, "Mạng riêng ảo - ưu thế của công nghệ, chi phí và bảo mật"

1.6. Các công nghệ và các chính sách an toàn Mạng riêng ảo

1.6.1. Sự cần thiết của chính sách an toàn Mạng

Chính sách an toàn mạng có vai trò quan trọng trong việc bảo mật của một tổ chức và từng bước được vận dụng để thực thi bảo mật mạng. Không có một sản phẩm hay một giải pháp chuẩn chung cho một chính sách an toàn mạng. Nó thường được tạo ra và thực thi theo yêu cầu cụ thể của từng tổ chức.

Một chính sách an toàn mạng thể hiện tầm nhìn của Công ty về cách thức sử dụng máy tính và cơ sở hạ tầng mạng để cung cấp các dịch vụ tốt nhất và nâng cao hiệu suất. Nó cũng phác thảo các thủ tục cần dùng để đối phó với các nguy cơ bảo mật, các vi phạm bảo mật.

Một chính sách an toàn làm cho khả năng đối phó với các rủi ro, các nguy cơ bảo mật trong một Công ty sẽ tốt hơn. Hơn nữa, không thể thực thi bảo mật nếu ta không xác định được cần bảo vệ cái gì.

Vì vậy cần có một chính sách bảo mật. Đó là một danh sách những gì sẽ được phép và không được phép, dựa vào đó để quyết định về bảo mật. Ta cũng có thể hình dung nó như là một tập các luật để quản lý người dùng truy cập tài nguyên của công ty, một thoả thuận chung để mọi người chấp nhận và tuân theo các luật đó.

Một chính sách an toàn mạng toàn diện của Công ty phải được xác định theo sự phân tích các yêu cầu thương mại và phân tích bảo mật. Các vấn đề sau đây sẽ cung cấp cho ta một số nguyên tắc chung:

+ Những người nào mà chúng ta muốn ngăn chặn?

+ Người dùng từ xa cần truy cập đến hệ thống và mạng của chúng ta hay không?

+ Hệ thống có chứa thông tin mật hoặc nhạy cảm không?

+ Phân loại các thông tin mật hoặc nhạy cảm như thế nào?

+ Mật khẩu hoặc mã hoá có đủ bảo vệ không?

+ Chúng ta có cần truy cập Internet hay không?

+ Bao nhiêu truy cập tới hệ thống của ta từ Internet hoặc những người dùng bên ngoài mạng(như: các đối tác thương mại, nhà cung cấp,…) mà ta muốn cho phép?

+ Hành động nào ta sẽ thực hiện nếu phát hiện sự vi phạm bảo mật?

+ Những ai trong Công ty của ta sẽ phải tuân thủ và giám sát chính sách này?

Đó là những nguyên tắc mang tính định hướng chung cho việc thiết lập và thực hiện một chính sách an toàn mạng.

1.6.2. Chính sách an toàn mạng

Nếu hệ thống của ta có kết nối Internet thì rất có thể phải đương đầu với nhiều nguy cơ tấn công tiềm ẩn. Gateway hoặc Firewal là những hệ thống bảo vệ tốt, tuy nhiên cần phải lưu ý rằng:

+ Gateway không nên chạy nhiều ứng dụng hơn mức cần thiết vì các ứng dụng có những khiếm khuyết có thể bị khai thác.

+ Gateway nên hạn chế tối đa các loại và số lượng giao thức được cho phép đi qua nó hoặc các kết nối Terminate tại gateway từ bên ngoài, vì các giao thức cũng có thể tiềm ẩn nhiều lỗ hổng bảo mật.

+ Bất kỳ một hệ thống nào có chứa thông tin mật hoặc nhạy cảm đều không nên cho phép truy cập trực tiếp từ bên ngoài.

+ Tất cả các dịch vụ trong một Intranet thuộc Công ty nên tối thiểu việc yêu cầu xác thực mật khẩu và kiểm soát truy cập thích hợp.

+ Truy cập trực tiếp từ bên ngoài luôn phải được xác thực và kiểm toán

Chính sách an toàn mạng xác định các dịch vụ sẽ được cho phép hoặc bị từ chối, cách thức các dịch vụ này sẽ được sử dụng và là ngoại lệ với các luật này. Mỗi luật trong chính sách an toàn mạng nên được thực thi trên một firewall hoặc RAS. Và chính sách an toàn mạng của một công ty phải trả lời được các câu hỏi sau:

+ Những ai được truy cập vào mạng của Công ty? Những Client, đối tác, khách hàng nào được cung cấp truy cập tới mạng của Công ty?

+ Những ai có thể kết nối tới mạng mở rộng, như của Client hay các đối tác.

+ Những ai có thể truy cập Internet từ mạng của Công ty?

+ Lúc nào thì tài khoản của một người dùng sẽ bị xoá?

+ Phải bảo mật các máy tính như thế nào trước khi chúng ở trong mạng có truy cập Internet không được bảo vệ.

+ Người dùng có thể tuỳ tiện tải các chương trình từ Internet hay không?

+ Kiểu mật khẩu nhân viên phải dùng là gì? Và có thường phải thay đổi hay không?

+ Các máy tính của người dùng từ xa, người dùng di động được bảo mật như thế nào? Họ phải làm gì để có thể truy cập an toàn tới mạng của công ty.

+ Những thông tin mật nào cần được bảo vệ? Có quy tắc lưu trữ các loại thông này hay không?

1.6.3. Chính sách an toàn Mạng riêng ảo

Trong khi một chính sách an toàn mạng truyền thống xác định luồng thông tin nào bị từ chối và luồng thông tin nào được phép đi qua, một chính sách bảo mật VPN mô tả các đặc tính của việc bảo vệ hiện trạng luồng thông tin. Theo một nghĩa nào đó, nó là một tập con của chính sách an toàn mạng , vì nó chỉ cô đọng hơn và phụ thuộc vào vấn đề cho phép luồng thông tin giữa các đích nào đó trước khi nó có thể được bảo vệ.

Một chính sách an toàn VPN mô tả hiện trạng luồng thông tin riêng được bảo vệ (nguồn, đích, các giao thức, các cổng) và các yêu cầu bảo mật (xác thực, mã hoá, độ dài khoá, quản lý khoá…). Chính sách an toàn VPN có thể được định nghĩa trên thiết bị, tuy nhiên nên được thực thi trong một thư mục tập trung để cung cấp sự quản lý và mở rộng tốt hơn. Về cơ bản, các thiết bị cần phải có các chính sách phù hợp với việc mô tả dòng lưu lượng trước khi nó được phép đi vào các thiết bị.

Trong khi thực hiện VPN cần lưu ý:

+ Chỉ có một kết nối mạng được cho phép.

+ VPN phải được thiết lập và quản trị bởi các nhóm quản trị của Công ty

+ Tất cả các máy kết nối tới mạng trong của công ty qua VPN phải dùng phần mềm Virus và cập nhật thường xuyên để quét

+ Người dùng VPN sẽ bị tự động ngắt kết nối nếu không có hoạt động gì sau một khoảng thời gian nhất định(chẳng hạn: sau 30 phút).

Câu hỏi ôn tập

1. Mạng riêng ảo là gì? Nêu một số ví dụ về Mạng riêng ảo?

2. Ba loại mô hình VPN là: _____, _____, và _____.

a. Intranet
b. Internet
c. Extranet
d. Remote Access

3. Khi tiếp cận cách thiết kế và thực hiện VPN cần xem xét những vấn đề nào?

4. Thuật ngữ RAS là viết tắt của: _____.

a. Remote Access Standard
b. Remote Access Storage
c. Remote Access Server
d. Remote Access Subsystem

5. Chọn câu đúng trong các câu sau đây?

a. Intranet VPNs là độc lập với một WAN router Backbone
b. Extranets VPN là giải pháp chi phí cao hơn và phức tạp hơn
c. QoS không thể được đảm bảo trong một Intranet VPNs

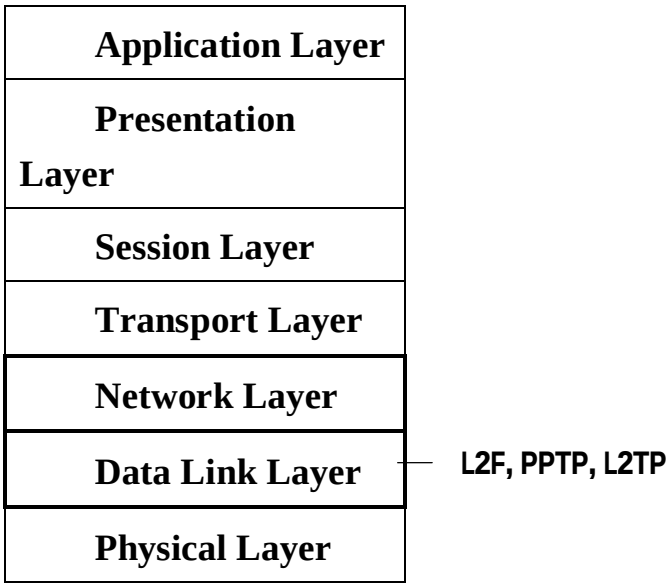
6. Sự cần thiết của chính sách an toàn mạng

7. Nêu các nguyên tắc chung cho việc thiết lập chính sách an toàn mạng?

8. Chính sách an toàn mạng riêng ảo cần quan tâm đến những vấn đề nào?

Chương 2. Giao thức mạng riêng ảo tại tầng 2

Trong chương này chúng ta thảo luận các giao thức cho phép một kết nối tại tầng 2, điển hình như PPP được định đường hầm qua một mạng khác, điển hình như mạng IP. Điều này giống như một phương pháp phức tạp kéo theo nhiều overhead(phần thông tin phụ thêm được đưa vào), nhưng một số lợi ích nhận được từ phương pháp này rất hữu dụng cho việc xây dựng VPN. Chúng ta sẽ thấy rằng các giao thức đường hầm này là cơ sở để xây dựng VPN và bảo mật các giao dịch qua VPN. Một số giao thức đường hầm được thực hiện tại tầng 2 - tầng liên kết dữ liệu - của mô hình OSI, như được mô tả trong hình 2.1



Hình 2.1 Vị trí các giao thức đường hầm tầng 2 trong mô hình OSI

Các giao thức này bao gồm: Giao thức đường hầm điểm - điểm (*PPTP*), Giao thức chuyển tiếp lớp 2 (*L2F*), Giao thức đường hầm lớp 2 (*L2TP*).

2.1. Giao thức PPP

PPP là một giao thức đóng gói làm cho khả năng vận chuyển lưu lượng của mạng qua một loạt các điểm liên kết được thực hiện một cách dễ dàng. Thuận lợi lớn nhất của PPP là nó có thể điều khiển bất kỳ DTE hoặc DCE nào bao gồm: EIA/TIA-232-C và ITU-T V.35. Một điểm ưa thích của PPP là nó không hạn chế tỷ lệ truyền dữ liệu. Trong khi truyền dữ liệu bị hạn chế bởi giao diện DTE/DCE đang dùng.

Cuối cùng, chỉ yêu cầu của PPP là sẵn sàng với các kết nối kép (2 cách). Nó có thể là đồng bộ hoặc không đồng bộ và có thể điều khiển cả các Switch hay các mode chuyên dụng.

Ngoài việc đóng gói các dữ liệu theo giao thức IP, không theo giao thức IP và việc truyền nó qua một loạt các điểm liên kết, PPP cũng chịu trách nhiệm về các chức năng sau:

- Chỉ định và quản trị các gói IP thành các gói không IP.

- Cấu hình và kiểm tra các liên kết đã thiết lập.

- Đồng bộ và không đồng bộ việc đóng gói các gói dữ liệu.

- Phát hiện lỗi trong khi truyền dữ liệu.

- Dồn kênh các giao thức mạng lớp hai.

- Thoả thuận các tham số không bắt buộc như nén dữ liệu và đánh địa chỉ.

PPP thực hiện các chức năng này theo ba chuẩn:

- Chuẩn đóng gói dữ liệu qua liên kết điểm - điểm.

- Chuẩn thiết lập, cấu hình và kiểm tra kết nối điểm - điểm với sự hỗ trợ của giao thức kiểm soát liên kết(Link Control Protocol – LCP).

- Chuẩn thiết lập, cấu hình các giao thức mạng khác nhau và phát hiện lỗi trong khi truyền theo dạng của giao thức kiểm soát mạng (Network Control Protocol - NCP) thích hợp.

2.1.1. Quá trình thực hiện PPP

Giao thức PPP được sử dụng để đóng gói các gói tin thành các khung PPP và gửi dữ liệu trên các kết nối điểm - điểm. Có năm bước cần tiến hành trong quá trình thương lượng kết nối PPP, đó là:

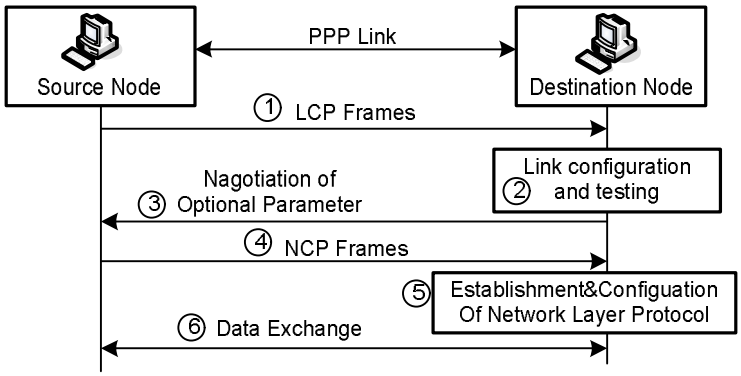
1. Sau khi các gói dữ liệu đã được đóng gói, Node nguồn (hoặc khởi tạo) gửi khung LPC qua kết nối điểm - điểm tới Node đích.

2. Các tham số này thường được dùng để cấu hình liên kết bằng việc chỉ rõ các tham số và kiểm tra liên kết đã được thiết lập.

3. Sau khi Node đích chấp nhận yêu cầu kết nối và một liên kết được thiết lập thành công, các tham số lựa chọn được thương lượng nếu đã chỉ rõ bởi các LCP.

4. Node nguồn sau đó gửi khung NCP để lựa chọn và cấu hình giao thức tầng mạng.

5. Sau khi giao thức tầng mạng yêu cầu được cấu hình thì cả hai bắt đầu trao đổi dữ liệu.



Hình 2.2 Thiết lập liên kết PPP và trao đổi dữ liệu

Khi một liên kết PPP đã được thiết lập, nó tồn tại cho đến khi LCP hoặc NCP ra hiệu kết thúc liên kết. Liên kết cũng có thể được kết thúc trong trường hợp nó bị lỗi hoặc người dùng can thiệp vào.

2.1.2. Định dạng gói PPP

Sáu trường tạo thành khung PPP, như minh hoạ trong hình 2.3. Mô tả của các trường cấu tạo thành khung PPP như sau:

Flag: Trường này xác định điểm bắt đầu và kết thúc của một khung. Độ dài của trường này là 1 byte.

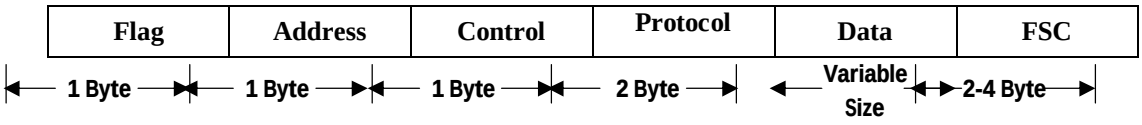
Address: Vì nó sử dụng các liên kết điểm - điểm. PPP không sử dụng các địa chỉ của các Node riêng lẻ. Vì thế, các trường này chứa chuỗi nhị phân là 11111111, đây là một địa chỉ Broadcast chuẩn. Độ dài của trường này là 1 byte.

Control: Trường này chứa chuỗi nhị phân là 00000011. Nó biểu thị rằng, Frame đang mang dữ liệu người dùng là một Frame không tuần tự. Độ dài của trường này là 1 byte.

Protocol: Trường này xác định giao thức mà dữ liệu được đóng gói trong trường dữ liệu của Frame. Giao thức trong trường này được chỉ rõ theo số đã gán trong RFC 3232. Độ dài của trường này là 2 byte. Tuy nhiên, trường này có thể thương lượng để là 1 byte nếu cả hai đồng ý.

Data: Trường này chứa thông tin đang được trao đổi giữa Node nguồn và đích. Độ dài của trường này có thay đổi, độ dài tối đa có thể lên đến 1500 byte.

FCS: Trường này chứa chuỗi kiểm tra giúp người nhận kiểm tra tính chính xác của thông tin đã nhận trong trường dữ liệu. Thông thường, độ dài của trường này là 2 byte. Tuy nhiên, việc thực thi PPP có thể thương lượng một FCS 4 byte để cải thiện việc phát hiện lỗi.



Hình 2.3 Định dạng của một Frame PPP điển hình

2.1.2. Kiểm soát liên kết PPP

Ngoài việc trao đổi thành công dữ liệu giữa hai Node, PPP cũng chịu trách nhiệm kiểm soát liên kết đã thiết lập giữa 2 thực thể truyền thông cuối. PPP sử dụng LCP cho chức năng này, trong đó LCP chịu trách nhiệm về các chức năng sau:

- Hỗ trợ việc thiết lập liên kết.

- Cấu hình liên kết đã thiết lập để thoả mãn các yêu cầu của các nhóm truyền thông.

- Duy trì hiệu suất của liên kết PPP đã thiết lập.

- Kết thúc liên kết nếu việc trao đổi dữ liệu giữa hai thực thể cuối đã hoàn tất.

LCP dựa trên kiểm soát liên kết gồm bốn pha: Thoả thuận và khởi tạo liên kết; Xác định chuẩn liên kết; Thoả thuận giao thức tầng mạng.

Sau đây ta sẽ mô tả chi tiết bốn pha trong kiểm soát liên kết.

- Thoả thuận và khởi tạo liên kết: Trước khi việc trao đổi dữ liệu dựa trên PPP giữa Node nguồn và đích được cho phép, LCP phải khởi tạo một kết nối giữa hai thực thể cuối và thoả thuận các tham số cấu hình. LCP sử dụng các Frame khởi tạo liên kết cho chức năng này. Khi mỗi thực thể cuối phản hồi lại bằng Frame cấu hình ACK của nó, pha này kết thúc.

- Xác định tiêu chuẩn liên kết: Đây là pha tuỳ chọn trong đó tiêu chuẩn của liên kết đã thiết lập được xác định cho các liên kết khác nhau đã sẵn sàng cho việc thoả thuận các giao thức tầng mạng.

- Thoả thuận giao thức tầng mạng: Trong pha này, ưu tiên giao thức tầng mạng của dữ liệu đã được đóng gói trong trường Protocol của Frame PPP được thoả thuận.

- Kết thúc liên kết: Đây là pha cuối cùng của LCP và Server để kết thúc liên kết đã thiết lập giữa hai thực thể cuối. Việc kết thúc liên kết có thể theo trình tự hoặc đột xuất. Kết thúc đúng trình tự là kết thúc sau khi việc trao đổi dữ liệu giữa hai thực thể cuối đã hoàn tất hay do yêu cầu của thực thể cuối. Kết thúc liên kết đột xuất có thể làm mất dữ liệu. Frame kết thúc liên kết dữ liệu được trao đổi giữa các nhóm có liên quan trước khi liên kết được giải phóng.

Ngoài Frame thiết lập và kết thúc liên kết, PPP sử dụng một loại Frame thứ ba gọi là Frame duy trì liên kết. Các Frame này như tên gọi của nó, được trao đổi trong trường hợp có vấn đề liên quan đến liên kết, thường được dùng để quản trị và debug các liên kết dựa trên PPP.

Mặc dù không được dùng trong VPN ngày nay, tuy nhiên công nghệ PPP là cơ sở của các giao thức đường hầm khác được dùng rộng khắp trong VPN ngày nay. Thực tế, tất cả các giao thức đường hầm thông dụng đều dựa trên PPP và đóng gói Frame PPP vào trong gói IP hoặc các gói dữ liệu khác để truyền qua mạng không đồng nhất.

2.2. Các giao thức đường hầm tại tầng 2 trong mô hình OSI

2.2.1. Giao thức đường hầm điểm (PPTP)

PPTP là giải pháp độc quyền cho phép truyền dữ liệu một cách an toàn giữa một Client từ xa và một Server của Doanh nghiệp bằng việc tạo ra một VPN qua một mạng dựa trên IP. Được phát triển bởi Consortium PPTP (Tập đoàn Microsoft, Ascend Communications, 3COM, US Robotics,và ECI Telematics). PPTP đề xuất dựa vào yêu cầu của VPN qua mạng không an toàn. PPTP không chỉ có khả năng bảo mật các giao dịch qua các mạng công cộng dựa trên TCP/IP mà còn cả các giao dịch qua mạng Intranet riêng.

Về phương diện lịch sử, hai hiện tượng đóng vai trò chính vào sự thành công của PPTP trong việc bảo mật các kết nối đường dài là:

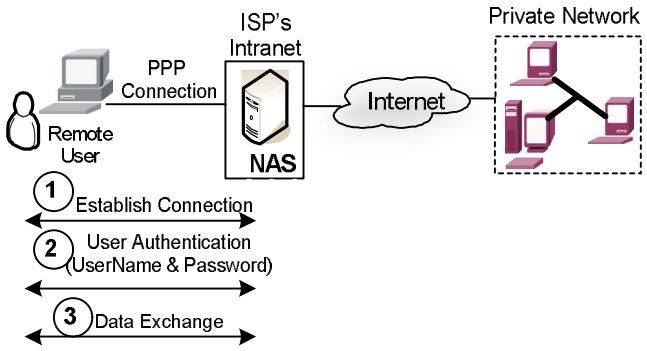
- Việc sử dụng các Mạng điện thoại chuyển mạch công cộng(PSTN): PPTP cho phép sử dụng PSTN(**Public Switched Telephone Network)** để thực thi VPN. Kết quả là, qúa trình triển khai VPN đơn giản đi rất nhiều và tổng chi phí thực thi giảm một cách đáng kể. Lý do này hoàn toàn dễ hiểu – vì những yếu tố cần thiết cho giải pháp kết nối doanh nghiệp quy mô rộng dựa trên đường Leased Line và các Server truyền thông chuyên dụng hoàn toàn bị loại bỏ.

- Hỗ trợ các giao thức không dựa trên IP: Mặc dù dành cho các mạng dựa trên IP, PPTP cũng hỗ trợ các giao thức mạng khác như: TCP/IP, IPX, NetBEUI, và NetBIOS. Vì vậy, PPTP đã chứng tỏ là thành công trong việc triển khai VPN qua một mạng LAN riêng cũng như qua mạng công cộng.

PPP đóng vai trò chính trong các giao dịch dựa trên PPTP. Ta sẽ thảo luận chi tiết hơn vấn đề này trong phần tiếp sau đây.

2.2.1.1. Vai trò của PPP trong các giao dịch PPTP

PPTP là một sự mở rộng logic của PPP, PPTP không thay đổi dưới công nghệ PPP, nó chỉ định nghĩa một cách vận chuyển lưu lượng PPP mới qua các mạng công cộng không an toàn.



Hình 2.4 Mô tả vai trò của PPP trong các giao dịch dựa trên PPTP

Khá giống PPP, PPTP không hỗ trợ nhiều kết nối. Tất cả các kết nối được hỗ trợ bởi PPTP phải là kết nối điểm - điểm, ngoài ra, PPP đáp ứng các chức năng sau trong giao dịch dựa trên PPTP:

- Thiết lập và kết thúc các kết nối vật lý giữa các thực thể truyền thông cuối.

- Xác thực các Client PPTP.

- Mã hoá các gói dữ liệu IPX, NetBEUI, NetBIOS, và TCP/IP để tạo các gói PPP và bảo mật việc trao đổi dữ liệu giữa các nhóm liên quan.

2.2.1.2. Các thành phần của giao dịch PPTP

Bất kỳ một giao dịch dựa trên PPTP nào cũng gồm ít nhất 3 thành phần, các thành phần này bao gồm:

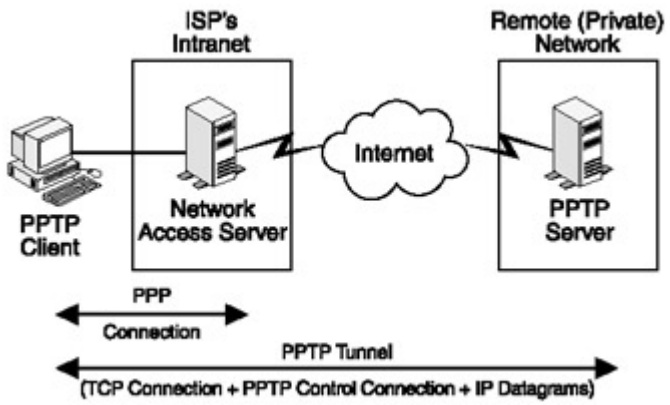
- Một Client PPTP.

- Một Server truy cập mạng (Network Access Server - NAS).

- Một Server PPTP.

1. PPTP Client

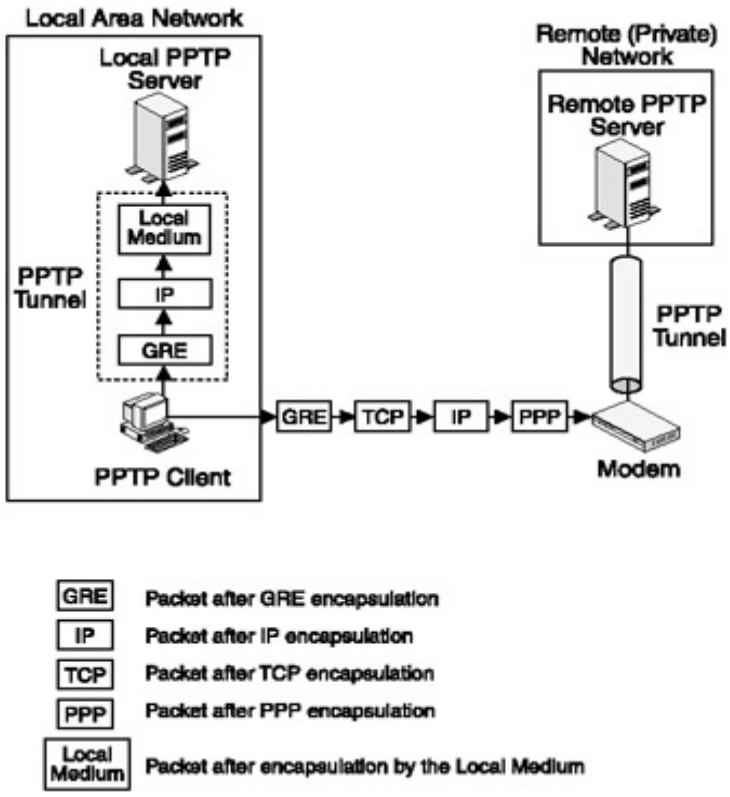
Một PPTP Client là một Node mạng hỗ trợ PPTP và có yêu cầu đến Node khác cho một phiên VPN. Nếu kết nối được yêu cầu từ một Server từ xa, PPTP Client phải sử dụng các dịch vụ trên NAS của ISP. Vì thế, PPTP Client phải được kết nối tới một Modem, cái thường được dùng để thiết lập một kết nối quay số PPP tới ISP.



Hình 2.5 Đường hầm PPTP và ba thành phần của giao dịch dựa trên PPTP

PPTP Client cũng phải được kết nối tới một thiết bị VPN và như vậy nó có thể định đường hầm yêu cầu tới thiết bị VPN trên mạng từ xa. Liên kết đến thiết bị VPN từ xa trước hết sử dụng kết nối quay số tới NAS của ISP để thiết lập một đường hầm giữa các thiết bị VPN qua Internet hoặc qua mạng trung gian khác.

Không giống như yêu cầu từ xa cho phiên VPN, yêu cầu cho một phiên VPN tới Server cục bộ không đòi hỏi một kết nối tới NAS của ISP. Cả Client và Server đều được kết nối vật lý đến cùng một mạng LAN, việc tạo ra một kết nối tới NAS của nhà cung cấp là không cần thiết. Client trong trường hợp này chỉ cần yêu cầu một phiên quay số đến thiết bị VPN trên Server. Như vậy thủ tục định tuyến của các gói PPTP cho một yêu cầu từ xa và một yêu cầu cục bộ là khác nhau, các gói của hai yêu cầu được xử lý khác nhau. Các gói PPTP đến Server cục bộ được đặt trên thiết bị vật lý gắn kèm với card mạng của PPTP Client. Gói PPTP đến Server từ xa được định tuyến qua một thiết bị vật lý gắn với một thiết bị truyền thông như một Router. Tất cả được minh hoạ như trong hình 2.6.



Hình 2.6 Truyền các gói PPTP đến Node đích

2. Các Server PPTP

Server truy cập PPTP là một Node mạng có hỗ trợ PPTP và có khả năng bảo quản các yêu cầu cho phiên VPN từ các Node từ xa hay cục bộ. Để phản hồi các yêu cầu từ xa, các Server này cũng phải hỗ trợ khả năng định tuyến. Một RAS và hệ điều hành mạng khác có hỗ trợ PPTP, chẳng hạn WinNT 4.0 có khả năng hoạt động như một Server PPTP.

3. Các Server truy cập mạng PPTP (PPTP NAS)

Các NAS PPTP được đặt tại Site PPTP và cung cấp kết nối Internet tới các Client đang sử dụng đường quay số PPP. Xác suất nhiều Client cùng đồng thời yêu cầu một phiên VPN là rất cao.

Các Server này phải có khả năng hỗ trợ các Client này. Ngoài ra, các PPTP Client không chỉ hạn chế với hệ điều hành mạng của Microsoft, vì vậy các NAS PPTP phải có khả năng hỗ trợ các Client dựa trên Window, các máy Unix. Tuy nhiên, điều quan trọng là các Client này hỗ trợ kết nối PPTP tới NAS.

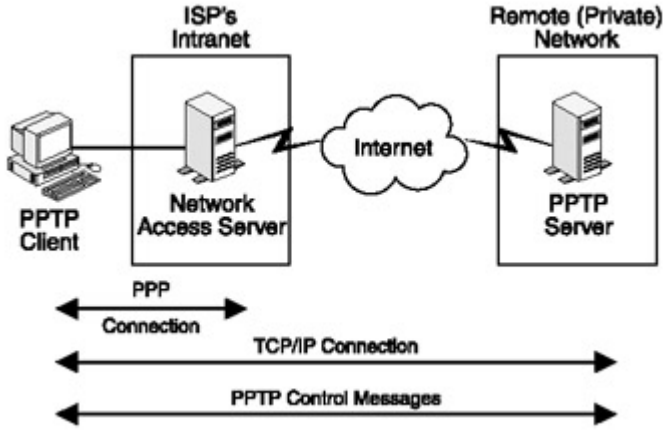
2.2.1.3. Các tiến trình PPTP

Bao gồm ba tiến trình để truyền thông an toàn dựa trên PPTP qua phương tiện không an toàn. Ba tiến trình đó là:

Thiết lập kết nối dựa trên PPP. Kiểm soát kết nối. Tạo đường hầm PPTP và truyền dữ liệu.

1. Kiểm soát kết nối PPTP

Sau khi một kết nối vật lý dựa trên PPP được thiết lập giữa PPTP Client và Server, quá trình kiểm soát kết nối PPTP bắt đầu. Như trong hình 2.7, Kiểm soát kết nối PPTP được thiết lập dựa trên địa chỉ IP của PPTP Client và Server. Nó sử dụng cổng TCP phân phối động và cổng TCP giành riêng số 1723. Sau khi kiểm soát kết nối được thiết lập, nó thực hiện việc kiểm soát và quản lý các thông điệp được trao đổi giữa các nhóm truyền thông. Các thông điệp này có nhiệm vụ duy trì, quản lý và kết thúc đường hầm PPTP. Các thông điệp này bao gồm cả chu kỳ giao dịch của các thông điệp "PPTP-Echo-Request, PPTP-Echo-Reply" chúng giúp phát hiện lỗi kết nối giữa PPTP Server và Client.



Hình 2.7 Các thông điệp kiểm soát trao đổi dữ liệu PPTP qua PPP

Một số thông điệp thường dùng để kiểm soát PPTP được liệt kê trong bảng sau đây:

Bảng 2.1 Các thông điệp kiểm soát PPTP thông dụng

Name	Description
Start-Control-Connection-Request	Yêu cầu từ PPTP Client để thiết lập kết nối

Start-Control-Connection-Reply	Phản hồi từ PPTP server tới thông điệp Start-Control-Connection-Request của Client
Outgoing-Call-Request	Yêu cầu từ PPTP client tới server để thiết lập một đường hầm PPTP.
Outgoing-Call-Reply	Phản hồi từ PPTP server tới thông điệp Outgoing-Call-Request của Client.
Echo-Request	Cơ chế duy trì hoạt động từ Server hoặc Client. Nếu nhóm đối diện không trả lời thông điệp này thì đường hầm bị kết thúc.
Echo-Reply	Phản hồi tới thông điệp Echo-Request từ thực thể cuối đối diện.
Set-Link-Info	Thông điệp từ phía khác tới thiết lập các lựa chọn liên quan đến PPP.
Call-Clear-Request	Thông điệp từ PPTP client bắt đầu kết thúc đường hầm.
Call-Disconnect-Notify	Phản hồi từ PPTP server tới Call-Clear-Request của Client. Nó cũng là thông điệp khởi tạo việc kết thúc đường hầm từ Server
WAN-Error-Notify	Thông điệp từ PPTP server đến tất cả các PPTP Client đã kết nối để thông báo lỗi trong giao diện PPP của server.
Stop-Control-Connection-Request	Thông điệp từ PPTP client hoặc server để thông báo đến thực thể cuối khác để kết thúc kiểm soát kết nối.
Stop-Control-Connection-Reply	Phản hồi từ thực thể cuối bên kia tới thông điệp Stop-Control-Connection-Request.

Như đã mô tả trong hình 2.8, các thông điệp kiểm soát PPTP được đóng gói vào trong các gói TCP. Vì vậy, sau khi đã thiết lập một kết nối PPP với Server hoặc Client từ xa, một kết nối TCP được thiết lập. Kết nối này sau đó thường được dùng để trao đổi các thông điệp kiểm soát PPTP.

Data Link Header	***IP Header***	**TCP Header**	**TCP**	**PPTP Control Message**	**Data Link Trailer**

Hình 2.8 Kiểm soát PPTP trong gói dữ liệu TCP

2. Xử lý và định đường hầm dữ liệu PPTP

Một gói dữ liệu PPTP phải trải qua nhiều giai đoạn đóng gói. Đó là các giai đoạn sau:

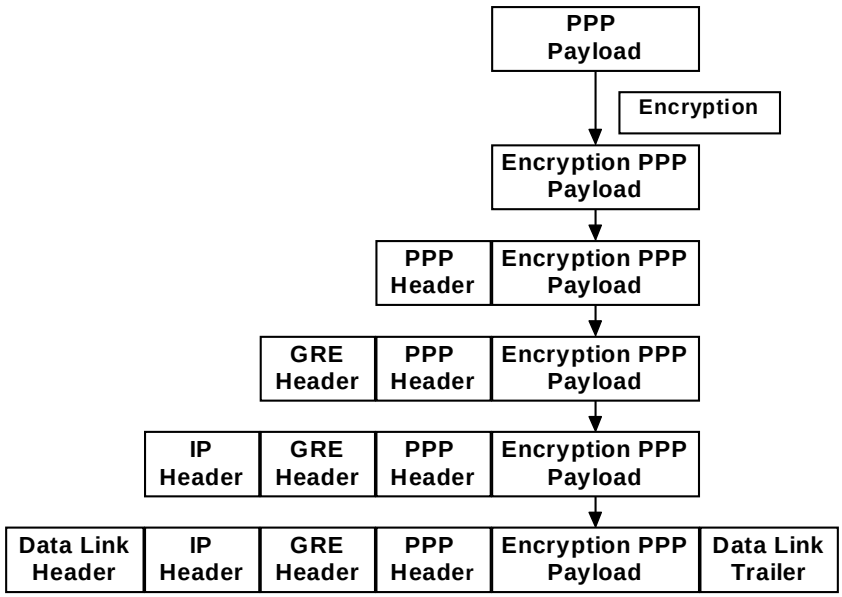
Bao gói dữ liệu: Thông tin gốc được mã hoá và sau đó bao gói vào bên trong một Frame PPP. Một tiêu đề PPP được thêm vào Frame.

Bao gói Frame PPP: Frame PPP kết quả sau đó được bao gói vào trong một sự đóng gói định tuyến chung(GRE) đã sửa đổi. Tiêu đề GRE sửa đổi chứa một trường ACK 4 byte và một bit ACK tương ứng thông báo sự có mặt của trường

ACK. Hơn nữa, trường khoá trong frame GRE được thay bởi một trường có độ dài 2 byte gọi là độ dài tải và một trường có độ dài 2 byte gọi là định danh cuộc gọi. PPTP client thiết lập các trường này khi nó tạo đường hầm PPTP.

Bao gói các gói dữ liệu GRE: Tiếp theo, một tiêu đề IP được thêm vào khung PPP, và được bao gói vào trong gói GRE. Tiêu đề IP này chứa địa chỉ IP của PPTP client nguồn và PPTP Server đích.

Bao gói tầng liên kết dữ liệu: Như chúng ta đã biết, PPTP là một giao thức tạo đường hầm tầng 2, vì vậy, tiêu đề tầng liên kết dữ liệu và lần theo sự đánh dấu là các quy luật quan trọng trong đường hầm dữ liệu. trước khi được đặt lên các phương tiện truyền phát, tầng liên kết dữ liệu thêm vào tiêu đề của chính nó và đánh dấu cho các gói dữ liệu. Nếu gói dữ liệu phải chuyển qua một đường hầm PPTP cục bộ, gói dữ liệu sẽ được đóng gói vào trong một đánh dấu và tiêu đề theo công nghệ - LAN(như Ethenet chẳng hạn). Mặt khác, nếu đường hầm được trải qua một liên kết WAN, tiêu đề và đánh dấu luôn được thêm vào gói dữ liệu một lần.



Hình 2.9 Mô tả tiến trình xử lý dữ liệu PPTP đường hầm

Chú ý: GRE là một cơ chế đóng gói thông dụng đơn giản cho các dữ liệu dựa trên IP. GRE thường được dùng bởi các ISP để chuyển tiếp thông tin định tuyến trong Intranet của họ. Tuy nhiên, các Router backbone thuộc Internet của ISP sẽ

lọc lưu lượng dựa trên GRE này. Vì vậy các đường hầm đã được thiết lập có thể mang dữ liệu một cách an toàn và bí mật tới người nhận.

Khi dữ liệu PPTP được truyền thành công đến đúng người nhận, người nhận phải xử lý các gói dữ liệu đã được đóng gói bằng đường hầm để thu được dữ liệu gốc. Quá trình này là ngược lại với quá trình định đường hầm dữ liệu PPTP. Như ta thấy trong hình 2.10, để lấy lại dữ liệu gốc thì Node PPTP của người nhận phải thực hiện các bước sau:

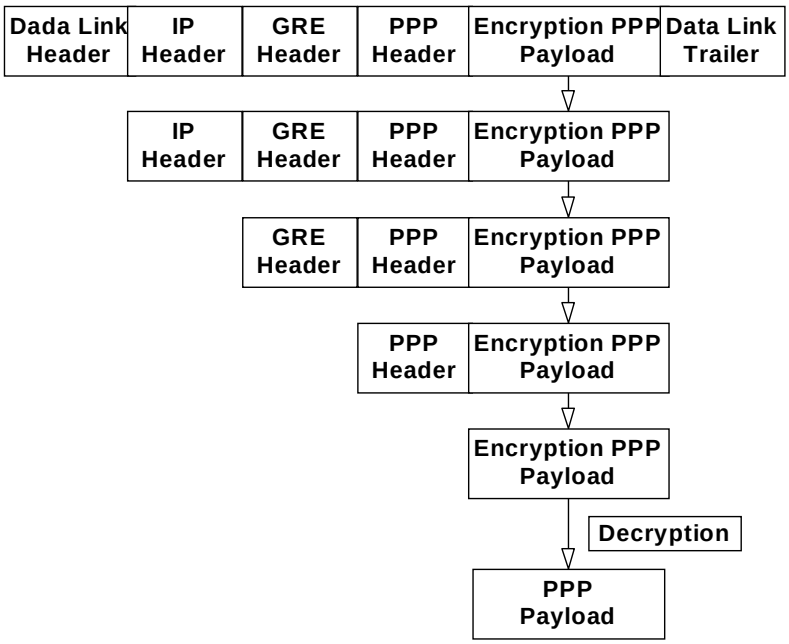
- Người nhận loại bỏ tiêu đề và đánh dấu của tầng liên kết dữ liệu đã được thêm vào bởi người gửi.

- Tiếp đó, loại bỏ tiêu đề GRE

- Tiêu đề IP được xử lý và loại bỏ

- Tiêu đề PPP được xử lý và loại bỏ.

- Cuối cùng, thông tin gốc được giải mã (nếu được yêu cầu)



Hình 2.10 Qúa trình xử lý gói dữ liệu để nhận được gói dữ liệu gốc

2.2.1.4. Bảo mật PPTP

PPTP đưa ra nhiều dịch vụ bảo mật xây dựng sẵn khác nhau cho PPTP Server và Client. Các dịch vụ bảo mật này bao gồm: Mã hóa và nén dữ liệu, xác thực, kiểm soát truy cập và lọc gói tin.

Hơn nữa các cơ chế bảo mật được đề cập ở trên, PPTP có thể được dùng chung với Firewall và Router.

1. Mã hoá và nén dữ liệu PPTP

PPTP không cung cấp một cơ chế mã hoá để bảo mật dữ liệu. Thay vào đó, nó sử dụng dịch vụ mã hoá được đề xuất bởi PPP. PPP lần lượt sử dụng mã hoá Microsoft Point–to-Point, nó dựa trên phương pháp mã hoá chia sẻ bí mật.

2. Xác thực dữ liệu PPTP

PPTP hỗ trợ các cơ chế xác thực của Microsoft sau đây:

a. Giao thức xác thực có thăm dò trước của Microsoft(MS-CHAP)

MS-CHAP là phiên bản thương mại của Microsoft và được dùng cho xác thực dựa trên PPP. Vì sự tương đồng cao với CHAP, các chức năng của MS-CHAP khá giống với CHAP. Điểm khác nhau chính giữa chúng là trong khi CHAP dựa trên RSA và thuật toán MD5 thì MS-CHAP dựa trên RSA RCA và DES. Mục đích là MS-CHAP được phát triển chỉ cho các sản phẩm Microsoft, nó không được hỗ trợ bởi các nền khác.

b. Giao thức xác thực mật khẩu(PAP)

Là giao thức đơn giản và là giao thức xác thực đường quay số thông dụng nhất. Nó cũng được dùng để xác thực các kết nối dựa trên PPP. Tuy nhiên nó gửi ID và mật khẩu của người dùng qua liên kết mà không mã hoá. Và như vậy, nó không đưa ra được sự bảo vệ từ việc phát lại hay thử lặp và các tấn công lỗi. Một lỗ hỗng của PAP khác là các thực thể truyền thông cuối chỉ được xác thực một lần khi khởi tạo kết nối. Vì vậy, nếu kẻ tấn công vượt qua được một lần thì không còn phải lo lắng về vấn đề xác thực trong tương lai nữa!. Vì lý do này, PAP được xem như là một giao thức xác thực ít phức tạp nhất và không phải là cơ chế xác thực được ưa thích trong VPN.

3. Kiểm soát truy cập PPTP

Sau khi một Client PPTP từ xa được xác thực thành công, sự truy cập của nó đến các tài nguyên trong mạng bị hạn chế bởi mục đích bảo mật nâng cao. Mục tiêu này được hoàn thành bởi việc thực thi bổ sung cơ chế kiểm soát truy cập như: Quyền truy cập, mức cho phép, nhóm và lọc gói PPTP

Lọc gói PPTP cho phép một Server PPTP trên mạng riêng chỉ chấp nhận và định tuyến các gói chỉ từ các Client PPTP đã được xác thực thành công. Kết quả là, chỉ các Client PPTP đã được xác thực mới có thể truy cập lại tới mạng từ xa đã xác định.

Trong cách này, PPTP không chỉ cung cấp các cơ chế xác thực, kiểm soát truy cập và mã hoá, mà còn làm tăng thêm sự an toàn của mạng.

4. PPTP với FireWall và Router

Các thiết bị PPTP chấp nhận lưu lượng TCP và IP tại cổng 1723 và 47. Tuy nhiên, khi PPTP dùng chung với FireWall và Router, lưu lượng đã được dự tính cho các cổng này được định tuyến qua Firewall hoặc Router, chúng lọc lưu lượng trên cơ sở danh sách kiểm soát truy cập (ACL) và các chính sách bảo mật khác, PPTP nâng cao các dịch vụ bảo mật mà nó đưa ra.

2.2.1.5. Các tính năng của PPTP

1. Tính sẵn có

PPTP được hỗ trợ trong nhiều hệ điều hành: trong Window NT Server, trong Workstation. Vì vậy, PPTP thực sự sẵn có trên các Platform của người sử dụng. Không cần mua thêm các phần mềm bổ sung vì Microsoft đã đưa ra cách nâng cấp PPTP trong tất cả các phiên bản Windows, được bổ sung trong nhiều nhánh của các Switch truy cập từ xa như các thiết bị Ascend, 3Com và ECI Telematics. PPTP đã trở thành một phần của các gói tin hệ điều hành mạng và phần lớn các Switch truy cập từ xa. Một nhà quản trị mạng Window NT có thể thử nghiệm một VPN ngay lập tức mà không cần tốn thêm một chi phí nào.

2. Dễ thi hành

Nhiều nhà quản trị mạng Window NT đã quen thuộc với cách thiết lập các giao thức mạng và RAS vì vậy sử dụng PPTP cũng không khó khăn với họ.

Những người sử dụng từ xa quay số kết nối tới RAS Server thông qua các ISP sử dụng Switch truy cập từ xa(Remote Accsess Switch) có hỗ trợ PPTP chỉ cần bổ sung địa chỉ IP của RAS Server vào Profile của họ, ISP dễ dàng đóng gói các gói tin PPP theo khuôn dạng PPTP.

3. Tạo đường hầm đa giao thức

Đây là một tính năng vượt trội của PPTP, một vài phần mềm tạo đường hầm chỉ cho phép tạo đường hầm với các gói tin IP nhưng giao thức PPTP có thể tạo đường hầm cho tất cả các giao thức mà máy chủ RAS cho phép.

4. Khả năng sử dụng các địa chỉ IP không đăng ký một cách đồng bộ

Khi một người dùng VPN tạo một kết nối PPTP tới máy chủ RAS sẽ được máy chủ gán cho một địa chỉ IP. Địa chỉ này có thể là một phần trong dãi địa chỉ IP của tổ chức vì thế, hệ thống người sử dụng RAS có thể trực tuyến trên mạng IP của tổ chức đó.

Các tổ chức thỉnh thoảng không sử dụng địa chỉ IP đăng ký (là những địa chỉ được cung cấp bởi cơ quan có thẩm quyền, sẽ là duy nhất trên hệ thống mạng) trên hệ thống mạng riêng. Cơ quan thẩm quyền Internet Assigned Numbers (IANA) sẽ thiết lập các khối địa chỉ IP không đăng ký để sử dụng trên các mạng riêng hoặc Intranet và các hệ thống mạng này không cho phép các truy cập Internet hay các truy cập qua Router. Nếu một công ty có sử dụng một tập các địa chỉ không đăng ký khi một RAS Client sử dụng giao thức PPTP để thiết lập kết nối, sẽ được cung cấp một địa chỉ trong số địa chỉ đó và truy cập tới mạng nội bộ của công ty. Nếu một người sử dụng ở xa quay số kết nối tới ISP và cố gắng truy cập tới mạng không hỗ trợ giao thức PPTP, thì Firewall của tổ chức sẽ phải mở ra một cổng nào đó cho người sử dụng vào mạng cục bộ, điều này có thể tạo ra lỗ hỗng. Vì vậy, không phải khi nào họ kết nối tới ISP là cũng có thể vào mạng cục bộ.

2.2.2. Chuyển tiếp tầng 2 (L2F)

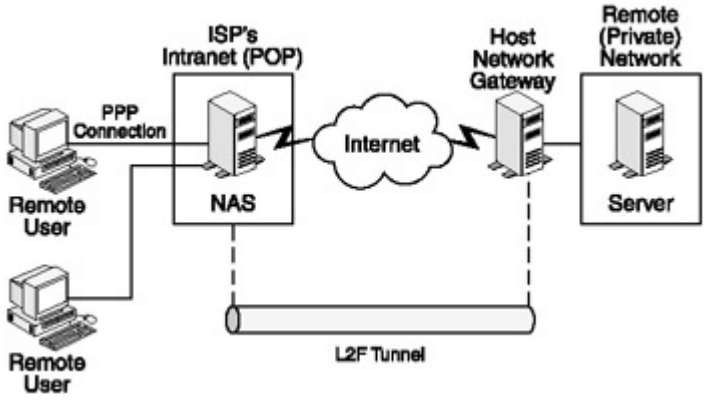
Như đã đề cập trước đây, các dịch vụ mạng quay số truyền thống được thực hiện qua Internet và vì vậy dựa trên công nghệ IP. Điều này giải thích tại sao giải pháp đường hầm lại thông dụng như PPP và PPTP, chứng tỏ thành công hơn của cơ sở hạ tầng IP so với các công nghệ mạng đương thời như ATM, FR. Bảo mật là vấn đề khác. Bất chấp các yêu cầu của Microsoft về giao dịch bảo mật, PPTP dựa trên MS-CHAP không thật sự an toàn. Vấn đề này làm cho các tổ chức công nghiệp và các chuyên gia tìm đến các giải pháp thay thế có thể đem lại sự bảo mật liền mạch cho nhiều dịch vụ quay số ảo và nhiều giao thức.

Cisco System cùng với Nortel là một trong các nhà cung cấp hàng đầu các giải pháp theo hướng:

- Có khả năng bảo mật các giao dịch.

- Cung cấp truy cập qua cơ sở hạ tầng của Internet và các mạng công cộng trung gian khác.

- Hỗ trợ nhiều công nghệ mạng như ATM, FDDI, IPX, Net-BEUI, và Frame Relay.



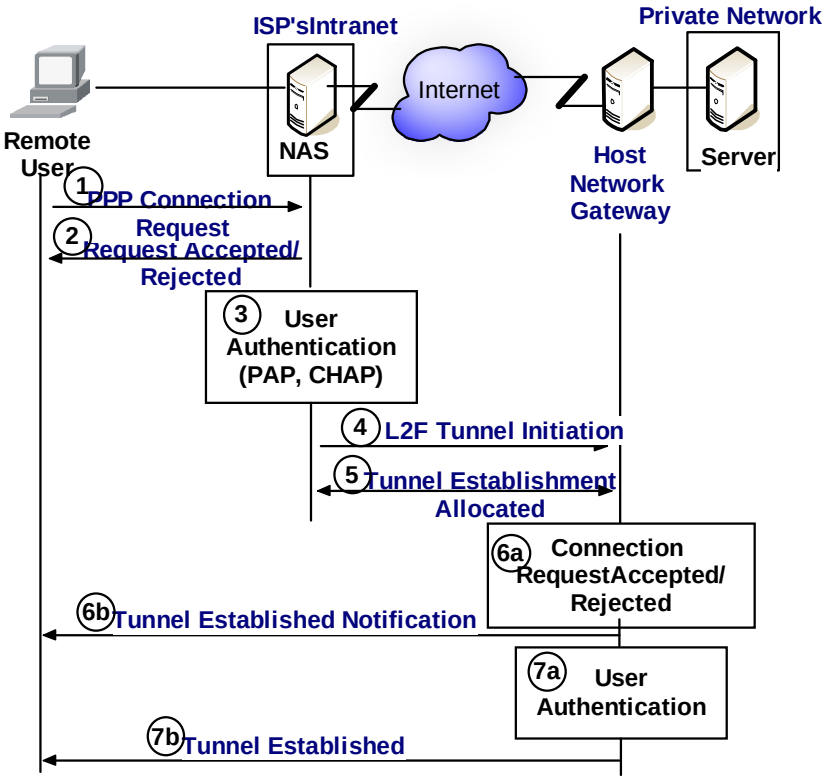
Hình 2.11 Đường hầm L2F từ POP của ISP tới Gateway của một mạng riêng

Sau thời gian dài tìm kiếm, Cisco hiện tại đang mở rộng nghiên cứu L2F. Ngoài việc thực hiện đầy đủ những mục đích trên, L2F mang lại những thuận lợi khác trong công nghệ truy cập từ xa. Các đường hầm L2F có thể hỗ trợ nhiều phiên đồng thời trong cùng một đường hầm. Theo cách nói đơn giản hơn là nhiều người dùng từ xa có thể cùng truy cập vào mạng cục bộ riêng qua một kết nối quay số đơn. L2F đạt được điều này bằng cách định nghĩa nhiều kết nối trong một đường

hầm nơi mỗi kết nối mô tả một dòng PPP đơn. Hơn nữa, các dòng này có thể bắt đầu từ một người dùng từ xa đơn lẻ hoặc từ nhiều người dùng. Vì một đường hầm có thể hỗ trợ nhiều kết nối đồng thời, một vài kết nối được yêu cầu từ một Site ở xa tới ISP và từ POP của ISP tới Gateway của mạng riêng. Điều này đặc biệt hữu ích trong việc giảm chi phí người dùng. Hình 2.11 mô tả đường hầm L2F

2.2.2.1. Tiến trình L2F

Khi một Client quay số từ xa khởi tạo một kết nối tới Host cục bộ trong một Intranet riêng.



Hình 2.12 Thiết lập một đường hầm L2F giữa người dùng từ xa và Server

Các tiến trình sau được thực hiện tuần tự:

1. Người dùng từ xa khởi tạo một kết nối PPP tới ISP của họ. Nếu một người dùng từ xa là một phần của mạng LAN, người dùng có thể tận dụng ISDN hoặc liên kết để kết nối tới ISP. Nếu người dùng không phải là một phần của bất kỳ Intranet nào, họ có thể cần sử dụng các dịch vụ của PSTN.

2. Nếu NAS đặt tại POP của ISP chấp nhận yêu cầu kết nối, kết nối PPP được thiết lập giữa NAS và người dùng.

3. Người dùng được xác thực bởi ISP cuối cùng, cả CHAP và PAP đều được sử dụng cho chức năng này.

4. Nếu không có đường hầm nào tới Gateway của mạng đích tồn tại, thì một đường hầm sẽ được khởi tạo.

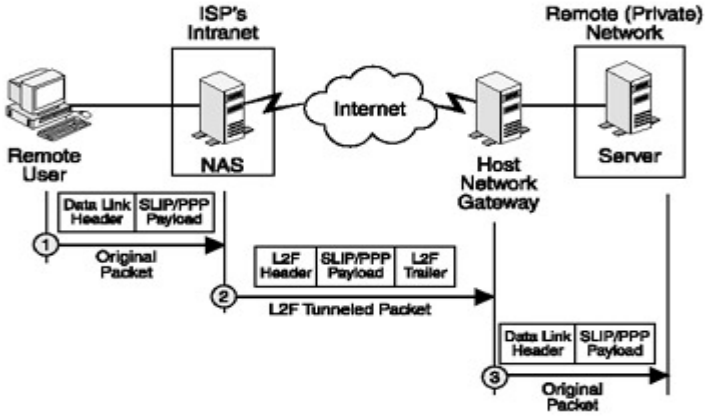
5. Sau khi một đường hầm được thiết lập thành công, một ID (MID) đa công duy nhất được phân phối tới các kết nối. Một thông điệp thông báo cũng được gửi tới các Gateway của máy chủ mạng. Thông điệp này thông báo cho Gateway về yêu cầu kết nối từ một người dùng ở xa.

6. Gateway có thể chấp nhận hoặc từ chối yêu cầu kết nối này. Nếu yêu cầu bị từ chối, người dùng sẽ được thông báo lỗi và kết nối quay số bị kết thúc. Trong trường hợp yêu cầu được chấp nhận, máy chủ Gateway gửi thông báo khởi tạo cài đặt tới Client từ xa, phản hồi này có thể bao gồm cả thông tin xác thực, nó được dùng bởi Gateway để xác thực người dùng từ xa.

7. Sau khi người dùng được xác thực bởi máy chủ Gateway mạng, một giao diện ảo được thiết lập giữa 2 đầu cuối.

2.2.2.2. Đường hầm L2F

Khi một người dùng từ xa đã được xác thực và yêu cầu kết nối được chấp nhận, một đường hầm giữa NAS của nhà cung cấp và Gateway máy chủ mạng được thiết lập, như trong hình 2.13.



Hình 2.13 Quá trình định đường hầm dữ liệu dựa trên L2F

Sau khi đường hầm giữa 2 đầu cuối được thiết lập xong. Các Frame tầng 2 có thể được trao đổi qua đường hầm như sau:

1. Người dùng từ xa chuyển tiếp các frame thông thường tới NAS đặt tại ISP.

2. POP cắt bỏ thông tin tầng liên kết dữ liệu hay các byte trình diễn, thêm vào tiêu đề L2F và đánh dấu frame. Sau khi frame được đóng gói mới thì được chuyển tiếp tới mạng đích qua đường hầm.

3. Máy chủ Gateway mạng chấp nhận các gói đường hầm này, cắt bỏ tiêu đề L2F, đánh dấu và chuyển tiếp các frame tới Node đích trong mạng Intranet.

Node đích xử lý các frame nhận được như là các gói không qua đường hầm.

Chú ý: Đường hầm L2F được xem như là một "Giao diện ảo"

Bất kỳ một phản hồi nào từ máy chủ đích trong mạng phải qua quá trình ngược lại. Đó là, host gửi một frame tầng liên kết dữ liệu thông thường tới Gateway, Gateway này sẽ đóng gói frame vào trong một gói L2F (như trong hình 2.14) và chuyển tiếp nó tới NAS đặt tại Site của ISP. NAS cắt bỏ thông tin L2F từ các frame và thêm vào thông tin tầng liên kết dữ liệu thích hợp với nó.

Frame sau đó được chuyển tiếp tới người dùng từ xa.

L2F Header	Payload Packet(PPP/SLIP)	L2F CheckSum

Hình 2.14 định dạng gói L2F

2.2.2.3. Bảo mật L2F

L2F cung cấp các dịch vụ: Mã hoá dữ liệu và xác thực

1. Mã hoá dữ liệu L2F

L2F sử dụng MPPE cho các chức năng mã hoá cơ bản. Tuy nhiên nó không an toàn với các kỹ thuật Hacking tiên tiến ngày nay. Và nó cũng phải sử dụng mã hoá dựa trên IPSEC để đảm bảo dữ liệu được giao dịch bí mật. IPSec sử dụng hai giao thức cho chức năng mã hoá: đóng gói tải bảo mật(*ESP*) và xác thực tiêu đề (*AH*). Thêm vào đó, để làm tăng tính bảo mật của khoá trong pha trao đổi khoá, IPSec cũng sử dụng một giao thức bên thứ ba đó là trao đổi khoá Internet(*IKE*).

2. Xác thực dữ liệu L2F

Xác thực L2F được hoàn thành tại hai mức. Mức thứ nhất của xác thực dựa trên L2F xuất hiện khi một người dùng từ xa sử dụng đường quay số tới POP của ISP. Tại đây, quá trình thiết lập đường hầm được bắt đầu chỉ sau khi người dùng được xác thực thành công. Mức thứ hai của xác thực được thực hiện bởi máy chủ Gateway của mạng, nó không thiết lập một đường hầm giữa hai điểm đầu cuối cho đến khi nó xác thực người dùng từ xa.

Giống như PPTP, L2F cũng sử dụng các dịch vụ bảo mật được hỗ trợ bởi PPP cho xác thực. Kết quả là L2F sử dụng PAP để xác thực một Client từ xa khi một Gateway L2F nhận một yêu cầu kết nối. L2F cũng sử dụng lược đồ xác thực như sau để nâng cao tính bảo mật dữ liệu:

- Giao thức xác thực có thăm dò trước*(CHAP)*

- Giao thực xác thực mở rộng (EAP)

2.2.2.4. Các ưu và nhược điểm của L2F

Mặc dù L2F yêu cầu mở rộng để khắc phục sự khác nhau với LCP và các tuỳ chọn xác thực, nhưng nó đắt hơn PPTP vì nó là giải pháp chuyển tiếp Frame ở mức thấp, nó cũng cung cấp một giải pháp VPN nền cho mạng doanh nghiệp tốt hơn PPTP.

Những ưu điểm chính của việc thực thi một giải pháp L2F bao gồm:

- Nâng cao tính bảo mật của các phiên giao dịch.

- Độc lập với nền.

- Không cần phải đàm phán với ISP.

- Hỗ trợ nhiều công nghệ mạng như: ATM, FDDI, IPX, NetBEUI, và Frame Relay.

Ngoài những ưu điểm trên, nó cũng có một số nhược điểm:

- Việc thực thi giải pháp dựa trên L2F phụ thuộc nhiều vào ISP, nếu ISP không hỗ trợ L2F thì không thể thực hiện được giải pháp này.

- L2F không cung cấp kiểm soát luồng. Và như vậy, nếu đường hầm bị đầy thì các gói dữ liệu có thể bị xoá tuỳ tiện. Điều này là nguyên nhân của việc phải phát lại gói dữ liệu, nó làm chậm tốc độ truyền.

- Do kết hợp cả xác thực và mã hoá, các giao dịch thực hiện qua đường hầm dựa trên L2F là chậm khi so sánh với PPTP.

Cùng với sự phát triển của L2F, có hai công nghệ đường hầm: L2F và PPTP cạnh tranh nhau trên thị trường VPN. Hai giao thức này không tương thích nhau. Kết quả là, các tổ chức đã gặp khó khăn vì yêu cầu của mỗi nơi một khác. IETF quyết định kết thúc sự rắc rối này bằng cách kết hợp cả hai công nghệ thành một giao thức và được dùng như một chuẩn trong giải pháp VPN. L2PT là kết quả của sự kết hợp này.

2.2.3. Giao thức đường hầm lớp 2 (L2TP)

Được phát triển bởi IETF và được tán thành bởi các hãng lớn, như: Cisco, Microsoft, 3COM, và Ascend. L2TP là một sự kết hợp của các giao thức VPN trước đây như PPTP và L2F. Thực tế, nó là sự kết hợp những gì tốt nhất của PPTP và L2F. L2TF cung cấp sự mềm dẻo, khả năng mở rộng, giải pháp truy cập từ xa chi phí thấp của L2F và khả năng kết nối điểm - điểm nhanh nhất của PPTP.

Điểm mấu chốt của những thuận lợi được mang lại bởi L2TP là sự tích hợp các đặc trưng của L2F và PPTP. Đó là những lợi ích sau:

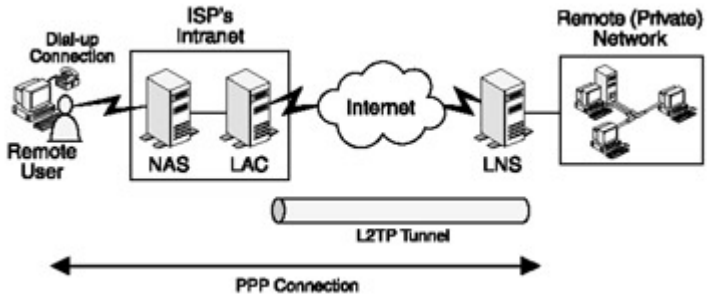
- L2TP hỗ trợ nhiều giao thức và công nghệ mạng, như IP, ATM, FR và PPP. Kết quả là nó có thể hỗ trợ các công nghệ riêng biệt bằng một thiết bị truy cập thông thường.

- L2TP không yêu cầu bổ sung thêm bất kỳ phần mềm nào như thêm trình điều khiển hay hỗ trợ hệ điều hành. Cho nên người dùng từ xa cũng như người dùng trong Intranet riêng không cần phải thực thi các phần mềm đặc biệt.

- L2TP cho phép những người dùng từ xa chưa đăng ký địa chỉ IP có thể truy cập một mạng từ xa qua một mạng công cộng.

- Xác thực và cấp quyền L2TP được thực hiện bởi Gateway của mạng chủ. Vì vậy, ISP không cần phải duy trì một cơ sở dữ liệu xác thực người dùng hay quyền truy cập cho người dùng từ xa. Hơn nữa, trong mạng Intranet cũng có thể định nghĩa chính sách bảo mật và truy cập cho chính họ. Điều này làm cho tiến trình thiết lập đường hầm nhanh hơn nhiều so với các giao thức đường hầm trước.

Đặc trưng chính của đường hầm L2TP là L2TP thiết lập đường hầm PPP mà không giống với PPTP là không kết thúc tại Site của ISP gần nhất. Để thay thế, đường hầm này mở rộng tới Gateway của mạng chủ (mạng đích). Như trong hình 2.15. Yêu cầu đường hầm L2TP có thể bị kết thúc bởi người dùng từ xa hoặc Gateway của ISP.



Hình 2.15 Đường hầm L2TP

Lúc một Frame PPP được gửi qua đường hầm L2TP, chúng được đóng gói lại như các thông điệp giao thức UDP. L2TP sử dụng các thông điệp UDP này cho cả dữ liệu đường hầm cũng như việc duy trì đường hầm. Cũng vì vậy, dữ liệu đường hầm L2TP và các gói duy trì đường hầm không giống với các giao thức trước có cùng cấu trúc gói.

2.2.3.1. Thành phần của L2TP

Các giao dịch dựa trên L2TP tận dụng 3 thành phần cơ bản sau: Một Server truy cập mạng (*NAS*), một bộ tập trung truy cập L2TP (*LAC*) và một Server mạng L2TP *(LNS*).

1. Server truy cập mạng (NAS)

Là thiết bị truy cập điểm - điểm, cung cấp kết nối Internet theo yêu cầu tới những người dùng quay số từ xa (qua một đường ISDN hoặc PSTN) dùng kết nối PPP. NAS chịu trách nhiệm xác thực những người dùng từ xa tại điểm ISP sau cùng và quyết định một xem kết nối quay số ảo có phải là yêu cầu thật hay không.

Giống như NAS của PPTP, NAS của L2TP được đặt tại vị trí ISP và hoạt động như một Client trong tiến trình thiết lập đường hầm L2TP. NAS có thể trả lời và hỗ trợ nhiều yêu cầu kết nối đồng thời và có thể hỗ trợ nhiều loại Client (Sản phẩm của Microsoft, Unix, Linux,…)

2. Bộ tập trung truy cập L2TP (LAC)

Vai trò của LAC trong công nghệ đường hầm L2TP là thiết lập một đường hầm qua mạng công cộng (như PSTN, ISDN, hoặc Internet) tới LNS của mạng chủ sau cùng. Trong khía cạnh này, LAC server như là điểm kết thúc của môi trường vật lý giữa Client sau cùng và LNS của mạng chủ.

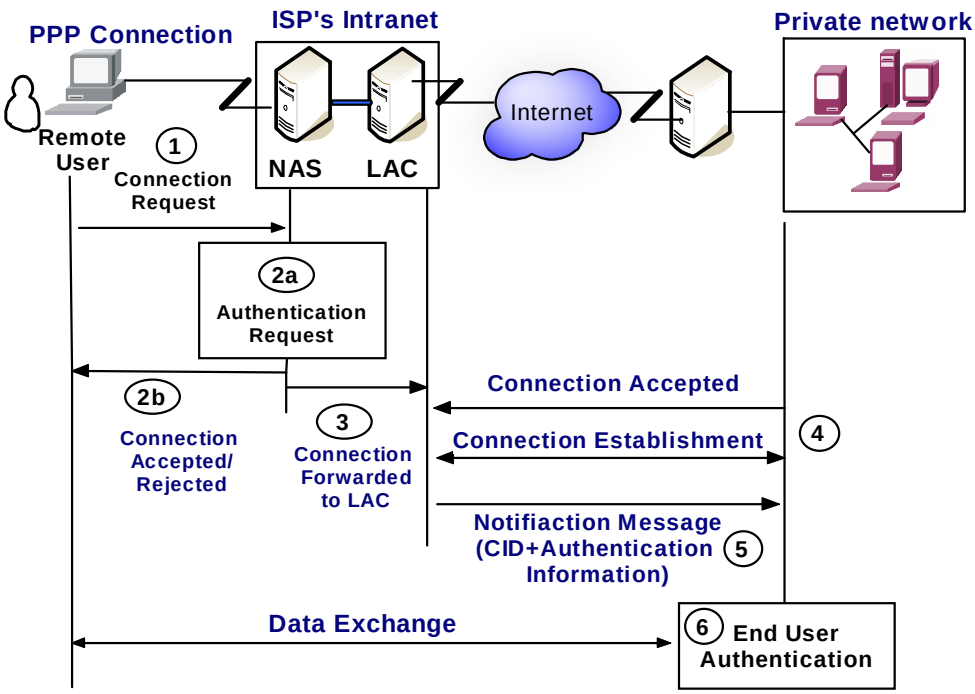
Một điều quan trọng là LAC thường được đặt tại điểm xuất hiện của ISP nhằm cung cấp kết nối vật lý cho người truy cập từ xa.

3. Server mạng L2TP(LNS)

LNS là điểm cuối đầu kia của một kết nối từ xa. Nó được đặt tại mạng trung tâm và có thể cho phép một hoặc nhiều cuộc kết nối từ xa cùng lúc.

Khi một LNS nhận một yêu cầu cho một yêu cầu kết nối ảo từ một LAC, nó thiết lập đường hầm và xác thực người dùng đã khởi tạo kết nối. Nếu LNS chấp nhận yêu cầu kết nối, nó tạo một giao diện ảo.

2.2.3.2. Các tiến trình L2TP



Hình 2.16 Mô tả quá trình thiết lập đường hầm L2TP

Khi một người dùng từ xa cần thiết lập một đường hầm L2TP qua mạng Internet hoặc mạng công cộng, tuần tự các bước như sau:

1) Người dùng từ xa gửi một yêu cầu kết nối tới NAS của ISP gần nhất và đồng thời khởi tạo một kết nối PPP với ISP sau cùng.

2) NAS chấp nhận yêu cầu kết nối sau khi xác thực người dùng cuối, NAS sử dụng phương pháp xác thực dựa trên PPP, như PAP, CHAP, SPAP và EAP cho chức năng này.

3) NAS sau đó khởi động LAC, nơi chứa thông tin về LNS của mạng đích.

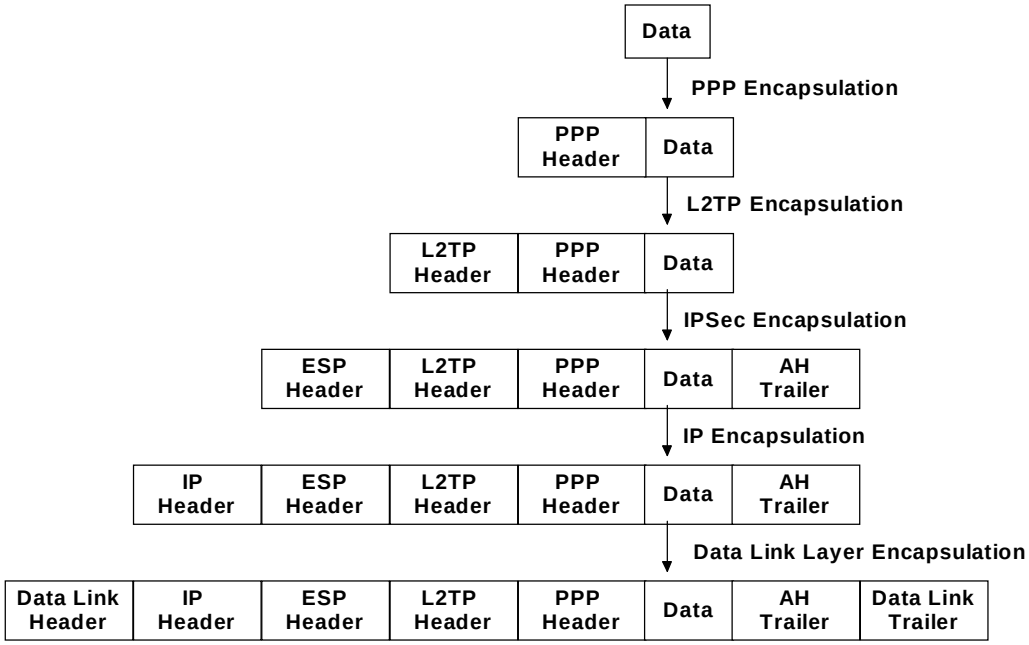
4) Tiếp theo, LAC thiết lập một đường hầm LAC-LNS qua mạng trung gian giữa hai đầu cuối. Môi trường đường hầm này có thể là ATM, Frame Relay hoặc IP/UDP.

5) Sau khi đường hầm đã được thiết lập thành công, LAC phân phối một định danh cuộc gọi(Call ID - CID) để kết nối và gửi thông điệp thông báo tới LNS, thông điệp này chứa thông tin mà có thể được dùng để xác thực người dùng từ xa (người yêu cầu đường hầm ban đầu). Thông điệp này cũng mang cả tuỳ chọn LCP đã được thương lượng giữa người dùng với LAC.

6) LNS sử dụng thông tin nhận được trong thông điệp thông báo để xác thực người dùng cuối. Nếu người dùng được xác thực thành công và LNS chấp nhận yêu cầu tạo lập đường hầm, một giao diện PPP ảo được thiết lập với sự trợ giúp của các tuỳ chọn nhận được từ thông điệp thông báo.

7) Người dùng từ xa và LNS bắt đầu trao đổi dữ liệu qua đường hầm.

2.2.3.3. Dữ liệu đường hầm L2TP



Hình 2.17 Quá trình xử lý định đường hầm dữ liệu L2TP

Tương tự như các gói đường hầm PPTP, các gói L2TP cũng trải qua nhiều mức đóng gói. Các giai đoạn này được minh hoạ trong hình 2.17, bao gồm:

- Đóng gói PPP của dữ liệu: Không giống như đóng gói dựa trên PPTP, dữ liệu không được mã hoá trước khi đóng gói. Chỉ tiêu đề PPP được thêm vào gói dữ liệu gốc được tải.

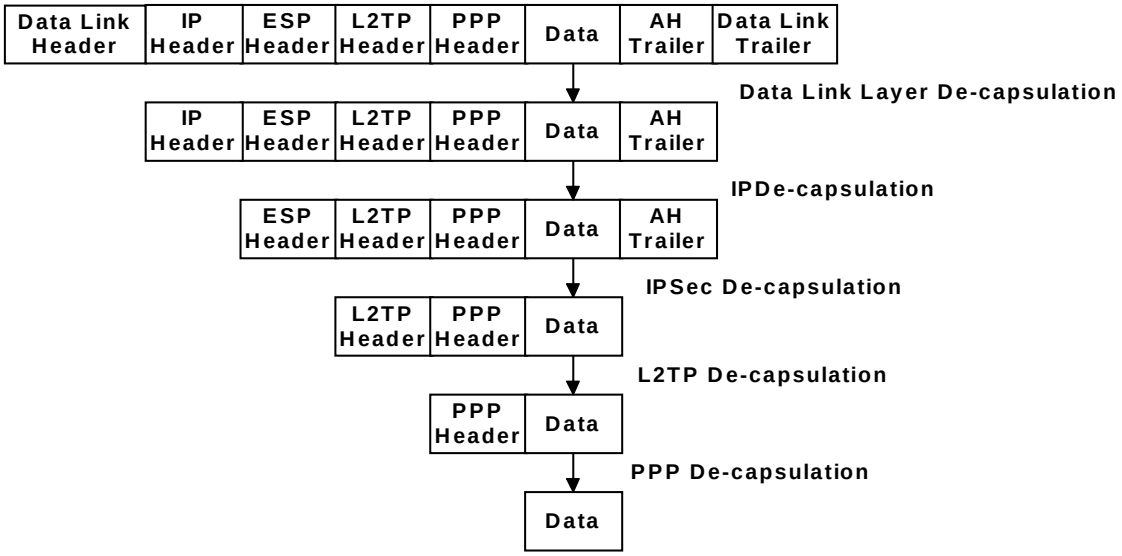
- Đóng gói L2TP của các Frame: Sau khi gói tải gốc được đóng gói vào trong một gói PPP, một tiêu đề L2TP được thêm vào.

- Đóng gói UDP của các Frame: Tiếp theo, các gói dữ liệu L2TP đã đóng gói lại được đóng gói vào trong một Frame UDP. Tiếp sau đó, tiêu đề UDP được thêm vào Frame L2TP đã đóng gói. Cổng nguồn và đích trong UDP này được thiết lập là 1701.

- Đóng gói IPSec của các gói dữ liệu UDP: Sau khi các Frame L2TP được đóng gói UDP, UDP này được mã hoá và một tiêu đề đóng gói tải bảo mật IPSec được thêm vào nó. Một đánh dấu xác thực tiêu đề IPSec cũng được gắn vào để mã hoá và đóng gói dữ liệu.

- Đóng gói IP các gói dữ liệu IPSec đã bọc gói: Tiếp theo, tiêu đề IP cuối cùng được thêm vào các gói IPSec đã đóng gói. Tiêu đề IP này chứa địa chỉ IP của LNS và người dùng từ xa.

- Đóng gói tầng liên kết dữ liệu: Một tiêu đề tầng liên kết dữ liệu và đánh dấu cuối cùng được thêm vào gói IP nhận được từ việc đóng gói IP cuối cùng. Tiêu đề và đánh dấu này giúp cho gói dữ liệu tới được Node đích. Nếu Node đích là node cục bộ, tiêu đề và đánh dấu dựa trên công nghệ mạng LAN. Trong trường hợp khác, nếu gói dữ liệu giành cho đích ở xa, một tiêu đề PPP và đánh dấu được thêm vào gói dữ liệu đường hầm L2TP.



Hình 2.18 Tiến trình mở gói dữ liệu đường hầm L2TP

Tiến trình mở gói dữ liệu đường hầm là ngược lại của thủ tục tạo đường hầm. Khi một thành phần L2TP (LNS hoặc người dùng cuối) nhận một gói dữ liệu đường hầm L2TP, trước tiên nó loại bỏ tiêu đề tầng liên kết dữ liệu và đánh dấu, tiếp đó gói dữ liệu được loại bỏ tiêu đề IP, gói dữ liệu sau đó được xác thực bằng việc dùng thông tin được mang trong tiêu đề ESP IPSec và đánh dấu AH, tiêu đề ESP IPSec cũng được dùng để giải mã thông tin. Tiếp theo tiêu đề UDP được xử lý và loại bỏ. Định danh đường hầm và CID trong tiêu đề L2TP phục vụ để định danh đường hầm L2TP và phiên làm việc. Cuối cùng, tiêu đề PPP được xử lý và loại bỏ, gói tải PPP được chuyển tiếp tới thiết bị giao thức thích hợp để xử lý. Hình 3.18 mô tả các tiến trình này.

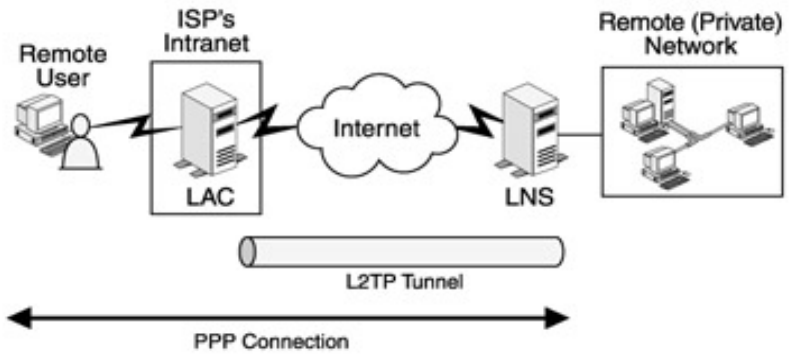
2.2.3.4. Mô hình đường hầm L2TP

L2TP hỗ trợ 2 mô hình đường hầm: Đường hầm tự nguyện (Voluntary) và đường hầm bắt buộc (Compulsory). Những đường hầm này vận dụng một luật quan trọng trong việc truyền dữ liệu từ một người dùng cuối này đến người dùng khác.

1. Đường hầm L2TP kiểu bắt buộc

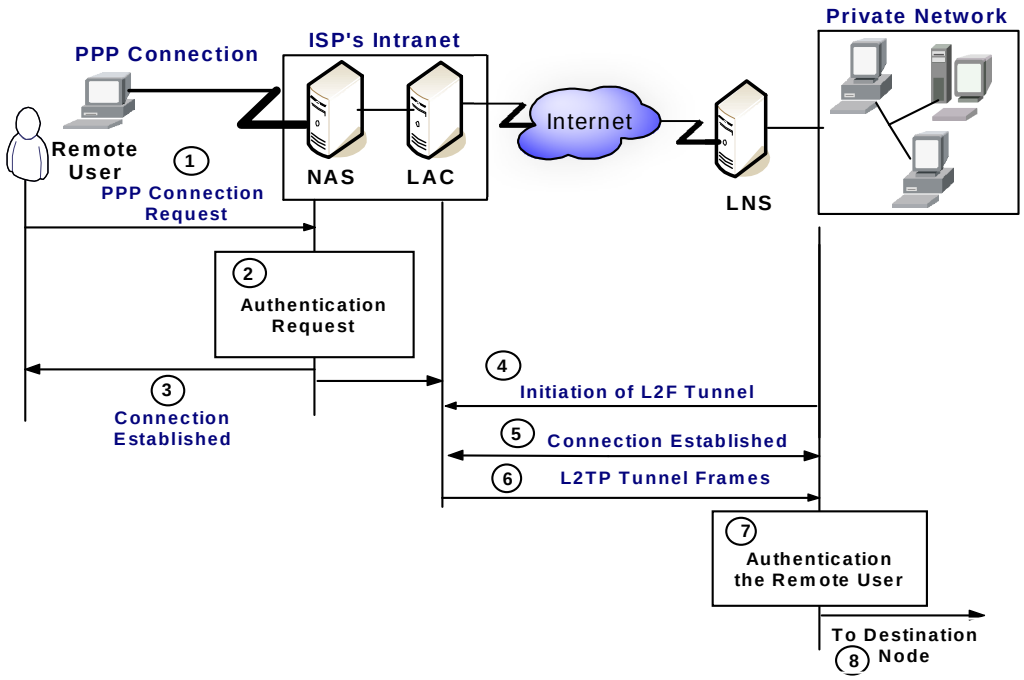
Một đường hầm L2TP bắt buộc, như ta thấy trong hình 2.19 được thiết lập giữa LAC của ISP sau cùng và LNS của mạng chủ. Điều quan trọng để thiết lập thành công một đường hầm như vậy là ISP có khả năng hỗ trợ công nghệ L2TP. Hơn nữa, ISP cũng phải dùng một luật khoá trong việc thiết lập các đường hầm L2TP.

Trong đường hầm L2TP bắt buộc, người dùng cuối (hay client) chỉ là một thực thể bị động. Khác với việc phát ra yêu cầu kết nối gốc, người dùng cuối không có vai trò trong tiến trình thiết lập đường hầm. Vì vậy, không có thay đổi lớn được yêu cầu tại người dùng cuối L2TP.



Hình 2.19 Đường hầm L2TP bắt buộc

Việc tạo lập đường hầm L2TP được cân nhắc một tuỳ chọn tốt hơn từ quan điểm của bảo mật vì kết nối đường quay số tại người dùng cuối được dùng để thiết lập kết nối PPP với ISP. Kết quả là, người dùng không thể truy cập ngoại trừ qua Gateway trong Intranet. Nó cho phép người quản trị mạng thực thi các cơ chế bảo mật nghiêm ngặt, kiểm soát truy cập và các chiến lược kiểm toán.



Hình 2.20 Thiết lập một đường hầm L2TP bắt buộc

Các bước thiết lập đường hầm bắt buộc được mô tả như trong hình 2.20 và bao gồm:

1) Người dùng từ xa yêu cầu một kết nối từ NAS cục bộ tới ISP.

2) NAS xác thực người dùng, tiến trình xác thực này cũng giúp cho NAS biết được về định danh của người dùng yêu cầu kết nối. Nếu định danh của người dùng ánh xạ tới một thực thể trong cơ sở dữ liệu được duy trì ở ISP, dịch vụ đó cho phép người dùng được ánh xạ. NAS cũng xác định điểm cuối của đường hầm L2TP.

3) Nếu NAS chấp nhận kết nối, một liên kết PPP được thiết lập giữa ISP và người dùng từ xa.

4) LAC khởi tạo một đường hầm L2TP tới LNS tại mạng chủ sau cùng.

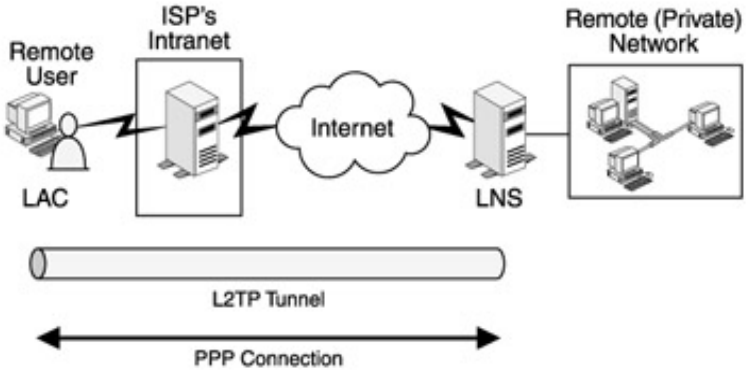
5) Nếu kết nối được chấp nhận bởi LNS, các Frame PPP trải qua việc tạo đường hầm L2TP.

6) LNS chấp nhận các Frame và khôi phục lại Frame PPP gốc.

7) Cuối cùng, LNS xác thực người dùng và nhận các gói dữ liệu. Nếu người dùng được xác nhận thành công, địa chỉ IP thích hợp được ánh xạ tới Frame và sau đó các Frame được chuyển tiếp tới Node đích trong Intranet.

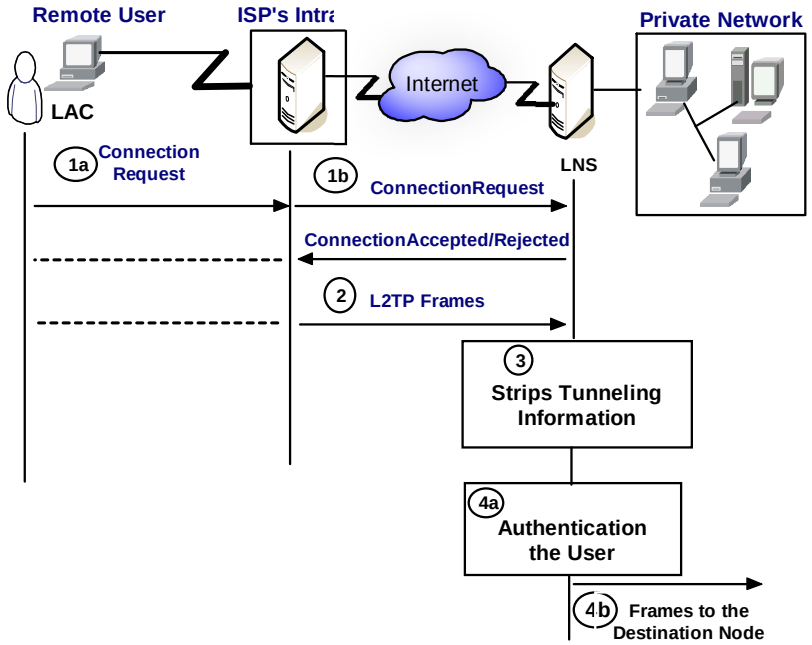
2. Đường hầm L2TP kiểu tự nguyện

Một đường hầm tự nguyện L2TP như trong hình 2.21 được thiết lập giữa người dùng từ xa và LNS đặt tại mạng chủ cuối cùng. Trong trường hợp này, người dùng từ xa tự hoạt động như một LAC. Bởi vì luật của ISP trong việc thiết lập đường hầm tự nguyện L2TP là tối thiểu. Cơ sở hạ tầng của ISP là trong suốt với người dùng cuối. Điều này có thể làm cho bạn nhớ về đường hầm dựa trên PPP trong Intranet của ISP là trong suốt.



Hình 2.21 Đường hầm L2TP tự nguyện

Ưu điểm lớn nhất của đường hầm L2TP tự nguyện là nó cho phép người dùng từ xa kết nối đến Internet và thiết lập nhiều phiên VPN đồng thời. Tuy nhiên để sử dụng những ưu điểm này, người dùng từ xa phải gắn vào nhiều địa chỉ IP. Một trong nhiều IP này được dùng cho kết nối PPP tới ISP và thường được dùng để hỗ trợ cho mỗi đường hầm L2TP riêng biệt. Tuy nhiên ưu điểm này cũng có thể là một bất lợi đối với client từ xa, vì mạng chủ có thể dễ dàng bị tấn công.



Hình 2.22 Quá trình thiết lập đường hầm L2TP tự nguyện

Việc thiết lập một đường hầm loại này là đơn giản hơn thiết lập đường hầm bắt buộc vì người dùng từ xa tận dụng một kết nối PPP đã được thiết lập trước tới ISP sau cùng. Các bước thiết lập đường hầm bao gồm:

1) LAC (trong trường hợp này là người dùng từ xa) phát ra một yêu cầu đường hầm tới LNS.

2) Nếu yêu cầu đường hầm được chấp nhận bởi LNS, LAC tạo đường hầm cho các Frame PPP trên L2TP xác định và chuyển tiếp các frame này qua đường hầm.

3) LNS nhận được Frame đã qua đường hầm, loại bỏ thông tin đường hầm và xử lý Frame.

4) Cuối cùng, LNS xác thực định danh người dùng và nếu người dùng được xác thực thành công, thì chuyển tiếp Frame tới Node đích trong Intranet.

Tiến trình thiết lập đường hầm L2TP tự nguyện được minh hoạ trong hình 2.22

Việc sử dụng L2TP trong VPN yêu cầu chi phí thấp tuy nhiên bên cạnh đó còn nhiều vấn đề về bảo mật vẫn chưa đáp ứng được.

2.2.3.5. Kiểm soát kết nối L2TP

Chúng ta nhớ lại, PPTP sử dụng các kết nối TCP riêng cho việc duy trì đường hầm. Trường hợp khác, kiểm soát kết nối L2TP và các Frame quản trị được dựa trên UDP. Định dạng của thông điệp kiểm soát L2TP được mô tả như trong hình 2.23

Data Link Header	*IP Header*	*IPSec ESP Header*	*UDP Header*	*L2TP Message*	*IPSec ESP Trailer*	*IPSec ESP Authentication Trailer*	*Data Link Trailer*

Hình 2.23 Định dạng thông điệp kiểm soát L2TP

Gói dữ liệu UDP, trên thông điệp kiểm soát L2TP là cơ sở, là khả năng kết nối. Điều này hàm ý rằng chúng có thể được phát ra ngoài trình tự và không được chấp nhận bởi người nhận ở phía bên kia. Vì lý do này, L2TP vận dụng kỹ thuật sắp tuần tự thông điệp. Kỹ thuật này đảm bảo rằng các thông điệp được phân phát tới những người dùng cuối đúng trình tự. Hai trường dữ liệu quan trọng: Next-Receiver và Next-Sent được sử dụng trong thông điệp kiểm soát L2TP để chắc chắn rằng các gói dữ liệu được phát tới người dùng hợp lệ.

Bảng 2.2: Liệt kê một số thông điệp duy trì và kiểm soát L2TP được sử dụng

Name	Description
Start-Control-Connection-Request	Yêu cầu từ Client L2TP để thiết lập kết nối điều khiển
Start-Control-Connection-Reply	Phản hồi từ Server L2TP với thông điệp Start-Control-Connection-Request của Client. Thông điệp này cũng được gửi như một trả lời cho thông điệp Outgoing-Call-Reply.
Start-Control-Connection-Connected	Trả lời từ Client L2TP cho thông điệp Start-Control-Connection-Reply của LNS.
Outgoing-Call-Request	Yêu cầu từ Client L2TP tới LNS để tạo đường hầm L2TP. Yêu cầu này chứa Call ID để định dang một yêu

Name	Description
	cầu trong đường hầm.

Outgoing-Call-Reply	Trả lời từ LNS L2TP cho thông điệpOutgoing-Call-Request của Client.
Hello	Thông điệp Keep-alive gửi bởi LNS hoặc Client. Nếu thông điệp này không được chấp nhận bởi thực thể cuối khác thì đường hầm bị kết thúc.
Set-Link-Info	Thông điệp từ bên ngoài khác để thiết lập các tuỳ chọn PPP đã thương lượng.
Call-Disconnect-Notify	Phản hồi từ Server L2TP để cho biết yêu cầu nào đó trong đường hầm L2TP để được kết thúc.
WAN-Error-Notify	Thông điệp từ Server L2TP (LNS) tới tất cả các Client L2TP đã được kết nối để thông báo lỗi trong giao diện PPP của Server.
Stop-Control-Connection-Request	Thông điệp từ Client hoặc Server L2TP để thông báo cho các thực thể cuối khác về việc kết thúc kết nối điều khiển.
Stop-Control-Connection-Reply	Phản hồi ngược lại từ thực thể cuối đối với thông điệp Stop-Control-Connection-Request.
Stop-Control-Connection-Notification	Phản hồi ngược lại từ thực thể cuối để cho biết đường hầm bị kết thúc.

2.2.3.6. Bảo mật L2TP

L2TP sử dụng phương thức xác thực PPP để xác thực người dùng. Sơ đồ xác thực bao gồm:

- PAP và SPAP.

- EAP.

- CHAP.

Ngoài các cơ chế xác thực đã nói ở trên. L2TP còn sử dụng IPSec để xác thực các gói dữ liệu riêng. Mặc dù điều này làm giảm đáng kể tốc độ giao dịch. Dùng IPSec để xác thực từng gói đảm bảo rằng Hacker và Cracker không thể thay đổi được dữ liệu và đường hầm của bạn.

2.2.3.7. Những ưu và nhược điểm của L2TP

Những thuận lợi chính của L2TP được liệt kê như sau:

- L2TP là giải pháp chung. Trong nhiều trường hợp khác, nó độc lập với Platform, nó cũng hỗ trợ nhiều công nghệ mạng. Hơn nữa, nó cũng hỗ trợ giao dịch qua liên kết WAN Non-IP mà không cần một IP.

- Đường hầm L2TP là trong suốt đối với ISP cũng như với người dùng từ xa. Vì vậy không cần phải cấu hình thêm tại ISP hoặc người dùng cuối cùng.

- L2TP cho phép một tổ chức kiểm soát xác thực người dùng thay cho ISP.

- L2TP cung cấp kiểm soát luồng và kết quả là các gói dữ liệu có thể bị loại bỏ một cách tuỳ ý nếu đường hầm bị đầy. Điều này làm cho các giao dịch L2TP nhanh hơn các giao dịch dựa trên L2F.

- L2TP cho phép người dùng từ xa chưa đăng ký địa chỉ IP truy cập tới một mạng từ xa qua một mạng công cộng.

- L2TP cũng nâng cao bảo mật do sử dụng mã hóa đường truyền tải dựa trên IPSec trong khi tạo lập đường hầm và thực thi khả năng xác thực trên từng gói của IPSec.

Tuy nhiên nó cũng có một số nhược điểm. Đó là:

- L2TP chậm hơn PPP hoặc L2F vì nó sử dụng IPSec để xác thực từng gói tin nhận được.

2.2.4. So sánh các giao thức đường hầm truy cập từ xa

Bảng sau đưa ra một sự so sánh giữa 3 giao thức đường hầm truy cập từ xa nổi bật, L2F, PPTP, L2TP

Bảng 2.3 Tổng hợp so sánh 3 giao thức VPN được tích hợp với tầng 2

Feature	PPTP	L2F	L2TP
Hỗ trợ nhiều giao thức	Yes	Yes	Yes
Hỗ trợ nhiều liên kết PPP	No	Yes	Yes
Hỗ trợ nhiều kết nối trên đường hầm	No	Yes	Yes
Các chế độ hoạt động được hỗ trợ	Incoming & Outgoing	Incoming	Incoming
Các chế độ đường hầm được hỗ trợ	Voluntary	Voluntary & Compulsory	Voluntary & Compulsory

Feature	PPTP	L2F	L2TP
Giao thức Carrier	IP/GRE	IP/UDP, IP/FR, IP/ATM	IP/UDP, IP/FR, IP/ATM
Giao thức kiểm soát	TCP, Port: 1723	UDP, Port: 1701	UDP, Port: 1701
Các cơ chế xác thực	MS-CHAP, PAP	CHAP, PAP, SPAP, EAP, IPSec, RADIUS RADIUS & & TACACS	CHAP, PAP, SPAP, EAP, IPSec, TACACS
Các cơ chế mã hoá	MPPE	MPPE, IPSec	MPPE, IPSec, ECP

2.5. Lập mã và xác thực trong các giao thức đường hầm tại tầng 2

Phần này chúng ta sẽ thảo luận về các tùy chọn xác thực và mã hóa được sử dụng cho các giao thức đường hầm tại tầng 2 đã đề cập ở trên

2.5.1. Các tùy chọn xác thực

Xác thực là một trong những yêu cầu then chốt với các giải pháp VPN, một số kỹ thuật xác thực truy cập từ xa thường được sử dụng và sự thích hợp của chúng cho các giải pháp VPN.

2.5.1.1. Giao thức xác thực mật khẩu (Password Authentication Protocol - PAP)

Là giao thức đơn giản nhất và là giao thức xác thực kết nối đường quay số tới ISP thông dụng nhất. Nó cũng được dùng để xác thực các kết nối dựa trên PPP, xác thực người dùng PPP trước khi một kết nối được thiết lập. Tuy nhiên nó gửi ID và mật khẩu của người dùng qua liên kết mà không mã hoá. Và như vậy, nó không đưa ra được sự bảo vệ từ việc phát lại hay thử lặp và các tấn công lỗi. PAP có các lỗ hỗng khác là các thực thể truyền thông cuối chỉ được xác thực một lần khi khởi tạo kết nối. Vì vậy, nếu kẻ tấn công vượt qua được một lần thì không còn phải lo lắng về vấn đề xác thực trong tương lai nữa!. Vì lý do này, PAP được xem như là một giao thức xác thực ít phức tạp nhất và không phải là cơ chế xác thực được ưa thích trong VPN.

2.5.1.2. Giao thức xác thực có thăm dò trước (Challenge Handshake Authentication Protocol - CHAP)

CHAP được phát triển để nhằm vào việc giải quyết vấn đề gửi mật khẩu dạng rõ trong khi sử dụng PAP. Trong CHAP khi một Client thay đổi định danh, nó đáp

lại bằng một giá trị hàm băm nhận được qua hàm băm MD5. Nếu giống với giá trị tại Server cuối sử dụng cùng thủ tục như ở Client thì Client được xác thực thành công, không có mật khẩu rõ được trao đổi trong tiến trình. Vấn đề khác thường tích hợp với PAP là thực thể truyền thông cuối chỉ được xác thực một lần trong một tiến trình trao đổi thông tin. Vì CHAP xác thực nhiều lần trong một phiên, nó tạo ra khó khăn cho kẻ tấn công muốn phá vỡ quá trình truyền thông.

2.5.1.3. Giao thức xác thực có thăm dò trước của Microsoft (Microsoft CHAP)

MS-CHAP là phiên bản thương mại của Microsoft và được dùng cho xác thực dựa trên PPP. Vì sự tương đồng cao với CHAP, các chức năng của MS-CHAP khá giống với CHAP. Điểm khác nhau chính giữa chúng là trong khi CHAP dựa trên RSA và thuật toán MD5 thì MS-CHAP dựa trên RSA RCA và DES. Mục đích là MS-CHAP được phát triển chỉ cho các sản phẩm Microsoft, nó không được hỗ trợ bởi các nền khác.

2.5.1.4. Giao thức xác thực mật khẩu Shiva (Shiva Password Authentication Protocol - SPAP)

SPAP là một phương pháp độc quyền cho việc xác thực các Client quay số và một số Client Microsoft. Nó cung cấp một giao thức thăm dò trước 2 bước giữa Client và Server với một Password đã mã hóa. Trong một số kịch bản, SPAP có thể cung cấp thêm một số chức năng như CallBack, đổi mật khẩu và tạo các kết nối ảo.

2.5.1.5. Giao thực xác thực mở rộng (Extensible Authentication Protocol - EAP)

Không giống như các phương pháp PAP và CHAP, chúng được thực thi tại thời gian cấu hình LCP, trong khi thiết lập kết nối PPP. EAP được thực hiện sau pha LCP, lúc xác thực PPP được thực hiện. Vì lý do đó, EAP cho phép xác thực phạm vi rộng vì tăng số lượng các tham số kết nối có thể được dùng tuỳ chọn như thông tin xác thực.

2.5.1.6. Kiến trúc bảo mật IP (IP Security)

Kiến trúc IPSec bao gồm 2 giao thức: Giao thức xác thực tiêu đề (Authentication Header - AH) và giao thức bao gói tải bảo mật(Encapsulating Security Payload - ESP). Cả 2 giao thức đều xác thực trên từng gói dữ liệu trong

một phiên làm việc, thay cho trên từng người dùng tại thời điểm thiết lập phiên làm việc hay nhiều lần trong một phiên. AH và ESP cũng cung cấp sự bảo vệ lại. Điều này làm cho xác thực IPSecurity an toàn hơn nhiều so với các tùy chọn xác thực PPP truyền thống, nhưng nó cũng phát sinh một quá trình xử lý Overhead khá cao tại các thiết bị thực hiện. IPSec là giao thức bảo mật được khuyến cáo cho L2TP và có thể được sử dụng cùng với L2F cũng như với PPTP về mặt lý thuyết

2.5.1.7 RADIUS and TACACS

RADIUS và TACACS cung cấp một trung tâm xác thực với người dùng truy cập từ xa. Cả 2 công nghệ làm việc theo cách tương tự nhau. Một Server truy cập từ xa thực thi một RADIUS hay TACACS Client để chuyển tiếp các yêu cầu xác thực tới một Server trung tâm, nơi yêu cầu được xử lý và được cấp quyền truy cập hoặc từ chối truy cập. RADIUS và TACACS cũng cho phép chuyển thông tin cấu hình từ Client tới một cơ sở dữ liêu trung tâm. RADIUS có thể được kết nối vào một hệ thống xác thực trung tâm khác như Kerberos, DCE và RACF

2.5.1.8. ID bảo mật

ID bảo mật được phát triển bởi công ty Security Dynamic, dựa trên khả năng xác thực 2 nhân tố. Người dùng không chỉ yêu cầu một Password để xác thực thành công mà còn cả một mã PIN bí mật dưới dạng một số ngẫu nhiên có thể thay đổi qua mỗi lần. Password được lưu trữ trong một cơ sở dữ liệu tại Server và được so sánh với Password do người dùng nhập vào khi đăng nhập. Số ngẫu nhiên được tạo cho mỗi người dùng tại Server và được thay đổi trong mỗi một khoảng thời gian nhất định. Người dùng được cung cấp một thiết bị dưới dạng một thẻ bài chứa khoá (key chain token) hoặc một thẻ thông minh (smart card), trong đó có một con chip vi xử lý thực hiện việc tính toán số ngẫu nhiên giống như là Server. Chip đó có một đồng hồ đồng bộ hoàn toàn với Server vì vậy người dùng có khả năng đăng nhập thành công bằng việc nhập vào Password và PIN đã có trên thiết bị thẻ. SecureID dựa trên mô hình Client/Server tương tự với RADIUS và TACACS, trong đó một Server truy cập hoạt động như một Client/Proxy SecureID để chuyển tiếp yêu cầu xác thực tới Server trung tâm, Server này thường được gọi là

ACE/Server. SecureID cũng được dùng như một hệ thống xác thực thứ cấp với RADIUS.

2.5.2. Tuỳ chọn mã hoá

Mã hoá và trao đổi khoá là 2 yêu cầu then chốt với VPN, trong phần sau ta sẽ thảo luận về một số kỹ thuật mã hoá truy cập từ xa thường được sử dụng và sự thích hợp của chúng với VPN

2.5.2.1. Mã hoá điểm tới điểm của Microsoft(Microsoft Point-to-Point Encryption - MPPE)

MPPE sử dụng hàm băm MD4 được tạo khi xác thực bằng phương pháp MS-CHAP để nhận được khóa mật cho một kết nối PPP. Đây là một phương pháp mã hoá điển hình được dùng cho PPTP với các Client Microsoft. Thuật toán mã hoá dùng cho MPPE là RC4 với khoá 40bit, nó được xem là rất yếu với những kỹ thuật Hacker tiên tiến ngày nay. Microsoft cũng đưa ra một phiên bản với khoá 128bit cho thị trường Mỹ. Microsoft thực thi PPTP theo cách thức là cứ sau 256 gói dữ liệu được mã hóa thì Refresh lại khóa

2.5.2.2. Giao thức kiểm soát mã hóa(Encryption Control Protocol - ECP)

ECP có thể được dùng để thương lượng mã hóa với một kết nối PPP, làmột kết nối đã được thiết lập và xác thực. ECP cho phép sử dụng các thuật toán mã hóa khác nhau trong mỗi chỉ thị nhưng không cung cấp khả năng Refresh khóa. Thuật toán mã hóa chuẩn là DES nhưng khách hàng có thể tự chọn thuật toán mà họ ưa thích để thực hiện.

2.5.2.3. IPSec

IPSec mang lại chức năng mã hóa với giao thức đóng gói tải bảo mật và sử dụng giao thức trao đổi khóa Internet cho việc sinh khóa và làm tươi khóa. ESP có khả năng mã hóa trên từng gói dữ liệu trong một phiên giao dịch và đưa ra thuật toán mã hóa ở các mức độ: thấp, trung bình, mạnh và rất mạnh để có thể lựa chọn từ DES 40bit đến Trip DES 192bit. IKE xác thực các bên cần trao đổi thông tin mật dựa trên các thuật toán xác thực mạnh cũng như mã hóa các thông điệp làm tươi khóa. Các khóa được sinh bởi IKE sau đó được sử dụng bởi IKE. ESP cung

cấp tùy chọn xác thực trên từng gói dữ liệu và bảo vệ lại. Điều này làm cho IPSec phức tạp và an toàn hơn các tùy chọn xác thực PPP truyền thống. Nhưng nó cũng làm xuất hiện quá trình xử lý Overhead nhiều hơn tại thiết bị thực thi. IPSec là giao thức bảo mật được khuyến cáo cho L2TP và cũng có thể được dùng với L2F.

Tổng kết

Trong chương này, chúng ta đã tìm hiểu về các giao thức được hầm tại tầng 2 của mô hình OSI. Các giao thức này là PPTP, L2F, L2TP. Chúng ta cũng tìm hiểu chi tiết về cách thức làm việc của các giao thức, bao gồm cả các thành phần, các tiến trình và việc duy trì kiểm soát kết nối được áp dụng cho mỗi giao thức. Chúng ta đã xem xét các tiến trình thiết lập một đường hầm của mỗi giao thức cũng như việc xử lý dữ liệu đường hầm và quy tắc của nó trong việc bảo mật dữ liệu. Chúng ta cũng đã xem xét khía cạnh bảo mật của mỗi giao thức, bao gồm cả các cơ chế mã hóa và xác thực khác nhau được sử dụng bởi mỗi giao thức để bảo đảm an toàn cho dữ liệu trong khi truyền qua đường hầm. Cuối cùng, chúng ta xem xét những ưu nhược điểm của mỗi giao thức.

Câu hỏi ôn tập

1. Những giao thức đường hầm nào sau đây được gắn với tầng 2 của mô hình OSI?

a. PPTP
b. L2F
c. IPSec
d. L2TP

2. Cổng mạng được dùng bởi L2F cho việc thiết lập và kiểm soát kết nối là_____.

a. TCP: 1701
b. UDP: 1723
c. UDP: 1701
d. TCP: 1723

3. Cổng mạng được dùng bởi PPTP cho việc định đường hầm dữ liệu tới đích là_____.

a. IP: 47
b. TCP: 47
c. UDP: 47
d. TCP: 1723

4. Frame hợp lệ nào sau đây được dùng cho việc kiểm soát kết nối?

a. Link Control Protocol
b. Link termination
c. Network Control Protocol
d. Link establishment

5. Giao thức đường hầm nào sau đây được hỗ trợ bởi Windows NT 4.0 Server?

a. PPTP
b. L2TP
c. L2F
d. Tất cả giao thức trên

6. Những thành phần nào sau đây là của một đường hầm L2TP?

a. LLC
b. LNS
c. NAS
d. LSN

7. Giao thức đường hầm đầu nào sau đây lần đầu tiên cho phép nhiều kết nối trên đường hầm?

a. PPTP
b. L2TP
c. L2F
d. Không có giao thức nào

8. Câu nào sau đây về L2F là đúng?

a. It is a proprietary tunneling protocol by Cisco.
b. It offers advanced flow-control services.
c. It supports voluntary tunnels.
d. It supports compulsory tunnels.

9. Giao thức đường hầm nào sau đây hỗ trợ IKE?

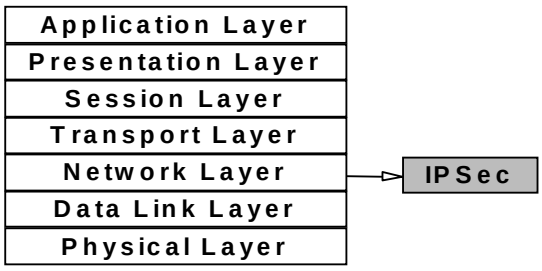
a. PPTP
b. L2TP
c. IPSec
d. L2F

Chương III Các giao thức mạng riêng ảo tại tầng 3

Trong chương II chúng ta đã nghiên cứu về các giao thức mạng riêng ảo, như PPTP, L2TP, L2F tại tầng 2 của mô hình OSI. Trong chương này sẽ nghiên cứu giao thức mạng riêng ảo hoạt động tại tầng 3 của mô hình OSI. Với đặc tính quản lý khóa, bảo mật và xác thực mạnh của IPSec, nó nổi bật lên như một chuẩn mạng riêng ảo thực tế. Trong thực tế, phần lớn giải pháp mạng riêng ảo ngày nay thường dựa trên IPSec. Vì vậy, IPSec là gì? Làm thế nào để nó đảm bảo an toàn cho các giao dịch trong khi truyền dữ liệu? Tại sao nó lại trở nên thông dụng? Chương này sẽ cố gắng trả lời các câu hỏi này.

Đúng như tên gọi, giao thức IPSec thực hiện việc bảo mật các gói IP. Giao thức IPSec cung cấp khả năng xác thực nguồn thông tin, kiểm tra tính toàn vẹn và bảo mật nội dung thông tin.

Thuật ngữ IPSec là viết tắt của Internet Protocol Security. Nó dựa vào một bộ của các giao thức (AH, ESP, FIP-140-1, và các chuẩn khác) mà đã được IETF phát triển. Mục đích chính đằng sau sự phát triển của IPSec là cung cấp một khung bảo mật tại lớp 3(Lớp mạng) của mô hình OSI, như trong hình 3.1



Hình 3.1 Vị trí của IPSec trong mô hình OSI

3.1. Kiến trúc an toàn IP (IPSec)

Trong phần này chúng ta sẽ xem xét khái quát về kiến trúc an toàn cho giao thức Internet(IPSec) - một công nghệ mà phần lớn các giải pháp mạng riêng ảo đều dựa vào nó.

3.1.1. Giới thiệu chung và các chuẩn

Kiến trúc IPSec cung cấp một bộ khung an toàn tại tầng IP với cả IPV4 và IPV6. Bằng cách cung cấp khả năng an toàn tại tầng này, các giao thức tầng giao

vận và các ứng dụng có thể dùng IPSec để đảm bảo an toàn mà không phải thay đổi gì cả.

Một số ứng dụng cung cấp dịch vụ bảo mật trên tầng ứng dụng như SSL hay TLS. Đối với các giao thức này, trình ứng dụng gọi tới ứng dụng bảo mật do tầng dưới cung cấp để tạo các ứng dụng bảo mật (ví dụ như giao diện cung cấp các hỗ trợ bảo mật -SSPI). Trong sản phẩm Window 2000 cung cấp giao diện chung cho phép các ứng dụng ở tầng trên truy nhập vào các module bảo mật ở tầng dưới), các ứng dụng ít nhất cần nhận thức được vấn đề bảo mật. IPSec giải quyết được yêu cầu này bằng cách chuyển vấn đề bảo mật xuống tầng 3. Điều này cho phép các ứng dụng duy trì được tính không phụ thuộc vào hạ tầng bảo mật của các tầng dưới. Các gói IP sẽ được bảo vệ mà không phụ thuộc vào các ứng dụng đã sinh ra chúng. Nói một cách khác, các ứng dụng không cần biết tới vấn đề bảo mật trên nền IP. Các quy tắc bảo mật được định nghĩa thống nhất giữa các nhà quản trị mà không phụ thuộc vào một ứng dụng nào được chạy trên hệ thống và IPSec là trong suốt đối với các ứng dụng. Điều này đem lại những lợi ích vô cùng to lớn, đó là khả năng xác thực, bảo mật và kể cả mã hoá dữ liệu được truyền qua bất kỳ mạng IP nào. Như vậy, IPSec cung cấp khả năng bảo mật đầu cuối - tới - đầu cuối giữa các máy tính và mạng máy tính.

IPSec là một kiến trúc an toàn dựa trên chuẩn mở, nó có các đặc trưng sau:

- Cung cấp tính xác thực, mã hóa, toàn vẹn dữ liệu và bảo vệ sự phát lại

- Cung cấp khả năng tạo và tự động làm tươi các khóa mật mã một cách an toàn

- Sử dụng các thuật toán mật mã mạnh để cung cấp tính bảo mật

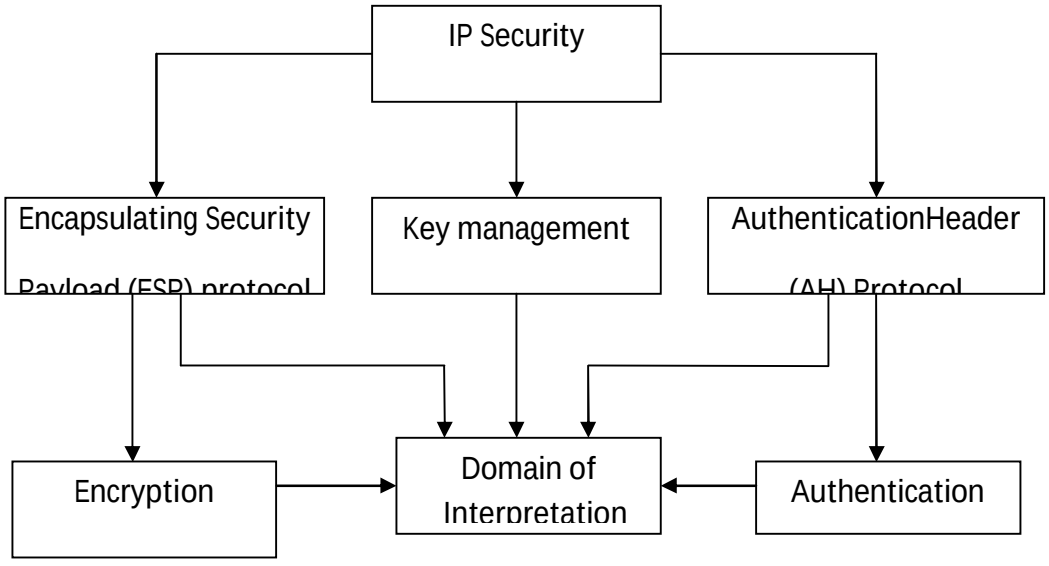
- Cung cấp khả năng xác thực dựa trên chứng chỉ số

- Điều chỉnh các thuật toán mật mã và các giao thức trao đổi khoá

- Cung cấp tính năng an toàn cho các giao thức đường hầm truy cập từ xa như L2TP, PPTP

IPSec cung cấp khả năng bảo mật thông tin giữa hai đầu cuối nên chỉ có nơi gửi và nơi nhận là cần biết chi tiết về các vấn đề liên quan đến bảo mật. Các thiết bị khác nằm trên đoạn đường giữa hai đầu không phải bận tâm đến công việc mã hoá, trao đổi khoá bảo mật vv… khi chuyển tiếp dữ liệu. Đối với khách hàng, điều này đồng nghĩa với việc một chế độ bảo mật mức cao có thể được thiết lập mà không đòi hỏi sự đầu tư hay thay đổi quá lớn đối với hạ tầng mạng, người ta gọi giải pháp VPN ứng dụng giao thức IPSec là "Desktop VPN" vì toàn bộ chức năng bảo mật dữ liệu được thực hiện ngay tại trạm làm việc và các thiết bị mạng không cần quan tâm đến các công tác bảo đảm an toàn. Khi sử dụng các thuật toán xác thực và mã hoá dữ liệu đã được chuẩn hoá, IPSec đã khai thác tối đa lợi ích của các công nghệ này và tạo ra một cách tiếp cận hiệu quả tới mục tiêu bảo vệ luồng dữ liệu truyền trên mạng.

Công việc bảo mật các gói tin IP được thực hiện bằng hai giao thức: Xác thực tiêu đề(AH) và đóng gói tải bảo mật(ESP). AH được sử dụng để đảm bảo tính toàn vẹn của dữ liệu, cung cấp khả năng bảo vệ trước sự giả mạo và chế độ xác thực đối với máy chủ. ESP cũng thực hiện các chức năng tương tự như AH nhưng nhưng kèm thêm khả năng bảo mật dữ liệu. Cũng cần nhấn mạnh rằng cả hai giao thức này đều không chỉ ra bất kỳ một thuật toán mã hoá và xác thực cụ thể nào mà chỉ tạo ra khả năng ứng dụng tốt nhất một trong các thuật toán đang hiện hành.



Hình 3.25: Kiến trúc bộ giao thức IPSec

Bộ giao thức IPSec mang lại ba khả năng chính, đó là:

- Đảm bảo tính toàn vẹn và xác thực dữ liệu: IPSec cung cấp một cơ chế mạnh để xác minh tính xác thực của người gửi và nhận ra bất kỳ sự thay đổi nào không bị phát giác trước đó về nội dung của gói dữ liệu bởi người nhận không mong muốn. Giao thức IPSec mang lại sự bảo vệ tốt chống lại sự giả mạo, do thám hoặc tấn công dịch vụ.

- Sự tin cậy: Giao thức IPSec mã hoá dữ liệu bằng việc dùng các kỹ thuật mật mã cao cấp, nó ngăn chặn những người dùng trái phép truy cập dữ liệu trong khi nó đang được truyền đi. IPSec cũng sử dụng các cơ chế đường hầm để dấu địa chỉ IP của Node nguồn và đích đối với kẻ nghe trộm.

- Quản lý khóa: IPSec sử dụng giao thức bên thứ ba, trao đổi khoá Internet (IKE) để thương lượng giao thức bảo mật và thuật toán mã hóa trước và trong một phiên làm việc. Quan trọng hơn, IPSec phân phối, kiểm soát khoá và cập nhật các khoá này khi được yêu cầu.

Hai khả năng thứ nhất của IPSec, xác thực tính toàn vẹn dữ liệu và sự tin cậy được cung cấp bởi hai giao thức khoá trong bộ giao thức IPSec. Các giao thức này bao gồm AH và ESP.

Khả năng thứ ba, quản trị khoá, nằm trong địa hạt của giao thức khác. Nó được chấp nhận bởi bộ IPSec vì dịch vụ quản lý khoá tốt của nó

3.1.2. Liên kết bảo mật IPSec (SA-IPSec)

Liên kết bảo mật là một khái niệm cơ sở của giao thức IPSec. Như một lời trích dẫn của các nhà phát triển IPSec: Một SA là một kết nối logic theo hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec, được định danh một cách duy nhất bởi ba phần sau:

<Security Parameter Index, IP Destination Address, Security Protocol>

Một IPSec SA được xác định là:

- Các thuật toán, khoá, các giao thức xác thực.

- Mô hình và khoá cho các thuật toán xác thực được dùng bởi các giao thức AH hoặc ESP của IPSec thích hợp.

- Các thuật toán mã hoá, giải mã và các khoá.

- Thông tin liên quan đến khoá như: thời gian thay đổi và thời gian sống của khoá.

- Thông tin liên quan đến chính SA, bao gồm: địa chỉ nguồn SA, thời gian sống.

Sau đây ta sẽ lần lượt xem xét ba phần của một SA

Hình 3.3 Mô tả ba trường của một IPSec SA

Như hình minh hoạ 3.3, một SA gồm 3 trường

- **SPI(Security Parameter Index):** Là một trường 32 bít, nó định danh giao thức bảo mật, được xác định bởi trường giao thức bảo mật(Security Protocol), từ IPSec thích hợp đang sử dụng. SPI được mang như một phần trên tiêu đề của giao thức bảo mật và thường được lựa chọn bởi hệ thống đích trong khi thương lượng thiết lập SA. SPI chỉ có ý nghĩa lôgic, được định nghĩa bởi người tạo SA. SPI nhận các giá trị trong phạm vi 1 đến 255, giá trị 0 được dùng cho mục đích thực thi đặc biệt cục bộ

- **Địa chỉ IP đích:** Đây là địa chỉ IP của Node đích. Mặc dù nó có thể là một địa chỉ broadcast, unicast hoặc multicast, các cơ chế quản trị SA hiện tại được định nghĩa chỉ với các địa chỉ unicast.

- **Giao thức bảo mật:** Trường này mô tả giao thức bảo mật IPSec, nó có thể là AH hoặc ESP.

Trước khi hai máy chủ có thể liên lạc được với nhau sử dụng giao thức IPSec, chúng cần thống nhất các hướng dẫn cho phiên làm việc đó (ví dụ như cách xác thực lẫn nhau hay thuật toán mã hoá hai bên cùng sử dụng). Đây chính là việc liên

kết bảo mật, đó chính là thoả thuận cách thức thống nhất được sử dụng cho việc bảo mật dữ liệu giữa hai đầu cuối.

Một SA IPSec sử dụng hai cơ sở dữ liệu:

+ ***Cơ sở dữ liệu chính sách bảo mật (SPD):*** duy trì thông tin về dịch vụ bảo mật trong một danh sách có thứ tự của các thực thể chính sách vào ra. Rất giống với các luật và bộ lọc gói tin của Firewall. Các thực thể này định nghĩa lưu lượng phải được xử lý và lưu lượng được bỏ qua trên các chuẩn IPSec.

+ ***Cơ sở dữ liệu liên kết bảo mật(SAD):*** duy trì thông tin liên quan tới mỗi SA. Thông tin này bao gồm cả các khoá và thuật toán, khoảng thời gian sống của SA, chế độ giao thức và số tuần tự.

Liên kết bảo mật là đa hướng, có nghĩa là cần thiết lập các liên kết bảo mật khác nhau cho luồng dữ liệu đi và đến. Thêm vào đó, nếu máy chủ liên lạc với một hay nhiều máy chủ khác trong cùng một thời điểm thì cũng cần thiết lập từng đó liên kết. Các liên kết bảo mật được lưu trữ trong cơ sở dữ liệu tại mỗi máy tính với chỉ số về thông số bảo mật (SPI) cho mỗi phần tiêu đề AH và ESP tương ứng. Phía nhận sẽ sử dụng các thông số này để quyết định sẽ áp dụng liên kết bảo mật nào để xử lý gói tin vừa nhận được. Trên thực tế, thủ tục trao đổi khoá Internet (IKE) là thủ tục cho phép quản lý việc tạo ra các liên kết bảo mật và tạo ra các khoá bảo mật để bảo vệ nội dung thông tin. IKE sử dụng thuật toán Diffie- Hellman để tạo ra và quản lý các khoá bí mật, thiết lập kênh trao đổi khoá đối xứng dùng cho việc mã hoá và giải mã thông tin giữa hai đầu, cuối.

3.1.3. Các giao thức của IPSec

Đó là các giao thức xác thực tiêu đề (AH) và giao thức đóng gói tải bảo mật (ESP). Các giao thức này có thể được cấu hình để bảo vệ toàn bộ phần thân của gói tin IP hoặc chỉ riêng phần thông tin liên quan đến các giao thức ở tầng trên.

AH được định nghĩa bởi nhóm làm việc RFC 2402, đảm bảo tính toàn vẹn dữ liệu trên đường truyền bằng khoá H (Hàm băm – Hashing function). AH thực hiện phần thuật toán băm cả phần đầu và phần thân của gói tin IP nhưng không áp dụng cho các thông tin sẽ thay đổi trên đường truyền như số đếm của mỗi nút mạng, vì

thế AH cho phép thay đổi thông tin địa chỉ và đảm bảo dữ liệu của gói tin IP sẽ không bị nghe trộm. Điều này dẫn đến một chức năng nữa của AH là khả năng chống lại việc giả mạo (đột nhập vào giữa đường truyền của các gói tin và tạo ra các gói tin giả) khi sử dụng các số thứ tự tăng dần gắn vào mỗi gói tin. Tuy nhiên, AH không cung cấp khả năng mã hoá dữ liệu.

ESP là một giao thức Internet được nhóm công tác RFC 2406 định nghĩa. Khi được sử dụng riêng rẽ hoặc kết hợp với giao thức AH, ESP đảm bảo tính toàn vẹn và chức năng mã hoá dữ liệu. Các thuật toán mã hoá do ESP hỗ trợ bao gồm DES-CBC, DES 56 bit và 3DES. Ngoài ra ESP còn cho phép kiểm tra tính toàn vẹn của gói tin thông qua HMAC MD5 và HMAC SHA.

3.1.3.1. Giao thức xác thực tiêu đề (AH)

Giao thức xác thực tiêu đề thêm một tiêu đề vào gói IP. Như tên gọi của nó, tiêu đề này phục vụ cho việc xác thực gói dữ liệu IP gốc tại người nhận cuối cùng, tiêu đề này giúp nhận biết bất kỳ sự thay đổi nào về nội dung của gói dữ liệu bởi người dùng không mong muốn trong khi đang truyền, tuy nhiên AH không đảm bảo tính tin cậy.

Để tạo một AH, một giá trị mã thông điệp cần xác thực qua hàm băm (HAMC) được tạo tại người gửi. Giá trị băm này được tạo trên cơ sở của SA, cái xác định trình tự giao dịch sẽ được áp dụng cho gói dữ liệu. Mã kết quả được gắn kèm vào gói dữ liệu sau tiêu đề IP gốc. Tại người nhận cuối, HAMC được giải mã và được dùng để thiết lập việc xác thực người gửi cũng như tính toàn vẹn của thông điệp.

AH không mang lại sự tin cậy trong một giao dịch. Nó chỉ thêm một tiêu đề vào gói IP, phần còn lại của nội dung gói dữ liệu được để mặc. Hơn nữa, AH không bảo vệ bất kỳ trường nào trong tiêu đề IP vì một trong số đó có thể thay đổi trong quá trình truyền, chỉ các trường nào không thay đổi trong quá trình truyền là được bảo vệ bởi AH. Địa chỉ IP nguồn và địa chỉ IP đích là những trường như vậy và vì thế được bảo vệ bởi AH. Tóm lại, giao thức AH có các đặc trưng cơ bản như sau:

- Cung cấp tính toàn vẹn dữ liệu và bảo vệ chống phát lại

- Sử dụng mã xác thực thông điệp được băm(HMAC), dựa trên chia sẻ bí mật

- Nội dung các gói tin không được mã hoá

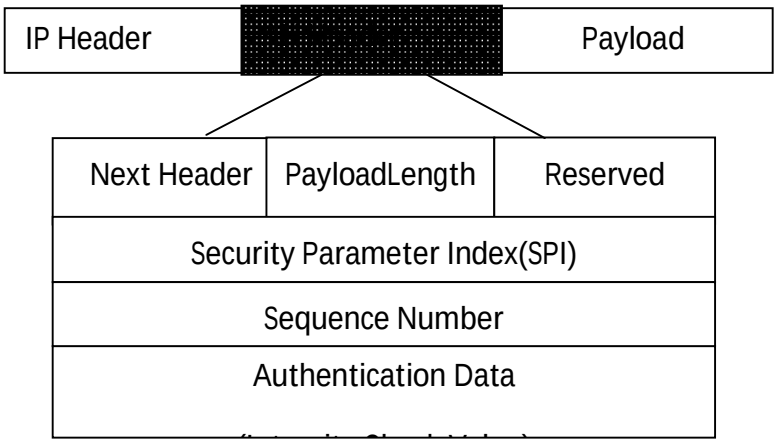
- Không sử dụng các trường changeable IP header để tính toán giá trị kiểm tra tính toàn vẹn(IVC)

1. Khuôn dạng gói tin

Khuông dạng của gói tin theo giao thức AH được minh hoạ như trong hình 3.4. Các trường trong AH header đều là bắt buộc.

- Next Header: Trường này nhận biết giao thức bảo mật, có độ dài 8 bít để xác định kiểu dữ liệu của phần Payload phía sau AH. Giá trị của trường này được chọn từ các giá trị của IP Protocol number được định nghĩa bởi IANA (Internet Assigned Numbers Authority).

- Payload Length: Trường này chỉ định độ dài của thông điệp gắn sau tiêu đề AH.



- Reserved: Trường 16 bit dự trữ để sử dụng cho tương lai, giá trị của trường này bằng 0.

- SPI: Là một số 32 bit bất kì, cùng với địa chỉ IP đích và giao thức an ninh mạng cho phép nhận dạng một thiết lập an toàn duy nhất cho gói dữ liệu. SPI thường được lựa chọn bởi phía thu.

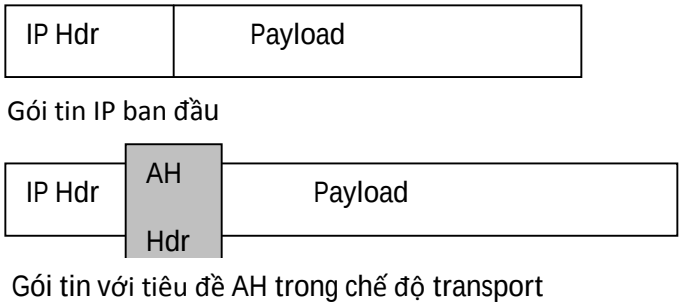
- Sequence Number(SN): Trường gồm 32 bit không dấu đếm tăng dần để sử dụng cho việc chống trùng lặp. Chống trùng lặp là một lựa chọn nhưng trường này là bắt buộc đối với phía phát. Bộ đếm của phía phát và thu khởi tạo 0 khi một liên kết an toàn (SA) được thiết lập, giá trị SN mỗi gói trong một SA phải hoàn toàn khác nhau để tránh trùng lặp. Nếu số gói vượt quá con số 2^{32} thì một SA khác phải được thiết lập.

- Authentication Data: Trường có độ dài biến đổi chứa một giá trị kiểm tra tính toàn vẹn (ICV) cho gói tin, ICV được tính bằng thuật toán đã được chọn khi thiết lập SA. Độ dài của trường này là số nguyên lần của 32 bit, chứa một phần dữ liệu đệm để đảm bảo độ dài của AH là n*32 bit. Giao thức AH sử dụng một hàm băm và băm toàn bộ gói tin trừ trường Authentication Data để tính ICV.

2. Chế độ hoạt động

AH có thể sử dụng ở hai chế độ: Chế độ truyền tải (Transport) và chế độ đường hầm(Tunnel).

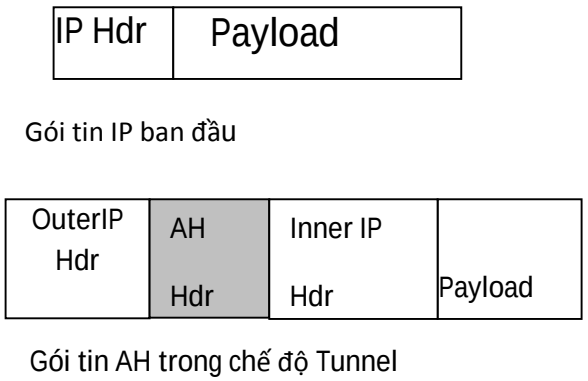
- Chế độ Transport: Chế độ Transport cho phép bảo vệ các giao thức lớp trên cùng với một số trường trong IP Header. Trong chế độ này, AH được chèn vào sau IP Header và trước một giao thức lớp trên như TCP hoặc UDP. Chế độ Transport thường được sử dụng bởi các Host chứ không được sử dụng bởi Gateway. Ưu điểm của chế độ này là đỡ tốn kém chi phí xử lý nhưng nó có khuyết điểm là các trường có thể thay đổi không được xác thực.



Hình 3.5. Gói tin IP trước và sau khi xử lý AH trong chế độ Transport

- Chế độ Tunnel: Trong chế độ Tunnel, một gói tin IP khác được thiết lập dựa trên các gói tin IP cũ. Header của gói IP cũ (bên trong) mang địa chỉ nguồn và

đích cuối cùng, còn Header của gói IP mới (bên ngoài) mang địa chỉ để định tuyến trên Internet. Trong chế độ này, AH bảo vệ toàn bộ gói tin bên trong bao gồm cả Header. Đối với gói tin IP bên ngoài thì vị trí của AH như là trong chế độ transport.



Hình 3.6: Khuôn dạng gói tin AH trong chế độ Tunnel.

Ưu điểm của chế độ Tunnel là bảo vệ toàn bộ gói IP và các địa chỉ cá nhân trong IP Header, tuy nhiên có nhược điểm là tốn chi phí hơn nhiều để xử lý các gói tin.

3. Các thuật toán xác thực

Các thuật toán xác thực để tính ICV được xác định bởi các liên kết bảo mật (SA). Các thuật toán xác thực thích hợp là các thuật toán hàm băm một chiều MD5 và SHA1 (Các thuật toán này bắt buộc một ứng dụng AH phải hỗ trợ). MD5 là chữ viết tắt của Message Digest #5 do Ron Rivest thuộc RSA Security Inc phát minh, tính giá trị Hash 128 bit từ một bản tin nhị phân có độ dài tuỳ ý. SHA được phát triển bởi NIST và NSA, SHA-1 tính giá trị Hash 160 bit từ một bản tin nhị phân có độ dài tuỳ ý. SHA-1 tương tự như MD5 nhưng an toàn hơn do kích thước băm lớn hơn.

4. Xử lý gói đầu vào

Quá trình xử lý gói đầu vào được thực hiện ngược với quá trình xử lý gói đầu ra

- Ghép mảnh: Nếu cần thiết, sẽ tiến hành ghép mảnh trước khi xử lý AH.

- Tìm kiếm SA: Khi đã nhận được một gói tin chứa AH Header, phía thu sẽ xác định một SA phù hợp với địa chỉ IP đích, AH và SPI. Thông tin trong SA sẽ cho biết có cần kiểm tra trường Sequence Number(SN) hay không, có cần thêm trường Authentication Data hay không, các thuật toán và khoá để giải mã ICV. Nếu không có SA nào phù hợp thì phía thu sẽ loại bỏ gói tin.

- Kiểm tra SN: Nếu bên thu không chọn dịch vụ chống lặp thì không cần kiểm tra trường SN. Nếu phía thu có sử dụng dịch vụ chống lặp cho một SA thì bộ đếm gói thu phải được khởi tạo = 0 khi thiết lập SA. Với mỗi gói tin vào khi phía thu tiếp nhận, sẽ kiểm tra có chứa số SN không lặp lại của bất kỳ gói nào trong thời gian tồn tại của SA đó. Nếu bị lặp, gói tin đó sẽ bị loại bỏ.

5. Xử lý gói đầu ra

- Tìm SA: AH được thực hiện trên một gói tin khi đã xác định gói tin đó được liên kết với một SA, SA đó sẽ yêu cầu xử lý gói tin.

- Tạo SN: Bộ đếm phía phát khởi tạo giá trị 0 khi một SA được thiết lập. Khi truyền một gói tin, bộ đếm sẽ tăng lên 1 và chèn giá trị này vào trường SN. Nếu phía phát lựa chọn dịch vụ AntiReplay sẽ kiểm tra để đảm bảo không bị lặp trước khi chèn một giá trị mới vào trường SN.

- Tính ICV: AH ICV được tính dựa trên các dữ liệu sau:

+ Các trường trong IP Header có giá trị không đổi hoặc có giá trị không dự đoán được trong quá trình truyền tới điểm cuối.

+ Bản thân AH Header: Next Header, Payload, Length, Reserved, SPI, SN, Authentication Data (được đặt bằng 0), và explicit padding (nếu có).

+ Dữ liệu của các giao thức lớp trên.

+ Các trường có giá trị thay đổi sẽ được coi bằng 0 trong phép tính ICV các trường có giá trị thay đổi nhưng có thể dự đoán được thì sẽ giữ nguyên giá trị.

- Padding: Có hai loại chèn padding là Authenticaiton Data và Implicit Packet Padding (chèn dữ liệu ngầm định).

+ Authenticaiton Data Padding: Nếu đầu ra của thuật toán xác thực là 96 bit thì không cần chèn thêm dữ liệu. Nhưng nếu ICV có kích thước khác thì phải chèn thêm, nội dung của phần chèn thêm là tuỳ chọn và được đặt sau Authentication Data.

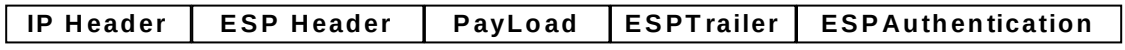
+ Implicit Packet Padding: Đối với một số thuật toán xác thực, chuỗi byte để tính ICV phải là một số nguyên lần của khối n byte. Nếu độ dài gói IP không thoả mãn điều kiện đó thì Implicit Packet Padding sẽ được thêm vào phía cuối của gói. Các byte này bằng 0 và không được truyền đi cùng gói.

- Phân mảnh: Khi cần thiết, phân mảnh sẽ được thực hiện

3.1.3.1. Giao thức đóng gói tải bảo mật(ESP)

Mục đích chính của ESP là cung cấp sự tin cậy thêm vào xác thực người gửi và xác minh tính toàn vẹn của dữ liệu trong khi truyền. ESP mã hoá nội dung của gói dữ liệu bằng cách dùng các thuật toán mã hoá, như đã xác định bởi SA. Một số thuật toán được sử dụng bởi ESP bao gồm: DES-CBG, NULL, CAST-128, IDEA và 3DES. Các thuật toán xác thực thường được dùng tương tự như trong AH là HMAC-MD5 và HMAC-SHA.

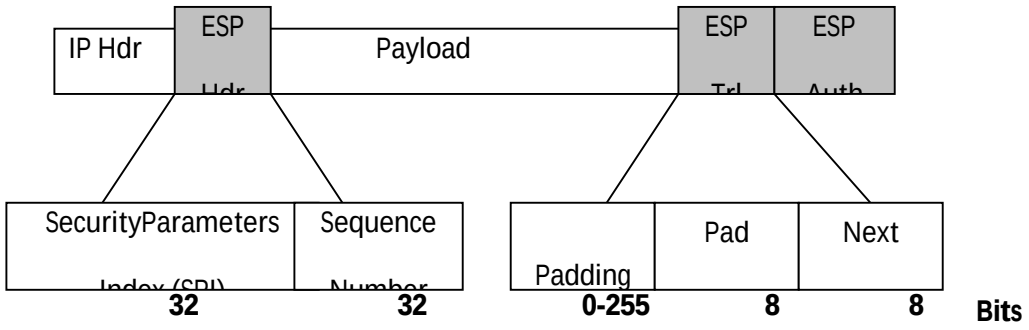
Như đã so sánh với AH, AH mang lại tính xác thực và toàn vẹn dữ liệu đối với gói dữ liệu IP. ESP không bảo vệ toàn bộ gói dữ liệu. Chỉ có payload được bảo vệ, như trong hình 3.7. Tuy nhiên, ESP rất mạnh trong nhóm mã hoá. Nó cũng không chiếm dụng nhiều CPU. Kết quả là nó nhanh hơn AH. Nhưng 24 byte mà nó thêm vào gói dữ liệu có thể làm chậm xuống việc phân đoạn và tính toán thông lượng.



Hình 3.7 Gói IP sau khi tiêu đề ESP và Trailer ESP được thêm vào

1. Khuông dạng gói dữ liệu dựa trên ESP

Khuôn dạng của gói ESP phức tạp hơn so với khuôn dạng của AH, nó không chỉ gồm ESP header mà còn ESP trailer và ESP Authentication data. Dữ liệu tải(Payload) được định vị giữa header và trailer.



Hình 3.8 Khuôn dạng ESP

Các trường trong ESP đều là bắt buộc:

- SPI: Là một số 32 bit bất kỳ, cùng với địa chỉ IP đích và giao thức an ninh, ESP cho phép nhận dạng duy nhất SA cho gói dữ liệu này. Các giá trị SPI từ 1 đến 255 được dành riêng để sử dụng trong tương lai. Giá trị SPI = 0 để chỉ ra chưa có SA nào tồn tại.

- SN: Giống như AH, trường SN chứa một giá trị đếm tăng dần để chống lặp lại. Mỗi SA được lựa chọn thì giá trị của trường này bắt đầu là 0.

- Payload Data: Trường có độ dài biến đổi chứa dữ liệu mô tả trong Next Header. Payload Data là trường bắt buộc, được mã hoá bởi các thuật toán mã hoá, các thuật toán mã hoá này được lựa chọn ngay khi thiết lập SA. Trường này có độ dài bằng một số nguyên lần 1 byte.

- Padding: Trường này được thêm vào để đoạn được mã hoá là một số nguyên lần của một khối các byte. Ngoài ra trường còn dùng để che dấu độ dài thực của Payload.

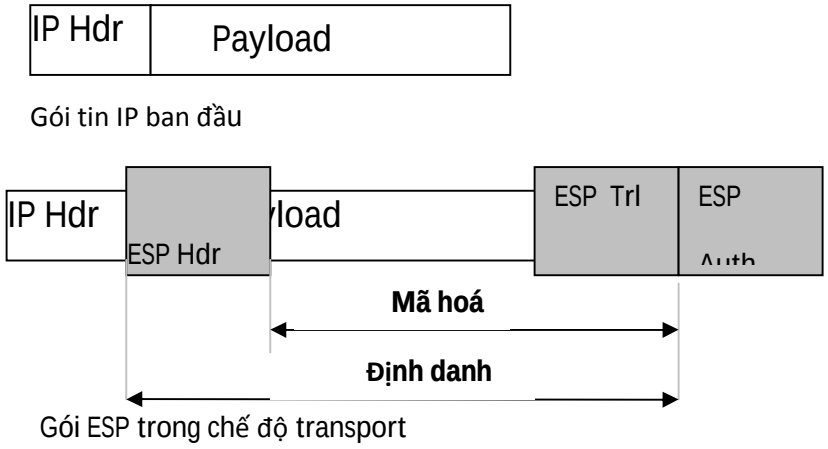
- Pad Length: Trường này xác định số byte padding đã thêm vào (0 đến 225)

- Next Header: Là trường 8 bit bắt buộc, nó chỉ ra kiểu dữ liệu trong Payload Data. Ví dụ một giao thức bậc cao hơn như TCP. Giá trị của trường được chọn trong chuẩn IP Protocol Number được đưa ra bởi IANA.

- Authentication Data: Trường có độ dài biến đổi chứa giá trị ICV được tính cho gói ESP từ SPI đến Next Header. Authentication là trường không bắt buộc, được thêm vào nếu dịch vụ Authentication được lựa chọn cho SA đang xét. Các

thuật toán để tính ICV là các thuật toán hàm băm một chiều MD5 hoặc SHA giống với AH.

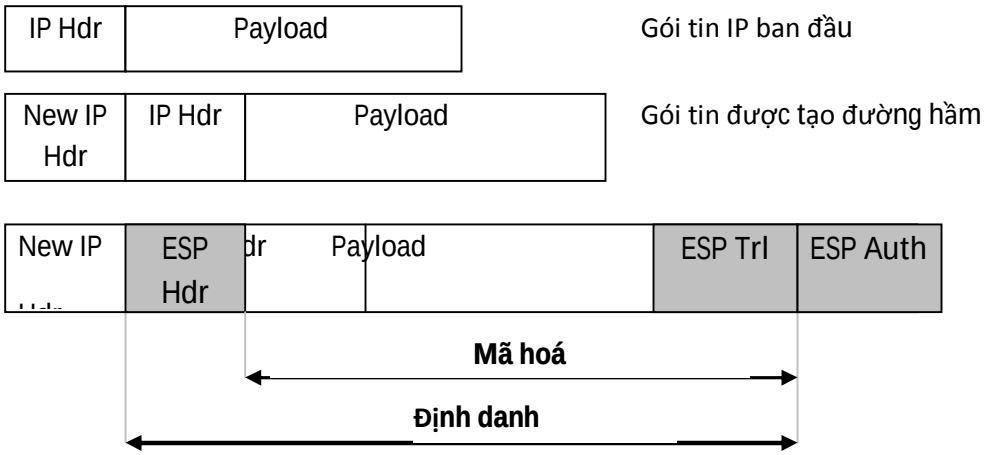
2. Chế độ hoạt động



Hình 3.8 Gói ESP trong chế độ Transport

ESP cũng được sử dụng ở hai chế độ: Transport và Tunnel

- Chế độ Transport: Chế độ Transport cho phép bảo vệ các giao thức lớp trên nhưng không bảo vệ IP Header. Các gói tin IP cũ được cắt phần tiêu đề ra, sau đó tiêu đề ESP được đưa vào giữa. ESP trailer sẽ được đưa vào cuối gói tin, cuối cùng là Authentication Data được đưa thêm vào. Chế độ Transport không mã hoá cũng không xác thực IP Header, tuy nhiên nó có chi phí xử lý thấp, chỉ được dùng cho các Host.



Hình 3.9 Gói ESP trong chế độ Tunnel

- Chế độ Tunnel: Trong chế độ này, gói IP mới được xây dựng cùng với một IP Header mới. Các IP Header bên trong mang địa chỉ nguồn và đích cuối cùng, còn IP Header bên ngoài mang địa chỉ định tuyến qua Internet. Ở chế độ này, ESP sẽ bảo vệ cả gói tin IP ban đầu bao gồm: Payload và IP header. Đối với gói IP bên ngoài thì vị trí của ESP giống như trong chế độ Transport.

3. Các thuật toán sử dụng trong ESP

Các thuật toán bắt buộc bao gồm:

- Các thuật toán mật mã: DES ở chế độ CBC, AES, NULL. Thuật toán mã hoá được xác định bởi SA. ESP làm việc với các thuật toán mã hoá đối xứng. Với sự có mặt của trường Padding, các thuật toán mã hoá có thể có đặc tính khối hoặc luồng.

- Các thuật toán xác thực: Mã xác thực bản tin MAC sử dụng MD5, mã xác thực bản tin MAC sử dụng SHA, NULL (Không sử dụng mã xác thực)

4. Xử lý gói tin đầu ra

Quá trình xử lý gói đầu ra bao gồm các bước sau:

- Tìm kiếm SA: Giống như AH, ESP được thực hiện trên một gói tin chỉ khi nào bộ điều khiển IPSec đã xác định gói tin đó được liên kết với một SA.

- Mã hoá gói tin: Tuỳ thuộc vào chế độ Tunnel hay Transport mà ESP thực hiện đóng gói toàn bộ gói tin hay chỉ đóng gói phần Payload. Thêm Padding nếu cần thiết, mã hoá các trường Payload Data, Padding, PadLength, Next Header theo các thuật toán đã được chỉ ra bởi SA. Nếu dịch vụ xác thực được lựa chọn thì việc mã hoá được thực hiện trước, quá trình mã hoá không bao gồm trường Authentication Data. Và quá trình xác thực được thực hiện sau. Thứ tự xử lý này cho phép nhanh chóng xác định và loại bỏ các gói lỗi hoặc lặp lại mà không cần phải giải mã gói tin, đồng thời cho phép phía thu xử lý song song cả hai việc: giải mã và xác thực.

- Tạo SN: Quá trình này được thực hiện giống với AH.

- **Tính ICV:** Nếu dịch vụ xác thực được lựa chọn thì phía phát sẽ tính các giá trị ICV trên gói dữ liệu ESP gồm các trường sau: SPI, SequenceNumber, Payload Data, Padding, PadLength và Next Header. Trong đó 4 trường cuối ở dạng đã mã hoá. ICV được tính dựa vào các thuật toán xác thực dùng hàm băm một chiều như MD5 và SHA-1.

- **Phân mảnh:** Nếu cần thiết thì phân mảnh sẽ được thực hiện sau khi đã xử lý ESP.

5. Xử lý gói tin đầu vào

Quá trình xử lý gói đầu vào gồm các bước ngược với quá trình xử lý gói tin đầu ra.

- **Ghép mảnh:** Ghép mảnh được thực hiện trước khi xử lý ESP. Nếu một gói tin cần xử lý ESP ở dạng phân mảnh thì phía thu phải loại bỏ gói tin đó.

- **Tìm kiếm SA:** Khi nhận được một gói tin chứa ESP Header, phía thu sẽ xác định một SA phù hợp dựa trên địa chỉ đích, giao thức bảo mật và SPI. Nếu không thể tìm thấy một SA nào phù hợp cho phiên truyền dẫn này thì phía thu sẽ loại bỏ gói tin.

- **Kiểm tra SN:** Giống với kiểm tra SN trong AH.

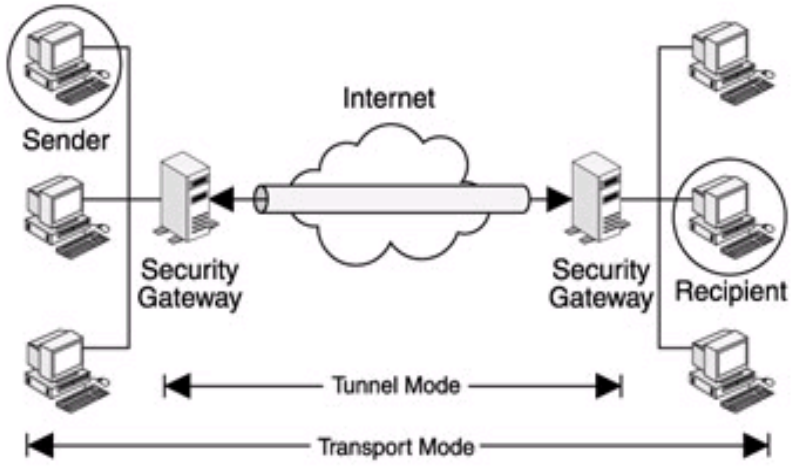
- **Kiểm tra ICV:** Nếu dịch vụ xác thực được lựa chọn phía thu sẽ tính ICV của gói ESP ngoại trừ trường Authentication Data rồi so sánh với ICV của gói tin nhận được. Nếu hai giá trị ICV này trùng nhau thì gói tin là hợp lệ, nếu không gói tin sẽ bị loại bỏ. Việc kiểm tra được tiến hành như sau: Trước tiên trường Authentication Data được tách ra khỏi ESP và lưu lại, sau đó kiểm tra độ dài gói ESP còn lại, nếu Padding đã được ngầm định thì các byte 0 được thêm vào sau trường Next Header sau đó sẽ tính ICV và so sánh với giá trị ICV được lưu trong trường Authentication Data.

- **Giải mã gói tin:** Đầu tiên là giải mã ESP bao gồm các trường Payload Data, Padding, Padlength, NextHeader sử dụng khoá, thuật toán mật mã đã xác định bởi SA. Sau đó xử lý phần Padding theo đặc điểm của thuật toán, loại bỏ nó trước khi

đưa lên các lớp trên. Cuối cùng là xây dựng lại gói tin IP ban đầu tuỳ thuộc vào chế độ Transport hay Tunnel. Nếu là Transport, xây dựng lại gói tin ban đầu từ IP Header và thông tin giao thức lớp trên trong Payload của ESP. Nếu là Tunnel, xây dựng lại gói tin ban đầu từ IP Header của gói bên ngoài và toàn bộ gói IP bên trong.

3.1.4. Các chế độ IPSec

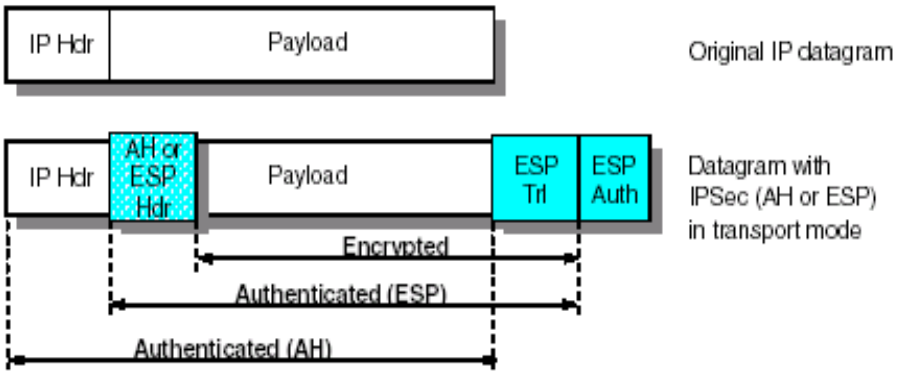
Các giao thức của IPSec có thể thực hiện các liên kết an toàn trong hai chế độ: Transport và Tunnel. Như được mô tả trong hình 3.10, cả AH và ESP đều có thể hoạt động cả trong hai chế độ



Hình 3.10 Hai chế độ IPSec

3.1.4.1. Chế độ Transport

Chế độ Transport bảo vệ các giao thức tầng trên và các ứng dụng. Trong chế độ này, tiêu đề IPSec được chèn vào giữa tiêu đề IP và tiêu đề của giao thức tầng trên như được minh họa trong hình 3.11



Hình 3.11 IPSec – chế độ Transport

Trong giao thức ESP, ESP trailer và dữ liệu xác thực ESP được thêm vào sau phần dữ liệu gốc được tải. Tiêu đề mới được chèn vào trước phần dữ liệu được tải

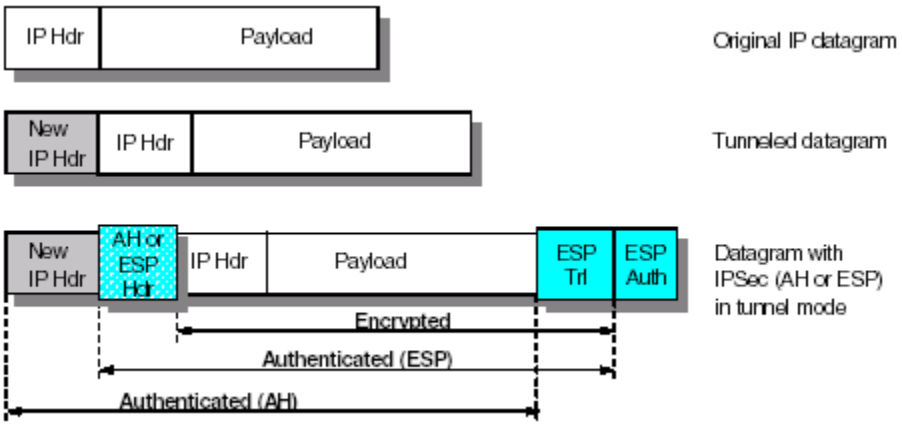
Chế độ Transport được dùng bởi các host, không được dùng bởi các getway. Các Getway thậm chí không yêu cầu hỗ trợ chế độ Transport.

Ưu điểm của chế độ Transport là xử lý ít Overhead, vì vậy nó nhanh hơn. Một nhược điểm của nó là các trường hay thay đổi không được xác thực. ESP trong chế độ Transport không cung cấp tính năng xác thực và mã hóa với các tiêu đề IP. Đây là một nhược điểm vì các gói tin sai (tấn công giả mạo) có thể vẫn được phân phối cho quá trình xử lý ESP. Một nhược điểm khác là địa chỉ gói IP gốc phải được dùng để phân phối. Điều này có thể là một vấn đề nới địa chi IP riêng được dùng, hoặc nơi cấu trúc địa chỉ mạng bên trong cần được dấu trong mạng công cộng.

3.1.4.2. Chế độ Tunnel

Không giống như chế độ Transport, chế độ Tunnel bảo vệ toàn bộ gói IP. Toàn bộ gói IP được đóng gói vào trong một gói IP khác và tiêu đề IPSec được chèn vào giữa tiêu đề IP gốc và tiêu đề IP mới. Trong chế độ này, khái niệm đường hầm được áp dụng.

Với giao thức ESP thì gói dữ liệu gốc trở thành gói dữ liệu tải cho gói ESP mới và kết quả là cả mã hóa cũng như xác thực được thực thi nếu được chọn. Tuy nhiên, tiêu đề IP mới vẫn không được bảo vệ.



Hình 3.12 IPSec – chế độ Tunnel

Chế độ Tunnel được sử dụng bởi các Getway. Như vậy, giữa 2 firewall chế độ Tunnel luôn được dùng cho luồng thông tin đang lưu chuyển qua các firewall giữa các mạng an toàn qua một đường hầm IPSec.

Mặc dù các Getway được hỗ trợ chỉ với chế độ Tunnel, thông thường chúng vẫn có thể làm việc được trong chế độ Transport. Chế độ này được cho phép khi Getway hoạt động như một Host, đó là trường hợp luồng thông tin được giành riêng cho chính nó. Ví dụ: các lệnh SNMP, hoặc các yêu cầu báo lại ICMP.

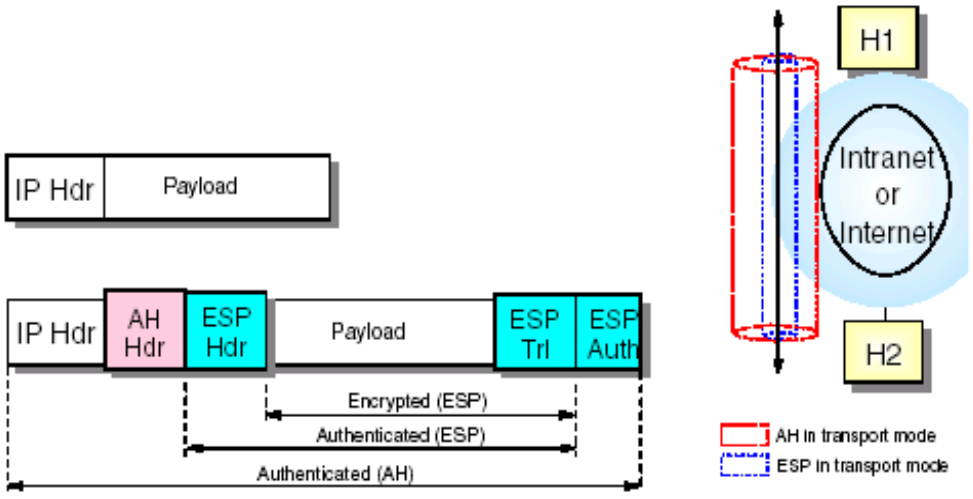
Trong chế độ Tunnel các địa chỉ IP của tiêu đề ngoài không cần phải giống với các địa chỉ của tiêu đề bên trong. Ví dụ, hai getway bảo mật có thể thực hiện một đường hầm AH có xác thực tất cả các luồng thông tin giữa các mạng chúng kết nối cùng nhau.

Ưu điểm của chế độ Tunnel là nó bảo vệ tất cả gói IP đã được đóng gói và khả năng sử dụng các địa chỉ riêng. Tuy nhiên, có một quá trình xử lý Overhead nhiều hơn bình thường gắn liền với chế độ này

3.1.5. Sự kết hợp giữa các SA

Các giao thức AH và ESP có thể được áp dụng riêng lẻ hoặc kết hợp cùng nhau. Trong một số trường hợp yêu cầu tính bảo mật cao, cần phải kết hợp giữa AH và ESP. Sự kết hợp giữa các giao thức IPSec.

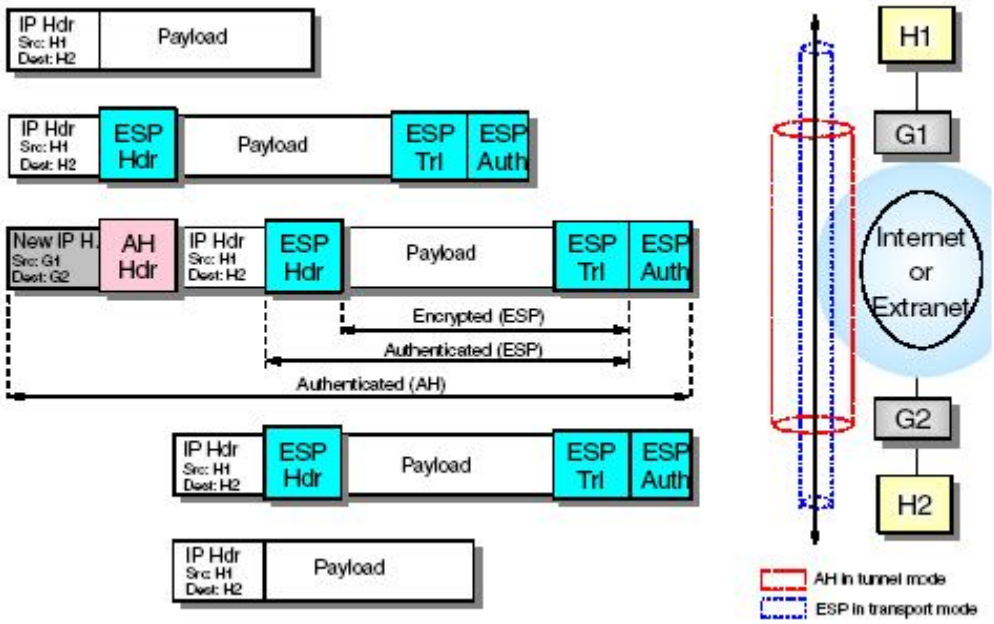
3.1.5.1. Kết hợp giữa AH và ESP trong chế độ Transport



Hình 3.13 Kết hợp AH và ESP trong chế độ Transport

Gói IP ban đầu được tách Header ra, tiếp theo phần Payload được xử lý ESP sau đó được xử lý bằng AH. Cuối cùng, IP Header được thêm vào. Như vậy gói tin sẽ được đảm bảo an toàn 2 lớp: lớp bên ngoài là AH, lớp bên trong là ESP.

3.1.5.2. Kết hợp AH và ESP ở chế độ Tunnel



Hình 3.14 Kết hợp AH và ESP trong chế độ Tunnel.

Ban đầu, gói tin IP được xử lý ESP ở chế độ Transport, tiếp theo đó toàn bộ gói tin ESP được xử lý AH trong chế độ Tunnel.

3.2. Giao thức trao đổi khoá Internet

3.2.1. Giới thiệu chung và các chuẩn

Bản thân giao thức IPSec không có khả năng thiết lập SA. Do đó quá trình được chia làm 2 phần: IPSec cung cấp xử lý ở mức gói và giao thức quản lý trao đổi khoá Internet thoả thuận các SA, IKE được chọn làm giao thức chuẩn để thiết lập các SA cho IPSec. IKE tạo ra một đường hầm được xác thực và mã hoá, sau đó là thoả thuận SA cho IPSec. Quá trình này yêu cầu hai hệ thống xác thực lẫn nhau và thiết lập các khoá sử dụng chung.

Được biết đến đầu tiên là ISAKMP/Oakley, trong đó ISAKMP là viết tắt của Internet Security Association and Key Management Protocol (Liên kết bảo mật Internet và Giao thức quản lý khoá).

IKE trợ giúp các nhóm liên lạc thương lượng các tham số bảo mật và các khoá xác thực trước khi một phiên IPSec an toàn được thực thi. Các tham số bảo mật được thương lượng này sẽ được định nghĩa một lần trong SA. Ngoài việc thương lượng và thiết lập các tham số bảo mật và các khoá mật mã, IKE cũng thay đổi các tham số và khoá khi được yêu cầu trong một phiên làm việc, IKE cũng chịu trách nhiệm xoá các khoá và các SA này sau khi một phiên truyền tin được hoàn tất.

Những ưu điểm chính của IKE bao gồm:

- IKE không phục thuộc vào công nghệ. Vì vậy nó có thể được dùng với bất kỳ cơ chế bảo mật nào.

- IKE mặc dù không nhanh, nhưng hiệu quả cao vì một số lượng lớn các SA được thương lượng với một số thông điệp vừa phải.

Theo cấu trúc làm việc của ISAKMP. IKE làm việc qua hai pha.

Hai pha trao đổi khoá sẽ tạo ra IKE SA và một đường hầm an toàn giữa hai hệ thống. Một phía sẽ đưa ra một trong các thuật toán, phía kia sẽ chấp nhận hoặc loại bỏ kết nối. Khi hai bên đã thống nhất được các thuật toán sẽ sử dụng thì chúng sẽ tạo khoá cho IPSec. IPSec sử dụng một khoá dùng chung khác với khoá của IKE, khoá này có được nhờ sử dụng thuật toán Diffie-Hellman một lần nữa hoặc sử dụng lại khoá dùng chung có được từ trao đổi Diffie-Hellman ban đầu. Sau khi quá

trình được hoàn tất thì IPSec SA được thiết lập. Quá trình thực hiện IKE gồm 2 pha, đó là : IKE Phase I và IKE Phasse II

3.2.2. Các yêu cầu quản lý khoá đối với IPSec

Các giao thức IPSec AH và ESP yêu cầu là các chia sẻ bí mật được biết với tất cả các nhóm tham gia có yêu cầu khoá một cách thủ công hoặc phân phối khoá. Vấn đề đặt ra là các khoá có thể bị mất, bị tổn hại hoặc đơn giản là bị hết hạn. Kỹ thuật thủ công không mềm dẻo khi có nhiều liên kết an toàn được quản lý. Một cơ chế trao đổi khoá tinh vi cho IPSec phải đáp ứng các yêu cầu sau:

- Độc lập với các thuật toán mật mã cụ thể
- Độc lập với các giao thức trao đổi khoá cụ thể
- Xác thực các thực thể quản lý khoá
- Thiết lập SA qua tầng vận tải "không đảm bảo"
- Sử dụng hiệu quả các tài nguyên
- Cung cấp khả năng tạo yêu cầu của host và các phiên SA

Giao thức IKE được thiết kế để đáp ứng các yêu cầu đó. Nó dựa trên các liên kết bảo mật Internet và cấu trúc của giao thức quản lý khoá và giao thức phân phối khoá Oakley. IKE có các đặc trưng sau:

- Có các thủ thục tạo khoá và xác thực danh tính
- Tự động làm tươi khoá
- Giải quyết bải toán "khoá đầu tiên"
- Mỗi giao thức bảo mật có không gian các SPI riêng của nó
- Có các tính năng bảo vệ được xây dựng sẵn
    + Chống được các tấn công từ chối dịch vụ
    + Chống được tấn công chiếm quyền điều khiển phiên và kết nối
- Bảo mật toàn diện
- Cách tiếp cận dựa trên 2 pha

+ Pha 1 - Thiết lập các khoá và SA cho trao đổi khoá

+ Pha 2 - Thiết lấp các SA cho truyền dữ liệu

- Được thực thi như ứng dụng qua UDP, cổng 500

- Hỗ trợ các chứng chỉ cho Host và người dùng

- Sử dụng xác thực mạnh với trao đổi khoá ISAKMP

+ Chia sẻ trước các khoá

+ Các khoá không thực sự được chia sẻ, chỉ một thẻ bài được dùng cho việc tạo khoá cần thiết

+ Các chữ ký số

+ Hệ mật khoá công khai

Như đã đề cập, IKE yêu cầu 2 pha phải được hoàn tất trước khi luồng dữ liệu được bảo vệ với AH và ESP

3.2.3. Pha thứ nhất của IKE

Pha IKE thứ nhất xác thực người dùng cuối, sau đó thiết lập một phiên IKE bảo mật cho việc thiết lập SA. Rồi sau đó các nhóm truyền tin thương lượng một ISAKMP SA thích hợp với nhau, nó bao gồm cả thuật toán mã hoá, hàm băm và phương thức xác thực để phục vụ cho việc bảo vệ khoá mật mã. Ở dưới khung làm việc ISAKMP sử dụng SA được thiết lập trong pha này. Sau khi cơ chế mã hoá và hàm băm được đồng ý, một khoá bảo mật chủ chia sẻ được tạo. Các thông tin sau thường được dùng để tạo khoá mật chia sẻ này bao gồm:

- Các giá trị Diffie-Hellman.

- SPI của ISAKMP SA theo dạng của Cookie.

- Một số ngẫu nhiên.

- Nếu hai nhóm đồng ý sử dụng một khoá công khai dựa trên xác thực, họ cũng cần trao đổi ID của họ.

Sau khi trao đổi các thông tin cần thiết, cả hai tạo khoá của họ bằng việc dùng các khoá mật đã chia sẽ này. Theo cách thông thương, khoá mật mã được tạo mà không có bất kỳ một sự trao đổi thực sự nào qua mạng.

IKE Phase thứ nhất thoả thuận các tập chính sách IKE, xác thực đối tác và thiết lập kênh an toàn giữa các đối tác. IKE Phase1 gồm 2 chế độ: Main Mode và Aggressive mode. IKE Phase1 bao gồm các trao đổi sau:

a. Thống nhất các thuật toán mã hoá và xác thực

Trao đổi này để bảo vệ các trao đổi thông tin IKE được thoả thuận giữa các đối tác.

- Ban đầu bên A gửi một Message đến B ở dạng chưa mã hoá(ClearText), Message được đóng gói trong một gói tin IP thông thường và nằm trong phần UDP Payload với giao thức lớp trên là UDP.

IP	UDP	ISAK MP Header	SA	Proposal	Transform	...	Proposal	Transform

Hình 3.15 Message 1

- Message này thông báo và yêu cầu bên B lựa chọn các giao thức và các thuật toán được đưa ra ở các trường Proposal và Transform tương ứng, đồng thời tạo ra một giá trị ngẫu nhiên gọi là Cookie A (Initiator Cookie) đưa vào trường ISAKMP Header.

- Tương tự, bên B sẽ trả lời bên A bằng một Message có cấu trúc tương tự như trên, thông báo sẽ chọn giao thức và thuật toán nào, đồng thời đưa ra một giá trị ngẫu nhiên Cookie B (Responder Cookie) vào trường ISAKMP Header.

b. Trao đổi khoá

Tạo các khoá bí mật chung. IKE sẽ sử dụng thuật toán Diffie- Hellman (DH) để tạo một khoá bí mật dùng chung giữa bên A và bên B.

- Bên A gửi:

+ Số nguyên tố lớn N.

+ Số g là một phần tử nguyên thuỷ của Z^*_N.

+ Hàm f(x)= g^X mod N với X là số ngẫu nhiên thuộc Z^*_N do A chọn và gửi f(x) cho B.

- Bên B chọn ngẫu nhiên y thuộc Z^*_N và tính f(y) = g^Y mod N rồi gửi cho A. Sau khi nhận được giá trị f(x), bên B tính $S_B = f(x)^Y$ mod N. Còn A, sau khi nhận được giá trị f(y) của B, A tính: $S_A = f(y)^X$ mod N.

- Dễ dàng chứng minh: $S_B = S_A = S$ và do đó giá trị này được dùng làm khoá chung bí mật mà chỉ có A và B mới có được.

- Cần chứng minh: $S_B = S_A$

- Thật vậy: $S_B = f(x)^Y$ mod N = $(g^X$ mod N$)^Y$ mod N = g^{XY} mod N.
Mặt khác : $S_A = f(y)^X$ mod N = $(g^Y$ mod N$)^X$ mod N = g^{XY} mod N= S_B

- Trao đổi khoá bí mật trình bày ở trên được gọi là trao đổi khoá Diffie-Hellman

- Như vậy, bên A và B đều có khoá chung bí mật là S.

IP Header	UDP Header	ISAKMP Header	g^x	N_i

Hình 3.16 Message 2

c. Xác thực đối tác

Trong trao đổi này hai bên trao đổi các thông tin nhận dạng của nhau thông qua chữ ký số. Messeage 3 được gửi để nhận dạng.

IP Header	UDP Header	ISAKMP Header	Identity	Certificate	Signature

Hình 3.17 Message 3

Các thông tin nhận dạng là các trường sau: Identity, Certificate, Signature đã được mã hóa bằng các giao thức, thuật toán được xác định tại bước trao đổi thức nhất và các khoá chung bí mật đã được thiết lập ở bước trao đổi khoá bí mật.

3.2.4. Pha IKE thứ II

Trong khi pha I thương lượng việc thiết lập SA cho ISAKMP. Pha II giải quyết việc thiết lập SA cho IPSec. Trong pha này, SA được sử dụng bởi nhiều dịch vụ đã được thương lượng. Các cơ chế xác thực, hàm băm, thuật toán mã hoá được bảo vệ theo sau các gói IPSec (dùng AH và ESP) như là một phần của pha SA.

Pha II thương lượng xuất hiện thường xuyên hơn pha I. Điển hình, một thương lượng có thể lặp lại trong 4-5 phút. Sự thay đổi thường xuyên này của khoá mật mã nhằm ngăn chặn Hacker có thể bẻ các khoá này, và sau đó là nội dung của các gói dữ liệu gốc.

Oakley là một giao thức mà IKE dựa vào. Oakley lần lượt định nghĩa 4 chế độ IKE thông dụng.

Thông thường một phiên trong pha II tương đương một phiên đơn trong pha I. Tuy nhiên nhiều pha II trao đổi cũng có thể được hỗ trợ bởi một trường hợp pha I. Điều này làm cho các giao dịch IKE thường rất chậm trở nên tương đối nhanh hơn.

IKE Phase thứ hai có tác dụng:

- Thoả thuận các tham số bảo mật IPSec, các tập chuyển đổi IPSec (IPsec Transform Sets) để bảo vệ đường hầm IPSec.

- Thiết lập các thoả thuận bảo mật IPSec SA.

- Định kỳ thoả thuận lại IPSec SA để đảm bảo tính an toàn của đường hầm.

- Thực hiện trao đổi Diffie-Hellman bổ sung (tạo ra các khoá mới).

Trước tiên, bên A gửi cho bên B một Message, đề xuất các SA để bên B lựa chọn, đồng thời trao đổi một khoá bằng thuật toán DH. Message được đóng gói trong gói tin có khuôn dạng như sau:

IP Header	UDP Header	ISAKMP Header	Hash	SA	Proposal	Transform	…	Proposal	Transform	KE	ID

Hình 3.18 Message 1 của phase2

Trường Hash mang mã Hash của các trường phía sau nó và các trường này cũng được mã hóa bằng các khoá và thuật toán được thoả thuận từ Phase thứ nhất. Các trường Proposal và Transform mang các thông tin về giao thức và các thuật toán mã hoá, xác thực đề nghị để bên B lựa chọn. Trường KE mang các thông tin về trao đổi khoá bí mật theo thuật toán Diffie-Hellman.

Khi bên B nhận được message từ A và xác thực nó sau khi tính lại mã Hash, bên B sẽ trả lời lại bên A một message khác có cấu trúc tương tự như message mà

bên A gửi để thông báo cho bên A biết về giao thức và các thuật toán được sử dụng, các thông tin để trao đổi khoá chung ở trường KE.

3.2.5. Các chế độ IKE

Bốn chế độ IKE: Main Mode. Aggressive mode. Quick mode. New Group mode.

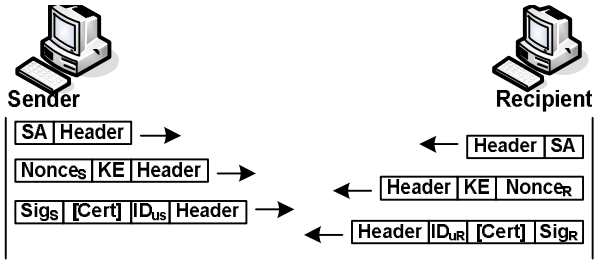
3.2.5.1. Main Mode

Main mode xác minh và bảo vệ các định danh của các nhóm có liên quan trong giao dịch. Trong chế độ này, sáu thông điệp được trao đổi giữa các thực thể truyền thông cuối. Trong các thông điệp này:

Hai thông điệp đầu tiên được dùng để thương lượng chính sách bảo mật cho việc trao đổi.

Hai thông điệp tiếp theo được dùng để trao đổi khoá Diffie-Hellman và Nonce. Các khoá sau này đóng một vai trò quan trọng trong các cơ chế mã hoá. Nonce phải được đánh dấu bởi các nhóm ngược lại cho chức năng xác minh.

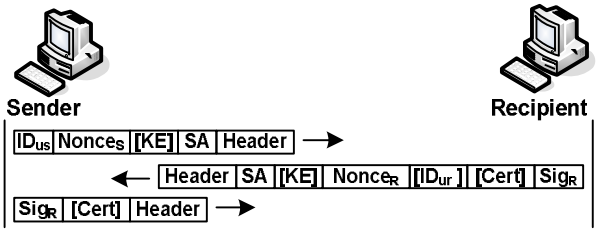
Hai thông điệp cuối cùng của chế độ này được dùng để xác thực các nhóm truyền thông có sự hỗ trợ của chữ ký, hàm băm và tuỳ chọn chứng chỉ. Hình 3.40 mô tả một giao dịch trong chế độ IKE Main



- Header: Một tiêu để ISAKMP tương ứng với chế độ được dùng
- SA: Kết hợp bảo mật được thương lượng
- Nonce: Một số ngẫu nhiên gửi cho việc ký số
- KE: Dữ liệu trao đổi khóa với trao đổi khoá Differ-Helman

Hình 3.19 Trao đổi thông điệp trong chế độ Main IKE

3.2.5.2. Aggressive mode



- Header: Một tiêu đề ISAKMP tương ứng với chế độ được dùng

- SA: Kết hợp bảo mật được thương lượng

- Nonce: Một số ngẫu nhiên gửi cho việc ký số

- KE: Khoá trao đổi dữ liệu cho trao đổi khoá Differ-Helman

Hình 3.20 Mô tả một phiên giao dịch trong chế độ IKE Aggressive

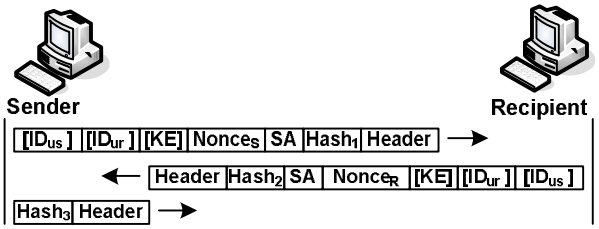
Được thiết lập tương tự như Main mode. Khác nhau giữa hai chế độ chỉ là trong Main mode gồm sáu thông điệp, còn trong chế độ này chỉ ba thông điệp được trao đổi. Kết quả là chế độ này nhanh hơn Main mode. Các thông điệp được trao đổi trong chế độ này như sau:

Thông điệp thứ nhất được dùng để hỗ trợ một chính sách bảo mật, cho đi qua dữ liệu cần thiết.

Thông điệp thứ hai hoạt động như để đáp lại thông điệp thứ nhất. Nó xác thực người nhận và hoàn thành chính sách bảo mật cùng với các khoá.

Thông điệp cuối cùng của chế độ này được dùng để xác thực người gửi

3.2.5.3. Quick Mode



- Header: Một tiêu đề ISAKMP tương ứng với chế độ được dùng

- SA: Kết hợp bảo mật được thương lượng

- Nonce: Một số ngẫu nhiên gửi cho việc ký số

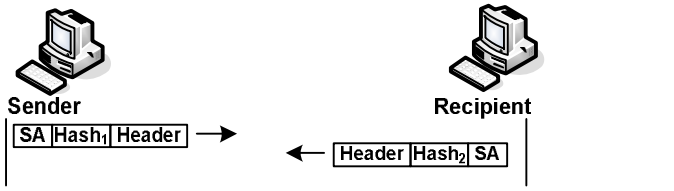
Hình 3.21 Trao đổi thông điệp trong chế độ Quick IKE, thuộc pha thứ II

Chế độ IKE thứ ba, Quick Mode là một chế độ pha II. Nó được dùng để thương lượng với SA về các dịch vụ bảo mật IPSEc. Hơn nữa, Quick Mode cũng tạo ra các khoá mới cần thiết. Nếu chính sách bảo mật chuyển tiếp đầy đủ được thảo luận trước pha I, một quá trình trao đổi khoá Diffie-Hellman được khởi tạo. Trường hợp khác, các khoá mới được tạo bằng việc dùng các giá trị hàm băm.

Trao đổi thông điệp trong chế độ Quick mode được mô tả như trong hình 3.42

3.2.5.4. Chế độ New Group

Chế độ này được dùng để thương lượng với một nhóm riêng mới làm cho khả năng trao đổi khoá Diffie-Hellman trở nên dễ dàng. Hình 3.43 mô tả chế độ New group. Mặc dù chế độ này xuất hiện sau pha I, nhưng nó không phải là một phần của pha II.



- Header: Một tiêu để ISAKMP tương ứng với chế độ được dùng

- SA: Kết hợp bảo mật được thương lượng

Hình 3.22 Trao đổi thông điệp trong chế độ Newgroup IKE

Thêm vào đó, trong bốn chế độ IKE thường được thực thi, có chế độ truyền tin, chế độ này là sự kết hợp bởi pha thứ hai và SA, chế độ này đề ra các nhóm liên quan với một số thông tin được bổ sung, và thường liên quan tới các lỗi trong thương lượng. Ví dụ, nếu việc giải mã bị lỗi tại người nhận hoặc chữ ký không được xác thực thành công. Chế độ truyền tin được dùng để thông báo tới các bên khác.

3.3. Quá trình hoạt động của IPSec

Quá trình hoạt động của IPSec được thực hiện như sau:

- Ban đầu các lưu lượng cần bảo vệ được chỉ ra cho IPSec, tiếp theo IKE Phase1 sẽ thoả thuận một kết hợp bảo mật IKE SA, thiết lập một kênh truyền thông an toàn và xác thực đối tác.

- IKE Phase 2 sẽ thoả thuận các thông số của IPSec SA trên kênh an toàn vừa được thiết lập. Những thông số này được sử dụng để thống nhất việc bảo vệ dữ liệu trao đổi giữa hai bên. Các khoá được lưu trữ trong cơ sở dữ liệu SA.

- Sau đó các gói dữ liệu được xử lý AH hoặc ESP với các thuật toán mã hoá, xác thực và các khoá được chỉ ra bởi SA.

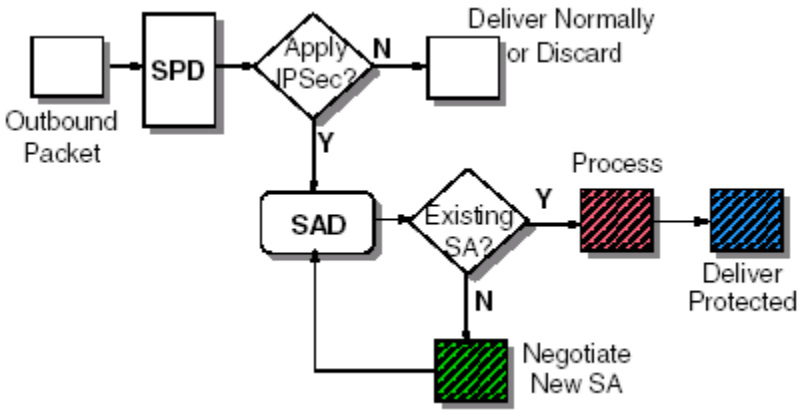
- Cuối cùng khi kết thúc, đường hầm IPSec bị xoá.

3.4. Xử lý hệ thống IPSec/IKE

Đây là điều quan trọng để hiểu được cách thức các hệ thống xử lý các gói dữ liệu, lúc các gói đó được chuyển đến có sử dụng IPSec và IKE. Với bảo mật IP được đặt đúng vị trí, các gói dữ liệu có thể không còn được xử lý, chuyển tiếp hoặc hủy bỏ một cách đơn giản nữa mà phải phụ thuộc vào chính sách bảo mật để xác định nếu quá trình xử lý IPSec bổ sung được yêu cầu và khi nó phải xẩy ra. Mặc dù có sự khác nhau không đáng kể giữa các Platform về cách thức chúng thực hiện IPSec trên các chồng IP riêng biệt của chúng, chức năng thông thường của quá trình xử lý IPSec với các hệ thống Host và Getway có thể được tổng kết lại như sau:

3.4.1. Xử lý IPSec cho đầu ra với các hệ thống máy chủ

Với IPSec hoạt động, bất kỳ các gói dữ liệu đi ra nào cũng đều phụ thuộc vào cơ sở dữ liệu chính sách bảo mật(SPD) để xác định nếu quá trình xử lý IPSec được yêu cầu hoặc những xử lý khác được thực hiện với các gói. Nếu IPSec được yêu cầu, cơ sở dữ liệu liên kết bảo mật(SAD) sẽ được tìm kiếm một SA đã tồn tại cho gói dữ liệu thích hợp với hồ sơ. Nếu không có trường hợp nào được tìm thấy và IKE cũng như yêu cầu các SA ngoại tuyến được hỗ trợ. Một quá trình thương lượng IKE sẽ được bắt đầu mà cuối cùng là dẫn đến việc thiết lập các SA mong muốn cho gói này. Cuối cùng, IPSec được áp dụng để các gói được yêu cầu bởi SA và gói dữ liệu được phân phối. Quá trình xử lý này được minh họa trong hình 3.23



Hình 3.23 IPSec – Xử lý đầu ra với hệ thống các Host

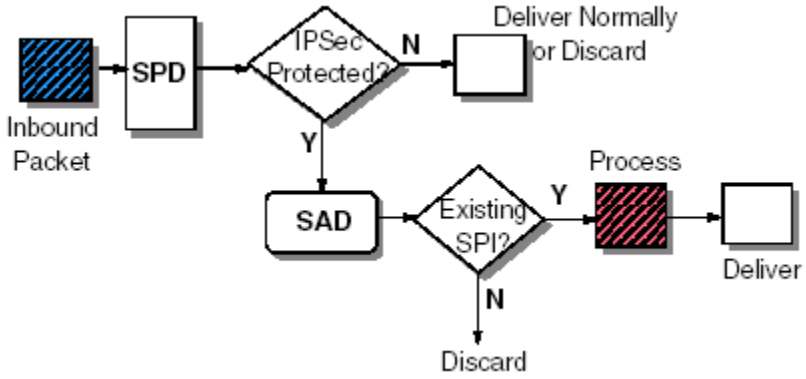
3.4.2. Xử lý đầu vào với các hệ thống máy chủ Host

Với IPSec hoạt động, bất kỳ gói dữ liệu đi vào nào cũng đều phụ thuộc vào SPD để xác định xử lý IPSec được yêu cầu hay các xử lý khác sẽ thực hiện với gói dữ liệu. Nếu IPSec được yêu cầu, SAD được truy cập đến để tìm một SPI đã tồn tại thích hợp với giá trị SPI chứa trong gói. Nếu không có giá trị nào phù hợp, về cơ bản có 2 tùy chọn.

1. Loại bỏ gói tin mà không cho người gửi biết(nhưng có thể ghi nhật ký sự kiện nếu được cấu hình). Tùy chọn này là ngầm định bởi hầu hết các IPSec ngày nay

2. Nếu IKE cũng như yêu cầu các SA nội tuyến được hỗ trợ, một thỏa thuận IKE mới được bắt đầu là kết quả cuối cùng trong việc thiết lập các SA với người gửi của gói dữ liệu gốc. Trong trường hợp này, sẽ không vấn đề gì nếu gói dữ liệu gốc được IPSec bảo vệ hoặc ở dạng rõ, nó chỉ tin tưởng vào chính sách cục bộ. Tuy nhiên, nó yêu cầu người gửi gói dữ liệu gốc đáp ứng thỏa thuận IKE, và nó dự tính rằng các gói sẽ bị hủy bỏ cho đến khi một SA được thiết lập

Cuối cùng, IPSec được áp dụng với các gói được yêu cầu bởi SA và các gói tải được phân phối tới tiến trình cục bộ. Quá trình xử lý này được minh họa như hình 3.24



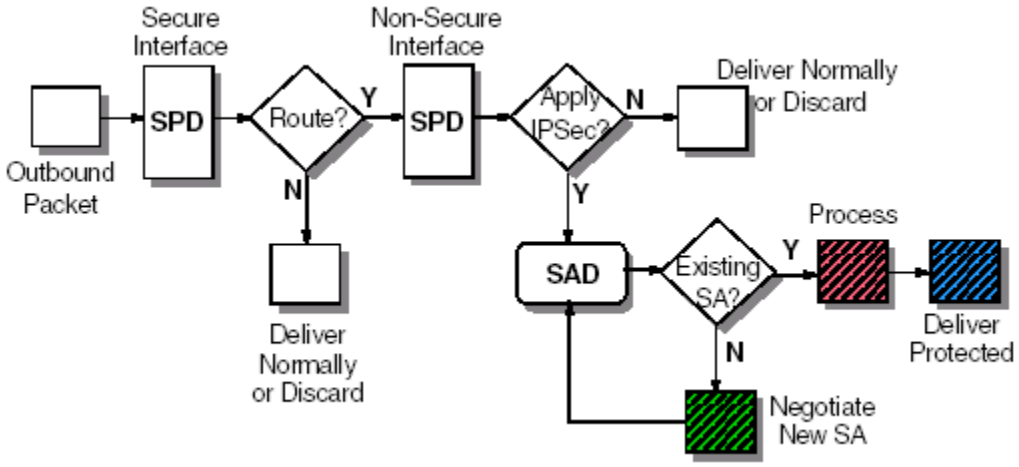
Hình 3.24 IPSec – Xử lý hướng nội với các hệ thống máy chủ Host

3.4.3. Xử lý đầu ra với các hệ thống cổng kết nối

Trên một hệ thống cổng kết nối, bất kỳ gói dữ liệu đi ra nào cũng thường tùy thuộc vào SPD của giao diện bảo mật để quyết định phải làm gì với nó. Nếu quyết định là để định tuyến gói dữ liệu, bảng định tuyến sẽ được tra cứu để quyết định nếu gói được phân phối tới tại cả. Nếu không có route được tìm thấy. Quá trình xử lý IPSec sẽ không được thực hiện, nhưng người gửi gói dữ liệu gốc có thể được cho biết về vấn đề này bằng cách dùng các thông điệp không tới được mạng ICMP.

Chúng ta thừa nhận rằng, các hệ thống cổng kết nối hoặc tận dụng các giao thức định tuyến hoặc định nghĩa sự định tuyến mặc định và như vậy một quyết định định tuyến thành công có thể được thực hiện.

Từ phạm vi trên, về bản chất quá trình xử lý là giống như trên các hệ thống Host. Gói dữ liệu sau đó được chuyển tiếp đến SPD của giao diện không bảo mật để quyết định xử lý IPSec được yêu cầu hay xử lý khác được thực hiện với gói dữ liệu. Nếu IPSec được yêu cầu, SAD được truy cập để tìm kiếm một SA đã có cho gói nào phù hợp với hồ sơ. Nếu không trường hợp nào được tìm thấy, và IKE cũng như yêu cầu các SA ngoại tuyến được hỗ trợ, một sự thỏa thuận IKE mới được bắt đầu mà cuối cùng là dẫn đến việc thiết lập các SA mong muốn cho gói dữ liệu này. Cuối cùng, IPSec được áp dụng cho các gói được yêu cầu bởi SA và gói dữ liệu được phân phối. Quá trình xử lý này được minh họa như trong hình 3.25



Hình 3.25 IPSec – Xử lý đầu ra với các hệ thống cổng kết nối

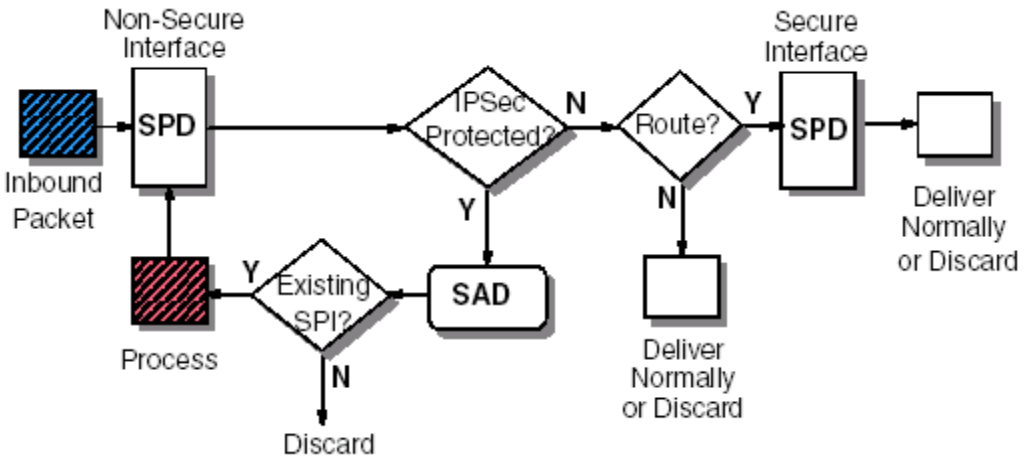
3.4.4. Xử lý đầu vào với các hệ thống cổng kết nối

Trên một hệ thống cổng kết nối có IPSec hoạt động, bất kỳ gói dữ liệu đi vào nào cũng tùy thuộc vào SPD để quyết định xem quá trình xử lý IPSec được yêu cầu hay các xử lý khác được thực hiện với gói đó. Nếu IPSec được yêu cầu, SAD được truy cập để tìm kiếm một SPI đã tồn tại phù hợp với giá trị SPI chứa trong gói dữ liệu. Nếu không có trường hợp nào tìm thấy, có 2 tùy chọn:

1. Hủy bỏ gói dữ liệu mà không báo cho người gửi biết, nhưng ghi vào nhật ký sự kiện nếu được cấu hình.

2. Nếu IKE cũng như yêu cầu các SA đầu vào được hỗ trợ, một sự thỏa thuận IKE mới được bắt đầu mà cuối cùng là dẫn đến việc thiết lập SA với người gửi gói dữ liệu gốc. Trong trường hợp này, gói dữ liêu gốc được bảo vệ bởi IPSec hoặc ở dạng rõ đều không quan trọng, nó chỉ tin tưởng vào chính sách cục bộ. Tuy nhiên, nó yêu cầu là người gửi phải đáp ứng thỏa thuận IKE, và nó dự tính các gói dữ liệu được hủy bỏ cho đến khi một SA được thiết lập.

Một gói dữ liệu được xử lý thành công bởi IPSec, nó có thể là một quá trình lặp với các bó SA, một quyết định chọn đường phải được thực hiện để làm gì với gói kế tiếp. Nếu gói dữ liệu được dự định chuyển đến Host khác, nó được phân phối qua giao diện thích hợp theo bảng định tuyến. Nếu gói dữ liệu dự định chuyển đến cổng kết nối của nó, dữ liệu tải được phân phối tới tiến trình xử lý cục bộ. Quá trình này được minh họa như trong hình 3.26



Hình 3.26 IPSec – Xử lý đầu vào với các cổng kết nối

Tổng kết chương III

Trong chương III đã trình bày chi tiết về giao thức mạng riêng ảo thông dụng nhất – IPSec, chương này cũng xem xét các cơ sở của IPSec và các liên kết bảo mật - một dạng cơ sở của giao thức IPSec. Xác thực tiêu đề(AH) và đóng gói tải bảo mật(ESP) là các giao thức IPSec chủ chốt. Trong khi AH bảo vệ toàn bộ gói dữ liệu gốc thì, ESP chỉ bảo vệ phân dữ liệu tải của thông điệp gốc. Tiếp đó ta cũng nghiên cứu các chế độ IPSec – Chế độ Tunnel và chế độ Transport – và các quy tắc thực hiện chúng trong việc bảo vệ gói dữ liệu IP gốc khỏi các truy cập trái phép, sự giả mạo, sự phân tích gói tin và đánh cắp gói tin. Cuối cùng là trình bài về trao đổi khóa Internet(IKE), nó giữ một vài trò quan trọng trong việc quản lý các khóa mật mã. Hai pha IKE được thảo luận. Bốn chế độ thực thi IKE thông dụng cũng được thảo luận một cách ngắn gọn.

Câu hỏi ôn tập

1. Which of the following fields make up an IPSec SA?

a. SPI
b. Payload
c. Destination IP Address
d. Security Protocol

2. Which of the following databases contain entries that might resemble a firewall rule?

a. SPD
b. SPI
c. SAP
d. SAD

3. _____ offers confidentiality and data integrity, but not the capability for key management.

a. IKE
b. AH
c. ESP
d. None of the above

4. Which of the modes listed below is NOT a valid IPSec mode?

a. Informational mode
b. Tunnel mode
c. Aggressive mode
d. Quick mode

5. Which of the following statements is true?

a. Main mode is slower than Quick mode.
b. ESP in Transport mode offers higher security than ESP in Tunnel mode.
c. Aggressive mode belongs to IKE Phase II.
d. All of the above statements are correct.

Chương IV Một số công nghệ an toàn bổ sung cho các mạng riêng ảo

Trong các chương trước chúng ta đã thảo luận về các công nghệ an toàn có thể được dùng để xây dựng mạng riêng ảo. Trong khi các công nghệ đó thường đủ và hiệu quả với các tác vụ đơn lẻ, nhưng có những trường hợp mà một mình các công nghệ đó không đáp ứng được yêu cầu cho một giải pháp VPN đầy đủ. Một trong những trường hợp như vậy là sử dụng chứng chỉ số, xác thực và mã hóa. Chương này sẽ mô tả ngắn gọn một số công nghệ an toàn có thể bổ sung thêm vào một giải pháp mạng riêng ảo hoặc đồng thời tồn tại trong một môi trường mạng riêng ảo dưới hoàn cảnh nào đó.

4.1. Xác thực với người dùng quay số truy cập từ xa

Quay số từ xa tới Intranet của công ty, cũng như tới Internet đã tạo ra Server truy cập từ xa(RAS), một phần rất quan trọng của các dịch vụ liên mạng ngày nay. Như chúng ta biết, càng ngày càng nhiều người dùng di động yêu cầu truy cập không chỉ tới tài nguyên mạng trung tâm mà cả với nguồn thông tin trên Internet. Sự phổ biến của Internet và Intranet trong các tổ chức đã thúc đẩy sự phát triển của các dịch vụ và thiết bị truy cập từ xa. Nhu cầu kết nối một cách đơn giản tới các tài nguyên của tổ chức từ các thiết bị máy tính di động như máy xách tay chẳng hạn ngày càng tăng. Sự xuất hiện của truy cập từ xa cũng là một trong các nguyên nhân của sự phát triển trong lĩnh vực bảo mật. Mô hình bảo mật xác thức – cấp quyền và kiểm toán(AAA) đã được phát triển để nhằm vào vấn đề bảo mật truy cập từ xa. AAA là một bộ khung được dùng để cấu hình ba chức năng an toàn cơ bản: xác thực, cấp quyền và kiểm toán. Ngày nay, mô hình an toàn AAA được sử dụng trong tất cả các kịch bản truy cập từ xa trong thực tế vì nó cho phép người quản trị mạng nhận dạng và trả lời ba câu hỏi quan trọng sau:

- Ai đang truy cập mạng?

- Người dùng được phép làm những gì? Và những hoạt động nào được hạn chế khi người dùng truy cập mạng thành công?

- Người dùng đang làm gì và lúc nào?

AAA được mô tả ngắn gọn như sau:

- Xác thực(Authentication): Xác thực là bước đầu tiên đối với bảo mật. Đây là hoạt động xác định một người dùng(hoặc thực thể) là ai trước khi anh ta có thể truy cập các tài nguyên trong mạng. Xác thực có thể dưới nhiều dạng, dạng truyền thống sử dụng một tên đăng nhập và một mật khẩu cố định. Hầu hết các máy tính làm việc theo cách này. Tuy nhiên, phần lớn mật khẩu cố định có những giới hạn nhất định trong lĩnh vực bảo mật. Nhiều cơ chế xác thực hiện đại sử dụng mật khẩu một lần hay một truy vấn dạng yêu cầu – đáp ứng (Ví dụ các giao thức xác thực: PAP, CHAP, EAP…).

Thông thường, xác thực xẩy ra lúc người dùng đăng nhập lần đầu tiên vào máy hoặc yêu cầu một dịch vụ từ nó

- Cấp quyền(Authorization): Đây là hoạt động xác định một người dùng được phép làm những gì. Nghĩa là muốn nói đến việc kiểm soát các hoạt động mà người dùng được phép thực hiện trong mạng và tài nguyên mà người dùng được phép truy cập. Kết quả là, cấp quyền cung cấp các cơ chế cho việc kiểm soát truy cập từ xa bằng các phương tiện như: cấp quyền một lần, cấp quyề cho mỗi dịch vụ, trên từng danh sách tài khoản người dùng hoặc chính sách nhóm.

Thông thường các thuộc tính, đặc quyền và quyền truy cập được biên dịch và lưu trữ tại một cơ sở dữ liệu trung tâm cho mục đích cấp quyền. Các thuộc tính và các quyền này quyết định những hoạt động mà một người dùng được phép thực hiện. Khi một người dùng cần được cấp quyền sau khi đã được xác thực thành công, các thuộc tính và quyền này được xác minh dựa vào cơ sở dữ liệu với người dùng và chuyển tiếp tới Server liên quan(ví dụ: Server truy cập từ xa). Thông thường, xác thực được thực hiện trước cấp quyền, nhưng điều đó là không nhất thiết phải yêu cầu như vậy. Nếu một tài nguyên mạng, như Server, nhận một yêu cầu cấp quyền mà không qua xác thực, Agent cấp quyền trên thiết bị mạng phải quyết định người dùng có thể truy cập thiết bị mạng và được phép thực hiện các dịch vụ đã xác định trong yêu cầu cấp quyền hay không

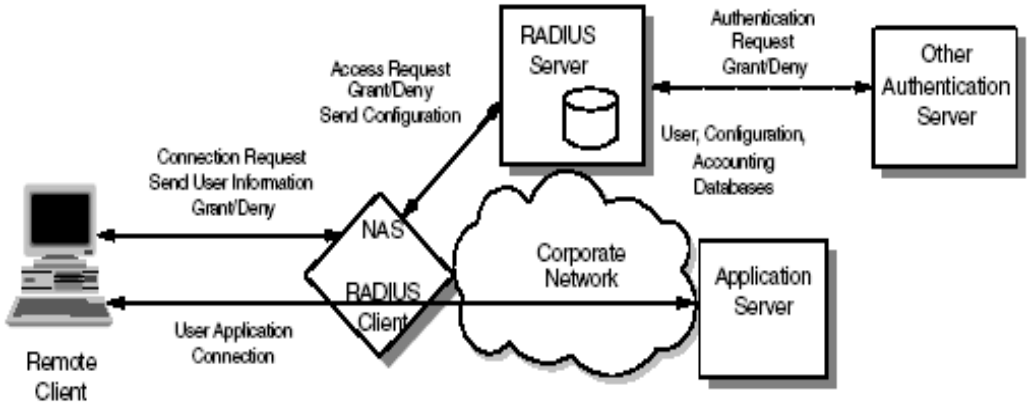
- Kiểm toán(Auounting): Đây là hoạt động điển hình thứ 3 sau xác thực và cấp quyền. Kiểm toán là ghi lại những hoạt động mà người dùng đã và đang thực hiện. Kiểm toán là cơ chế ghi lại những hoạt động mà người dùng thực hiện sau khi đã đăng nhập thành công vào mạng. Kiểm toán bao hàm việc: thu thập, ghi danh sách, kiểm toán, ghi nhật ký và báo cáo về các định danh người dùng, các lệnh đã được thực hiện trong một phiên, số lượng các gói được truyền tải, vv… Lúc một hoạt động của người dùng được ghi lại, thời gian nó được thực hiện, khoảng thời gian của toàn bộ phiên người dùng và khoảng thời gian với mỗi hoạt động riêng lẻ cũng được ghi lại. Thông tin chi tiết về người dùng giúp người quản trị mạng theo dõi được những hoạt động của người dùng và đưa ra những hành động phù hợp để duy trì an toàn mạng. Mặc dù, kiểm toán được xem là bước lôgic tiếp theo của xác thực và cấp quyền, nhưng nó có thể thực thi không theo tuần tự đó. Trong thực tế, kiểm toán có thể được thực thi ngay cả khi hoạt động xác thực và cấp quyền không được thực hiện.

Trong mô hình cơ sở dữ liệu bảo mật Client/Server phân tán, một số các Client, Server trong truyền thông xác thực một định danh của người dùng quay số qua một trung tâm cơ sở dữ liệu đơn hoặc một Server xác thực. Server xác thực lưu trữ tất cả thông tin về người dùng, các mật khẩu và các quyền ưu tiên truy cập của họ. Phân phối bảo mật đóng vai trò như một trung tâm về dữ liệu xác thực, nó an toàn hơn sự phân tán thông tin người dùng trên các thiết bị khác qua một mạng. Một Server xác thực đơn có thể hỗ trợ cả hàng trăm Server truyền thông, hàng nghìn người dùng. Các Server trong quá trình truyền thông có thể truy cập một Server xác thực cục bộ hoặc từ xa qua kết nối mạng diện rộng(WAN).

Một số đại lý cung cấp truy cập từ xa và IETF đã đi đầu trong việc cố gắng bảo đảm an toàn cho truy cập từ xa, các phương tiện bảo mật được chuẩn hoá. Dịch vụ xác thực người dùng quy số từ xa(RADIUS) và hệ thống kiểm soát truy cập các thiết bị cuối(TACACS) như là hai dự án đã mở ra bộ khung của chuẩn Internet và các đại lý truy cập từ xa.

Dịch vụ xác thực người dùng quay số từ xa(RADIUS)

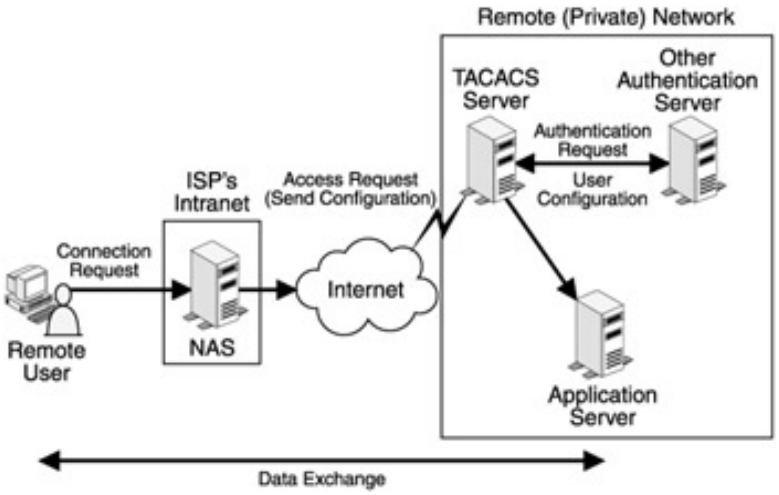
RADIUS là một hệ thống bảo mật phân tán được phát triển bởi Livingston Enterprises. RADIUS được thiết kế dựa trên những khuyến cáo trước đó từ nhóm Network Access Server Working Requirements của IETF. Một nhóm IETF làm việc với RADIUS được thành lập vào tháng 1 năm 1996 để đưa ra các chuẩn cho giao thức RADIUS, RADIUS bây giờ là một giải pháp bảo mật đường quay số được thừa nhận bởi IETF



Hình 4.1 Dịch vụ xác thực người dùng quay số từ xa RADIUS

Hệ thống kiểm soát truy cập thiết bị đầu cuối(TACACS)

Tương tự với RADIUS, TACACS là một giao thức chuẩn công nghiệp. Như trong hình 4.2, lúc một Client từ xa đưa ra một yêu cầu xác thực tới NAS gần nó nhất, yêu cầu này được chuyển tiếp tới TACACS. Sau đó TACACS chuyển tiếp ID và mật khẩu được cung cấp tới cơ sở dữ liệu trung tâm, cơ sở dữ liệu trung tâm này có thể là một cơ sở dữ liệu TACACS hoặc một cơ sở dữ liệu bảo mật mở rộng. Cuối cùng, thông tin được lấy lại và chuyển tiếp tới TACACS, nó lần lượt được chấp nhận hoặc từ chối yêu cầu kết nối trên cơ sở thông tin nó nhận được từ cơ sở dữ liệu



Hình 4.2 Xác thực từ xa dựa trên TACACS

Hiện tại, có hai phiên bản của TACACS trên thị trường, cả hai phiên bản này đều được phát triển bởi Cisco. Đó là:

- XTACACS (eXtended TACACS): Là một mở rộng của TACACS, nó hỗ trợ các tính năng cao cấp.

- TACACS+: Phiên bản này của TACACS ban đầu sử dụng một Server truy cập riêng dưới dạng Server TACACS+. Server này cung cấp các dịch vụ xác thực, cấp quyền và kiểm toán độc lập.

NAS giữ một vai trò quan trọng trong cả xác thực dựa trên RADIUS và dựa trên TACACS. Là một Client RADIUS hay TACACS, NAS mã hoá các thông tin(ID/Mật khẩu của người dùng) được cung cấp bởi người dùng từ xa trước khi chuyển tiếp nó tới Server xác thực tại mạng chủ cuối, NAS cũng có khả năng định tuyến một yêu cầu xác thực tới Server xác thực khác nếu Server xác thực đích không đến được.

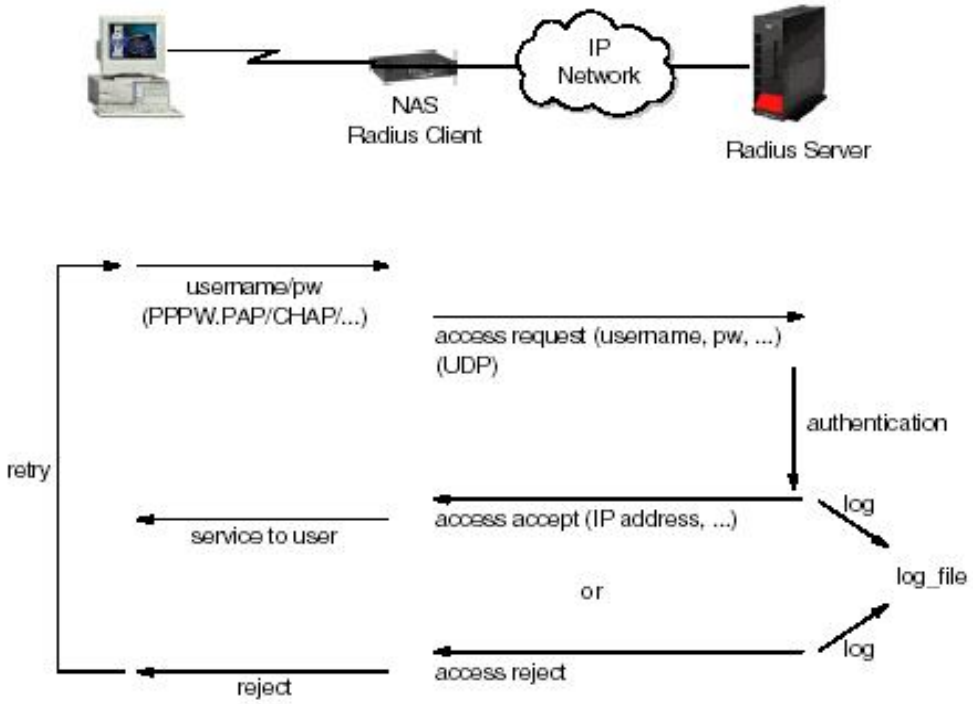
4.1.1. Hoạt động của RADIUS

RADIUS đầu tiên được phát triển bởi Livingston Enterprises, nhưng bây giờ thuộc quyền sở hữu của IETF và là một giao thức mở, có thể được phân phối dưới dạng mã nguồn và bất kỳ người nào cũng đều có thể sửa đổi.

Mặc dùng RADIUS ban đầu được phát triển cho người quản trị của NAS, các sản phẩm hỗ trợ được bổ sung thêm các ứng dụng/thiết bị khác như firewall, truy

cập trang web cá nhân, các tài khoản Email và các vấn đề bảo mật Internet liên quan đến xác thực khác.

RADIUS gồm 2 phần: Có Client RADIUS, ví dụ: NAS hay bất kỳ phần mềm khác như Firewall, Client gửi một yêu cầu AAA tới RADIUS Server. Mặt khác, có RADIUS Server, nó kiểm tra yêu cầu theo dữ liệu đã được cấu hình trước.



Hình 4.3. Luồng thông tin trong RADIUS

Mặc dù các Server xác thực RADIUS và TACACS có thể được cài đặt theo nhiều cách khác nhau, tuỳ thuộc vào lược đồ bảo mật của mạng mà chúng phục vụ, nhưng tiến trình cơ sở cho việc xác thực một người dùng về cơ bản là giống nhau. Sử dụng một Moderm, một người dùng quay số từ xa kết nối tới một Server từ xa (gọi là Server truy cập mạng NAS), với một Moderm số hoặc tương tự. Lúc một kết nối Moderm được tạo, NAS nhắc người dùng về tên đăng nhập và mật khẩu. NAS sau đó sẽ tạo ra yêu cầu xác thực từ gói dữ liệu được cung cấp, nó bao gồm cả thông tin định danh mà thiết bị NAS xác định gửi yêu cầu xác thực như: cổng đang được dùng cho kết nối Moderm và Tên đăng nhập/Mật khẩu

Một vai trò rất quan trọng được thực thi bởi Server xác thực, nó là một Server trong mạng để xác nhận tính hợp lệ của ID/mật khẩu người dùng cho mạng. Nếu một thiết bị được cấu hình cho xác thực qua một Server xác thực và thiết bị nhận một gói dữ liệu từ một giao thức xác thực, thiết bị gửi qua ID và Mật khẩu của người dùng tới Server cho việc xác thực. Nếu ID/mật khẩu của người dùng là đúng, Server phản hồi lại. Thiết bị sau đó có thể liên lạc với người khởi tạo yêu cầu ban đầu. Nếu Server không tìm thấy ID/mật khẩu của người dùng thì nó từ chối thiết bị và gửi phản hồi tới thiết bị. Thiết bị sau đó từ chối phiên với nơi mà nó đã nhận yêu cầu xác thực.

Server xác thực có thể là chính một Server RADIUS hoặc một Server khác dựa trên các công nghệ xác thực trung tâm khác như Kerberos, DCE, SecureID hoặc RACF. Một Server RADIUS có thể được cấu hình để chuyển tiếp yêu cầu tới một Server xác thực trung tâm và truy cập thành công hoặc từ chối thông tin và cấu hình trở lại Client.

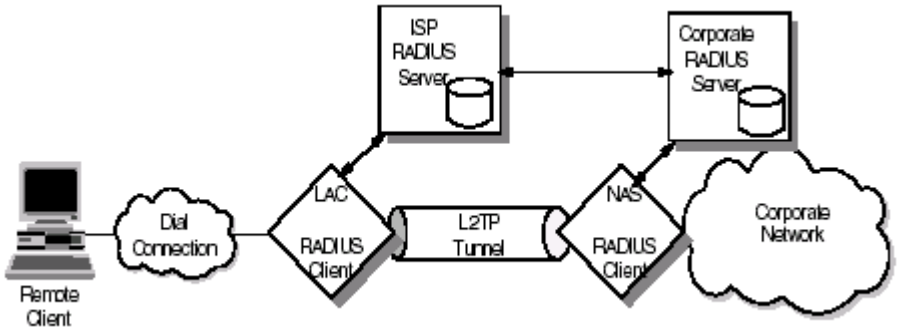
Với việc bảo vệ trước các cuộc nghe lén của hacker, NAS hoạt động như Client RADIUS hoặc TACACS, mã hoá mật khẩu trước khi nó gửi mật khẩu tới Server xác thực. Nếu Server bảo mật chính không đến được, Client bảo mật hoặc thiết bị NAS có thể định tuyến yêu cầu tới một Server thay thế kế tiếp. Lúc nhận được một yêu cầu xác thực, Server xác thực sẽ xác minh yêu cầu và sau đó giải mã gói dữ liệu để truy cập thông tin tên đăng nhập/mật khẩu của người dùng. Nếu tên đăng nhập/mật khẩu của người dùng là đúng, Server gửi một gói dữ liệu báo đã nhận xác thực. Gói dữ liệu báo nhận này có thể gồm cả thông tin lọc bổ sung như thông tin trên các yêu cầu tài nguyên mạng của người dùng và các mức cấp quyền. Server bảo mật có thể, với thể hiện dưới dạng NAS mà một người dùng cần TCP/IP và/hoặc Internet Packet Exchange (IPX) sử dụng PPP, hoặc cái mà người dùng cần SLIP để kết nối tới mạng. Nó có thể gồm cả thông tin trên tài nguyên mạng xác định mà người dùng được phép truy cập.

Để phá hỏng việc nghe lén trên mạng, Server bảo mật gửi một khóa xác thực hoặc chữ ký, nhận dạng của chính nó tới Client bảo mật. Một NAS nhận thông tin này, nó cho phép cấu hình ở mức cần thiết để cho phép người dùng quyền truy các

cập dịch vụ và tài nguyên mạng. Nếu tại bất kỳ điểm nào trong tất cả tiến trình đăng nhập mà các điều kiện xác thực cần thiết không thỏa mãn, Server cơ sở dữ liệu bảo mật sẽ gửi một thông điệp từ chối xác thực tới thiết bị NAS và người dùng bị từ chối truy cập mạng

4.1.2 Sử dụng RADIUS với các đường hầm tầng 2

RADIUS có thể được dùng để xác thực các đường hầm tầng 2 cũng như các kết nối PPP một phần quan trọng với các mạng riêng ảo. Có 2 mô hình đường hầm tại tầng 2, mô hình tự nguyện và bắt buộc. RADIUS có thể được dùng trong cả 2 trường hợp để xác thực người dùng và cấp quyền/từ chối một thiết lập đường hầm hay thiết lập phiên. Điều này bổ sung thêm một tầng bảo mật với kịch bản mạng riêng ảo tại tầng 2 vì cho đến khi đường hầm được thiết lập và phiên được thiết lập, không có luồng thông tin nào được phép chuyển qua đường hầm, thêm vào đó, việc xác thực và truy cập tới các đường hầm đó có thể được kiểm soát tập trung. Hình 4.4 minh họa các cách sử dụng RADIUS khác nhau đó trong một môi trường mạng riêng ảo mà trong đó các đường hầm bắt buộc được dùng liên quan tới một ISP để thiết lập một đường hầm hay bắt đầu một phiên mới qua một đường hầm đang tồn tại với tư cách là đại diện của một Client từ xa. ISP có thể dùng một server ủy quyền RADIUS để chuyển thiếp xác thực client trở lại Server xác thực trung tâm vì vậy không cần phải duy trì thông tin người dùng tại hai vị trí, ISP và Server trung tâm

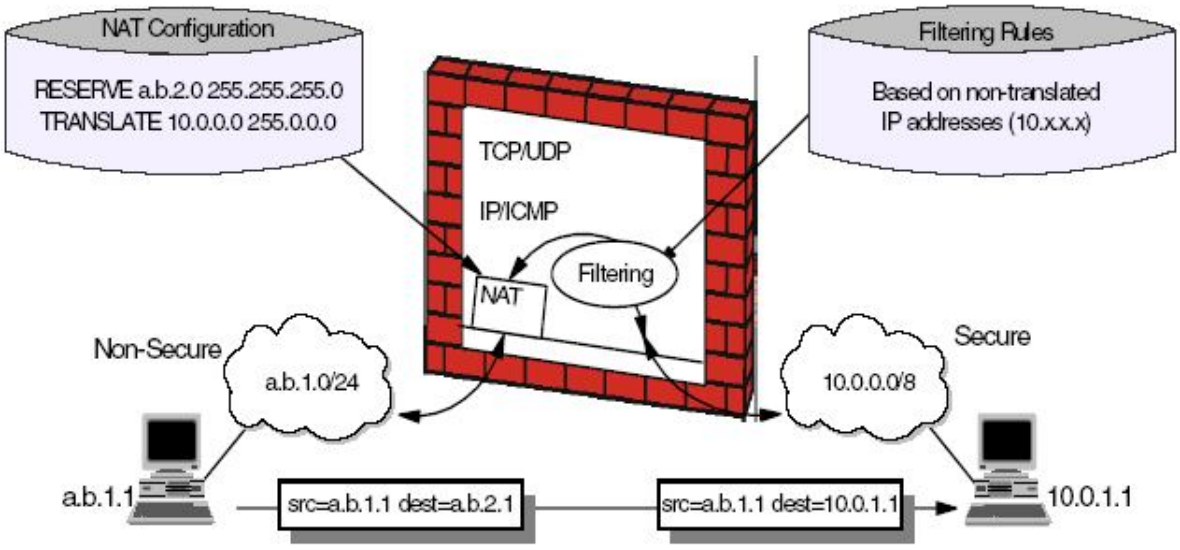


Hình 4.4 Sử dụng RADIUS với các đường hầm tầng 2

4.2 Chuyển dịch địa chỉ mạng(NAT)

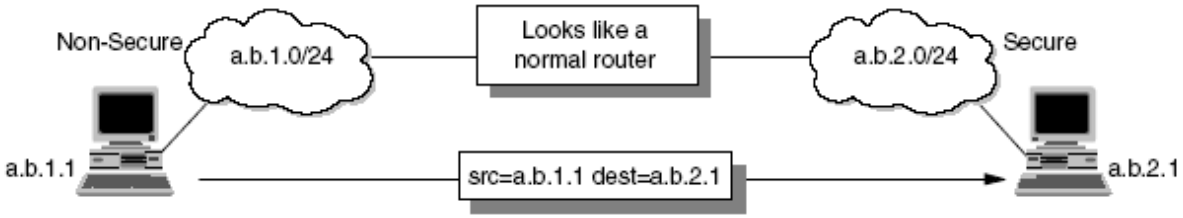
Ban đầu NAT được đề xuất như một giải pháp ngắn hạn cho vấn đề cạn kiệt địa chỉ IP. Tuy nhiên, NAT cũng là một phương tiện hiệu quả để ngăn chặn các Hacker và người dùng bên ngoài xâm nhập vào mạng. Để đảm bảo truyền thông giữa 2 nơi bất kỳ trên Internet, tất cả địa chỉ IP phải được gán một cách chính thức bởi IANA. Điều này trở nên khó khăn hơn để hoàn thành vì số lượng các dãi địa chỉ sẵn dùng bây giờ bị giới hạn. Trước đây, nhiều tổ chức sử dụng các địa chỉ IP cục bộ, không nghĩ tới yêu cầu kết nối Internet. Ý tưởng của NAT dựa trên thực tế là chỉ một số lượng nhỏ các Host trong một mạng riêng đang liên lạc với thế giới bên ngoài. Nếu mỗi Host được gán một địa chỉ IP từ quĩ địa chỉ IP chính thức chỉ lúc nó cần liên lạc, thì chỉ có một số lượng nhỏ địa chỉ chính thức được yêu cầu. NAT là một giải pháp cho các mạng có dãi địa chỉ IP riêng hoặc các địa chỉ trái phép và muốn liên các với các Host trên Internet. Trong thực tế, điều này có thể được hoàn tất bởi việc thực thi một firewall. Vì lý do, các Client liên lạc với Internet bằng việc sử dụng một Proxy hoặc SOCKS Server không để lộ địa chỉ của họ với Interner, nên địa chỉ của họ không phải dịch chuyển. Tuy nhiên, vì nhiều lý do, lúc một Proxy hay SOCKS không sẵn sàng hoặc không phù hợp với các yêu cầu đặc biệt, NAT phải được dùng để quản lý lưu lượng giữa mạng bên trong và bên ngoài để không quảng cáo địa chỉ các Host bên trong ra bên ngoài.

Xét một mạng bên trong có dựa trên không gian địa chỉ IP riêng và người dùng muốn dùng một giao thức ứng dụng không có cổng kết nối ứng dụng. Chỉ có tùy chọn là thiết lập kết nối mức IP giữa các Host ở mạng bên trong và các Host trên Internet, Vì các bộ định tuyến sẽ không biết cách thức định tuyến các gói IP trở lại địa chỉ IP riêng, không có điểm nào để gửi các gói IP với địa chỉ IP riêng là địa chỉ IP nguồn qua một Router vào Internet. Như trong hình 4.5, NAT lưu giữ các địa chỉ này bằng cách lấy địa chỉ IP của gói dữ liệu ra và dịch nó thành một địa chỉ chính thức, Với các gói vào nó dịch địa chỉ chính thức thành một địa chỉ trong.



Hình 4.5 Dịch chuyển địa chỉ mạng

Từ vị trí của hai Host trao đổi các gói IP với nhau, một mạng an toàn và một mạng không an toàn, NAT giống như một bộ định tuyến IP chuẩn chuyển tiếp các gói IP giữa 2 giao diện mạng(Xem hình 4.6)



Hình 4.6 NAT giữa mạng an toàn và mạng không an toàn

4.2.1. Sử dụng NAT với các mạng riêng ảo

NAT làm việc tốt với địa chỉ IP trong phần tiêu đề. Một số giao thức ứng dụng trao đổi thông tin địa chỉ IP trong phần dữ liệu ứng dụng của một gói IP, và thông thường NAT sẽ không có khả năng lưu giữ bản dịch chuyển của địa chỉ IP trong giao thức ứng dụng. Hiện tại, hầu hết sự thực thi xử lý giao thức FTP. Nên chú ý rằng sự thực thi của NAT cho các ứng dụng đặc biệt có thông tin IP trong dữ liệu ứng dụng là phức tạp hơn nhiều so với sự thực thi NAT chuẩn.

Giới hạn quan trọng khác của NAT là NAT thay đổi một số hoặc tất cả thông tin địa chỉ trong một gói IP. Lúc xác thực IPSec đầu cuối - đến - đầu cuối được dùng, địa chỉ của gói đã được thay đổi sẽ luôn thất bại khi kiểm tra tính toàn vẹn dưới giao thức xác thực tiêu đề(AH), vì bất kỳ một bít nào bị thay đổi trong gói dữ

liệu sẽ làm mất hiệu lực giá trị kiểm tra toàn vẹn đa được tạo bởi nguồn. Vì vậy giao thức IPSec đề xuất một số giải pháp để giải quyết vấn đề địa chỉ được lưu giữ trước bởi NAT, không cần thiết dùng NAT lúc tất cả các Host tạo nên tổng thể một mạng riêng ảo sử dụng các địa chỉ IP toàn cục duy nhất(Public). Việc ẩn địa chỉ có thể được hoàn tất bởi chế độ đường hầm của IPSec. Nếu một Công ty sử dụng các địa chỉ riêng trong mạng Intranet, chế độ đường hầm của IPSec giữ cho chúng không xuất hiện ở dạng rõ trong mạng công cộng, nó loại trừ sự cần thiết có NAT.

4.3. Giao thức SOCKS

Một cổng mạch vòng tiếp nhận TCP cũng như các kết nối UPD và không cung cấp thêm bất kỳ tiến trình xử lý hoặc lọc gói nào. Một cổng mạch vòng là một loại đặc biệt của cổng nối mức ứng dụng. Điều này là bởi các cổng nối mức ứng dụng có thể được cấu hình để chuyển qua tất cả thông tin của một người dùng đã được xác thực, được xem như là cổng mạch vòng(xem hình 4.7). Tuy nhiên trong thực hành, có sự khác nhau đáng kể giữa chúng:

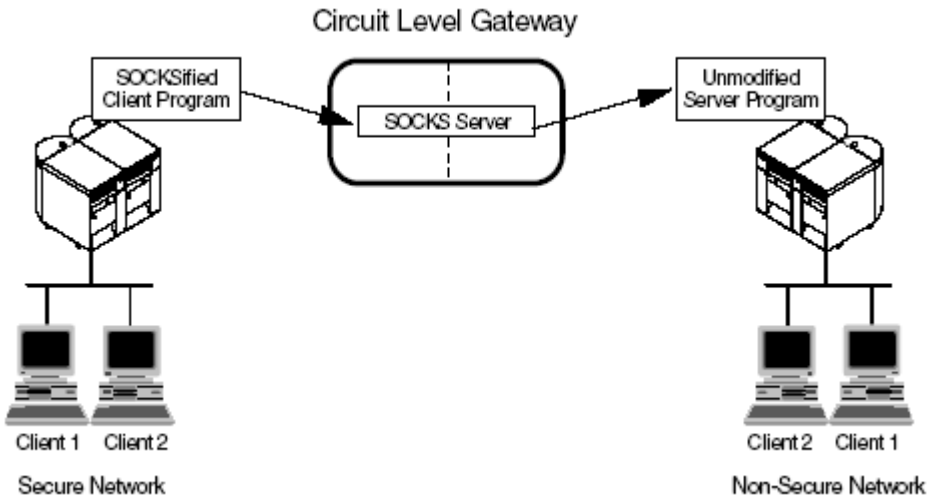
- Các cổng mạch vòng có thể sử dụng một số ứng dụng TCP/IP cũng như các ứng dụng UDP mà không phải sửa đổi gì trên Client cho mỗi ứng dụng. Như vậy, điều này làm cho các cổng mạch vòng trở thành một lựa chọn tốt để thoã mãn các yêu cầu của người dùng.

- Các cổng mạch vòng không cung cấp xử lý hoặc lọc gói. Như vậy một cổng nối dạng này thường xem như một cổng nối trong suốt.

- Các cổng nối mức ứng dụng thiếu hỗ trợ UDP.

- Các cổng mạch vòng thường được dùng cho các kết nối hướng ngoại, trong khi các cổng nối mức ứng dụng thường được dùng cho cả kết nối hướng ngoại và hướng ngoại.. Thông thường, trong trường hợp sử dụng kết hợp cả 2 loại, cổng mạch vòng thường được dùng cho các kết nối hướng ngoại còn cổng nối mức ứng dụng được dùng cho các kết nối hướng nội để thoả mãn yêu cầu bảo mật và yêu cầu của người dùng.

Một ví dụ dễ hiểu về cổng mạch vòng là SOCKS. Vì dữ liệu đi qua SOCKS không được giám sát hoặc lọc, một vấn đề bảo mật có thể nảy sinh. Để tối thiểu hoá các vấn đề bảo mật, các tài nguyên và dịch vụ tin cậy nên được dùng cho mạng ngoài (mạng không an toàn)



Hình 4.7 Cổng mạch vòng

SOCKS là một chuẩn cho các cổng mạch vòng. Nó không yêu cầu overhead của nhiều hơn một Server uỷ quyền thông thường trong đó một người dùng phải chủ ý kết nối trước hết là tới firewall trước khi có yêu cầu thứ 2 là kết nối tới đích. Người dùng khởi động một ứng dụng phía Client với địa chỉ IP của Server đích. Thay vì trực tiếp khởi động một phiên với Server đích, Client khởi tạo một phiên với Server SOCKS trên Firewall.

Server SOCKS sau đó xác minh địa chỉ nguồn và ID người dùng được cho phép để thiết lập kết nối tới mạng không an toàn, và sau đó tạo ra phiên thứ 2. SOCKS cần có một phiên bản mã nguồn Client mới và một tập riêng biệt các chính sách cấu hình trên Firewall. Tuy nhiên, máy server không cần thay đổi, thật vậy, nó không cần biết rằng phiên đang được tiếp bởi Server SOCKS. Cả Client và Server SOCKS đều cần có mã SOCKS. Server SOCKS hoạt động như một router mức ứng dụng giữa Client và Server ứng dụng thực. SOCKSv4 chỉ với các phiên TCP hướng ngoại. Nó rất đơn giản cho mạng riêng của người dùng, nhưng không được phân phối mật khẩu an toàn vì vậy nó không được dùng cho các phiên giữa người dùng mạng công cộng và các ứng dụng mạng riêng. SOCKSv5 với một số phương

pháp xác thực và vì thế được sử dụng cho các kết nối hướng nội, SOCKS cũng hỗ trợ các giao thức và ứng dụng dựa trên UDP.

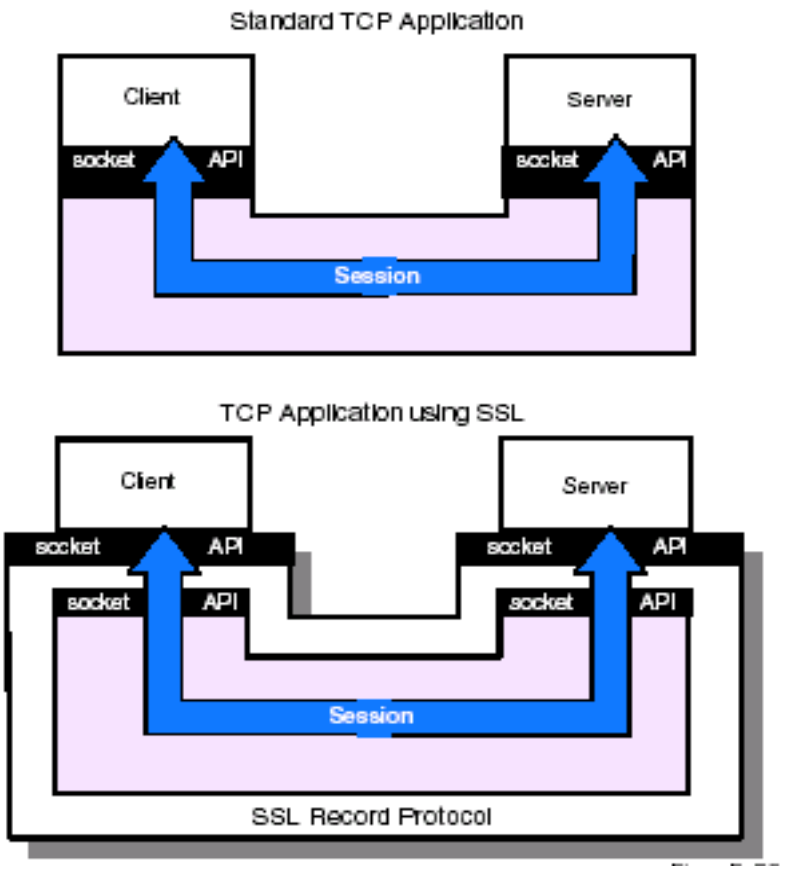
Phần lớn các trình duyệt Web là SOCKSified và người dùng có thể nhận được các ngăn xếp TCP/IP SOCKSified cho hầu hết các nền

4.4. Giao thức SSL và TLS

SSL là giao thức bảo mật được phát triển bởi hãng truyền thông Netscape, cùng với hãng bảo mật dữ liệu RSA. Mục đích chính của giao thức SSL là cung cấp một kênh riêng giữa các ứng dụng đang liên lạc với nhau, trong đó đảm bảo tính riêng tư của dữ liệu, tính toàn vẹn và xác thực cho các đối tác. SSL cung cấp một khả năng lựa chọn cho API socket TCP/IP chuẩn có thực thi bảo mật bên trong nó. Do đó, về lý thuyết nó có khả năng chạy với bất kỳ ứng dụng TCP/IP nào theo cách an toàn mà không phải thay đổi ứng dụng. Trong thực tế, SSL chỉ được thực thi với các kết nối HTTP, nhưng hãng truyền thông Netscape đã tuyên bố ý định tận dụng nó cho các kiểu ứng dụng khác, như giao thức NNTP và Telnet, và có một số miễn phí sẵn có trên Internet. Ví dụ, IBM đang sử dụng SSL để nâng cao tính bảo mật cho các phiên TN3270 trong các Host của nó, các phương tiện liên lạc cá nhân và các sản phẩm Server, miễn là cấu hình bảo mật truy cập được các Firewall.

SSL gồm có 2 tầng:

1. Tại tầng thấp, có một giao thức truyền dữ liệu sử dụng loại mật mã được xác định trước và kết hợp xác thực, gọi là giao thức bản ghi SSL, hình 4.8 minh họa giao thức này, và đối chiếu nó với một kết nối socket HTTP chuẩn



Hình 4.8 SSL – so sánh chuẩn giữa chuẩn và phiên SSL

2. Tại tầng trên, có một giao thức cho việc khởi tạo xác thực và truyền các khóa mã hóa, gọi là giao thức thăm dò trước SSL

Một phiên SSL được thiết lập như sau:

- Một người dùng phía Client(Trình duyệt) yêu cầu một tài liệu bằng một địa chỉ URL xác định bắt đầu bằng https(thay cho http)

- Mã phía Client nhận ra SSL yêu cầu và thiết lập một kết nối qua cổng TCP 443 tới mã SSL trên phía Server

- Client sau đó khởi tạo pha thăm dò trước SSL, dùng giao thức bản ghi SSL như một sự hỗ trợ. Tại đây không có sự mã hóa hay kiểm tra tính toàn vẹn gắn liền với kết nối.

Giao thức SSL đề ra các vấn đề an toàn sau:

+ Tính riêng tư: Sau khi khóa đối xứng được thiết lập trong khi thăm dò trước để khởi tạo, các thông điệp được mã hóa bằng khóa này.

+ Tính toàn vẹn: Các thông điệp chứa một mã xác thực thông điệp(MAC)

+ Tính xác thực: trong khi thăm dò trước, Client xác thực Server sử dụng khóa công khai. Nó cũng có thể dựa trên chứng chỉ

TLS được phát triển nhờ sử dụng SSL, giống như SSL, TLS cho phép các Server và Client cuối liên lạc một cách an toàn qua các mạng công cộng không an toàn.

Thêm vào các khả năng bảo mật được cung cấp bởi SSL, TLS cũng ngăn chặn kẻ nghe trộm, giả mạo, chặn bắt gói tin.

TLS cũng gồm 2 tầng: Giao thức bản ghi TLS và giao thức thăm dò trước TLS. Giao thức bản ghi TLS mang lại sự an toàn bằng cách tận dụng các cơ chế mã hóa, như DES chẳng hạn. Giao thức thăm dò trước TLS cung cấp khả năng xác thực 2 chiều bằng cách cho phép cả Server và Client xác thực lẫn nhau, hơn nữa 2 thực thể muốn liên lạc có thể thương lượng các thuật toán mã hóa và các khóa phục vụ cho việc trao đổi dữ liệu về sau giữa chúng.

Trong các kịch bản mạng riêng ảo, SSL và TLS có thể được thực thi tạo Server VPN cũng như tại Client đầu cuối

4.5. So sánh giao thức IPSec với SSL

Như đã mô tả trong Chương 3, “Các giao thức mạng riêng ảo tại tầng 3”, IPSec cung cấp tính năng mã hoá và xác thực mạnh cho lưu lượng IP và cũng cung cấp tính năng trao đổi và làm tươi khoá dựa trên chứng chỉ nhờ sử dụng IKE.

Để đi đến kết luận một cách thận trọng, ta phải đề xuất rằng những tính năng này là cần thiết giống như các tính năng mà SSL và TLS cung cấp. Trong phần này chúng ta lưu ý đến sự giống nhau và khác nhau cơ bản giữa IPSec và SSL và giải thích những phạm vi nào sử dụng cả hai giao thức.

Những điểm giống nhau:

- IPSec(qua IKE) và SSL cung cấp xác thực Client và Server

- IPSec và SSL cung cấp tính năng đảm bảo an toàn và xác thực đối với dữ liệu, thậm chí trên các mức khác nhau của chồng giao thức

- IPSec và SSL có thể dùng các thuật toán mật mã mạnh cho việc mã hoá và các hàm băm, có thể sử dụng xác thực dựa trên chứng chỉ (IPSec qua IKE)

- IPSec(qua IKE) và SSL cung cấp tính năng sinh khoá và làm tươi khoá mà không phải truyền bất kỳ khoá nào dưới dạng rõ hay ngoại tuyến

Những điểm khác nhau:

- SSL được thực thi như một API giữa tầng ứng dụng và tầng vận tải; IPSec được thực thi như một khung làm việc tại tầng liên mạng.

- SSL cung cấp tính năng bảo mật từ ứng dụng - tới - ứng dụng(ví dụ: giữa WebBrowser và WebServer); IPSec cung cấp tính năng bảo mật từ thiết bị - tới - thiết bị.

- SSL không bảo vệ lưu lượng UDP; IPSec thì có

- SSL hoạt động từ điểm cuối - tới - điểm cuối và không có khái niệm đường hầm. Điều này có thể là một vấn đề lúc lưu lượng cần được xem xét bằng cách kiểm tra nội dung và quét virus trước khi nó được phân phối thành công đến đích; IPSec có thể hoạt động theo hai cách, điểm cuối - tới - điểm cuối và như một đường hầm

- SSL có thể vượt qua NAT hoặc SOCKS, chúng dùng để che dấu cấu trúc địa chỉ bên trong hoặc tránh sự xung đột địa chỉ IP riêng; IPSec trong chế độ vận tải (end –to- end) không thể sử dụng NAT nhưng nó có thể dùng một đường hầm IPSec để đạt được mục tiêu tương tự và thậm chí bảo mật hơn NAT vì đường hầm cũng có thể được mã hoá.

- Các ứng dụng cần phải sửa đổi để sử dụng SSL. Điều này có thể là một vấn đề lúc ta không truy cập được mã nguồn của ứng dụng hoặc không có thời gian hay kinh nghiệm để thay đổi mã nguồn của ứng dụng; IPSec hoàn toàn trong suốt với các ứng dụng.

Thông thường SSL là tốt lúc ta chỉ có một ứng dụng được bảo vệ và nó đã sẵn có trong một phiên bản SSL-aware. Đây là trường hợp có một ứng dụng chuẩn đa dạng, không chỉ với WebBrowser và WebServer. Ngoài ra, nếu có tuỳ chọn của việc thực thi khái niệm 3-tier bằng cách tận dụng các cổng ứng dụng Web tại vành đai của mạng, SSL là một sự lựa chọn tốt. Nếu có một số lượng lớn các ứng dụng để bảo đảm an toàn có thể phải chọn giải pháp tốt hơn cho mạng. Trong trường hợp này, IPSec là sự lựa chọn tốt hơn. Trừ khi tự ta phát triển các ứng dụng, IPSec mềm dẻo hơn SSL để thực thi một chính sách bảo mật yêu cầu nhiều mức khác nhau và sự kết hợp của xác thực, mã hoá và đường hầm.

Cuối cùng nhưng không kém phần quan trọng, sự lựa chọn một công nghệ bảo mật thích hợp còn phụ thuộc vào mô hình giao dịch. Nếu mục đích của các Server ứng dụng là phải có khả năng truy cập mạng công cộng thì một thiết kế dựa trên Web và công nghệ bảo mật dựa trên SSL có lẽ là lựa chọn đúng. SSL là sẵn có trên bất kỳ một trình duyệt Web chuẩn nào và đó sẽ chỉ là công cụ được sử dụng và yêu cầu bởi người dùng. Tuy nhiên, những người dùng nên được hạn chế truy cập tới Server ứng dụng hay mạng của chúng ta, khi đó một mạng riêng ảo dựa trên IPSec và có thể cả một số công nghệ đường hầm tầng 2 là giải pháp được ưa thích hơn. Trong trường hợp này, những người tham gia và vai trò của họ trong việc trao đổi dữ liệu sẽ được xác định trước.

Tổng kết chương IV

Trong chương này chúng ta đã nghiên cứu thêm một số công nghệ bảo mật bổ sung cho mạng riêng ảo giúp cho người dùng cũng cố vững chắc quá trình truyền dữ liệu dựa trên mạng riêng ảo. Chúng ta đã xem xét về kỹ thuật xác thực từ xa như RADIUS, TACACS. Đây là những Server xác thực từ xa sẽ xác thực các yêu cầu kết nối từ xa. Các Server này có thể tự xác thực người dùng từ xa hoặc chuyển tiếp thông tin người dùng tới một cơ sở dữ liệu trung tâm để xác minh.

Chúng ta cũng xem xét các công nghệ bảo mật như NAT, SOCKS, SSL và cả TLS, những công nghệ này khi sử dụng với mạng riêng ảo có thể giúp cho người dùng có được môi trường an toàn hơn để truyền dữ liệu qua Internet và các mạng công cộng.

Cuối cùng là đưa ra một sự so sánh giữa hai giải pháp IPSec và SSL, đồng thời phân tích khả năng áp dụng chúng trong thực tế

Câu hỏi ôn tập

1. RADIUS stands for _____.

a. Remote Account Dial-In User Service
b. Remote Access Dial-In User System
c. Remote Access Dial-In User Service
d. Remote Account Dial-In User System

2. TACACS is a proprietary protocol by _____.

a. Cisco Systems
b. Netscape Communications Corporation
c. Microsoft Corporation
d. InterNIC

3. Keeping a tab on the duration of user activities is a part of _____.

a. Authentication
b. Authorization
c. Accounting
d. Authentication and Accounting

4. Which of the following security solutions helps preserve IP addresses?

a. SOCKS
b. SSL
c. TLS
d. NAT

5. Which of the following firewalls keep an account of connection status in addition to checking the IP addresses carried by the datagram?

a. Application proxy firewalls
b. Static stateful firewalls
c. Packet filter firewalls
d. Stateful packet inspection firewalls

6. What is the difference between a firewall and a SOCKSv4 server?

a. A firewall masks internal nodes from the outside world; SOCKS do not.
b. SOCKS authenticates remote users; firewalls do not.

c. Firewalls authenticate remote users; SOCKS do not.
d. There is no difference between the two.

7. Which of the following requires compulsory two-way authentication for an HTTP-based transaction?

a. SSL
b. SOCKS
c. TLS
d. NAT

PHẦN II XÂY DỰNG VÀ THỰC THI MẠNG RIÊNG ẢO

Phần I đã trình bày chi tiết về những vấn đề liên quan đến công nghệ mạng riêng ảo. Bây giờ chúng ta đã biết rõ những yêu cầu của một mạng riêng ảo, các khối dựng sẵn của mạng riêng ảo, các kiến trúc mạng riêng ảo khác nhau, và các thành phần đảm bảo an toàn của một thiết lập mạng riêng ảo. Bây giờ ta đã có những kiến thức nền tảng khá vững chắc về công nghệ đường hầm và các giao thức đường hầm khác nhau như: PPTP, L2F, L2TP và IPSec. Với những kiến thức trên, trong phần này ta sẽ bước sang việc xây dựng và thực thi mạng riêng ảo.

Chương V Xây dựng mạng riêng ảo

Trong chương này ta sẽ nghiên cứu về các vấn đề và những điểm cần lưu ý khác nhau trong khi thiết kế một giải pháp dựa trên mạng riêng ảo cho các tổ chức. Ta sẽ xem xét các vấn đề thiết kế mạng riêng ảo như: bảo mật, đánh địa chỉ và định tuyến, hiệu suất, khả năng mở rộng và khả năng tích hợp. Các vấn đề liên quan đến việc thực thi FireWall, NAT, DNS, phân phối khoá, quan hệ tin cậy giữa các thực thể liên quan cũng được đề cập. Chúng ta cũng xem xét các môi trường mạng riêng ảo: Remote Access, Intranet, Extranet để hiểu rõ các vấn đề liên quan trong khi thực thi mạng riêng ảo trong các môi trường này. Cuối cùng, ta sẽ nghiên cứu các bước thông thường để thực thi mạng riêng ảo, lựa chọn sản phẩm và nhà cung cấp dịch vụ, kiểm thử kết quả, thiết kế và thực thi mạng riêng ảo, quản trị và giám sát các thiết lập

5.1. Các vấn đề khi thiết kế mạng riêng ảo

Một bản thiết kế chi tiết và đầy đủ là cơ sở chính của một mạng. Và điều này cũng đúng với bất kỳ mạng riêng ảo nào. Nếu có sai sót trong việc phân tích các yêu cầu của một tổ chức và theo đó là kế hoạch cũng bị sai sót thì sẽ có ảnh hưởng rất nhiều về sau. Chẳng hạn, có thể có nhiều thứ gặp sự cố và làm việc không như mong muốn, Ngoài ra người dùng cuối cũng phải chịu các hậu quả của việc lập kế hoạch không hợp lý.

Lúc thiết kế mạng, người thiết kế cần phải luôn tuân thủ định hướng, không bỏ sót bất cứ thứ gì. Vấn đề chính mà ta cần phải xem xét lúc triển khai thiết kế mạng riêng ảo bao gồm như sau:

- Bảo mật
- Đánh địa chỉ IP và định tuyến
- Các vấn đề liên quan đến DNS
- Các vấn đề về Router/Gateway, Firewall và NAT
- Các xem xét về Client và Server
- Hiệu suất thực thi
- Khả năng mở rộng và tính tương thích

Sau đây, ta sẽ nghiên cứa riêng từng vấn đề này

5.1.1. Bảo mật

Một mạng riêng ảo mở rộng qua một mạng công cộng "không an toàn" để kết nối một cách an toàn tới các nguồn tài nguyên và các mạng chi nhánh của một tổ chức. Tuy nhiên, hầu hết các quản trị mạng vẫn còn xem nhẹ vấn đề bảo mật của một mạng riêng ảo. Đây là vấn đề chính cần xem xét khi thiết kế một mạng riêng ảo bởi vì trong mạng riêng ảo có sử dụng các mạng công cộng làm trung gian, mạng công cộng thường là mở với tất cả các cá nhân, đặc biệt với những cá nhân có ý đồ đen tối. Điều này làm cho mạng riêng ảo dễ bị tấn công trước nhiều mối đe doạ, bao gồm cả giả mạo, bắt gói, sửa đổi nội dung thông tin, các tấn công kiểu brute-force, tân công từ chối dịch vụ và các tấn công trên các giao thức mạng riêng ảo.

Khi xem xét các đặc điểm thiết lập mạng riêng ảo, bốn thành phần nổi bật của kết nối mạng riêng ảo rất dễ bị tấn công từ bên ngoài là:

- Người dùng từ xa (người dùng cuối hoặc Client VPN). Thực thể này có thể là một phần trong các nhân viên di động của tổ chức hoặc một người dùng cuối truy cập Intranet của tổ chức từ nhà. Thực thể này sử dụng một ID và Password để làm việc từ xa. Kết quả là, người dùng từ xa thường bị tất công vào ID hoặc Password. Nếu kẻ tấn công hoặc các cá nhân có ý đồ xấu thu được các ID và Password này, hắn ta dễ dàng truy cập lại vào Intranet của tổ chức và các tài nguyên trong đó

- Phân đoạn kết nối tới ISP. Một người dùng từ xa hay các chi nhánh yêu cầu một tuỳ chọn truy cập đề kết nối tới POP của ISP, nó sẽ lần lượt thiết lập kết nối tới mạng đích. Phân đoạn kết nối này có thể hoặc là một đường leased line hoặc một kết nối quay số từ xa. Kết nối đường Leased Line tồn tại giữa một chi nhánh ở xa và Intranet của ISP cung cấp thuê bao kết nối trực tiếp tới mạng ISP. Mặc dù một tuỳ chọn kết nối an toàn, đường leased line có thể bị mắc rẽ để nghe trộm và một kẻ tấn cộng có thể nghe trộm trên các cuộc truyền tin. Các kết nối quay số rẽ hơn khá nhiều so với đường thuê riêng leased line và thường được dùng để kết nối một người dùng từ xa với mạng của tổ chức. Các kết nối quay số có khả năng truy cập tới tất cả và do đó dễ dàng mắc rẽ vào để nghe trộm. Điểm yếu này làm cho chúng rất dễ bị nghe trộm. Vì vậy, các kết nối quay số không an toàn như đường leased line

Chú ý Không quan tâm đến phân đoạn kết nối, việc nghe trộm trên một phiên liên lạc có thể cung câp cho tấn công có một địa chỉ IP máy chủ từ xa hợp lệ. Kẻ tấn công này sau đó sử dụng thông tin này để giả mạo địa chỉ IP và phá vỡ hàng rào an toàn của tổ chức mà không gặp trở ngại nào. Một vấn đề chính yếu khác gắn liền với phân đoạn kết nối, dù là đường thuê riêng hay đường quay số, nếu chính ISP có ý đồ xấu thì nhà cung cấp dịch vụ có thể dễ dàng đọc được tất các dữ liệu trong phiên liên lạc và như vậy dễ dàng truy cập tới dữ liệu bí mật được truyền giữa một người dùng cuối và mạng Intranet của tổ chức.

- Mạng công cộng: Một mạng công cộng, đặc biệt là Internet , không nằm trong địa hạt của một cơ quan thẩm quyền đơn có thể kiểm soát tất cả các hoạt động và giao dịch qua nó. Hơn nữa, các điểm trung gian, chẳng hạn như các bộ định tuyến tạo nên Internet và hỗ trợ các đường hầm mạng riêng ảo có thể không dùng riêng cho các đường hầm của một tổ chức đơn. Một bộ định tuyến trung gian có thể đồng thời hỗ trợ nhiều đường hầm bắt nguồn từ nhiều mạng Intranet của nhiều tổ chức. Kết quả là lưu lượng từ một tổ chức có thể không hoàn toàn được biệt lập với lưu lượng của các tổ chức khác. Thêm vào đó, mạng công cộng bản chất là dùng chung, nó có thể được truy cập bởi bất kỳ ai muốn sử dụng nó. Một ý định của cá nhân hay một tổ chức với các trang thiết bị đúng và giỏi chuyên môn có thể dễ dàng gắn vào một phương tiện liên lạc và sử dụng nó để đem lại lợi ích riêng. Trong các trường hợp khác, một kẻ tấn công có thể giả mạo các gói dữ liệu hoặc thay đổi nội dung dữ liệu dẫn đến nhiều thiệt hại cho một tổ chức.

- Điểm truy cập mạng đích: Một Router, Gateway, Firewall hoặc một thiết bí NAT thường được đặt tại vành đai của mạng và các Server như là một điểm truy cập Intranet của một tổ chức. Các thiết bị này không chỉ phải đối mặt với các mối đe doạ bảo mật và các nổ lực xâm chiếm từ các thực thể bên ngoài mà còn cả từ các thực thể bất mãn ở bên trong. Thêm vào đó, nếu tổ chức hỗ trợ một mạng Extranet, các thiết bị ngày cũng dễ bị tấn công với các lưu lượng độc hại từ các đối tác thương mại bên ngoài.

Hình 5.1 Bốn thành phần dễ bị tấn công của kết nối mạng riêng ảo

Ở trên ta đã thảo luận về các lỗ hổng bảo mật trong một thiết lập mạng riêng ảo đầy đủ. Và như vậy, ta không thể bỏ qua các vấn đề bảo mật này. Ta cần giữ các bước hợp lý trong việc thực thi để đảm bảo rằng giải pháp mạng riêng ảo của ta là có thể chịu được tất cả các kiểu tấn công, mà vẫn cho phép khai thác Internet và hạ tầng mạng công cộng để giảm chi phí thực thi trong khi tăng mức độ an toàn của các giao dịch, vì vậy bảo vệ được hầu hết các khả năng tấn công vào tổ chức - dữ liệu.

IPSec đã được thảo luận chi tiết trong các chương của phần I được xem là câu trả lời cho hầu hết các mối quan tâm bảo mật liên quan đến 4 thành phần dễ bị tấn

công trong mạng riêng ảo. Nó đảm bảo sự an toàn của dữ liệu trong khi truyền. IPSec bảo mật dữ liệu bằng cách mã hoá mỗi gói dữ liệu với các thuật toán mã hoá mạnh. Kết quả là kẻ nghe trộm hoặc thậm chí cả ISP trung gian không thể đọc được dữ liệu. Hơn nữa, IPSec xác thực mỗi gói dữ liệu riêng lẻ ngoài việc xác thực người dùng cuối một lần. Điều này làm giảm khả năng giả mạo.

Thêm hai khía cạnh bảo mật của bất kỳ giao dịch nào dựa trên mạng riêng ảo là quan hệ tin cậy và trao đổi khoá giữa các bên liên quan. Nếu một trong hai khía cạnh này bị tổn hại thì sự an toàn của toàn bộ thiết lập mạng riêng ảo có thể bị tổn hại.

Vấn đề quan hệ tin cậy:

Tin cậy là một phần không thể thiếu của việc đảm bảo an toàn cho bất kỳ hệ thống nào, bao gồm cả thiết lập mạng riêng ảo của ta. Tuy nhiên, sự tin cậy có thể bị khai thác để giành được quyền truy cập vào thiết lập an toàn cẩn mật của ta. Vì vậy, cần phải để ý các vấn đề sau khi quyết định mức tin cậy trong thiết lập của ta với các thực thể bên ngoài:

+ Các ứng dụng như Telnet, FTP rất dễ bị tấn công. Cân nhắc để sử dụng các ứng dụng an toàn hơn, như SSH để thay thế

Chú ý Vì sự phức tạp của các cơ chế bảo mật mà SSH sử dụng, hiệu suất của SSH qua VPN sẽ bị chậm.

+ Không chạy các dịch vụ thêm trên Server VPN. Server VPN phải chạy không chỉ tối thiểu các ứng dụng và dịch vụ liên quan đến mạng riêng ảo mà còn phải tối thiểu hoá các dịch vụ mà kẻ xâm nhập có thể truy cập trong trường hợp xâm nhập thành công.

+ Mặc dù việc không tin cậy hoàn toàn các Client VPN đã xác thực là không thích hợp, ta nên duy trì một mức không tin cậy hợp lý. Nếu cung cấp truy cập hạn chế tới các tài nguyên và thiết bị, nhưng vẫn cho phép người dùng thực hiện các hoạt động cần thiết liên quan đến công việc của họ, ta có thể giảm hậu quả của sự xâm nhập trong đó kẻ tấn công nhằm vào các máy của người dùng cuối. Cũng có thể dùng firewal để hạn chế các truy cập nói trên

Các xem xét liên quan đến trao đổi khoá:

Trao đổi khoá giữa các bên liên quan là một khía cạnh khác của bảo mật mà khi bị tổn hại có thể dẫn đến tổn hại rất lớn trong mạng. Vì thế, điều cốt yếu là khả năng phân phối các khoá một cách an toàn, đặc biệt trong trường hợp sử dụng mật mã đối xứng, như ta đã biết, trong mật mã đối xứng thường sử dụng một khoá mật cho cả lập mã và giải mã. Vì thế, nếu khoá này rơi vào tay một kẻ xâm nhập, nó sẽ mang lại cho kẻ xâm nhập khả năng truy cập tới các giao dịch đang tiếp diễn. Sẽ là hợp lý khi sử dụng IPSec, bảo mật SSH và các ứng dụng dựa trên SSL/TSL, nó tránh được việc trao đổi khoá dưới dạng rõ.

Mật mã phi đối xứng không giống như mật mã đối xứng, không dựa vào một khoá cho việc giải mã và lập mã. Trái ngược với các mật mã đối xứng, mật mã phi đối xứng trao đổi các khoá công khai giữa các bên liên quan và sử dụng các khoá mật tương ứng với chúng cho chức năng giải mã. Tuy nhiên, các cơ chế này không phải tuyệt đối an toàn và rất dễ bị tổn thương với các tấn công kiểu Man-in-the-Middle. Trong kiểu tấn công này, kẻ xâm nhập có thể thay thế khoá công khai của anh ta, và như vậy hoàn toàn truy cập được vào liên lạc giữa hai người dùng cuối hợp lệ. Vì vấn đề này, ta cần phải xác nhận lại khoá công khai với những người liên lạc khác sau khi pha trao đổi khoá hoàn tất, nhưng trước khi pha trao đổi dữ liệu bắt đầu. Mặc dù để thực hiện như vậy mọi lúc là không thể, một sự kiểm tra chéo ngẫu nhiên của các khoá công khai nhận được rất nên được thực hiện.

Một điểm mà ta phải luôn lưu ý, bất kể mật mã đối xứng hay phi đối xứng thì các khoá không bao giờ lưu trữ trên một điểm cuối VPN, nơi chúng dễ dàng bị truy cập bởi kẻ xâm nhập. Một giải pháp khả thi cho vấn đề này là lưu trữ các khoá trong một vị trí tập trung, được bảo vệ tốt thay vì lưu trữ tất cả các khó trên một Server VPN riêng. Mặc dùng quá trình truy cập khoá có thể bị kéo dài, nhưng trong thực tế, nó không chỉ giảm gánh nặng lưu trữ trên Server VPN mà còn nâng cao việc bảo đảm an toàn cho các khoá.

5.1.2. Vấn đề đánh địa chỉ và định tuyến mạng riêng ảo

Một vấn đề quan trọng khác trong việc lập kế hoạch và thiết kế mạng riêng ảo là việc đảm bảo rằng các địa chỉ IP cần được gán cho các thiết bị mạng riêng ảo phải có kế hoạch và hợp lý. Hơn nữa, cũng cần phải đảm bảo rằng lược đồ định tuyến không chỉ có khả năng điều khiển kết nối mạng công cộng dựa trên địa chỉ IP toàn cục, mà còn sẽ có khả năng thích ứng với bất kỳ về lược đồ đánh địa chỉ IP của ta trong tương lai. Ngoài ra, giới hạn hợp lý phải được giữ để đảm bảo rằng các đối tác thương mại bên ngoài và các Client từ xa cũng có thể kết nối tới mạng riêng ảo của chúng ta mà không gặp phải vấn đề trục trặc

5.1.2.1. Vấn đề đánh địa chỉ

Trong một mạng riêng, một công ty A không cần mua các địa chỉ IP duy nhất(được biết như là các địa chỉ IP toàn cầu) từ một cơ quan có thẩm quyền, nhưu InterNIC, IANA hoặc từ ISP. Công ty A có thể sử dụng các địa chỉ IP riêng hoặc bất kỳ một địa chỉ IP nào mà họ thích bởi vì truyền thông trong một mạng riêng không phải định tuyến ra ngoài phạm vi công ty. Kết quả là, các host và các thực thể đặt trong một mạng riêng không thể liên lạc với các mạng qua Internet hay các mạng công cộng khác và vì vậy nó biệt lập với thế giới bên ngoài

Chú ý: Các địa chỉ IP trong phạm vi 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 và 192.168.0.0 – 192.168.255.255 được dùng như các địa chỉ IP riêng và có thể được dùng trong một mạng riêng hoặc Intranet không sử dụng một mạng công cộng để kết nối tới các nhánh ở xa và người dùng từ xa

Lược đồ địa chỉ riêng không hoàn toàn đúng cho các mạng riêng ảo vì chúng còn dựa trên một mạng đường trục công công để truyền thông. Điều này ngụ ý rằng chỉ VPN Client và Server liên quan trong một giao dịch là cần một địa chỉ IP công cộng. Liên lạc thực sự trên giao diện VPN ảo sẽ làm việc với các địa chỉ IP riêng. Kết quả là, công ty A sẽ đòi hỏi ít nhất một khối địa chỉ IP duy nhất toàn cầu từ ISP. Ta sẽ xem xét các nhân tố sau lúc đánh địa chỉ các thiết bị mạng riêng ảo

- Nếu công ty A sử dụng đường leased line để kết nối tới ISP, các thiết bị mạng riêng ảo sẽ được cấp phát các địa chỉ IP tính. Các trường hợp khác, nếu sử dụng các kết nối quay số để kết nối tới ISP POP, các Client VPN được dùng bởi

những người dùng di động phải được cấp phát các địa chỉ IP động, mặc dù VPN Server sẽ vẫn đòi hỏi một địa chỉ IP tính để có khả năng truy cập. Tuy nhiên, có một sự kế thừa vấn đề gắn với các Client VPN sử dụng địa chỉ IP động. Ta không thể giới hạn truy cập tới VPN Server trên cơ sở các địa chỉ IP mà ISP có thể cấp phát cho các VPN Client mỗi lần khác nhau. Trong hoàn cảnh này, các VPN Server rất dễ bị tấn công bởi các nguy cơ bảo mật mà một kẻ tấn công có thể hành động như một người dùng tin cậy.

- Sẽ không vấn đề gì nếu sử dụng một VPN Server đơn hoặc nhiều VPN Server, tất cả phải được cấp phát một địa chỉ IP tĩnh. Nếu các VPN Server sử dụng các địa chỉ IP động, VPN Client không thể định vị được Server mong muốn.

- Nếu địa chỉ IP xung đột có thể cắt xén nếu cần hợp nhất hai mạng riêng, như trong trường hợp sát nhập hai tổ chức. Trong kịch bản này, nếu các mạng được hợp nhất sử dụng địa chỉ IP riêng thì rất có thể một số địa chỉ IP có thể xung đột. Việc thay đổi các địa chỉ IP xung đột là dễ dàng nếu chỉ với số lượng nhỏ các IP bị xung đột. Tuy nhiên, với một số lượng lớn thì có thể ta phải thay đổi lược đồ địa chỉ IP của ít nhất một mạng hoặc xấu nhất là toàn bộ mạng sau khi hợp nhất. Việc thay đổi lược đồ địa chỉ là rất mất nhiều thời gian. Có thể sử dụng khả năng cấu hình địa chỉ IP tự động, như sử dụng DHCP. Giao thức này cho phép một thiết bị mạng nhận được thông tin cấu hình, bao gồm cả một địa chỉ IP động khi thiết bị đó khởi động.

- Nếu không có đủ địa chỉ IP duy nhất toàn cầu, cách thích hợp nhất là sử dụng địa chỉ IP riêng trong mạng của công ty và một NAT tại vành đai mạng để kết nối với thế giới bên ngoài. NAT sẽ cấp phát một địa chỉ IP duy nhất bất cứ lúc nào một host bên trong cần kết nối tới Internet hoặc thiết lập một phiên mạng riêng ảo. Cách này sẽ giúp ta đảm bảo rằng không có xung đột IP khi thiết lập kết nối Internet hoặc một phiên mạng riêng ảo. Một điểm quan trọng ở đây là NAT và VPN có thể xung đột vì việc ghi đè tiêu đề

Chúng ta giả thiết rằng công ty A trước đây có một mạng truyền thống, trong đó các mạng Intranet khác nhau của công ty được kết nối với nhau qua các phương tiện thiết bị riêng, như đường leased-line hoặc frame relay. Chúng ta cũng giả thiết

rằng công ty A đã xây dựng một lược đồ địa chỉ cho mạng của họ. Vì mạng là độc lập và đường trục sử dụng chỉ các phương tiện thiết bị riêng, công ty A có thể sử dụng hoặc các địa chỉ IP nhập nhằng toàn cục(private) hoặc các địa chỉ duy nhất toàn cục(public) từ trung tâm thông tin mạng (Network Information Center - NIC).

Bởi vì việc gán địa chỉ IP công cộng được thực hiện bởi tổ chức có thẩm quyền trên phạm vi toàn cầu, họ rất rõ ràng. Các địa chỉ công cộng có khả năng định tuyến tới bất kỳ đâu. Tuy nhiên, vì việc gán địa chỉ riêng rất dễ dàng thực hiện mà không cần đến một tổ chức có thẩm quyền trên phạm vi toàn cầu, chúng có thể nhập nhằng khi sử dụng trong Internet công cộng và chỉ có thể có khả năng định tuyến được trong một mạng riêng của chính công ty. Tóm lại:

1. Nếu công ty A sử dụng các địa chỉ công cộng trong mạng của mình, các địa chỉ có thể tiếp tục được sử dụng mà không cần phải thay đổi trong môi trường mạng riêng ảo. Nếu có mong muôn che dấu chúng trong khi gói dữ liệu được truyên qua Internet, một đường hầm ESP có thể được sử dụng giữa các firewall.

2. Nếu một công ty A sử dụng các địa chỉ IP riêng trong mạng của mình, các địa chỉ cũng có thể tiếp tục được dùng trên tất cả các mạng con không có kết nối vật lý tới mạng Internet công cộng. Nếu không có các mạng con đó mà kết nối tới Internet công cộng, đặc biệt tồn tại các liên kết tại vành đai của mạng Intranet, một địa chỉ IP công công phải được sử dụng.

Chế độ đường hầm ESP hoặc AH và ESP kết hợp trong chế độ đường hầm giữa các firewall giữ cho cả hai làm việc. Tiêu đề IP mới của đường hầm sẻ sử dụng các địa chỉ toàn cục của hai firewall, cho phép các gói dữ liệu được định tuyến quan Internet giữa hai firewall (hoặc các router). Tiêu đề của gói IP gốc sẽ sử dụng các địa chỉ IP được gán cho người dùng trên Intranet, vì vậy các địa chỉ này sẽ được che dấu khỏi sự dò xét bởi các giao thức mã hoá của ESP

5.1.2.2. Vấn đề định tuyến

Như trong các mạng truyền thống, việc định tuyến trong mạng riêng ảo liên quan tới việc xử lý định tuyến tới một địa chỉ đích xác định. Trong định tuyến truyền thống, làm việc trên bất kỳ tuyến đường hiện tại có thể dùng được để tới bộ

định tuyến đích. Tuy nhiên, trong các mạng riêng ảo, các phương tiện định tuyến cũng đảm bảo tính sẵn sàng của chỉ các tuyến đường qua các kết nối và đường hầm mạng riêng ảo an toàn thay vì quan các mạmg công cộng trung gian.

Cần lưu ý các vấn đề sau đây khi quyết định lược đồ định tuyến cho mạng riêng ảo:

- Server mạng riêng ảo mà các Client từ xa kết nối tới, chỉ định một tuyến đường mặc định tới các Client VPN từ xa này. Bất kỳ tương tác khác giữa hai đầu cuối trong một phiên mạng riêng ảo đã cho được định tuyến qua tuyến đường đã được định nghĩa trước này. Tương tự, trong trường hợp của một Client quay số, nơi đường hầm được thiết lập giữa nhánh mạng của ISP và mạng đích, Client VPN sử dụng tuyến đường tới Intranet của ISP như tuyến đường mặc định.

- Nếu Server VPN được đặt sau một firewall, tất cả các tuyến đường mặc định nên trỏ vào các firewall đó.

- Nếu gán rõ ràng một tuyến đường (hoặc một tập các tuyến đường) tới mỗi Client cho một phiên mạng riêng ảo, ta có thể phải kiểm soát đầy đủ qua các đường dẫn giao dịch. Tuy nhiên, làm như vậy đòi hỏi phải cấu hình các tuyến đường trên mỗi Client một cách thủ công. Đây có thể là một công việc cực kỳ mệt mỏi nếu số lượng Client VPN lớn. Hơn nữa, khả năng tắc nghẽn mạng rất cao nếu số tuyến đường được gán rõ ràng có giới hạn.

- Ta có thể muốn sử dụng các tuyến đường tĩnh lúc thiết lập một giải pháp mạng riêng ảo lần đầu tiên. Các tuyến đường này được định nghĩa và cấu hình trước trên cả Server VPN cũng như Client VPN. Kết quả là các tuyến đường tĩnh này có thể giữ vai trò quan trọng trong việc kiểm thử một thiết lập mạng riêng ảo mới. Tương tự, các tuyến đường tĩnh này cũng có thể giúp ta gỡ rối các vấn đề liên quan đến định tuyến.

- Ngoại trừ việc kiểm thử các thiết lập mạng riêng ảo mới và trợ giúp khi gặp vấn đề, ta nên sử dụng các tuyến đường tĩnh một cách hạn chế vì chúng có thể là nguyên nhân dẫn đến nhiều sự quản lý và cấu hình lại overhead, đặc biệt nếu có

một thay đổi trong lược đồ đánh địa chỉ hoặc sự sắp xếp lại các thiết bị mạng riêng ảo

- Thông thường, trong một phiên mạng riêng ảo có sử dụng các đường hầm tự nguyện và mở rộng qua Internet, ta có thể hoặc truy cập các Host trên Internet hoặc các Host trên Intranet, miễn là một Gateway mặc định được sử dụng cho mạng riêng ảo, không đồng thời xẩy ra cùng một lúc cả hai. Vì vậy, ta sẽ cần cấu hình một tuyến đường mặc định giữa Client VPN và NAS của ISP. Điều này sẽ cho phép Client VPN truy cập đồng thời các Host dựa trên Intranet cũng như dựa trên Internet.

Chú ý Phương phát dễ nhất và an toàn nhất của việc gán các đường định tuyến cho các phiên mạng riêng ảo là cấu hình firewal, bộ định tuyến mạng riêng ảo mặc định, hoặc các cổng nối mạng riêng ảo mặc định với tất cả các đường định tuyến có thể liên quan đến mạng riêng ảo. Thực tế này sẽ tiết kiệm cho ta nhiều thời gian và công sức vì sau đó ta chỉ cần cấu hình một đường định tuyến mặc định trên tất cả các máy phía Client. Hơn nữa, như vậy có thể làm đơn giản hoá nếu Gateway, Router VPN hoặc firewall có thể chia sẻ thông tin định tuyến này với các thiết bị định tuyến khác. Kết quản là, ta sẽ không cần phải cấu hình mỗi một thiết bị một cách riêng lẻ.

Lý do Các Client VPN quay đó được cấp phát hai địa chỉ IP, thứ nhất là lúc thiết lập một kết nối PPP với nhánh mạng của ISP và thứ hai là trong khi thiết lập phiên mạng riêng ảo. Vì thế, ta phải rất cẩn thận trong khi gán các đường định tuyến cho các phiên mạng riêng ảo, vì nếu thêm một đường định tuyến PPP thay cho đường định tuyến mạng riêng ảo, tất cả các lưu lượng sẽ được định tuyến qua đường định tuyến PPP không an toàn dưới dạng không được mã hoá. Hơn nữa, nếu các gói có địa chỉ IP riêng chúng sẽ bị loại bỏ tại thiết bị định tuyến của ISP.

Các mạng riêng ảo cũng yêu cầu rằng phải lựa chọn giao thức định tuyến đúng. Ta sẽ cần chọn giao thức định tuyến theo các điều kiện và yêu cầu của tổ chức. Một số nhân tố có thể giup ta trong việc quyết định giao thức bao gồm:

- Giải thông được sử dụng bởi giao thức: Ví dụ, ta có thể muốn sử dụng BGP(Boder Gateway Protocol – Giao thức cổng biên) khi thực tế nó sử dụng một giải thông nhỏ.

- Overhead được phát sinh: Một số giao thức định tuyến phát sinh overhead truyền thông rất cao so với các giao thức khác. RIP là một ví dụ. Mặc dù IPSec không phải là một giao thức định tuyến, nhưng nó cũng phát sinh overhead cao.

- Chiều hướng liên lạc: Một số giao thức định tuyến, như RIP, chỉ hỗ trợ các địa chỉ Unicast, các giao thức khác như RIPv2 và Open Shortest Path First (OSPF) hỗ trợ các địa chỉ broadcast and multicast.

- Tính năng bảo mật được cung cấp: Một số giao thức định tuyến mang lại khả năng bảo mật cao

5.1.3. Các xem xét liên quan đến DNS

Hệ thống tên miền(Domain Name System - DNS) là một thư mục phân tán toàn cục được sử dụng cho việc chuyển đổi các địa chỉ dựa vào tên, Chẳng hạn như www.yahoo.com tương ứng với một địa chỉ IP là 64.58.76.223. Ta sẽ cân DNS trong mạng riêng ảo cho chức năng tương tự - ánh xạ các địa chỉ dựa vào tên của host để tương ứng chúng với các địa chỉ IP.

Trong mạng riêng ảo Intranet, chỉ cho phép truy cập tới các tài nguyên đặt trong mạng Intranet của tổ chức, ta sẽ cần tạo một Domain riêng biệt cho mạng chính và nhiều Domain riêng lẻ cho mỗi nhánh mạng từ xa. Ví dụ, ta có thể tạo một Domain là “MyIntranet.com” và tạo các Domain trong như là “RemoteBranch1.MyIntranet.com”, “RemoteBranch2.MyIntranet.com” v.v. Dễ dàng cấu hình máy chủ DSN để hỗ trợ kiến trúc Domain này. Hơn nữa, cũng sẽ cần thiết lập ít nhất một máy chủ Domain trong như là một máy chủ Domain thứ cấp cho mỗi Domain trong mà ta tạo ra. Điều này sẽ mang lại thuận lợi trong việc chia sẻ các các cập nhật và thông tin liên quan đến DNS khác giữa nhiều Domain trong.

Cấu hình trước đây quan tâm đến việc truy cập mạng riêng ảo dựa trên Intranet, các host bên trong sẽ không còn khả năng truy cập Intrernet. Nếu muốn các host bên trong có khả năng truy cập Internet hoặc các tài nguyên trong mạng Internet, ta cần thiết lập bổ sung một máy chủ DNS bên ngoài, nó sẽ nhận tất cả

truy vấn tới các host bên ngoài từ các DNS bên trong và anh xạ các địa chỉ theo tên bên ngoài tương ứng với các địa chỉ dạng số.

Trong trường hợp những người dùng di động sử dụng một mạng riêng ảo để truy cập Intrnanet, có một vấn đề cố hữ với các thiết lập DNS. Nếu những người dùng từ xa này phụ thuộc vào một kết nối đường quay số, các Client VPN kết nối tới Intranet sử dụng một địa chỉ IP mới mỗi lần. Và như vậy, ta không thể mã cứng DSN của ta để cung cấp cho các Client này.

Để giải quyết vấn đề này, ta sẽ cần thiết lập các máy Client cá nhân để sử dụng các máy chủ DNS bên trong. Nếu những người dùng từ xa yêu cầu một kết nối Internet đồng thời, ta phải cấu hình những đầu cuối từ xa này để tìm kiếm các máy chủ DNS bên ngoài thêm vào các máy chủ bên trong

Chú ý Khi kết nối tới Internet, ta có thể đối mặt với độ trễ rất lớn, hoặc thập chí ngừng ứng dụng trong khi phân giải tên/địa chỉ nếu ta thiết lập các host VPN trước hết tìm kiếm một máy chủ DNS bên trong và sau đó tìm kiếm một máy chủ DNS bên ngoài (trong cả hai kịch bản intranet và remote access). Điều này là bởi vì các host se tìm một máy chủ DNS bên ngoài sau khi đã tình kiếm qua tất cả các máy chủ DNS bên trong mà chúng được đăng ký. Và như vậy, host VPN nên tìm kiếm một máy chủ DSN bên trong có khả năng chuyển tiếp yêu cầu tới DNS của ISP. Kết quả là nhanh hơn nhiều vì nó cho phép lưu cache các tên được tìm kiếm.

Hơn nữa, để xem xét những điều mới được đề cập, ta cũng cần cảnh giác với các tính chất dễ bị tổn thương máy chủ DSN sau đây:

- Nếu xẩy ra lỗi bảo mật các máy chủ DNS, một kẻ xâm nhập có thể chiếm quyền điều khiển Server của ta và giành được toàn quyền kiểm soát qua các Domain đã đăng ký với chúng. Kiểu tấn công này được xem như là cướp Domain.

- Một kẻ xâm nhập có thể sử dụng các tấn công từ chối dịch vụ trên các máy chủ DNS của ta. Trong trường hợp này, các Domain bị tấn công sẽ không có khả đăng định vị các Host trong các Domain khác và Internet. Vì tất cả các máy chủ DNS dựa trên Internet liên lạc với mỗi máy chủ khác, kiểu tấn công này có thể dẫn đến sự chậm trễ toàn cục lan rộng trong tiến trình xử lý ánh xạ tên/ip.

- Nếu một kẻ xâm nhập giành được quyền truy cập vào máy chủ DNS của ta và sửa đổi các thông tin được lưu trong máy chủ để chuyển hướng bất kỳ lưu lượng

nào giành cho các địa chỉ hợp pháp tới một vị trí giả mạo, các Domain bị tấn công sẽ không nhận được bất kỳ lưu lượng dữ liệu nào giành cho chúng.

Để tránh các vấn đề này, cần phải bảo mật cho các máy chủ DNS trong cũng như ngoài

5.1.4. Các xem xét liên quan đến Firewall, Router, NAT

Như ta đã biết, các Router (hay Gateway), Firewall và các thiết bị NAT là các thiết bị ngoại biên. Ta cần xem xét một số vấn đề về sự an toàn và sự tích hợp của chúng trong một môi trường mạng riêng ảo.

5.1.4.1. Các xem xét liên quan đến Router

Router(và các Gateway) giữ một vai trò đáng kể trong việc định tuyến luồng lưu lượng qua một mạng dựa trên IP. Vì có các thiết bị ngoại biên này, mối quan tâm chính liên quan đến chúng là về tính an toàn của chúng. Nếu Router của ta được bảo mật kiém, chúng có thể dễ dàng bị nhắm tới bởi những kẻ xâm nhập, là những kẻ phái sinh luồng lưu lượng giả tạo gây ra các tấn công từ chối dịch vụ. Chúng cũng có thể được dùng bởi những kẻ xâm nhập để tấn công các Router khác.

Các xem xét khác liên quan đến Router và Gateway trong thiết lập mạng riêng ảo bao gồm:

- Các Router và Gateway trong môi trường mạng Internet thường được cấu hình để cho truyền qua lưu lượng được định tuyến tới các Router kế tiếp nhằm hướng tới mạng đích. Điều này hàm ý rằng chúng có thể "chuyển" một khối lượng lớn dữ liệu sang nơi khác. Tuy nhiên, hầu hết các Router không có khả năng lưu trữ một khối lượng lớn dữ liệu khi dữ liệu chuyển đến chúng. Kết quả là, hầu hết các Router rất dễ bị ảnh hưởng với các tấn công từ chối dịch vụ. Bằng việc giành được toàn bộ quyền kiểm soát Router, một kẻ xâm nhập có thể dễ dàng giành được quyền truy cập vào mạng gắn với nó và dẫn đến thiệt hại lớn với mạng Intranet.

- Các Router chia sẻ thông tin định tuyến với các Router ngang hàng để có khả năng định danh không làm gián đoạn thêm luồng lưu lượng chúng nhận được. Kết quả là, các Router phải chia sẻ một quan hệ tin cậy với các Router ngang hàng.

Đặc điểm này của các Router thường bị khai thác bởi những kẻ xâm nhập, những kẻ này sau khi thay đổi hoặc xoá các đường định tuyến đã tồn tại hoặc đưa các đường định tuyến giả tạo vào bảng định tuyến được duy trì bởi một hoặc nhiều Router. Kết quả của việc thay đổi thông tin này là các Router mà các bảng định tuyến của chúng đã được cảnh giác có thể bắt đầu hoạt động như các Router giả tạo và chuyển tiếp luồng lưu lượng tới các Route "không đáng tin cậy"

- Nếu đang lập kết hoạch thực thi nhiều Router và Gateway trong mạng Intranet, cần đảm bảo rằng tất cả hỗ trợ cùng mức bảo mật. Điều này sẽ ngăn chặn kẻ xâm nhập khai thác một điểm yếu bảo mật đơn lẻ để giành quyền truy cập tới mạng.

Bởi các vấn đề đã xác định trên, ta nên cẩn thận khi chọn lựa các Router cho thiết lập mạng riêng ảo. Ngoài hiệu suất tốt, cũng nên tìm kiếm các Router có khả năng mã hoá và xác thực mạnh. Những khả năng này không chỉ bảo vệ các Router của ta, mà còn ngăn chặn việc quét và đọc trái phép các thông tin đang được chuyển qua bởi chúng

5.1.4.2. Các xem xét liên quan đến Firewall

Mặc dù các Firewall có thể trợ giúp như các kỹ thuật bảo vệ chống lại các cuộc tấn công và xâm nhập từ bên ngoài, ta cần xem xét một số vấn đề sau trước khi thực thi một thiết lập mạng riêng ảo dựa trên firewall. Một số vấn đề này như sau:

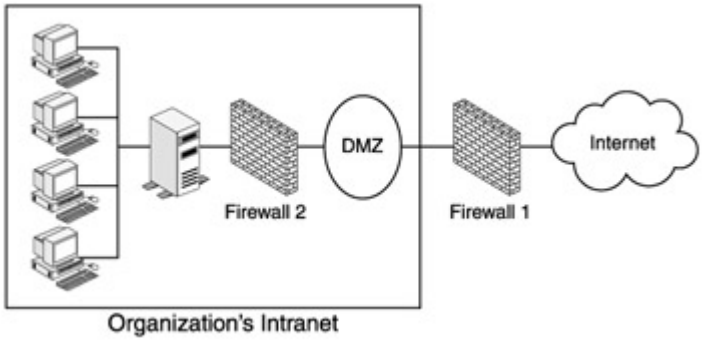
- Nếu đang lập kế hoạch thực thi các firewall hoạt động trên cơ sở các địa chỉ IP nguồn và đích, cổng nguồn và đích, giao thức được sử dụng nhưng không dựa trên nội dung của các gói dữ liệu, một kẻ xâm nhập có thể che dấu dữ liệu "độc hại" trong các gói dữ liệu được tải. Kết quả là, những dữ liệu độc hại này sẽ không bị phát hiện bởi Firewall. Vấn đề khác gắn với các Firewall này, cũng như với các Firewal lọc gói, đó là chúng không xử lý các giao dịch dựa trên nhiều kết nối động, chẳng hạn như các giao dịch FTP. Vì vậy, sẽ cần thiết lập các bộ lọc gói một cách rõ ràng để cho phép các luồng lưu lượng liên quan các giao dịch này.

- Các Firewal khác, như các Firewal Proxy ứng dụng và các Firewal kiểm duyệt trạng thái gói, các hoạt động của chúng phần lớn dựa trên nội dung của gói dữ liệu thêm vào các địa chỉ IP, địa chỉ cổng và các giao thưc được dùng. Tuy nhiên, phải nhớ rằng các Firewall Proxy ứng dụng không xử lý luồng lưu lượng dựa trên HTTPS và SSH-. Kết quả là, đặc trưng này có thể bị khai thác bởi những người bên ngoài để xâm nhập Firewall. Chức năng của Firewall kiểm duyệt trạng thái gói dữ liệu rất giống với Firewal Proxy ứng dụng. Tuy nhiên, hiệu suất của chúng tốt hơn nhiều. Vì vậy, dù có thể phải đầu từ nhiều hơn cho Firewall kiểm soát trạng thái gói dữ liệu, ta sẽ thăng đáng kể hiệu suất của toàn bộ thiết lập mạng riêng ảo

- Để vượt qua hầu hết các vấn đề liên quan đến Firewall, ta phải định nghĩa một chính sách bảo mật, chính sách bảo mật lần lượt định nghĩa cách thức một Firewall tương tác với thiết lập mạng riêng ảo. Trong chính sách bảo mật, ta cũng sẽ phải quyết định loại luồng lưu lượng nào nên được cho phép đi qua Firewall. Một cách đề xử lý tất các luồng lưu lượng một cách hoàn toàn lúc cấu hình hệ điều hành Firewall là không cho phép tất cả lưu lượng và dịch vụ, sau đó xử lý để cho phép các lưu lượng và dịch vụ được yêu cầu cho đến khi xây dựng xong toàn bộ các luật.

- Nếu đang lập kế hoạch để tạo một vùng DMZ(vùng mạng bảo vệ vành đai), đầu tiên ta sẽ cần quyết định những Server nào sẽ là một phần của vùng này. Một qui tắc để xác định là các Server chỉ đưa ra các dịch vụ mạng riêng ảo cần thiết nên là một phần của vùng này.

- Mặc dù một cách hiệu qua và không mất chi phí lớn của việc bảo mật Intranet và thiết lập mạng riêng ảo là xây dựng một kiến trúc bảo mật phân cấp dựa trên firewall sử dụng các kiểu Firewall khác nhau, như minh hoạ trong hình 5.2. Ví dụ, Firewall giữa Internet và DMZ có thể là một loại và Firewall giữa DMZ và Intranet có thể là một loại khác. Điều này sẽ giảm khả năng khai thác các điểm yếu giống nhau trong hệ thống Firewall ngoại vi để giành được quyền truy cập các tài nguyên mạng Intranet



Hình 5.2 Hệ thống Firewal phân cấp

Bằng việc cấu hình các Firewall để ghi nhật ký mọi yêu cầu kết nối và hoạt động xẩy ra qua các Firewall, và bằng cách phân tích đều đặn các dữ liệu này, ta có thể xác định các điểm yếu trong hệ thống Firewall và đưa ra các bước phù hợp

5.1.4.3. Các xem xét liên quan đến NAT

Luôn có hai vấn đề chính cần xem xét lúc thực thi giải pháp dựa trên NAT trong một môi trường mạng riêng ảo. Đó là

- Mặc dù NAT có thể hoạt động tự do trên PPTP, xem xét các NAT quan trọng nhất do bởi trong trường hợp các giao dịch dựa trên IPSec. Với công nghệ, các địa chỉ IP tầng 3 phải được thay đổi. Ngược lại. IPSec mã hoá và/hoặc đóng gói các địa chỉ IP tầng 3 của một gói với các địa chỉ mạng khác. Kết quả là, số hiệu cổng UDP được mã hoá và giá trị của nó được bảo vệ với một FCS mật mã. Điều này làm cho luồng lưu lượng IPSec không được dịch chuyển bởi các NAT vè NAT không có khả năng làm việc trên gói sau khi dữ liệu sau khi gói dữ liệu đi qua các xử lý định đường hầm mạng riêng ảo L2TP dựa trên IPSec hoặc IPSec. Hơn thế nữa, trong trường hợp xác thực IPSec đầu cuối tới đầu cuối, một gói có địa chỉ bị thay đổi sẽ luôn xẩy ra lỗi kiểm tra tính toàn vẹn. Cho nên, NAT có thể phá vỡ một đường hầm dựa trên IPSec, vì Server VPN sẽ luôn loại bỏ các gói dữ liệu. Vì vậy, nên tránh sử dụng NAT nếu đang có kế hoạch thực thi mã hoá và xác thực IPSec.

- NAT không xử lý dịch chuyển các địa chỉ IP tương ứng với các giao thức tầng ứng dụng. Vì vậy, không thể thực thi một giải pháp dựa trên NAT chuẩn. Ta sẽ phải tìm một NAT cao cấp để sử lý tình huống này

5.1.4.4. Các xem xét liên quan đến Client và Server mạng riêng ảo

Các Client và Server mạng riêng ảo là các điểm cuối của một thiết lập mạng riêng ảo đầy đủ. Trong khi Server mạng riêng ảo cung cấp các dịch vụ liên quan đến mạng riêng ảo, thì các Client sử dụng các dịch vụ này. Kết quả là, một số lượng đáng kể rơi vào lựa chọn của các Client và Server mạng riêng ảo.

Các xem xét chính liên quan tới các Server mạng riêng ảo bao gồm:

- Server mạng riêng ảo phải có hiệu suất cao

- Server chỉ chạy các dịch vụ cần thiết

- Server phải có khả năng kết nối tới được và có khả năng xử lý để xác thực các Client mạng riêng ảo. Ta phải sử dụng các địa chỉ IP tĩnh cho chức năng đó. Nếu Server được cấp phát một địa chỉ riêng, bộ dịch chuyển địa chỉ mạng được yêu cầu và như vậy Server có thể truy cập được bởi các Host ở bên ngoài, đặc biệt nếu mạng Intranet cũng hỗ trợ Extranet.

- Nếu NAT đang được sử dụng, nó phải được thực thi tại Server VPN để tránh các xung đột giữa NAT và VPN

- Nếu Server VPN được kết nối trực tiếp với Internet và Firewall được đặt sau Server VPN (giữa Server VPN và Intranet), ta phải cấu hình Server chỉ cháp nhận luồng lưu lượng VPN và loại bỏ các gói dữ liệu không VPN. Tuy nhiên, nếu Server VPN nằm sau Firewall, cả Server cũng nhưu Firewall phải được cấu hình để chỉ chấp nhận các gói dữ liệu liên quan đến VPN.

Còn khi lựa chọn và thực thi các Client VPN, ta phải xem xét các vấn đề sau:

- Nên chọn lựa việc cấu hình thủ công các Client VPN chỉ nếu số lượng Client là giới hạn. Nếu thiết lập mạng riêng ảo hỗ trợ một số lượng lớn các Client, ta sẽ phải tìm kiếm các công cụ có thể giúp cấu hình các máy Client này. Ví dụ, nếu số lượng Client lớn, ta có thể xem xét sử dụng trình quản lý kết nối Microsoft trong môi trường mạng riêng ảo dựa trên Microsoft.

- Nên chọn các Client VPN sau khi phân tích và hiểu rõ các yêu cầu của tổ chức. Điều này là quan trọng bởi vì, mặc dù ta có thể có một thiết lập đầy đủ và

hiệu suất cao, một Client hiệu suất thấp có thể trở thành chỗ dễ bị tắc nghẽn khi nó không có khả năng duy trì với tốc độ nhanh của các giao dịch.

5.1.5. Hiệu suất thực thi

Hiệu suất của một mạng riêng ảo phần lớn phụ thuộc vào các Server VPN và hạ tầng mạng. Với ý nghĩ này, điều quan trọng là phải biết một số qui định trách nhiệm mà việc tối ưu hiệu suất đòi hỏi:

- Nên xem trước hiệu suất của các Server VPN một cách đều đặn, điều này sẽ giúp chúng ta định danh bất kỳ sự giảm sút nào về hiệu suất của các Server

- Duy trì nhật ký hệ thống một cách chi tiết của mỗi và mọi hoạt động liên quan đến mạng riêng ảo là điều hợp lý, ta nên chuyển định kỳ các file nhật ký này tới một máy riêng và như vậy lúc một kẻ xâm nhập chiến được quyền truy cập tới bất kỳ Server VPN nào, anh ta không thể sửa đổi file nhật ký để tránh bị phát hiện sớm.

- Nên giám sát toàn bộ hiệu suất mạng trên cơ sở quy tắc. Điều này giúp ta định danh các tắc nghẽn có thể xẩy ra và sẽ giúp ta xác định thiết lập mạng riêng ảo của ta có thể hỗ trợ bao nhiêu người dùng trước khi những người dùng này bắt đầu cảm thấy hiệu suất bị giảm sút.

- Các thuật toán mật mã, các lược đồ xác thực có thể phát sinh overhead đáng kể, và như vậy làm chậm hoạt động thông thường cùng với các hoạt động mạng riêng ảo. Ta có thể tăng hiệu suất của toàn mạng bằng cách phân tích kỹ lưỡng những ưu và nhược điểm của các thuật toán có thể thực thi, cân bằng giữa hiệu suất và bảo mật

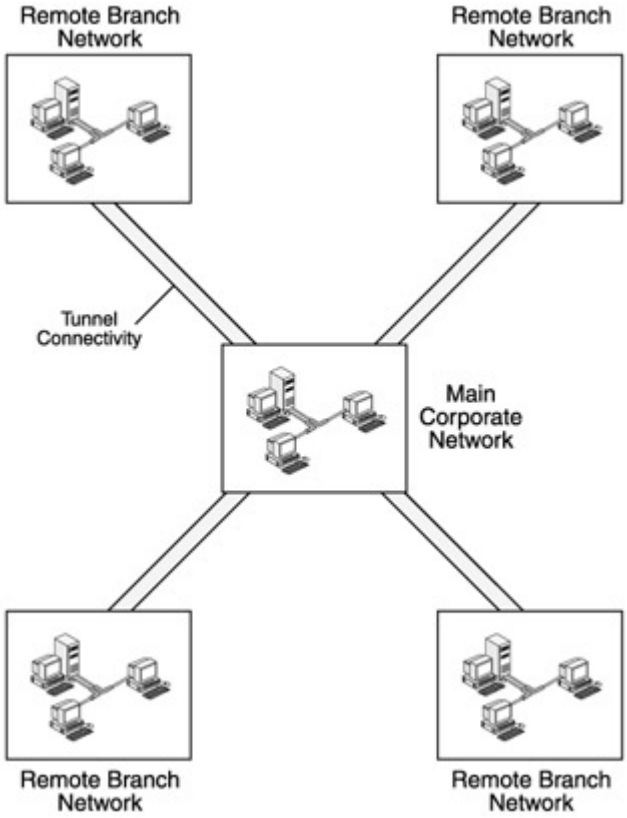
- Các Client VPN là khía cạnh khác của hiệu suất mạng riêng ảo. Cần kiểm soát các Client VPN được đặt trong Intranet và báo cho các Client di động từ xa trên đó phần mềm Client và hệ điều hành dùng để các giao dịch giữa người dùng cuối và các Server VPN không bị cản trở bởi hiệu suất thấp của các Client VPN

5.1.6. Khả năng mở rộng và liên tác

Giống như bất kỳ thiết lập mạng nào, một mạng riêng ảo phải có khả năng thích ứng với bất kỳ sự thay đổi nào trong tương lai do các yêu cầu và sự phát triển

của một tổ chức. Điều này đặc biệt đúng trong trường hợp các mạng riêng ảo thương mại gồm nhiều nhánh mạng. Bản thiết kế của ta sẽ xác định phạm vi của sự phát triển tương lai cũng như số lượng kết nối có thể được hỗ trợ bởi mạng riêng ảo hiện thời và tổng chi phí thực thi. Và như vậy, ta nên lựa chọn bản thiết kế mạng riêng ảo cẩn thận trước khi đi đến pha thực thi

Trong hầu hết các trường hợp, thiết lập thương mại được bao gồm một sự cấu hình tập trung hoá, nơi mạng chính của tổ chức hoạt động như một "Hub" của tất các các nhánh từ xa. Trong cấu hình này, mỗi nhánh mạng từ xa được kết nối với nhánh mạng chính qua một kết nối mạng riêng ảo, như trong hình 5.3

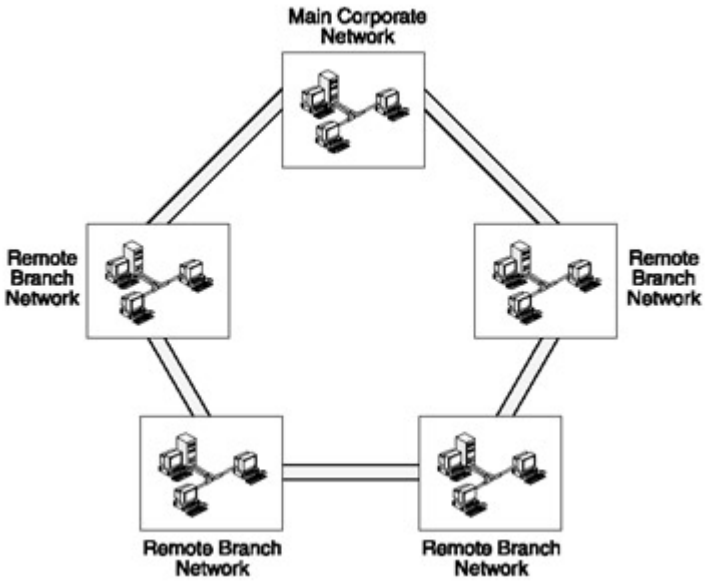


Hình 5.3 Mỗi nhánh mạng từ xa kết nới tới mạng trung tâm qua một mạng riêng ảo

Cấu hình được mô tả như trong hình 5.3 có khả năng mở rộng rất cao và dễ dàng thích ứng với các kết nối mạng riêng ảo từ bất kỳ nhánh mạng từ xa mới nào mà không gặp phải nhiều vấn đề và ảnh hưởng đến các nhánh khác. Chỉ cần sửa đổi tại mạng trung tâm. Vấn đề lớn gắn liền với mô hình này là nếu mạng trung tâm bị down, thì tất cả các kết nối cũng bị down. Ngoài ra, tất cả truyền thông được

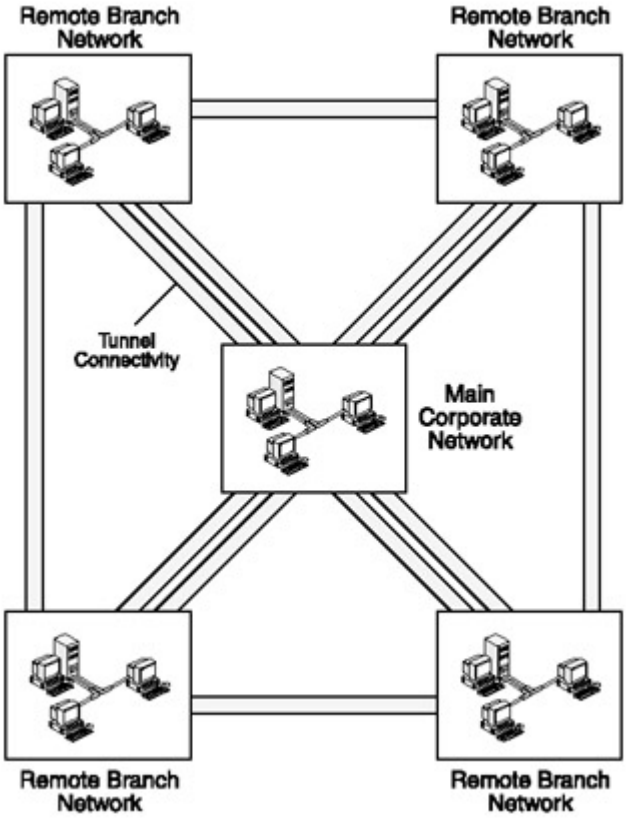
định tuyến qua mạng trung tâm, làm tăng overhead cho lưu lượng tại vị trí trung tâm. Thêm vào đó, một sự giảm hiệu suất của mạng trung tâm có thể ảnh hưởng tiêu cực tới hiệu suất của tất cả các nhánh mạng khác, làm giảm hiệu suất của toàn mạng

Cấu hình có thể khác là một cấu hình tương tự dạng vòng, trong đó mỗi nhánh mạng từ xa được kết nối tới trực tiếp với nhánh mạng kế cận nó. Cấu hình này được mô tả như trong hình 5.4. Đây là cấu hình chỉ có khả năng mở rộng ở một mức độ nhất định nếu số lượng nhánh mạng trong vòng quá lớn, hiệu suất của toàn mạng Intranet bị giảm sút một cách đáng kể.



Hình 5.4 Mỗi một nhánh mạng kết nối tới nhánh Intranet kế cận qua mạng riêng ảo

Một sự lựa chọn khác với cấu hình mạng riêng ảo tập trung là cấu hình tương tự mạng lưới, trong đó mỗi nhánh mạng được kết nối tới tất các các mạng từ xa khác. Hình 5.5 mô tả mô hình cấu hình này. Thiết lập này, dù dắt và khó để cài đặt và duy trì, nhưng tránh vấn đề "điểm đơn bị lỗi" và đảm bảo rằng một mạng không thể ảnh hưởng đến hiệu suất của các mạng được kết nối khác. Hơn nữa, mặc dù khả năng mởi rộng rất cao, thực tế việc thực thi mở rộng là khác khó khăn và tốn nhiều thời gian



Hình 5.5 Mỗi nhánh từ xa được kết nối với tất cả nhánh khác trong một Intranet qua một mạng riêng ảo.

Khả năng liên tác là một vấn đề quan trọng khác cần lưu ý lúc lựa chọn các phần từ của mạng riêng ảo, đặc biệt việc xem xét rằng những người quản trị hướng tới các sản phẩm thích hợp và tích hợp được đề xuất bởi những nhà cung cấp khác nhau để giảm tổng chi phí thực thi. Những sản phẩm được đề xuất bởi các nhà cung cấp khác có thể không liên tác bằng, vì vậy ta nên kiểm tra tính tương thích và liên tác của tất cả các sản phẩm mạng riêng ảo trước khi thực thi chúng trong mạng riêng ảo của chúng ta.

Một điểm khác là ta nên nhớ với việc quan tâm đến tính liên tác đó là sản phẩm VPN mà ta chọn phải làm việc suôn sẻ với nhiều nền khác nhau. Dù điều này có thể có vẻ như một sự lãng phí tiền bạc tại thời điểm này, đặc biệt nếu mạng Intranet của ta sử dụng chỉ với một số Platform, nhưng chiến lược này sẽ có ích cho ta lúc mở rộng và phát triển mạng riêng ảo.

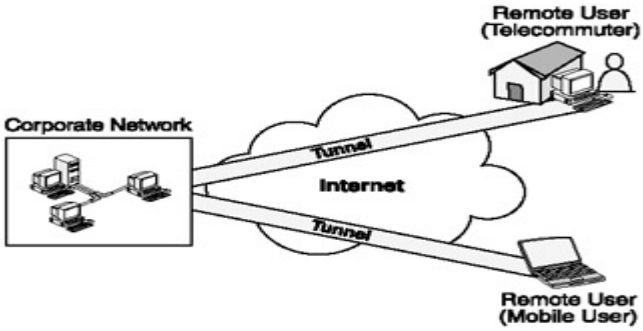
Ta phải có một ý tưởng tổng quát trong việc xem xét khi thiết kế một giải pháp mạng riêng ảo, có thể xem xét ba môi trường thực thi mạng riêng ảo thông dụng nhất và các đặc tính của chúng

5.2 Các môi trường mạng riêng ảo riêng lẻ

Như trong chương I "Tổng quan về mạng riêng ảo" đã giới thiệu, tùy thuộc vào chiến lược truy cập, mạng riêng ảo có thể được phân thành các loại như: Mạng riêng ảo truy cập từ xa, Mạng riêng ảo cục bộ, và Mạng riêng ảo mở rộng. Xem xét mỗi môi trường truy cập mạng riêng ảo này là điều kiện tốt để hiểu rõ các vấn đề mà ta phải đối mặt với mỗi môi trường.

5.2.1. Mạng riêng ảo truy cập từ xa

Môi trường mạng riêng ảo truy cập từ xa cho phép các Client từ xa, như các Client hay người dùng di động có thể truy cập tới mạng Intranet của công ty một cách an toàn qua mạng Internet mà không phải dựa trên các kế nối quay số đầu cuối - đến - đầu cuối, như minh hoạ trong hình 5.6



Các vấn đề có thể nảy sinh với môi trường này như sau:

- Bảo mật: Tốt nhất là cài đặt bộ định tuyến "sau" Firewall và cấu hình các Router chuyển tất cả dữ liệu đường hầm tới Firewall

- Lược đồ đánh địa chỉ: ISP cấp phát động các địa chỉ IP tới các Client từ xa này vì chúng sử dụng một kết nối quay số tới POP của ISP(không phải đến Intranet). Kết quả là, máy chủ mạng riêng ảo đặt trong mạng Intranet phải hỗ trợ khả năng định danh các Client này. Hơn nữa việc thiết lập máy chủ DNS như đã thảo luận trong phần trước "Các xem xét liên quan đến DNS", ta có thể giải quyết vấn đề này bằng các sử dụng IPSec. IKE, là một giao thức bến thứ ba được hỗ trợ

bởi IPSec, hỗ trợ khả năng định danh các Client từ xa qua các địa chỉ IP dưới dạng tên của chúng hơn là các địa chỉ IP dưới dạng số

- Phân phối khoá: Phân phối khoá không bao giờ nên xẩy ra ở dạng bản rõ. Một cơ chế phân phối khoá tự điều chỉnh, như IKE nên được sử dụng nếu số lượng Client từ xa lớn. Trong trường hợp số lượng Client từ xa giới hạn, quản lý khoá một cách thủ công cũng có thể thực hiện được. Tuy nhiên, thực tế việc quản lý khoá một cách thủ công không được khuyến cáo vì xác suất xẩy ra việc mật khoá là khá cao.

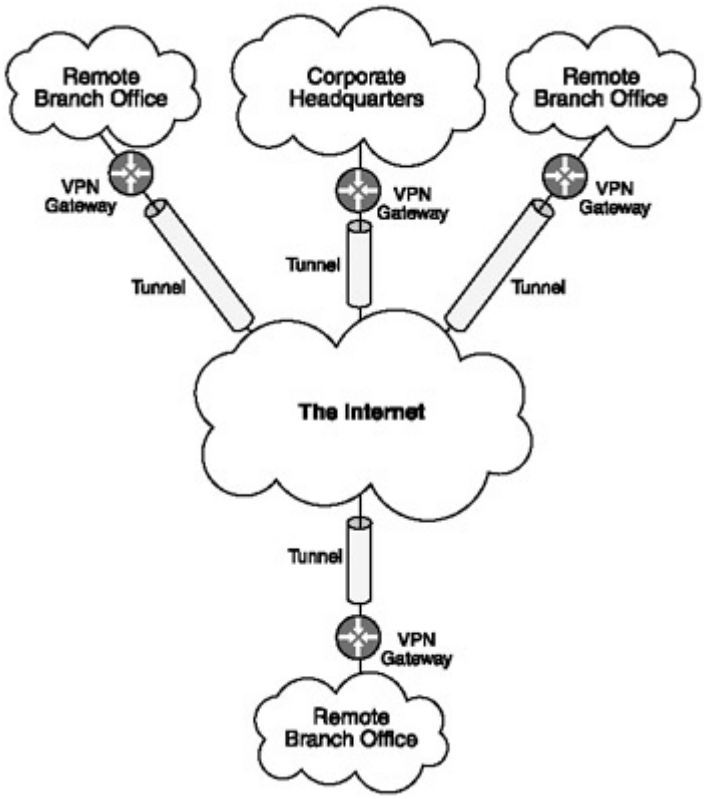
- Mã hoá và xác thực dữ liệu: Đây là điều rất quan trọng, dữ liệu được trao đổi giữa Server và Client được mã hoã cũng như được xác thực. Thêm vào đó, ta nên thiết lập các bộ lọc gói và chính sách bảo mật nghiêm ngặt để đảm bảo rằng các thiết bị ngoại vi như Router, Gateway hoặc Firewall sẽ từ chối dữ liệu không được xác thực hoặc không được mã hoá. Thậm chí, thông tin định tuyến giữa các Router và Gatewal cũng nên được mã hoá và xác thực

- Đường hầm: Thiết lập trực tiếp các đường hầm giữa các Host từ xa và máy chủ mạng riêng ảo là thích hợp. Dù điều này làm tăng tính an toàn, đặc biệt nếu mức độ tin cậy trong mạng Intranet khong cao, nhưng nó thường phát sinh các Overhead lớn và tương đối khó quản lý. Ta sẽ phải phân tích mức độ trinh cậy trong môi trường Intranet và sau đó quyết định giữa 2 tuỳ chọn(Các đường hầm giữa người dùng cuối với thiết bị ngoại vi, hoặc đường hầm giữa người dùng cuối với máy chủ mạng riêng ảo) để duy trì một mức an toàn cao

- Các giao thức đường hầm: Nếu các Client sử dụng các giao thức đường hầm không IP, các thiết bị mạng riêng ảo ngoại vi như Firewall và Router phải hỗ trợ các giao thức đường hầm thích hợp

5.2.2. Mạng riêng ảo cục bộ

Môi trường mạng riêng ảo cục bộ cho phép các nhánh mạng từ xa truy cập các phần khác trong mạng Intranet của tổ chức một cách an toàn qua mạng Internet mà không dựa trên các kênh thuê riêng và các kết nối quay số đầu cuối - tới - đầu cuối. như trong hình 5.7



Hình 5.7 Thiết lập mạng riêng ảo cục bộ

Những vấn đề nên được xem xét trong khi thiết kế một giải pháp mạng riêng ảo cho môi trường mạng riêng ảo cục bộ bao gồm:

- Bảo mật: Mặc dù các giao thực không bảo mật cần được thực thì trên các Router và Gateway bên trong, các thiết bị ngoại vi nên hỗ trợ một cơ chế bảo mật, chẳng hạn như IPSec. Hơn nữa, tốt nhất là, các thiết bị ngoại này nên được che dấu "sau" Firewall với các chính sách bảo mật được định nghĩa rõ ràng

- Lược đồ đánh địa chỉ: Vì thực tế là toàn bộ Intranet thuộc một tổ chức, đánh địa chỉ, việc đánh địa chỉ không phải là vấn đề vì các nhánh mạng từ xa kèm theo lược đồ đánh địa chỉ phong phú được sử dụng trong các phần khác của Intranet. Và như vậy, lược đồ đánh địa chỉ được dùng trong phần còn lại của Intranet có thể được sử dụng, miễn là tất các các địa chỉ trong Intranet là duy nhất. Do vậy, vấn đề đánh địa chỉ ít khi gặp trục trặc trong môi trường này.

- Phân phối khoá: Vì một mạng Intranet được tin cậy rộng rãi, phân phối khoá host t – to – host không phải là một nhu cầu chính. Tuy nhiên, các khoá sẽ được

trao đổi giữa các điểm dễ bị tấn công trong mô hình thiết lập này, cụ thể là các thiết bị ngoại vi như Router, Gateway. Với mục đích này, một cơ chế quản lý và trao đổi khoá một cách tự động và an toàn, chẳng hạn như IKE được khuyến cáo sử dụng

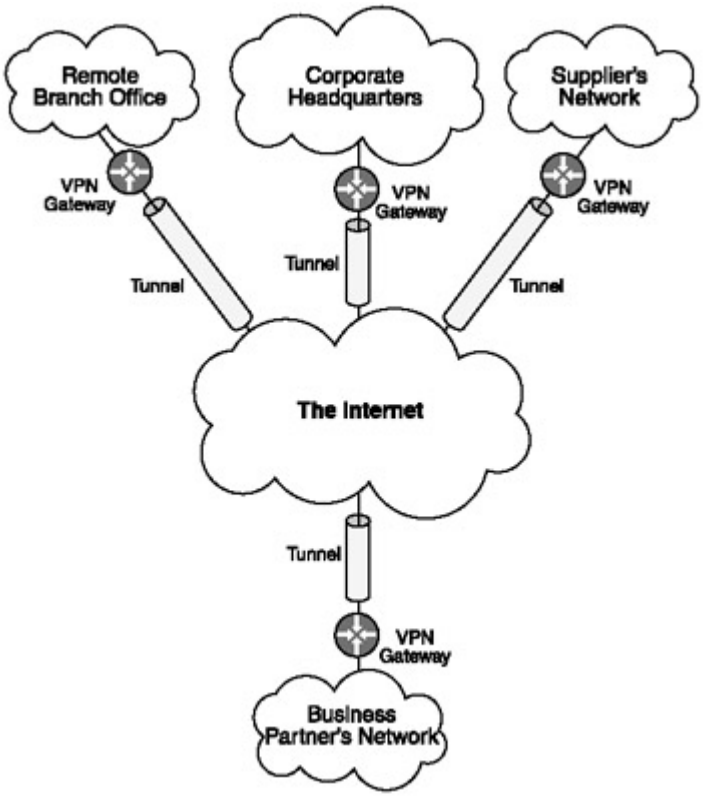
- Mã hoá và xác thực dữ liệu: Bất kỳ dữ liệu nào được trao đổi giữa Server và Client phải được mã hoã cũng như được xác thực. Mặc dù thực tế là chúng thuộc cùng mạng Intranet – nhưng vì dữ liệu được định tuyến qua Internet hoặc các mạng công cộng khác dễ bị tổn thương với các nguy cơ bảo mật và sự sai lệch. Khá giống với các chính sách bảo mật được dùng trong môi trường truy cập từ xa, nên thiết lập bộ lọc gói và ban hành các tiêu chuẩn nghiêm ngặt để đảm bảo rằng dữ liệu không được mã hoá hoặc xác thức sẽ bị loại bỏ tại vành đai mạng bởi các thiết bị ngoại vi. Thậm chí thông tin định tuyến trao đổi giữa các Router cũng nên được mã hoá và xác thực

- Đường hầm: Thiết lập các đường hầm trực tiếp giữa các thiết bị ngoại vi đặt tại mỗi nhánh mạng là điều thích hợp. Mặc dù thực tế là chúng nâng cao tính bảo mật, đặc biệt nếu mức độ tin cậy trong môi trường Intranet không cao, nhưng nó phát sinh một khối Overhead lớn và tương đối khó khăn trong việc quản lý. Nên phân tích mức độ tin cậy trong Intranet và sau đó quyết định giữa 2 tuỳ chọn như trong trường hợp của môi trường mạng riêng ảo truy cập từ xa để duy trì một mức độ an toàn cao

- Các giao thức đường hầm: Nếu các Client Clien sử dụng giao thức đường hầm không IP, các thiết bị VPN ngoại vi như Firewall và Router phải hỗ trợ các giao thức đường hầm thích hợp

5.2.3. Mạng riêng ảo mở rộng

Môi trường mạng riêng ảo mở trộng cho phép các thực thể mở rộng, như đối tác thương mại, nhà cung cấp có thể truy cập tới mạng Intranet của tổ chức một cách an toàn sử dụng Internet mà không phải dựa trên các kênh thuê riêng và các kết nối quay số, như minh hoạ trong hình 5.8



Hình 5.8 Thiết lập mạng riêng ảo mở rộng

Các xem xét thiết kế mà ta phải lưu ý khi thiết kế một giải pháp mạng riêng ảo cho môi trường này là:

- Bảo mật: Các phương tiện và giao thức bảo mật nghiêm ngặt cần được thực thi tại các Router, Gateway và Firewall ngoại vi. Hơn nữa, các thiết bị ngoại vi này nên được ẩn dấu sau firewall với các chính sách bảo mật được định nghĩa rõ ràng

- Lược đồ đánh địa chỉ và định tuyến: Trong môi trường này, ta không thể mong đợi các mạng mở không bị trục trặc. Nếu hai mạng sử dụng một lược đồ địa chỉ riêng, khả năng xung đột địa chỉ xẩy ra là rất cao. Điều này có thể dẫn đến vấn đề định tuyến khi Router và Gateway sẽ không có khả năng giải quyết các địa chỉ nhập nhằng này. Kết quả là, ta cần phải đảm bảo rằng

- Phân phối khoá: Vì một thiết lập mở rộng khá phức tạp và bao gồm cả đến các thực thể mở rông không tin cậy, thêm vào đó một số lượng lớn các Client và liên lạc, một cơ chế quản lý và phân phối khoá an toàn và tự động như IKE hoặc

ISAKMP/Oakley là bắt buộc với tất các các nhóm – Server, Client, Router, Gateway, Firewall…

- Mã hoá và xác thực dữ liệu: Bất kỳ dữ liệu nào được trao đổi giữa Server và Client phải được mã hoá đầu cuối - tới - đầu cuối cũng như xác thực một cách triệt để. Điều này là cần thiết vì dữ liệu có thể từ một môi trường không tin cậy và đã được định tuyến qua Internet hay các mạng công cộng khác, cho nên rất dễ gặp phải các nguy cơ bảo mật và sự sai lệch. Giống như chính sách bảo mạt được dùng trong môi trường truy cập từ xa và môi trường cục bộ, ta nên thiết lập các bộ lọc gói và thông qua các phương tiện nghiêm ngặt để đảm bảo rằng dữ liệu không được xác thực cũng như không được mã hoá sẽ bị loại bỏ tại vành đai mạng bởi các thiết bị ngoại vi. Thậm chí thông tin định tuyến giữa các Router cũng nen được mã hoá và xác thực.

- Đường hầm: Thiết lập các đường hầm trực tiếp giữa các thiết bị ngoại vi đặt tại mỗi mạng cuối là điều thích hợp. Mặc dù thực tế điều này nâng cao tính an toàn, đặc biệt nếu mức độ tin cậy trong mạng Intranet là không cao, nhưng nó phát sinh các Overhead lớn và tương đối khó quan lý. Ta sẽ phải phân tích mức độ tin cậy trong môi trường Intranet và sau đó quyết định giữa 2 tuỳ chọn(Các đường hầm giữa người dùng cuối với thiết bị ngoại vi, hoặc đường hầm giữa người dùng cuối với máy chủ mạng riêng ảo) để duy trì một mức an toàn cao.

- Các giao thức đường hầm: Nếu các Client từ xa sử dụng các giao thức đường hầm không IP, các thiết bị mạng riêng ảo ngoại vi, như Firewall và Router phải hỗ trợ các giao thức đường hầm thích hợp, các giao thức đường hầm với các cơ chế bảo mật mạnh thêm vào

Trong phần sau, ta sẽ xem xét các bước thông thường để thực thi mạng riêng ảo

5.3. Các bước chung để xây dựng mạng riêng ảo

Khi ta đã chú ý về bất kỳ công nghệ nào, một khi ta đã thực thi và bắt đầu sử dụng nó, thì nó trở thành một phần công việc của ta. Điều này cũng đúng với các mạng riêng ảo. Một khi đã thực thi, thậm chí trước khi ta thực hiện, mạng riêng ảo

trở thành một phần không thể thiếu của hoạt động giao dịch hằng ngày. Và như vậy, nếu có bất kỳ sai sót nào trong pha thực thi hay lập kế hoạch không chặt chẽ, những người dùng và tổ chức của ta sẽ chịu hậu quả, dẫn đến nhiều công việc phức tạp và mất nhiều thời gian.

Điều này lý giải tại sao ta phải thực sự hiểu các yêu cầu và các kế hoạch tương lai của tổ chức trước khi bắt đầu lập kế hoạch. Chỉ sau khi kế hoạch và tiếp đó là bản thiết kế phù hợp, nên chia thành các pha thực thi

Việc thực thi đầy đủ một giải pháp dựa trên mạng riêng ảo có thể khái quá thành năm bước sau:

- Chuẩn bị cơ sở
- Lựa chọn các sản phẩm và một nhà cung cấp dịch vụ
- Kiểm thử kết quả
- Thiết kế và thực thi giải pháp
- Quản trị và giám sát

Sau đây ta sẽ thảo luận chi tiết các bước này

5.3.1. Chuẩn bị cơ sở

Thực thi một giải pháp dựa trên mạng riêng ảo có thể làm giảm không đáng kể hiệu suất của mạng Intranet. Và như vậy, điều quan trọng là ta phải nghiên cứu đầy đủ các khả năng để chọn lựa các dịch vụ và sản phẩm tối ưu. Hơn nữa, phần cơ sở được làm càng tỉ mĩ, sự hoàn vốn đầu tư càng tối ưu.

Ta cần xác định các thông tin sau như một phần của pha nghiên cứu và phân tích này:

- Một ước lượng sơ bộ về số lượng người dùng: Cần có một ước lượng sơ bộ về số lượng người dùng mong muốn để xác định phạm vi của giải pháp mạng riêng ảo và các dịch vụ. Số lượng này cũng sẽ giúp ta quyết định số lượng các cổng mạng riêng ảo tối ưu mà ta nên có.

- Phân loại người dùng tuỳ theo yêu cầu của họ: Ta sẽ cần phải nghiên cứu hồ sơ của người dùng một cách thấu đáo để xác định các yêu cầu của họ và phân loại vào các nhóm khác nhau bao gồm nhóm người dùng thuộc chi nhánh văn phòng, nhóm người dùng di động, nhóm nhân viên làm việc tại nhà. Những người dùng thuộc nhóm chi nhánh văn phòng thường không di động và yêu cầu truy cập không bị giới hạn tới mạng của văn phòng trung tâm và các nhánh mạng khác trong Intranet. Nhóm người dùng di động là một tập người dùng với các hồ sơ luôn di chuyển, họ thường sử dụng một máy xách tay để truy cập Intranet của tổ chức. Điển hình là họ sử dụng kết nối mạng riêng ảo để truy cập email và một số các tài nguyên cần thiết khác. Nhóm nhân viên làm việc tại nhà truy cập Intranet của tổ chức với thời gian ngắn và các tài nguyên giới hạn

- Các yêu cầu truy cập và kết nối: Bước tiếp theo là xác định các yêu cầu kết nối và truy cập mạng của mỗi loại người dùng VPN. Ta cần xác định kiểu kết nối mạng WAN có thể được cung cấp theo ngân quỹ của ta và các ràng buộc hiệu suất của nó. Ta cũng cần xác định tốc độ dữ liệu trung bình được yêu cầu cho những loại kết nối và những người dùng khác nhau

- Các yêu cầu an toàn: An toàn trong một thiết lập dựa trên màng riêng ảo đòi hỏi tính bí mật, toàn vẹn và xác thực. Để đảm bảo tất cả những yếu tố này trong các giao dịch mạng riêng ảo của ta, cần phải thực thi các phương tiện an toàn khác nhau, chẳng hạn như các cơ chế mã hoá, các cơ chế xác thực và cả các giải pháp an toàn dựa trên phần cứng như RADIUS, AAA, TACACS, Firewall, NAT,… Ta không thể chọn tuỳ tiện bất kỳ một phương tiện nào trong số trên, mà cần phân tích các yêu cầu của tổ chức để hiểu giải pháp nào nên được thực thi. Sự lựa chọn giải pháp bảo mật thích hợp cũng tuỳ thuộc vào mức bảo mật và toàn vẹn được yêu cầu bởi luồng lưu lượng mạng. Ví dụ, nếu tổ chức đề cập đến dữ liệu nhạy cảm trong giao dịch thương mại điện tử, ta sẽ cần thực thi một hoặc nhiều giải pháp an toàn để đảm bảo tính bí mật, toàn vẹn và xác thực thích hợp của dữ liệu

5.3.2. Lựa chọn các sản phẩm và nhà cung cấp dịch vụ

Sau khi ta đã phân tích và hiểu rõ các yêu cầu của tổ chức và những mong muốn của người dùng, lúc này ta tiến hành chọn lựa các sản phẩm để thực thi mạng riêng ảo. Việc này không phải dễ dàng đưa ra quyết định vì có nhiều sản phẩm phần cứng và phần mềm mạng riêng ảo hiện có. Xem xét các ràng buộc về ngân sách, phương pháp tốt nhất để chọn các sản phẩm là đáp ứng các yêu cầu của ta và khả năng tài chính.

Một số tham số sẽ giúp ta chọn lựa các sản phẩm phần cứng cũng như phần mềm thích hợp cho mạng riêng ảo là:

- Các tham số liên quan đến hiệu suất, như thông lượng được duy trì liên tục mức cao nhất và thời gian phản hồi thấp nhất

- Các tham số liên quan đến an toàn, như các cơ chế mã hoá và xác thực được hỗ trợ

- Các tham số liên quan đến phiên làm việc, như tốc độ tuyền dữ liệu cao nhất

- Số lượng kết nối đồng thời được hỗ trợ

Chú ý Ta phải cẩn thận trong khi lựa chọn các cơ chế mã hoá và xác thực. Mặc dù chúng nâng cao tính an toàn, nhưng chúng cần nhiều CPU để tính toán và như vậy có thể làm giảm hiệu suất toàn phần của mạng. Kết quả là, nên dung hoà giữa tính an toàn và hiệu suất.

Vì ta vẫn còn chưa xong pha thực thi, đây là điểm mà trong đó ta có thể quyết định giải pháp tận dụng dựa trên các phân tích sản phẩm và cơ sở của ta. Nhà cung cấp dịch vụ sẽ có yêu cầu về khả năng kỹ thuật và kinh nghiệm được yêu để thiết kế và thực thi một giải pháp mạng riêng ảo thích ứng với các yêu cầu của tổ chức. Hơn nữa, giải pháp tận dụng cũng sẽ dẫn đến gánh nặng trong việc quản lý và giám sát lên vay chúng ta. Tuy nhiên, hạn chế ở đây là việc xử lý an toàn của tổ chức qua một tổ chức bên ngoài (người ngoài cuộc). Điều này không thể chấp nhận được với các tổ chức và người quản trị. Vì vậy, ta nên phân tích chi tiết SLA mà nhà cung cấp dịch vụ đem lại cho ta. Một sự hiểu biết sâu sắc mỗi điểm trong SLA cũng sẽ giúp ta xác minh rằng nhà cung cấp dịch vụ đang cung cấp mức dịch vụ đúng như trong SLA

5.3.3. Kiểm thử kết quả

Nếu quyết định được áp dụng thực thi trong một nhóm của thiết lập mạng riêng ảo, ta sẽ cần kiểm tra và đánh giá mỗi sản phẩm mạng riêng ảo mà ta đã chọn. Điều này sẽ giúp ta đảm bảo tính đúng đắn trước khi bắt đầu lựa chọn các sản phẩm phần cứng và phần mềm tương thích với mỗi sản phẩm khác.

Thông thường, việc kiểm thử được thực hiện với một phạm vi nhỏ thí điểm có kết hợp nhiều nhóm người dùng khác nhau. Mỗi khía cạnh của mạng riêng ảo nên được kiểm thử và ta nên xem cách mỗi sản phẩm sẽ hoạt động trong môi trường thực. Thí nghiệm này cũng đảm bảo rằng các sản phẩm được cấu hình đúng và được thự thi trên các đặc tính kỹ thuật

Nếu ta đã quyết định sử dụng các dịch vụ của nhà cung cấp, một thí nghiệm nhỏ để kiểm thử và xác minh giải pháp đưa ra bởi nhà cung cấp dịch vụ trong môi trường thực được khuyến cáo.

Nếu thí nghiệm xẩy ra lỗi, ta sẽ cần thay thế các sản phẩm không đáp ứng đầy đủ các yêu cầu hoặc cấu hình lại chúng.

5.3.4. Thiết kế và thực thi giải pháp

Ta hoàn tất để sang pha thiết kế và thực thi chỉ sau khi pha kiểm thử thành công. Trong pha thiết kế và thực thi, ta sẽ thực thi giải pháp mạng riêng ảo mềm dẻo theo kế hoạch của tổ chức

Sau khi giải pháp đã được thực thi thành công, ta cần kiểm thử lại toàn bộ thiết lập. Sau khi kiểm thử thành công, ta cũng có thể cần tinh chỉnh giải pháp để tối ưu hoá tính an toàn và hiệu suất của nó

5.3.5. Giám sát và quản trị

Việc quản lý và duy trì mạng là một quá trình liên tục. Đến giám sát một thiết lập mạng riêng ảo phạm vi lớn là rất phức tạp. Vì vậy cần vạch ra một chiến lược để quản lý và giám sát mạng của ta

Những thói quen sau sẽ giúp ta đảm bảo rằng mạng riêng ảo luôn tối ưu

- Thu thập cách sử dụng và thống kê hiệu suất đều đặn

- Duy trì file nhật ký chi tiết mỗi hành động liên quan đến mạng riêng ảo, kể cả các hành động thành công.

Một sự am hiểu sâu sắc về cách mà nhà cung cấp dịch vụ thực thi giải pháp mạng riêng ảo cung giữ một vai trò quan trọng trong việc giám sát và đánh giá hiệu suất, hiệu quả và tính đầy đủ của giải pháp được cung cấp.

Công nghệ mạng đang phát triển rất nhanh chónh, công nghệ mạng riêng ảo cũng vậy. Vì thế, thỉnh thoảng ta phải cần cập nhật cho thiết lập mạng riêng ảo của ta, ta cũng cần di trú tới các nền và các môi trường khác nhau để thích ứng với sự phát triển trong tương lại của tổ chức cũng như các yêu cầu của tổ chức

Hầu hết những người thiết kế và quản trị mạng sẽ chỉ cho ta, công việc của ta không kết thúc với sự thực thi một giải pháp. Ta cần phải quản lý và giám sát giải pháp, và như vậy nó cung cấp hiệu suất như hợp đồng. Thi thoảng, ta cũng cần định danh, hỗ trợ và giải quyết bất kỳ vấn đề nào có thể nảy sinh

Tổng kết

Trong chương này, chúng ta đã xem xét các vấn đề khác nhau cần phải lưu ý lúc thiết kế một giải pháp dựa trên mạng riêng ảo cho một tổ chức. Chương này đã nghiên cứu vấn đề thiết kế mạng riêng ảo, như tính an toàn, đánh địa chỉ và định tuyến, hiệu suất, tính mền dẻo và khả năng liên tác.

Các vấn đề khác liên quan đến việc thực thi của các Firewall, NAT, DNS, mức đọ tin cậy trong Intranet và phân phối khoá được đề cập

Ta cũng đã nghiên cứu một cách riêng lẻ mỗi môi trường mạng riêng ảo – Remote access, Intranet và Extranet để hiểu rõ các vấn đề và các khả năng khác nhau mà ta có thể phải lập kế hoạch lúc thực thi mạng riêng ảo trong mỗi môi trường này.

Cuối cùng, ta đã xem xét về 5 bước tổng quát trong việc thực thi một giải pháp bảo mật dựa trên mạng riêng ảo cho mạng Intraneet của một tổ chức. Các bước này bao gồm pha nghiên cứu để xác định yêu cầu của tổ chức và những người dùng cuối của hệ thống, một pha lựa chọn để chọn các sản phẩm và nhà cung cấp dịch vụ, một pha kiểm thử để kiểm tra các sản phẩm và nhà cung cấp

dịch vụ được chọn, một pha thiết kế và thực thi, và một pha giám sát và quản trị để đánh giá hiệu suất và các khía cạnh khác của mạng riêng ảo một cách đều đặn.

Chương VI Xây dựng mạng riêng ảo truy cập từ xa

6.1. Các thành phần trong mạng riêng ảo truy cập từ xa

6.1.1. Giới thiệu chung

Việc triển khai một mạng riêng ảo có nhiều dịch vụ và chức năng cần phải làm việc cùng nhau một cách trôi chảy và dễ dàng, vì vậy những người dùng truy cập từ xa có thể được định danh và xác thực; các được hầm có thể được tạo lập, duy trì và quản lý cho hàng trăm người dùng; việc định tuyến có thể kiểm soát tất cả luồng lưu lượng qua Gateway, và trong khi tất các những thứ này đang tiếp tục, hiệu suất và sự an toàn cần được duy trì. Các thành phầm phải được cài đặt để tạo ra một hệ thống mạng riêng ảo hoạt động đúng đắn. Để đưa ra quyết định đúng lúc triển khai các kết nối mạng riêng ảo truy cập từ xa, ta phải hiểu tất cả các thành phần liên quan. Trong chương "Tổng quan về mạng riêng ảo" chúng ta đã thảo luận về kiểu kịch bản mạng riêng ảo truy cập từ xa, trong đó nhiều Client truy cập tới một cổng kết nối đơn vào các tài nguyên trong mạng Intranet. Trong phần này ta sẽ mô tả các thành phần của các kết nối mạng riêng ảo truy cập từ xa và các quan điểm thiết kế gắn với chúng

Hình 6.1. Các thành phần của một mạng riêng ảo truy cập từ xa

Các thành phần chính là

- Các Client VPN
- Hạ tầng mạng Internet
- Server VPN, và các thiết bị khác như Gateway
- Hạ tầng mạng Intranet
- Máy chủ AAA
- Hạ tầng cấp phát chứng chỉ số

6.1.2. Các thành phần

1. Các Client VPN

Client VPN có thể là một máy tính hoặc thiết bị có khả năng tạo một kết nối PPTP hoặc L2TP

Các Client VPN có nhiều loại, nhiều dạng và nhiều kích cỡ. Một số Client VPN điển hành được sử dụng rộng rãi ngày nay là:

- Người dùng Laptop kết nối tới Intranet của tổ chức đề truy cập email và các tài nguyên khác

- Những người quản trị từ xa sử dụng Internet để kết nối tới mạng của tổ chức để cấu hình mạng hoặc các dịch vụ ứng dụng.

- Nhiều người dùng khác tận dụng ưu điểm về khả năng kỹ thuật của giải pháp truy cập từ xa, chẳng hạn như các giải pháp truy cập mạng không giây, các hệ thống kiểm soát từ xa, các mạng truyền thông

Trong khuôn khổ của giáo trình này, sẽ tập trung vào các Client thông dụng nhất, chẳng hạn như Client sử dụng hệ điều hành WinXP và Windows 2000 Pro của Microsoft.

Các Client VPN có thể cấu hình các kết nối mạng riêng ảo một cách thủ công bằng việc tạo các kết nối trên hệ điều hành, hoặc người quản trị hệ thống có thể đơn giản hoá bằng các công cụ sẵn có trên hệ điều hành.

2. Hạ tầng mạng Internet

Trong các thảo luận của chúng ta về giải pháp truy cập từ xa với mạng riêng ảo, chúng ta sẽ làm việc với các kết nối qua Internet. Điều này có nghĩa là chúng ta dựa vào Internet, nó là mạng trung gian, cung cấp các dịch vụ và phương tiện truyền thông tới người dùng. Để tạo một kết nối mạng riêng ảo tới một máy chủ mạng riêng ảo qua Internet, ta cần kiểm chứng các mục sau trước khi bất kỳ kết nối nào được tạo

- Tên máy chủ mạng riêng ảo phải có khả năng giải quyết: Đảm bảo rằng tên DNS của máy chủ mạng riêng ào khó khả năng xử lý từ Internet bằng việc đặt một bản ghi DNS thích hợp hoặc trên máy chủ DNS Internet hoặc trên máy chủ DNS

của ISP. Kiểm thử khả năng xử lý bằng công cụ Ping để ping tới tên của mỗi máy chủ mạng riêng ảo

- Máy chủ mạng riêng ảo phải có khả năng kết nối tới: Đảm bảo rằng các địa chỉ IP của máy chủ mạng riêng ảo có khả năng kết nối tới từ Internet

- Luồng lưu lượng VPN phải được phép từ máy chủ mạng riêng ảo: Cấu hình bộ lọc gói cho luồng lưu lượng PPTP, L2TP hoặc cả hai kiểu trên các Firewall và giao diện máy chủ mạng riêng ảo thích hợp đang kết nối tới Internet và mạng vành đai

3. Các giao thức xác thực

Để xác thực người dùng, các giao thức xác thực thường được sử dụng là:

- Giao thức xác thực mật khẩu (PAP)

- Giao thức xác có thăm dò trước (CHAP)

- Giao thức xác thực có thăm dò trước của Microsoft (MS-CHAP)

- Giao thức MS-CHAP phiên bản 2 (MS-CHAP v2)

- Giao thức xác thực – hàm băm thông điệp MD5 mở rộng (EAP-MD5)

- Giao thức xác thực - bảo mật tầng vận tải mở rộng (EAP-TLS)

Với các kết nối PPTP, có thể sử dụng MS-CHAP, MS-CHAP v2, hoặc EAP-TLS. Chỉ 3 giao thức này cung cấp một cơ chế để tạo khoá mã hoá giống nhau trên cả Client và Server. MPPE sử dụng khoá mã hoá này để mã hoá tất cả dữ liệu PPTP trên kết nối mạng riêng ảo. MS-CHAP and MS- CHAP v2 là các giao thức xác thực dựa vào mật khẩu.

Với các kết nối L2TP, bất kỳ giao thức xác thực nào cũng có thể được dùng vì việc xác thực xuất hiện sau khi Client VPN và Server VPN thiết lập một kênh liên lạc an toàn, chẳng hạn như ta đã biết đó là liên kết an toàn IPSec (SA). Tuy nhiên, nhưng giao thức có khả năng xác thực mạnh được khuyến cáo sử dụng.

4. Các giao thức định đường hầm mạng riêng ảo

Cùng với việc quyết định một giao thức xác thực, ta cần quyết định giao thức đường hầm nào sẽ dùng cho việc triển khai mạng riêng ảo. Hai giao thức định đường hầm mạng riêng ảo truy cập từ xa thông dụng là

- Giao thức định đường hầm điểm - tới - điểm (PPTP)

- Giao thức định đường hầm tầng 2 với IPSec (L2TP/IPSec)

5. Máy chủ mạng riêng ảo

Máy chủ mạng riêng ảo là trung tâm của toàn bộ hoạt động mạng riêng ảo. Máy chủ mạng riêng ảo thực hiện các công việc sau:

- Lắng nghe kết nối PPTP và các thương lượng SA IPSec cho kết nối L2TP

- Xác thực và cấp quyền cho các kết nối mạng riêng ảo trước khi cho phép dữ liệu lưu chuyển

- Hoạt động như một Router chuyển tiếp dữ liệu giữa các Client VPN và các tài nguyên trên Intranet

- Hoạt động như một điểm cuối của đường hầm mạng riêng ảo

Máy chủ mạng riêng ảo thường có 2 hoặc nhiều hơn 2 cardmang để kết nối tới Internet và cả Intranet

6. Hạ tầng mạng Intranet

Hạ tầng mạng của Intranet là một phần tử quan trọng của thiết kế mạng riêng ảo. Không có thiết kế thích đáng, các Client VPN không có khả năng thu được các địa chỉ IP và xử lý các tên trong mạng cục bộ, và các gói không thể được chuyển tiếp giữa các Client và các tài nguyên mạng Intranet, các Client sẽ không có khả năng truy cập tới bất kỳ tài nguyên nào trên mạng Intranet

Giải quyết vấn đề đặt tên

Nếu ta sử dụng DSN để xử lý các tên máy chủ trong mạng Intranet, đảm bảo rằng máy chủ mạng riêng ảo được cấu hình với các địa chi IP của DNS bên trong thích hợp. Để đảm bảo việc xử lý tên với các tài nguyên bên ngoài mạng Intranet, cấu hình DNS bên trong để truy vấn các máy chủ ISP bên ngoài. Đây là điều quan

trọng, nếu không thực hiện như vậy, các Client VPN sẽ không thực hiện chức năng một cách đúng đắn. Máy chủ VPN nên được cấu hình DNS một cách thủ công. Như một phần của quá trình thương lượng PPP, các Client VPN nhận địa chỉ IP của DNS. Theo ngầm định các Client VPN kết thừa các địa chỉ DNS đã cấu hình trên máy chủ mạng riêng ảo

7. Cơ sở hạ tầng AAA

Cơ sở hạ tầng cho việc xác thực, cấp quyền và kiểm toán là một phần sống còn của cơ sở hạ tầng mạng riêng ảo vì nó là hệ thống giữ cho tính năng an toàn thực hiện trên giải pháp truy cập từ xa. AAA kiểm soát tất cả truy cập tới Gateway; xử lý tất cả các đăng nhập một lần và vấn đề truy cập tài nguyên. Cơ sở hạ tầng AAA tồn tại để:

- Xác thực giấy uỷ nhiệm của các Client VPN

- Cấp quyền cho các kết nối mạng riêng ảo

- Ghi lại việc tạo ra và kết thúc kết nối mạng riêng ảo cho chức năng kiểm toán

Cơ sở hạ tầng AAA bao gồm

- Máy chủ mạng riêng ảo

- Một máy chủ RADIUS

- Một máy điều khiển tên miền

Các chính sách truy cập từ xa

Các chính sách truy cập từ xa là một tập có thứ tự các luật định nghĩa những kết nối nào được chấp nhận hay từ chối. Với các kết nối được chấp nhận, các chính sách truy cập từ xa cũng có thể định nghĩa để các hạn chế kết nối. Với mỗi luật, có một hoạc nhiều hơn các điều kiện, một tập các thiết lập hồ sơ và một tập các thiết lập mức cho phép truy cập từ xa. Các nỗ lực kết nối được đánh giá dựa vào các chính sách truy cập từ xa, nó cố gắng xác định kết nối nào phù hợp tất cả các điều kiện của mỗi chính sách. Nếu nổ lực kết nối không phù hợp với tất cả các điều kiện của bất kỳ một chính sách nào, thì nó sẽ bị từ chối.

Nếu một kết nối phù hợp với tất cả các điều kiện của một chính sách truy cập từ xa và được cấp phát mức cho phép truy cập từ xa, hồ sơ chính sách truy cập từ xa xác định một tập các hạn chế kết nối. Các đặc tính quay số của tài khoản người dùng cũng cung cấp một tập các hạn chế. Chính sách truy câp từ xa bao gồm các phần tử sau:

- Các điều kiện:

Các điều kiện chính sách truy cập từ xa là một hoặc nhiều thuộc tính mà được so sánh với các thiết lập của nổ lực kết nối. Nếu có nhiều điều kiện, tất cả các điều kiện phải phù hợp với thiết lập của nổ lực kết nối để cho nó phù hợp với chính sách. Với các kết nối mạng riêng ảo, ta thường sử dụng các điều kiện sau:

+ Loại cổng NAS: Bằng việc thiết lập điều kiện này với mạng riêng ảo, ta có thể xác định tất cả các kết nối mạng riêng ảo.

+ Kiểu đường hầm: Với điều kiện này, ta có thể chỉ rõ các chính sách khác nhau với các kết nối PPTP và L2TP

+ Nhóm: Với các nhóm, ta có thể cấp quyền hoặc từ chối truy cập theo nhóm thành viên

- Mức cho phép: Ta có thể dùng các thiết lập mức cho phép để cấp quyền hoặc từ chối truy cập từ xa nếu mức cho phép truy cập từ xa của tài khoản người dùng được thiết lập để kiểm soát truy cập qua chính sách truy cập từ xa. Trường hợp khac, thiết lập mức cho phép trên tài khoản người dùng xác định mức cho phép truy cập từ xa.

- Các thiết lập hồ sơ: Một hồ sơ chính sách truy cập là một tập các thuộc tính được áp dụng với một kết nối lúc nó được xác thực. Với các kết nối mạng riêng ảo, ta có thể sử dụng các thiết lập hồ sơ như sau:

+ Các ràng buộc quay số có thể được dùng để định nghĩa bao lâu thì kết nối có thể tồn tại trước khi bị kết thúc bởi máy chủ mạng riêng ảo.

+ Mặc dù sử dụng các bộ lọc gói IP, việc thiết lập IP có thể định nghĩa các loại lưu lượng IP được cho phép với các kết nối mạng riêng ảo truy cập từ xa. Với

hồ sơ các bộ lọc gói, ta có thể cấu hình lưu lượng IP được cho phép nhận từ các Client truy cập từ xa(Bộ lọc đầu vào) hoặc được gửi tới Client từ xa (Bộ lọc đầu ra)

+ Các thiết lập xác thực có thể định nghĩa giao thức Client VPN phải sử dụng để gửi giấy uỷ nhiệm của nó và cấu hình của các loại EAP, chẳng hạn EAP-TLS.

Việc ngăn chặn các luồng lưu lượng được định tuyến từ Client VPN

Một khi Client VPN thiết lập thành công một kết nối PPTP hoặc L2TP, theo ngầm định bất kỳ gói nào gửi qua kết đều nhận được bởi máy chủ mạng riêng ảo và chuyển tiếp chúng. Các gói gửi qua kết nối có thể bao gồm:

- Các gói có nguồn gốc từ máy tính Client truy cập từ xa

- Các gói gửi tới máy Client truy cập từ xa bởi các máy khác

Lúc máy Client truy cập từ xa tạo ra kết nối mạng riêng ảo, theo ngầm định nó tạo một đường định tuyến mặc định vì vậy tất cả luồng lưu lượng phù hợp với đường định tuyến mặc định được gửi qua kết nối mạng riêng ảo. Nếu các máy tính khác đang chuyển tiếp luồng lưu lượng tới Client VPN truy cập từ xa, xem các máy Client truy cập từ xa như một Router, mà luồng lưu lượng cũng được chuyển tiếp qua kết nối mạng riêng ảo. Đây là một vấn đề an toàn vì máy chủ mạng riêng ảo không xác thực các máy tính đang chuyển tiếp luồng lưu lượng tới Client VPN truy cập từ xa

8. Cơ sở hạ tầng chứng chỉ số

Để thực hiện việc xác thực dựa trên chứng chỉ cho các kết nối L2TP hoặc xác thực người dùng dựa trên chứng chỉ cho các kết nối mạng riêng ảo sử dụng EAP-TLS, một cơ sở hạ tầng, được biết đến như cơ sở hạ tầng khoá công khai (PKI), dùng để phát hành các chứng chỉ để đệ trình trong quá trình xác thực và để xác nhận tính hợp lệ của chúng chỉ đang được đệ trình.

Như vậy ta thấy, các kết nối mạng riêng ảo truy cập từ xa gồm nhiều thành phần. Client VPN phải được cấu hình để tạo kết nối mạng riêng ảo tới máy chủ VPN. Cơ sở hạ tầng mạng phải hỗ trợ khả năng kết nối tới được giao diện máy chủ

mạng riêng ảo trên mạng Intranet và hỗ trợ xử lý tên DNS của máy chủ mạng riêng ảo. Ta phải xác định giao thức xác thực và giao thức mạng riêng ảo để sử dụng. Cơ sở hạ tầng mạng Intranet phải hỗ trợ xử lý đặt tên của các tài nguyên trong Intranet, định tuyến tới các Client truy cập từ xa và các tài nguyên cách ly. Cơ sở hạ tầng AAA phải được cấu hình để cung cấp tính năng xác thực sử dụng Domain, xác thực sử dụng các chính sách truy cập từ xa, và kiểm toán các kết nối mạng riêng ảo truy cập từ xa. Với các kết nối L2TP/IPSec hoặc lúc sử dụng xác thực EAP-TLS, một cơ sở hạ tầng chứng chỉ phải được sử dụng để phát hành chứng chỉ người dùng và chứng chỉ máy tính

6.2. Triển khai mạng riêng ảo truy cập từ xa

6.2.1. Triển khai truy cập từ xa dựa trên PPTP hoặc L2TP/IPSec

Nhiều thủ tục triển khai truy cập từ xa là giống nhau khi ta sử dụng PPTP hoặc L2TP/IPSec, nhưng ta cần xem xét một số điểm khác biệt nổi bật trong khi thiết lập, tuỳ thuộc vào cái nào được sử dụng. Không kể tập hợp giao thức mà ta sử dụng, việc triển khai các kết nối mạng riêng ảo truy cập từ xa bao gồm các bước sau:

- Triển khai một cơ sở hạ tầng chứng chỉ số
- Triển khai một cơ sở hạ tầng Internet
- Triển khai một cơ sở hạ tầng xác thực, cấp quyền và kiểm toán
- Triển khai các máy chủ mạng riêng ảo
- Triển khai một cơ sở hạ tầng Intranet
- Triển khai các Client VPN

Sau đây ta sẽ thảo luận chi tiết hơn về các phần

6.2.1.1. Triển khai một cơ sở hạ tầng chứng chỉ số

Với các kết nối mạng riêng ảo dựa trên PPTP, một cơ sở hạ tầng chứng chỉ là cần thiết chỉ khi ta đang sử dụng các chứng chỉ người dùng được cài đặt cục bộ và xác thực EAP-TLS, mới L2TP/IPSec, cơ sở hạ tầng chứng chỉ số là điều bắt buộc. Nếu đang sử dụng chỉ một giao thức xác thực dựa trên mật khẩu như MS-CHAP

v2), thì không đòi hỏi cơ sở hạ tầng chứng chỉ và cơ sở hạ tầng này cũng không được dùng cho việc tạo kết nối mạng riêng ảo. Ta có thể lựa chọn việc sử dụng mật khẩu, miễn là các chứng chỉ cho phép xác thực 2 nhân tố và sẽ cho phép ta sử dụng các công nghệ an toàn của IPSec.

Để sử dụng một cơ sở hạ tầng chứng chỉ cho các kết nối mạng riêng ảo dựa trên PPTP, ta phải cài đặt một chứng chỉ máy tính trên máy chủ xác thực (Máy chủ mạng riêng ảo hoặc máy chủ RADIUS) và phân phối tới Client VPN hoặc một chứng chỉ người dùng trên mỗi máy Client VPN.

6.2.1.2. Triển khai một cơ sở hạ tầng Internet

Bây giờ ta đã có tất cả các dịch vụ cấp chứng chỉ đã triển khai, hãy chuyển sang khai thác hệ thống mạng riêng ảo đã cấu hình và triển khai. Bước thứ nhất là triển khai cơ sở hạ tầng Internet cho các kết nối mạng riêng ảo truy cập từ xa sẽ xử lý tất cả các yêu cầu kết nối và truy cập đến tới và từ Internet. Triển khai cơ sở hạ tầng Internet bao gồm:

- Đặt máy chủ mạng riêng ảo trong một mạng vành đai hoặc trên Internet
- Cấu hình giao diện Internet
- Bổ sung địa chỉ vào máy chủ hệ thống tên miền Internet

1. Đặt máy chủ mạng riêng ảo trong mạng vành đai hoặc trên Internet

Quyết định nơi đặt máy chủ liên quan đến Firewall Intranet của ta. Trong cấu hình thông dụng nhất, máy chủ mạng riêng ảo được đặt sau Firewall trên mạng vành đai giữa Intranet và Internet. Cấu hình này cho phép Firewall xử lý nhiều tác vụ bảo mật, chẳng hạn như xem xét các tấn công và lọc các luồng lưu lượng không mong muốn bên ngoài, cho phép máy chủ mạng riêng ảo xử lý luồng lưu lượng mạng riêng ảo truy cập từ xa. Nếu đang sử dụng một Firewall trước máy chủ mạng riêng ảo, cấu hình bộ lọc gói trên Firewall để cho phép luồng lưu lượng PPTP hoặc L2TP/IPSec khi được yêu cầu tới và từ địa chỉ IP của các giao diện mạng vành đai của máy chủ mạng riêng ảo.

2. Cấu hình giao diện Internet

Kết nối máy chủ mạng riêng ảo tới mạng vành đai với một card mạng và kết nối tới mạng Intranet với một card mạng khác. Cấu hình máy chủ mạng riêng ảo để chuyển tiếp các gói IP giữa Internet và Intranet, chẳng hạn nếu dùng hệ điều hành Windows thì dùng dịch vụ Routing anhd Remote Access Server

Với các kết nối kết nối tới Internet hoặc mạng vành đai, cấu hình giao thức TCP/IP với một địa chỉ IP công cộng, một subnet mask và cổng kết nối mặc định của hoặc Firewall(nếu Firewal được đặt trong một mạng vành đai) hoặc một Router của ISP(nếu máy chủ mạng riêng ảo được kế nối trực tiếp tới Internet và không có Firewall giữa máy chủ mạng riêng ảo và Router của ISP)

3. Bổ sung địa chỉ vào máy chủ DNS internet

Với các thiết bị mạng riêng ảo để thực hiện chức năng, người dùng sẽ cần phải có khả năng tìm thấy máy chủ mạng riêng ảo từ bất kỳ nơi nào trên Internet, vì vậy, ta cần thông báo tên máy chủ một cách đúng đắn. Để đảm bảo rằng tên của máy chủ mạng riêng ảo(ví dụ, vpn.fis.com) có thể được xử lý với các địa chỉ IP thích hợp của nó theo một trong 2 thủ tục sau. Bạn có thể bổ sung địa chỉ DNS vào máy chủ DNS nếu đang cung cấp dịch vụ phân giải tên DNS cho người dùng Internet(Nếu là trường hợp này, đảm bảo rằng ISP của ta biết nó và rằng máy chủ DNS của ta có thể phản hồi yêu cầu bởi các máy chủ DNS của ISP). Như một sự lựa chọn, ta có thể bổ sung vào ISP của ta một bản ghi DNS tới máy chủ DNS nếu ISP đang cung cấp dịch vụ phân giải tên DNS cho người dùng Internet. Kiểm tra lại tên của máy chủ mạng riêng ảo có thể được xử lý với địa chỉ IP công cộng lúc kết nối tới Internet hay không

6.2.1.3. Triển khai một cơ sở hạ tầng AAA

Một khi ta làm cho tên máy chủ mạng riêng ảo có thể xử lý trên Internet, ta muốn chắc chắn rằng chỉ những người dùng mà ta đồng ý cấp quyền truy cập tới các dịch vụ mạng riêng ảo. Bước kế tiếp là triển khai hệ thống định danh, được xem như là các dịch vụ AAA. Việc triển khai cơ sở hạ tầng AAA cho các kết nối mạng riêng ảo truy cập từ xa bao gồm

- Cấu hình dịch vụ thư mục cho tài khoản người dùng và nhóm

- Cấu hình máy chủ xác thực Internet IAS chính

- Cấu hình IAS với các Client RADIUS

- Cấu hình chính sách mạng riêng ảo truy cập từ xa

Cấu hình dịch vụ thư mục cho tài khoản người dùng và nhóm

Dịch vụ thư mục là trung tâm bảo mật của mạng riêng ảo

+ Phải đảm bảo rằng tất cả người dùng tạo kết nối truy cập từ xa có một tài khoản tương ứng

+ Thiết lập mức cho phép truy cập từ xa trên tài khoả để cho phép truy cập hay từ chối truy cập để quản lý truy câp từ xa theo người dùng hoặc theo nhóm thông qua chính sách truy cập từ xa

+ Tổ chức những người dùng từ xa thành nhóm thích hợp để thuận tiện trong việc áp dụng chính sách truy cập từ xa theo nhóm

Cấu hình máy chủ IAS chính

Máy chủ IAS sẽ cho phép ta xử lý tất các các liên lạc liên quan tới xác thực và cấp quyền. Đây sẽ là nguồn tài nguyên máy chủ sống còn và việc mất các dịch vụ xác thực có thể làm dừng hoạt động của toàn mạng, Vì vậy cần thiết phải có IAS thứ 2 để dự phòng

Máy chủ IAS chính phải có khả năng truy cập các thuộc tính tài khoản trong các Domain thích hợp. Nếu IAS đang được cài trên một máy điều khiển miền, không yêu cầu phải cấu hình cho IAS truy cập các thuộc tính tài khoản trong Domain mà nó thuộc. Nếu IAS không được cài trên một máy điều khiển miền, ta phải cấu hình máy chủ IAS chính để nó có thể đọc các thuộc tính của tài khoản người dùng trong Domain

Nếu máy chủ IAS xác thực và cấp quyền cho các nổ lực kết nối mạng riêng ảo với các tài khoản người dùng trong các Domain khác, kiểm tra lại xem các Domain khac có quan hệ tin cậy hai chiều với Domain mà máy chủ IAS là thành viên hay không.

Nếu các tài khoản trong các Domain khác nhau không có quan hệ tin cậy hai chiều với Domain mà IAS là thành viên, ta phải cấu hình một RADIUS uỷ quền giữa hai Domain không tin cậy nhau

Cấu hình IAS với Client RADIUS

Ta phải cấu hình máy chủ IAS chính với máy chủ mạng riêng ảo như Client RADIUS. Cấu hình này sẽ cho phép cả máy chủ IAS chính và phụ truy cập các dịch vụ RADIUS để xác thực người dùng.

Cấu hình chính sách truy cập từ xa

Chính sách truy cập từ xa sẽ cho phép đưa thêm các yêu cầu an toàn cho những người dùng truy cập đến mạng từ mạng bên ngoài. Nó sẽ định nghĩa những ai được phép truy cập hệ thống và cách họ được cho phép để truy cập nó. Chẳng hạn, nếu bạn muốn những người dùng từ xa truy cập máy chủ mạng riêng ảo chi nếu họ đang sử dụng L2TP/IPSec như một giao thức đường hầm hoặc chỉ nếu họ sử dụng EAP-TLS như một giao thức xác thực, chính sách truy cập từ xa định nghĩa các tham số mà chúng được cho phép sử dụng để kết nối

6.2.1.5. Triển khai máy chủ mạng riêng ảo

Để cho người dùng có thể truy cập, chúng ta cần thiết lập các máy chủ mạng riêng ảo. Triển khai các máy chủ mạng riêng ảo cho các kết nối mạng riêng ảo truy cập từ xa bao gồm

- Cấu hình mỗi kết nối của máy chủ mạng riêng ảo tới Intranet

- Thiết lập bộ định tuyến mạng riêng ảo

6.2.1.6. Triển khai cơ sở hạ tầng Intranet

Bây giờ máy chủ đã thiết lập TCP/IP cơ sở và tất cả các quyết định về giao thức và kết nối AAA đã được thực hiện, ta cần đảm bảo rằng các tài nguyên trong mạng Intranet là có khả năng truy cập được với máy chủ mạng riêng ảo và như vậy nó có thể xử lý các liên lạc tới các Client truy cập từ xa. Triển khai cơ sở hạ tầng mạng Intranet cho các kết nối mạng riêng ảo truy cập từ xa bao gồm các công việc sau:

- Cấu hình bộ định tuyến trên máy chủ mạng riêng ảo

- Kiểm tra trình phân giải tên và khả năng kết nối tới Intranet từ máy chủ mạng riêng ảo

- Cấu hình bộ định tuyến cho vùng địa chỉ subnet

- Cấu hình các tài nguyên cách ly

Cấu hình bộ định tuyến trên máy chủ mạng riêng ảo

Với các máy chủ mạng riêng ảo để chuyển tiếp luồng lưu lượng tới các vị trí trong Intranet, ta phải cấu hình chúng với hoặc các đường định tuyến tĩnh mà tổng kết tất cả các địa chỉ có khả năng đã dùng trên Intranet hoặc với các giao thức định tuyến và như vậy máy chủ mạng riêng ảo có thể hoạt động như một bộ định tuyến động và tự động bổ sung các đường định tuyến cho các mạng con Intranet vào bảng định tuyến của nó. Thực tế tốt nhất là ta nên sử dụng sự tổng kết đường định tuyến để đi đến phần còn lại của mạng trong. Đó là cách mà người quản trị máy chủ mạng riêng ảo dễ thực thiện và ta không phải lo lắng về việc hỗ trợ định tuyến động trên máy chủ mạng riêng ảo. Nếu tổng kết đường định tuyến không có khả năng, sử dụng định tuyến động để đảm bảo rằng máy chủ mạng riêng ảo biết tất cả những thay đổi topo mạng

Kiểm tra trình phân giải tên và khả năng kết nối tới Intranet từ máy chủ mạng riêng ảo

Từ mỗi máy chủ mạng riêng ảo, kiểm tra xem máy chủ có thể phân giải các tên và liên lạc thành công với các tài nguyên Intranet hay không. Ta thực hiện công việc này bằng lệnh Ping, truy cập trang Web với trình duyệt, và kiểm tra kết nối máy in tới máy chủ trong Intranet. Công việc này đảm bảo để sử dụng DNS dựa trên mạng Intranet và việc cấu hình trên các giao diện Intranet của máy chủ mạng riêng ảo là đúng đắn. Nếu Client được thiết lập DNS dựa vào bên ngoài, sẽ không có khả năng kết nối tới các máy chủ bên ngoài(nếu đường hầm bị disable) hoặc các máy chủ bên ngoài sẽ không có khả năng xử lý các tên cho tài nguyên Intranet(nếu đường hầm được enable).

Cấu hình định tuyến cho phạm vi địa chỉ mạng con

Nếu ta đã cấu hình các máy chủ mạng riêng ảo với vùng địa chỉ một cách thủ công và các phạm vi trong vùng là một phạm vi mạng con, ta phải đảm bảo rằng đường định tuyến hoặc các đường định tuyến mô tả vùng địa chỉ mạng con hay các vùng được mô tả trong cơ sở hạ tầng định tuyến Intranet của ta. Ta có thể đảm bảo điều này bằng việc hoặc bổ sung các đường định tuyến tính mô tả phạm vi địa chỉ mạng con như các đường định tuyến tĩnh tới các Router kề cạnh của máy chủ mạng riêng ảo, và sau đó sử dụng giao thức định tuyến của Intranet chúng ta để phổ biến đường định tuyến tới các bộ định tuyến khác. Khi sử dụng các phương thức này, phải đảm bảo cho phép phân phối lại các đường định tuyến tĩnh trên bộ định tuyến kế tiếp để phổ biến các đường định tuyến tĩnh cho các giao thức định tuyến động.

Ngoài ra, nếu ta đang sử dụng giao thức thông tin định tuyến(RIP) hoặc Open Shortest Path First (OSPF), ta có thể cấu hình máy chủ mạng riêng ảo sử dụng các vùng địa chỉ mạng con như các bộ định tuyến RIP hoặc OSPF. Với OSPF, ta phải cấu hình máy chủ mạng riêng ảo như một bộ định tuyến biên hệ thống tự trị(ASBR). Cấu hình này cho phép bộ định tuyến OSPF(máy chủ mạng riêng ảo) công khai các đường định tuyến tĩnh trong hệ thống tự trị OSPF

Cấu hình các tài nguyên cách ly

Nếu ta đang dùng kiểm soát cách ly truy cập mạng, ta nên cách ly dịch vụ với người dùng bằng việc chỉ rõ một máy chủ DNS, máy chủ File, máy chủ Web với các trang web chưa chính sách mạng theo đúng các chỉ lện và thành phần trong một mạng con độc lập

6.2.1.6. Triển khai các Client VPN

Bây giờ ta đã có các máy chủ xác thực. Máy chủ mạng riêng ảo được thiết lập với các chính sách tuy cập của chúng và có khả năng thực hiện các kết nối từ người dùng từ xa, truy cập tài nguyên của tổ chức và liên lạc trên bộ định tuyến mạng của tổ chức. Bước tiếp theo ta làm cho các Client có khả năng truy cập máy chủ mạng riêng ảo.

Tổng kết

Để triển khai một giải pháp truy cập từ xa dựa trên PPTP, thực hiện các bước như sau

+ Nếu đang sử dụng xác thực EAP-TLS, tạo một cơ sở hạ tầng chứng chỉ số để phát hành các chứng chỉ người dùng tới các Client VPN và máy chủ xác thực

+ Kết nối máy chủ mạng riêng ảo với Internet

+ Triển khai cơ sở hạ tầng AAA(gồm cả máy chủ RADIUS)

+ Triển khai các Client VPN

Để triển khai một giải pháp truy cập từ xa dựa trên L2TP/IPSec, ta thực hiện các bước sau:

+ Tạo một cơ sở hạ tầng cung cấp chứng chỉ để phát hành chứng chỉ cho Client VPN và máy chủ mạng riêng ảo

+ Kết nối máy chủ mạng riêng ảo với Internet

+ Triển khai cơ sở hạ tầng AAA(gồm cả máy chủ RADIUS)

+ Sửa đổi cơ sở hạ tầng Intranet để phân phối đường định tuyến và vùng cách ly

+ Triển khai các Client VPN

Câu hỏi ôn tập

Chương VII Xây dựng mạng riêng ảo Site – to – Site

7.1. Các thành phần của mạng riêng ảo Site – to – Site

Trong chương VI ta đã xem xét các thành phần của mạng riêng ảo truy cập từ xa – đó là, mạng riêng ảo có nhiều người dùng từ xa kết nối tới một cổng kết nối mạng riêng ảo để truy cập các tài nguyên bên trong. Kiểu kết nối mạng riêng ảo khác là dạng từ nhánh mạng - tới – nhánh mạng (Site – to – Site), trong đó, hai Router tạo một đường hầm qua Internet và hoạt động như một liên kết mạng WAN giữa hai nhánh mạng. Người dùng bên cả hai phía của liên kết không cần biết về kết nối mạg riêng ảo vì liên kết hoàn toàn trong suốt với họ. Mạng riêng ảo Site – to – Site cho phép các công ty sử dụng Internet để kết nối các văn phòng của họ lại với nhau bằng việc sử dụng đường hầm mạng riêng ảo và công nghệ mã hoá, và như vậy, tiết kiệm được chi phí trên các liên kết mạng WAN riêng đắt đỏ. Để quyết định triển khai kết nối mạng riêng ảo Site – to – Site (được xem như là Router - tới – Router) ta phải hiểu tất cả các thành phần liên quan. Để hiểu tất cả các chức năng của mạng riêng ảo Site – to – Site, chúng ta cần bắt đầu với một mô tả tổng qua về công nghệ định tuyến theo yêu cầu quay số, nó cho phép các Router mạng riêng ảo có thể cho phép hoặc không cho phép các đường hầm mạng riêng ảo một cách tự động dựa trên luồng lưu lượng mà các Router đang xem xét

7.1.1. Định tuyến theo yêu cầu quay số

Định tuyến theo yêu cầu quay số qua các kết nối quay số (chẳng hạn như đường điện thoại hoặc mạng tích hợp dịch vụ số - ISDN), các kết nối mạng riêng ảo , và giao thức PPP qua các kết nối Ethernet (PPPoE). Định tuyến theo yêu cầu quay số cho phép chuyển tiếp các gói dữ liệu qua một liên kết PPP. Liên kết PPP được mô tả trên Router như là một giao diện theo yêu cầu quay số, nó có thể được dùng để tạo các kết nối khi được yêu cầu qua đường quay số, không thường xuyên hay truyền thông liên tục. Các kết nối theo yêu cầu quay số cho phép ta sử dụng các đường điện thoại quay số thay thế các đường leased line những tình huống luồng lưu lượng thấp và thúc đẩy kết nối của Internet để kết nối các văn phòng chi nhánh với các kết nối mạng riêng ảo. Khi các liên kết luôn luôn « sẵn sàng« , nó được xem như là một kết nối thường trực. Nếu liên kết chỉ « sẵn sàng« lúc cần thiết

– đó là, một kết nối được thiết lập chỉ lúc « quan tâm« luồng lưu lượng hiện tại và kết nối đó được huỷ bỏ lúc truyền tin hoàn tất- Nó sẽ tối thiểu hoá các chi phíe điện thoại và các vấn đề về độ trễ cao trong định tuyến. Cấu hình này được xem như một kết nối khi có yêu cầu.

Định tuyến theo yêu cầu quay số không giống như truy cập từ xa. Trong khi truy cập từ xa kết nối một máy tính đơn vào mạng, định tuyến theo yêu cầu quay số kết nối toàn bộ các mạng. Tuy nhiên, cả hai đều sử dụng PPP như giao thức để thương lượng và các thực kết nối, đóng gói dữ liệu đã gửi qua nó. Một số tính năng và đặc điểm của các kết nối theo yêu cầu quay số :

- Các thuộc tính quay số cho các tài khoản người dùng

- Tính năng an toàn(các giao thức xác thực và mã hoá)

- Các chính sách truy cập từ xa được sử dụng

- Dịch vụ AAA

- Địa chỉ IP được gán và cấu hình

- Các tính năng PPP được dùng, như MMPC, BAP

Trong khi khái niệm định tuyến theo yêu cầu quay số là khá đơn giản thì việc cấu hình nó lại khá phức tạp bởi các nhân tố sau:

- Đánh địa chỉ đầu cuối của kết nối : Kết nối phải được thực hiện qua các mạng dữ liệu công khai, như hệ thống thoại tương tự hay Internet. Một số điện thoại cho các kết nối theo yêu cầu quay số và tên máy chủ đầy đủ hay địa chỉ IP cho các kết nối mạng riêng ảo phải định danh được đầu cuối của kết nối

- Xác thực và cấp quyền cho người gọi. Bất kỳ ai gọi tới Router phải được xác thực và cấp quyền. Xác thực dựa trên tập các giấy uỷ nhiệm của người gọi được gửi qua trong khi xử lý thiết lập kết nối, các giấy uỷ quyền gửi qua phải tương ứng với một tài khoản. Việc cấp quyền là gán quyền dựa trên các thuộc tính quay số của tài khoản và các chính sách truy cập từ xa.

- Cấu hình tại 2 đầu cuối của kết nối : Hai đầu cuối của kết nối phải được cấu hình, ngay cả khi chỉ một đầu cuối của kết nối đang khởi tạo một kết nối theo yêu cầu quay số. Việc cấu hình chỉ một phía của kết nối nghĩa là các gói dữ liệu được định tuyến thành công chỉ trong một hướng. Thông thường, việc liên lạc truyền thông yêu cầu thông tin được lưu chuyển theo cả hai hướng. Vì vậy, mỗi phía của kết nối cần có thông tinh định tuyến về phía kia để hiểu luồng lưu lượng nào được đi qua liên kết. Không có thông tin này, việc định tuyến không làm việc đúng.

- Cấu hình các đường định tuyến tĩnh : Ta không nên sử dụng các giao thức định tuyên động qua các kết nối theo yêu cầu quay số nhất thời. Lí do là vì nếu việc cập nhật định tuyến xẩy ra thường xuyên hoặc có một khối lượng lớn luồng lưu lượng hội tụ trên mỗi phía của liên kết. Vì vậy, các Router cho các định danh mạng sẵn sàng qua giao diện theo yêu cầu quay số phải được bổ sung như các tuyến đường tĩnh, vào bảng định tuyến của các Router. Bằng cách sử dụng các đường định tuyến tĩnh, các liên kết theo yêu cầu quay số sẽ không phải là phần của chức năng định tuyến động và sẽ không phải cập nhật luồng lưu lượng

7.1.2. Giới thiệu các kết nối mạng riêng ảo Site – to – Site

Một kết nối mạng riêng ảo site – to – site là một kết nối theo yêu cầu quay số sử dụng một giao thức đường hầm như PPTP hoặc L2TP/IPSec để két nối hai phần của một mạng riêng. Mỗi Router mạng riêng ảo cung cấp một kết nối định tuyến tới mạng nào mà Router đó được gắn vào. Trên một kết nối mạng riêng ảo site – to – site, các gói dữ liệu đã gửi từ Router khác qua kết nối mạng riêng ảo không bắt đầu tại các Router.

Router gọi (VPN Client) khởi tạo kết nối, Router trả lời (VPN Server) lắng nghe các nỗ lực kết nối, nhập nỗ lực kết nối từ Router gọi và trả lời yếu cầu để tạo một kết nối. Router gọi xác thực nó với Router trả lời. Khi sử dụng các giao thức xác thực như MS-CHAPv2 hoặc EAP-TLS, Router trả lời cũng xác thực nó với Router gọi.

Các Router mạng riêng ảo cũng có thể là bất kỳ máy tính nào có khả năng tạo một kết nối PPTP sử dụng MPPE hoặc một kết nối định tuyến L2TP sử dụng mã hoá IPSec.

7.1.2.1. Các kết nối theo yêu cầu và thường trực

Một kết nối mạng riêng ảo site – to – site có thể là một trong hai kiểu sau: theo yêu cầu hoặc thường trực. Sau đây là các chi tiết về 2 loại kết nối này :

- Một kết nối site – to – site là một kết nối được tạo khi luồng lưu lượng phải được chuyển tiếp qua kết nối. Khi luồng lưu lượng « quan tâm« được xem xét bởi Router, kết nối được tạo, luồng lưu lượng được chuyển tiếp, và kết nối được kết thúc sau một thời gian chỉ ở trạng thái « rỗi ». Luồng lưu lượng « quan tâm » được quyết định bằng việc sử dụng các thiết lập bộ lọc theo yêu cầu để định danh luồng lưu lượng xác định. Ta có thể cấu hình cho hành vi huỷ kết nối ở trạng thái rỗi với Router trả lời cũng như Router gọi.

- Một kết nối site – to – site thường trực luôn được kết nối. Nếu kết nối bị huỷ bỏ, ngay lập tức được thử lại. Dễ dàng cấu hình được cho loại kết nối này trên cả Router trả lời và Router gọi

Nếu Router gọi đang kết nối tới Internet bằng cách sử dụng một liên kết quay số, chẳng hạn như một đường thoại tương tự hoặc ISDN, ta cần cấu hình kết nối mạng riêng ảo theo yêu cầu trên đường quay số bao gồm một giao diện đơn tại Router trả lời và hai giao diện tại Router gọi : một kết nối tới ISP và một cho kết nối mạng riêng ảo. Kết nối mạng riêng ảo theo yêu cầu quay số cũng yêu cầu một đường định tuyến bổ sung trong bảng định tuyến IP của Router gọi và như vậy Router mạng riêng ảo sẽ khởi tạo kết nối tới ISP lúc luồng lưu lượng cho nhánh mạng từ xa được nhận, Router mạng riêng ảo sẽ luôn nhận một thông báo lỗi «không kết nối được tới đích «.

Với các kết nối mạng riêng ảo hoặc theo yêu cầu hoặc thường trực, Router trả lời thường xuyên được kết nối tới Internet vì vậy nó có thể luôn sẵn sàng chấp nhận các cuộc gọi. Khái niệm này khá quan trọng để hiểu vì sao ta không thể có cả hai phía của liên kết dùng đường quay số tới Internet. Nếu điều này được thực

hiện, kết nối sẽ chỉ được thiết lập nếu thay đổi Router trả lời được kết nối tới Internet

7.1.2.2. Hạn chế sự khởi tạo các kết nối theo yêu cầu

Trong hầu hết các trường hợp, ta không muốn để bất kỳ luồng lưu lượng nào cũng khởi chạy một kết nối mạng riêng ảo. Ta muốn chỉ luồng lưu lượng « có thực« kích hoạt kết nối. Để ngăn chặn Router gọi tạo ra các kết nối không cần thiết, ta nên hạn chế Router gọi tạo các kết nối theo yêu cầu bằng các cách sau đây :

- Lọc yêu cầu quay số: Ta có thể dùng bộ lọc yêu cầu quay số để cấu hình hoặc các loại luồng lưu lượng IP không tạo ra một kết nối theo yêu cầu hoặc các loại như vậy. Sau đó có thể thiết lập các bộ lọc sẽ định danh luồng lưu lượng «quan tâm« có thể khởi tạo hoặc ngăn chặn khởi tạo liên kết.

- Các giờ quay số ra: Ta có thể qui định giờ quay số ra để cấu hình các giờ mà một Router gọi hoặc được phép hoặc không được phép tạo một kết nối mạng riêng ảo. Thiết lập này có thể hữu ích nếu ta không muốn các hoạt động xẩy ra ngoài các giờ đã định rõ, Ví dụ, nếu muốn luồng lưu lượng Email kích hoạt một liên kết, và ta chỉ muốn luồng lưu lượng trong khi đang là khoảng thời gian « off » vào buổi tối, ta có thể sử dụng thiết lập giờ quay số ra ngoài để hạn chế sự kích hoạt đường hầm.

Tại cùng thời điểm, trên Router trả lời, ta có thể dùng chính sách truy cập từ xa để cấu hình thời gian khi các kết nối vào được cho phép nếu đó là những kết nối làm cho môi trường mạng riêng ảo của ta ý nghĩa hơn

7.1.2.3. Các kết nối được khởi tạo một chiều và hai chiều

Nếu ta chỉ muốn nhánh mạng từ xa khởi tạo mạng riêng ảo khi cần, muốn sử dụng các thiết lập kết nối một chiều. Với các kết nối được khởi tại một chiều, một Router mạng riêng ảo luôn là Router gọi và một Router luôn là Router trả lời. Các kết nối được khởi tạo một chiều rất thích hợp với một kết nối thường trực có Topo mà trong đó Router tại văn phòng chi nhánh chỉ là Router khởi tạo kết nối. Cài đặt một chiều cho phép kiểm soát tập trung hơn, đặc biệt, khi nhánh mạng từ xa ở

trong một múi giời khác mà sẽ làm việc quản lý thời gian khó khăn với văn phòng trung tâm. Sự khác nhau lớn giữa một chiều và hai chiều là Router gọi không cần có một liên kết luôn luôn sẵn sàng. Các kết nối được khởi tạo một chiều yêu cầu cấu hình chi tiết như sau:

- Router trả lời được cấu hình như một LAN và Router theo yêu cầu quay số.

- Một tài khoản người dùng được bổ sung vào Router trả lời để lưu các giấy uỷ quyền xác thực của Router gọi mà được truy cập và xác minh bởi Router trả lời.

- Một giao diện theo yêu cầu quay số được cấu hình tại Router trả lời với cùng tên như tài khoản người dùng đã được cấu hình bởi Router gọi. Giảo diện này không sử dụng để quay số ra ngoài, vì vậy nó không được cấu hình với host name hoặc địa chỉ IP của Router gọi hoặc với các giấy uỷ quyền người dùng hợp lệ

Với các kết nối khởi tạo hai chiều, Router VPN có thể là Router gọi hoặc Router trả lời, tuỳ thuộc vào ai đang khởi tạo kết nối. Vì điều này, cả hai phía phải luôn sẵn sàng, nó làm tăng thêm chi phí cấu hính. Cả hai Router VPN phải được cấu hình để cả hai khởi tạo và chấp nhận một kết nối mạng riêng ảo. Ta có thể sử dụng các kết nối khởi tạo hai chiều lúc kết nối mạng riêng ảo không kích hoạt 24/24 và luồng lưu lượng từ Router khác được dùng để tạo một kết nối theo yêu cầu. Các kết nối mạng riêng ảo hai chiều yêu cầu như sau:

- Cả hai Router phải được kết nối tới Internet bằng một liên kết WAN thường trực.

- Cả hai Router phải được cấu hình như mạng LAN và Router theo yêu cầu quay số.

- Các tài khoản người dùng phải được bổ sung cho cả hai Router trên mỗi phía của liên kết sao cho các giấy uỷ quyền xác thực cho Router gọi được truy cập và xác minh bởi Router trả lời bất cứ lúc nào chiều gọi được khởi tạo.

- Các giao diện theo yêu cầu quay số, với tên giống nhau như tài khoản người dùng được dùng bởi Router gọi, phải được cấu hình đầy đủ tại cả hai Router, bao

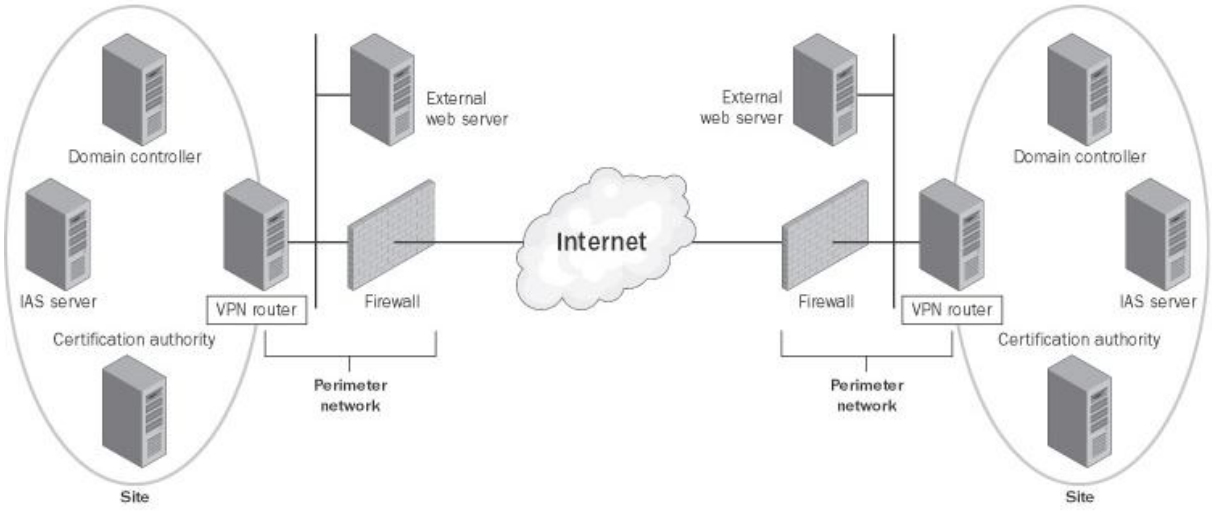
gồm các thiết lập cho host name hoặc địa chỉ IP của Router trả lời và các giấy uỷ quyền tài khoản người dùng.

Bảng 7.1 liệt kê một cấu hình ví dụ cho định tuyến được khởi tạo hai chiều giữa Router 1, một Router theo yêu cầu quay số trên nhánh mạng của thành phố A và Router 2, một Router theo yêu cầu quay số trên nhánh mạng tại thành phố B

Router	Tên giao diện	Tên tài khoản trong giấy uỷ quyền
Router 1	DD_A	DD_B
Router 2	DD_B	DD_A

7.1.3. Các thành phần của mạng riêng ảo Site – to – Site

Không giống với mạng riêng ảo truy cập từ xa, các liên kết Site – to – Site đòi hỏi cả hai phía của liên kết phải có một tập đầy đủ các tài nguyên để làm việc với nhau. Các thành phần của mạng riêng ảo Site – to – Site được minh hoạ như trong hình 7.1



Hình 7.1 Các thành phần của mạng riêng ảo Site – to – Site

Các thành phần chính là:

- Các Router VPN
- Cơ sở hạ tầng mạng Internet
- Cơ sở hạ tầng mạng chi nhánh
- Cơ sở hạ tầng AAA
- Cơ sở hạ tầng chứng chỉ

7.1.3.1. Các Router VPN

Các Router VPN là các Server kiểm soát tất cả các hoạt động kết nối từ xa của liên kết Site – to – Site. Chúng là trung tâm của hệ thống mạng riêng ảo Site – to – Site. Các Router VPN là các thực thể khởi tạo hoặc nhận các kết nối theo yêu cầu quay số dựa trên VPN và có các thành phần cơ bản sau được cài đặt trên đó:

- Dịch vụ định tuyến : Dịch vụ này được cài đặt trên cả Router gọi và Router trả lời

- Các Port : Một port là một kênh liên lạc vật lý hay lôgic có khả năng hỗ trợ một kết nối PPP đơnh. Các cổng vật lý dựa các thiết bị được cài đặt trên Router VPN, chẳng hạn như card mạng hay modem. Các cồng VPN là các cổng lôgic xử lý các thương lượng và tham số kết nối logic cho các kết nối

- Các giao diện mạng : Một giao diện được cấu hình trên Router gọi mô tả lại kết nối PPP và chứa các thông tin cấu hình như kiểu của cổng để dùng(Ví dụ, PPTP hay L2TP/IPSec), địa chỉ sử dụng để tạo kết nối(đó là, một địa chỉ IP hoặc một tên Domain để kết nối tới Internet), các phương pháp xác thực, các yêu cầu mã hoá và các uỷ quyền xác thực.

- Tài khoản người dùng : Với mỗi Router gọi để được xác thực, các giấy uỷ nhiệm của nó phải được xác minh bởi các thuộc tính của một tài khoản người dùng tương ứng. Nếu Router trả lời được cấu hình với xác thực RADIUS, Server RADIUS phải truy cập tới tài khoản người dùng cho các giấy uỷ quyền xác thực của Router gọi

Với một kết nối khởi tạo một chiều, ta có thể cấu hình các đường định tuyến IP tĩnh được thêm vào bảng định tuyến của Router trả lời khi kết nối được tạo. Việc làm này sẽ cho phép Router gọi biết được subnet nào đang sẵn sàng trên phía bên kia và xác định có thiết lập liên kết sử dụng các đường định tuyến tĩnh đó hay không

- Các đường định tuyến: Để chuyển tiếp luồng lưu lượng qua một kết nối mạng riêng ảo, các đường định tuyến IP trong bảng định tuyến của Router VPN được cấu hình để sử dụng giao diện đúng.

Với các kết nối được khởi tạo một chiều, cấu hình Router gọi theo cách thông thường. Với Router trả lời, ta có thể cấu hành tài khoản người dùng đã chỉ rõ trong giấy uỷ quyền xác thực của Router gọi với các đường định tuyến IP tính

- Chính sách truy cập từ xa: Trên Router trả lời hoặc trên máy chủ dịch vụ xác thực Internet đang hoạt động như một Server RADIUS với Router trả lời, để xác định các tham số kết nối đã xác định với các kết nối theo yêu cầu quay số, tạo một chính sách truy cập từ xa riêng cho những người dùng hay nhóm người dùng với Router gọi như các thành viên của chính sách. Một chính sách truy cập từ xa riêng cho các kết nối theo yêu cầu quay số không được đòi hỏi

Một Router gọi ta làm như sau :

- Khởi tạo các kết nối VPN dựa trên hành động của người quản trị lúc một gói đang chuyển tiếp cho phù hợp với một đường định tuyến sử dụng một giao diện theo yêu cầu quay số dựa trên mạng riêng ảo.

- Chờ xác thực và cấp quyền trước khi chuyển tiếp các gói

- Hoạt động như một Router chuyểntiếp các gó dữ liệu giữa các Node trong nhánh mạng của nó và Router trả lời

- Hoạt động như một điểm cuối của kết nối mạng riêng ảo

Router trả lời ta làm như sau :

- Lắng nghe các kết nối đang cố gắng thực hiện

- Xác thực và cấp quyền cho các kết nối VPN trước khi cho phép dữ liệu luôn chuyển

- Hoạt động như một Router chuyển tiếp các gói dữ liệu giữa các Node trong nhánh mạng của nó và Router gọi

- Hoạt động như một điểm cuối của kết nối mạng riêng ảo

Các Router VPN điển hình có hai card mạng được cài đặt, một để kết nối tới Internet, một để kết nối tới Intranet.

Với các kết nối mạng riêng ảo Site – to – Site, một Router khởi tạo một kết nối mạng riêng ảo tới Server VPN và các Client không cần tự khởi chạy một VPN - tất cả luồng lưu lượng sẽ được xử lý bởi các Router cuối. Tiếp theo, Server VPN có thể khởi tạo một kết nối mạng riêng ảo tới Router VPN khác

Cài đặt một chứng chỉ trên Router VPN :

Nếu các Router VPN đang tạo các kết nối L2TP/IPSec hoặc sử dụng xác thực EAP-TLS, các chứng chỉ phải được cài đặt trên Router VPN. Với các kết nối L2TP/IPSec, một chứng chỉ phải được cài đặt trên cả Router gọi và trả lời để cung cấp xác thực cho việc khởi tạo một phiên IPSec. Với xác thực EAP-TLS, một chứng chỉ phải được cài đặt trên Server xác thực(hoặc Router trả lời hoặc một Server RADIUS) và chứng chỉ phải được cài đặt trên Router gọi.

7.1.3.2. Cơ sở hạ tầng Internet

Để tạo một kết nối mạng riêng ảo tới một Router trả lời qua Internet, ta cần đảm bảo rằng trình phân giải tên, IP và định tuyến, các dịch vụ được cấu hình và hoạt động đúng. Ta cần nhớ ba vấn đề chính cho việc thiết lập các kết nối thành công:

- Tên của Router trả lời phải có khả năng phân giải được

- Có khả năng kết nối tới được Router trả lời

- Luồng lưu lượng VPN phải được cho phép và từ Router trả lời

1. Trình phân giải tên của Router trả lời

Trong khi nó có khả năng để cấu hình các giao diện với các tên của các Router trả lời với một kết nối nào được tạo, ta nên sử dụng địa chỉ các IP hơn là các tên. Sử dụng địa chỉ IP thay cho tên loại bỏ được một số sự phức tạp trong cài đặt và kiểm thử.

2. Khả năng kết nối tới được Router trả lời

Để có thể kết nối tới được, Router trả lời phải được gán một địa chỉ IP công cộng để những gói dữ liệu được chuyển tiếp bởi cơ sở hạ tầng định tuyến của Internet. Nếu ta đã gán một địa chỉ IP tĩnh công cộng từ một ISP hoặc một cơ quan

đăng ký Internet, thì điều này không phải là một vấn đề. Trong một số cấu hình, Router trả lời được gán chính xác với một địa chỉ IP riêng và có một địa chỉ IP tĩnh được công bố trên Internet. Một thiết bị dịch chuyển địa chỉ mạng giữa Internet và Router trả lời để dịch chuyển địa chỉ IP hiện thời và đã công bố của Router trả lời trong các gói dữ liệu tới và từ Router trả lời.

Trong khi cơ sở hạ tầng định tuyến có thể thay thế, Router trả lời có thể không kết nối tới được vì sự bố trí của các Firewall, các Router lọc gói, các bộ dịch chuyển địa chỉ mạng, các cổng nối bảo mật hay các loại thiết bị khác ngăn chặn các gói dữ liệu đang được gửi hoặc nhận từ Router trả lời. Và như vậy, nếu Router trả lời được bảo vệ bởi bất kỳ tuỳ chọn nào trong số trên, ta cần đảm bảo rằng việc cấu hình và kiểm thử thích hợp có thể được thực hiện để đảm bảo việc xử lý các gói thích hợp bởi các thiết bị mạng này.

3. Các Router VPN và cấu hình Firewall

Có 3 cách tiếp cận điển hình về việc sử dụng một Firewall với một Router VPN.

- Router VPN được gắn kết trực tiếp tới Internet, và Firewall là giữa Router VPN và nhánh mạng. Trong cấu hình này, Router VPN phải được cấu hình với các bộ lọc gói chỉ cho phép luồng lưu lượng VPN vào và ra của giao diện Internet của nó. Firewall có thể được cấu hình để cho phép các loại xác định của luồng lưu lượng thuộc nhánh mạng trong.

- Firewall và Server VPN là thực thể giống nhau, trong trường hợp này, Server sẽ xử lý cả hai chức năng.

Ngoài ra còn một số vấn đề về giao thức xác thực và các giao thức mạng riêng ảo

7.1.3.3. Cơ sở hạ tầng mạng chi nhánh

Cơ sở hạ tầng của mạng chi nhánh là một phần tử quan trọng của thiết kế VPN. Các Router gọi không thể chuyển tiếp các gói mà không có cơ sở hạ tầng định tuyến thích hợp được đặt vào vị trí thích hợp

1. Trình phân giải tên

Nếu Router gọi được cấu hình với các địa chỉ IP của DNS, các địa chỉ IP DNS không được yêu cầu bởi Router trả lời trong khi thương lượng kết nối PPP. Nếu Router gọi không được cấu hình với các địa chỉ IP của DNS, DNS được yêu cầu. Router gọi không bao giờ yêu cầu địa chỉ IP của DNS từ Router gọi. Theo ngầm định, Router gọi không đăng ký nó với DNS của Router trả lời

2. Định tuyến

Mỗi Router mạng riêng ảo là một Router IP và như vậy phải được cấu hình đúng với tập các Router làm cho tất cả các vị trí đều có thể kết nối tới được. Đặc biệt, mỗi Router mạng riêng ảo cần như sau:

- Một đường định tuyến mặc định hướng tới một Firewall hay Router đã kết nối trực tiếp với Internet: Đường định tuyến này làm cho tất các các vị trí trên Internet đều có thể kết nối tới được. Không có một đường định tuyến mặc định, sẽ không có cách nào để định tuyến luồng lưu lượng tới Internet và tất các các gói có địa chỉ sẽ bị loại bỏ tại Router VPN

- Một hoặc nhiều đường định tuyến tập hợp các địa chỉ sử dụng trong nhánh mạng của Router VPN hướng tới Router nhánh mạng kề cận: Các đường định tuyến này làm cho tất cả các vị trí trong nhánh mạng của Router VPN có thể kết nối tới được từ Router VPN. Không có các đường này, tất cả các host trong nhánh mạng không kết nối được tới cùng subnet khi Router VPN không có khả năng kết nối tới được. Không có cách nào cho các thực thể cuối biết được những subnet nào không nằm trong phạm vị subnet của Router VPN. Vì không có các cập nhật đường định tuyến động qua liên kết, thông tin này cần được cung cấp một cách thủ công. Nếu có các subnet mà nhánh mạng từ xa không nên truy cập, ách đơn giản là loại trừ các subnet này khỏi tập các đường định tuyến tĩnh và chúng sẽ không có khả năng kết nối tới được

Để bổ sung một đường định tuyến mặc định hướng tới Internet, cấu hình giao diện Internet với một cổng kết nối ngầm định và sau đó cấu hình giao diện nhánh mạng không có cổng kết nối ngầm định.

Nếu nhánh mạng chỉ có một subnet đơn, không yêu cầu phải cấu hình thêm và giao thức định tuyến động cũng không cần thiết. Sử dụng giao thức định tuyến động chi trên các liên kết theo yêu cầu quay số lúc được gọi. Định tuyến tĩnh là giải pháp được khuyến cáo để tránh cho các kết nối khỏi bị phá vỡ.

Lúc một kết nối mạng riêng ảo được tạo, mỗi Router gửi luồng lưu lượng sử dụng một giao diện logic tương ứng với cổng PPTP hoặc L2TP của kết nối. Trong khi thương lượng PPP, các địa chỉ IP có thể được gán cho các giao diện lôgic này. Việc đảm bảo rằng các giao diện lôgic của Router VPN có thể kết nối tới được phụ thuộc cách mà ta cấu hình mỗi Router VPN để chứa các địa chỉ IP cho các Client truy cập từ xa.

7.1.3.4. Cơ sở hạ tầng AAA

Cơ sở hạ tầng AAA tồn tại để cung cấp xác thực các kết nối và ghi nhật ký hoạt động của các kết nối đó sao cho vấn đền an toàn của mạng có thể được giám sát. Một cơ sở hạ tầng AAA mạnh là điều kiện sống còn với sự an toàn của mật kỳ mạng truy cập từ xa hay mạng Site –to – Site nào. Cơ sở hạ tầng AAA thực hiện các nhiệm vụ sau:

- Xác thực các giấy uỷ quyền của các Router gọi

- Cấp quyền cho kết nối mạng riêng ảo

- Ghi lại các hoạt động của kết nối mạng riêng ảo phục vụ cho chức năng kiểm toán.

Cơ sở hạ tầng AAA thường bao gồm:

- Router trả lời

- Máy chủ RADIUS

- Các trình điều khiển miền

7.1.3.5. Cơ sở hạ tầng chứng chỉ số

Để thực thi xác thực dựa trên chứng chỉ cho các kết nối L2TP và xác thực người dùng dựa trên chứng chỉ cho các kết nối mạng riêng ảo sử dụng EAP-TLS.

Một cơ sở hạ tầng về chứng chỉ được bố trí để phát hành các chứng chỉ thích hợp cho quá trình xác thực và xác minh chức chỉ

7.2. Triển khai mạng riêng ảo Site – to – Site

Trong phần này trước chúng ta đã mô tả các phần tử cần thiết cho mạng riêng ảo theo mô hình kết nối Site – to – Site. Trong phần này chúng ta xem xét các bước để triển khai giải pháp mạng riêng ảo Site – to – Site dựa trên PPTP hoặc L2TP với IPSec. Việc triển khai giải pháp này bao gồm các bước cơ bản như sau:

- Triển khai cơ sở hạ tầng cung cấp chứng chỉ: Cho phép ta triển khai các dịch vụ cung cấp chứng chỉ cho cả hai phía của liên kết

- Triển khai cơ sở hạ tầng Internet: Cho phép ta kết nối tới Internet từ cả hai phía của liên kết

- Triển khai Router trả lời: Triển khai máy chủ mạng riêng ảo sẽ nhận các yêu cầu kết nối mạng riêng ảo

- Triển khai Router gọi: Triển khai máy chủ mạng riêng ảo sẽ khởi tạo các yêu cầu kết nối mạng riêng ảo

- Triển khai cơ sở hạ tầng AAA: Cho phép xác thực, cấp quyền và kiểm toán các kết nối cho cả hai phía của liên kết

- Triển khai cơ sở hạ tầng của nhánh mạng bên trong: Cho phép chuyển tiếp các gói dữ liệu tới các nhánh mạng qua kết nối mạng riêng ảo Site – to – Site

7.2.1. Triển khai cơ sở hạ tầng cung cấp chứng chỉ

Ta sẽ sử dụng các chứng chỉ số cho xác thực bất cứ khi nào có thể. Với các kết nối L2TP/IPSec, các chứng chỉ số như là một yêu cầu. Với các kết nối mạng riêng ảo dựa trên PPTP, một cơ sở hạ tầng chứng chỉ số chỉ cần thiết lúc ta sử dụng xác thực EAP-TLS. Nếu chỉ đang sử dụng một giao thức xác thực dựa trên mật khẩu như MS-CHAPv2, thì cơ sở hạ tâng chứng chỉ là không cần thiết.

Hầu hết những người quản trị sử dụng PPTP để tránh các vấn đề về các yêu cầu chứng chỉ số hay thích hợp hơn qua các NAT với một giao thức không IPSec.

Tuy nhiên, trong kịch bản Site – to – Site, sử dụng một phương thức xác thực dựa trên chứng chỉ số sẽ đạt được mức an toàn tốt nhất.

Để sử dụng xác thực EAP-TLS cho các kết nối mạng riêng ảo Site – to – Site, ta phải thực hiện các bước sau:

- Cài đặt dịch vụ cung cấp chứng chỉ cho người dụng trên mỗi Router gọi

- Cấu hình EAP-TLS trên Router gọi

- Cài đặt dịch vụ xác thức trên máy chủ xác thực(trên Router trả lời hoặc máy chủ RADIUS)

- Cấu hình EAP-TLS trên máy chủ xác thực và với chính sách bảo mật cho các kết nối site – to – site

7.2.2. Triển khai cơ sở hạ tầng Internet

Ý tưởng của các kết nối mạng riêng ảo Site – to – Site là sử dụng Internet như mạng trung gian cho các liên lạc mạng diện rộng của tổ chức, và như vậy loại trừ được đường thuê riêng chi phí đắt. Cơ sở hạ tầng Internet là phần mạng được kết nối trực tiếp tới mạng công cộng mà mạng riêng ảo sẽ được triển khai qua đó. Trong phần này, chúng ta sẽ xem xét tất cả các bước cho việc triển khai các Router VPN trên Internet. Triển khai cơ sở hạ tầng Internet cho các kết nối mạng riêng ảo bao gồm các bước sau:

- Đặt các Router VPN trong mạng vành đai hoặc trên Internet

- Cấu hình các giao diện Internet cho Router VPN

Bước đầu tiên trong việc triển khai các Router VPN là xác định vị trí đặt của chúng trong mối tương quan với Firewall Internet. Trong cấu hình thông dụng nhất, các Router VPN được đặt sau Firewall trên mạng vành đai giữa nhánh mạng của ta và Internet, ta cần phải cấu hình bộ lọc gói trên firewall để cho phép luồng lưu lượng mạng riêng ảo đến và đi từ địa chỉ IP của các giao diện mạng vành đai của Router VPN. Trên cả hai Server gọi và trả lời, ta đều phải thiết lập kết nối Internet. Với Card mạng kết nối tới Internet hay mạng vành đai, cấu hình giao thức

TCP/IP với một địa chỉ IP công cộng, một subnet mask và một cổng kết nối ngầm định của hoặc firewall hoặc một Router của ISP

7.2.2.1. Triển khai các Router trả lời

Chúng ta cần thiết lập Router trả lời với các cấu hình thích hợp cho một kết nối mạng riêng ảo Site – to – Site. Thủ tục bao gồm:

Cấu hình kết nối Router trả lời tới nhánh mạng và cài đặt dịch vụ định tuyến: Trên giao diện thứ 2 của Router trả lời, cấu hình card mạng kết nối tới nhánh mạng bằng cách cấu hình TCP/IP, bao gồm một địa chỉ IP, subnet mask, máy chủ DNS. Chú ý rằng, chúng ta không phải cấu hình cổng kết nối ngầm định trên các giao diện kết nối tới nhánh mạng. Nếu cấu hình một đường định tuyến ngầm định trên các giao diện kết nối tới nhánh mạng, nó sẽ tạo một đường định tuyến ngầm định đối lập với trong bản định tuyến và việc định tuyến tới Internet có thể không thực hiện đúng

Cấu hình giao diện kết nối :

Bây giờ chúng ta đã có những cơ sở về các dịch vụ định tuyến và các thiết lập TCP/IP trên Server. Chúng ta cần cấu hình đúng đắn giao diện mạng sẽ kiểm soát sự kích hoạt của kết nối mạng riêng ảo Site – to – Site.

7.2.2.2. Triển khai các Router gọi

Bây giờ chúng ta phải cấu hình cho Router gọi. Việc triển khai Router gọi cho một kết nối mạng riêng ảo Site – to – Site bao gồm các bước sau:

- Cấu hình kết nối của Router gọi tới nhánh mạng và cài đặt dịch vụ định tuyến: Cấu hình kết nối được kết nối tới nhánh mạng bằng việc cấu hình TCP/IP bao gồm một địa chi IP, một mặt nạ mạng con, các máy chủ DNS. Nếu ta cấu hình một đường định tuyến ngầm định trên kết nối nhánh mạng, nó sẽ tạo một đường định tuyến mặc định xung đột trong bảng định tuyến và việc định tuyến tới Internet có thể không thực hiện đúng

- Cấu hình giao diện: Dựa vào dịch vụ định tuyến, xác định tên cho giao diện, kiểu kết nối, giao thức đường hầm sẽ sử dụng, xác định địa chỉ đích là địa chỉ của Router trả lời, tạo các đường định tuyến tĩnh cho các mạng từ xa và gán các

đường định tuyến tĩnh cho giao diện, cung cấp các thông tin liên quan đến tài khoản người dùng cho việc xác thực kết nối về sau

7.2.3. Triển khai cơ sở hạ tầng AAA

Việc triển khai cơ sở hạ tầng AAA cho các kết nối mạng riêng ảo Site – to – Site bao gồm các bước sau:

- Cấu hình dịch vụ thư mục cho các tài khoản người dùng và các nhóm

- Cấu hình máy chủ xác thực Internet IAS

7.2.3.1. Cấu hình dịch vụ thư mục cho các tài khoản người dùng và các nhóm

Dịch vụ thư mục là tài nguyên trung tâm cho việc duy trì và kiểm soát tất cả các truy cập mạng, bao gồm cả các kết nối mạng riêng ảo Site – to – Site. Để cấu hình dịch vụ thư mục.

- Đảm bảo rằng tất cả các Router gọi đang tạo kết nối Site – to – Site có một tài khoản tương ứng

- Thiết lập các mức cho phép cho tài khoản người dùng trên mỗi Router gọi để cho phép hoặc từ chối truy cập để quản lý các truy cập từ xa của người dùng hoặc nhóm, thiết lập mức cho phép trên các tài khoản người dùng để kiểm soát truy cập qua chính sách truy cập từ xa.

- Tổ chức tài khoản người dùng trên Router gọi thành các nhóm thích hợp để thuận tiện trong việc áp dụng các chính sách truy cập từ xa.

7.2.3.2. Cấu hình máy chủ dịch vụ xác thực Internet(IAS)

Máy chủ dịch vụ xác thực Internet phải có khả năng truy cập đến các thông tin về thuộc tính của tài khoản. Nếu IAS được cài đặt riêng mà không phải trên máy chủ điều khiển miền, ta phải cấu hình để máy chủ IAS có thể đọc được các tài khoản của người dùng trong Domain

Nếu máy chủ IAS xác thực và cấp quyền cho các kết nối mạng riêng ảo với các tài khoản người dùng trong các Domain khác nhau, phải kiểm tra xem các Domain đó có một quan hệ tin cậy hai chiều với Domain mà máy chủ IAS là một thành viên hay không.

Nếu có các tài khoản trong các Domain khác và các Domain không có quan hệ tin cậy hai chiều với Domain mà máy chủ IAS là thành viên, ta phải cấu hình một RADIUS uỷ quyền giữa các Domain không có quan hệ tin cậy

7.2.4. Triển khai cơ sở hạ tầng mạng chi nhánh

Đến thời điểm này, chúng ta có các máy chủ VPN thiết lập và kết nối tới Internet, và chúng có khả năng xác thực mỗi tài khoản người dùng của các Server khác. Bây giờ chúng ta cần cấu hình các Router để chuyển tiếp luồng lưu lượng tới các mạng khác. Triển khai cơ sở hạ tầng mạng của một nhánh mạng với các kết nối mạng riêng ảo Site – to – Site bao gồm các bước sau

- Cấu hình định tuyến trên các Router VPN
- Kiểm tra khả năng nối tới được các Router VPN
- Cấu hình định tuyến cho các vùng địa chỉ thuộc mạng con ngoại lệ

7.2.4.1. Cấu hình định tuyến trên các Router VPN

Với các Router VPN để chuyển tiếp được luồng lưu lượng tới các vị trí trong nhánh mạng mà chúng được đặt vào, ta phải cấu hình chún với các đường định tuyến tĩnh khác nhau, những đường định tuyến tĩnh này tổng kết tất cả những địa chỉ có thể được dùng trên các nhánh mạng khác hoặc với các giao thức định tuyến và như vậy Router VPN có thể hoạt động như một Router động và tự động thêm các đường định tuyến cho các nhánh mạng con vào bảng định tuyến của nó

7.2.4.2. Kiểm tra khả năng kết nối tới được mỗi Router VPN

Từ mỗi Router VPN, kiểm tra xem Router VPN có khả năng phân giải tên và liên lạc thành công với các tài nguyền trong nhánh mạng của Router VPN hay không

7.2.4.3. Cấu hình định tuyến cho vùng địa chỉ IP ngoại lệ

Nếu đã cấu hình các Router VPN với một vùng địa chỉ tĩnh và vùng này thuộc vùng mạng con ngoại lệ, ta phải đảm bảo rằng đường định tuyến hoặc các vùng địa chỉ thuộc mạng con ngoại lệ mô tả các đường định tuyến được mô tả trong cơ sở hạ tầng định tuyến nhánh mạng của ta. Điều này được yêu cầu để kết nối tới được các

giao diện ảo của các Router gọi. Ta có thể đảm bảo điều này bằng việc bổ sung các đường định tuyến tĩnh hoặc các vùng địa chỉ thuộc vùng mạng con ngoại lệ mô tả các đường định tuyến như các đường định tuyến tĩnh tới các Router kế cận của các Router VPN và sau đó sử dụng giao thức định tuyến của nhánh mạng chúng ta để phân phôi đường định tuyến tới các Router khác. Khi ta bổ sung các đường định tuyến tĩnh, ta phải xác định cổng kết nối là giao diện nhánh mạng của Router VPN.

7.2.5. Triển khai cơ sở hạ tầng mạng ngoài chi nhánh

Mỗi Router cần biết về các đường định tuyến trong các nhánh mạng của các Router VPN khác và như vậy nó có thể chuyển tiếp đúng luồng lưu lượng tới các phía khác của kết nối mạng riêng ảo. Việc triển khai cơ sở hạ tầng ngoài chi nhánh bao gồm việc cấu hình mỗi Router VPN với tập các đường định tuyến cho các mạng con sẵn dùng trong các nhánh mạng khác. Điều này có thể thực hiện được theo các cách sau đây :

- Cấu hình thủ công các đường định tuyến trên mỗi Router VPN
- Thực hiện việc cập nhật tự động trên mỗi Router VPN
- Cấu hình giao thức định tuyến để hoạt động qua kết nối mạng riêng ảo

7.3. Xây dựng mạng riêng ảo chi nhánh

7.3.1. Mạng riêng ảo với các văn phòng chi nhánh không kết nối thường xuyên

7.3.1.1. Giới thiệu chung

Trong các chương trước, chúng ta đã thực hiện thiết lập các truy cập từ xa giữa các máy chủ mạng riêng ảo và các Client mạng riêng ảo. Chương này chúng ta xem xét các kết nối giữa các văn phòng chi nhánh ở xa

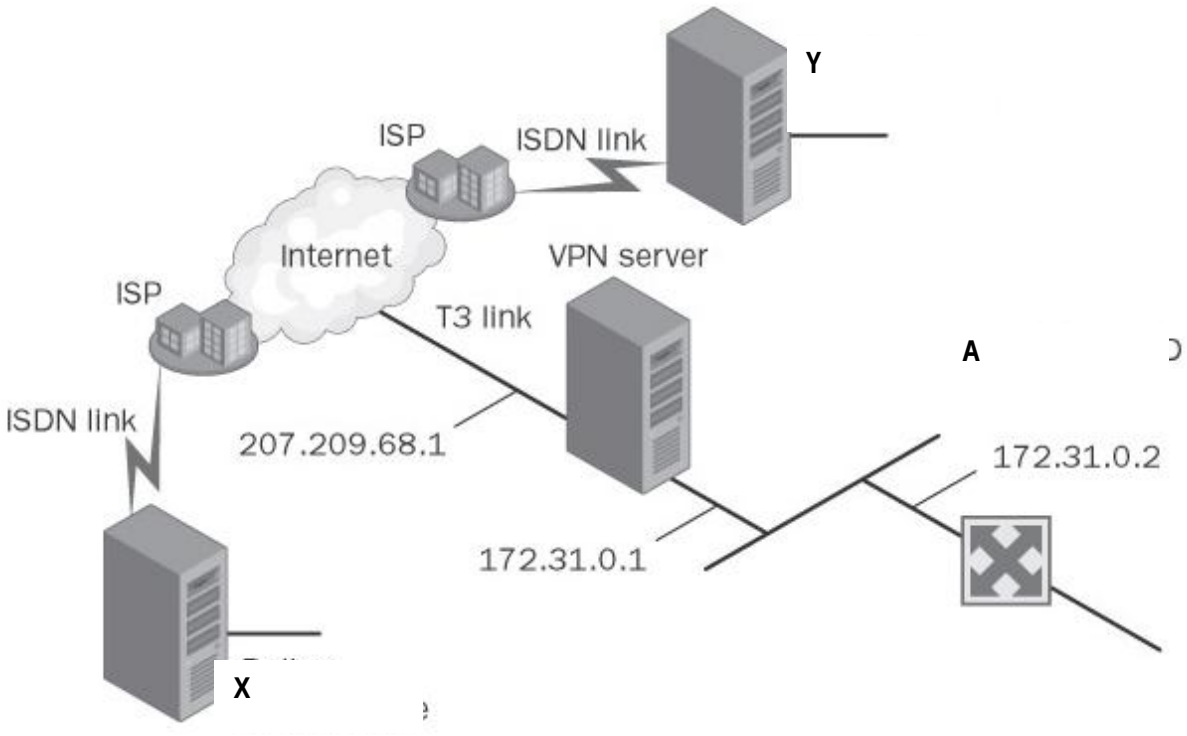
Giả sử có hai nhánh văn phòng ở xa X và Y của một Tổng công ty A được kết nối tới văn phòng trung tâm của Tổng công ty. Mỗi một nhánh văn phòng có một số nhân viên thỉnh thoảng cần kết nối với văn phòng trung tâm (Với ít hơn 10 người dùng tại một nhánh mạng, người dùng nên sử dụng hình thức truy cập từ xa. Điều này cho phép tổng công ty không phải hỗ trợ các dịch vụ dựa trên máy chủ từ xa tại văn phòng chi nhánh. Với nhiều hơn 10 người, kết nối dạng site – to – site với một máy chủ chuyên dụng là mô hình được ưa thích). Bộ định tuyến trong các

chi nhánh X và Y được yêu cầu với một card mạng tích hợp dịch vụ số (ISDN) để quay số tới một ISP để giành quyền truy cập tới Internet. Khi truy cập đã giành được, một kết nối mạng riêng ảo được tạo qua Internet.

Nhánh văn phòng X sử dụng địa chỉ mạng 192.168.28.0 với một mặt nạ mạng 255.255.255.0 (192.168.28.0/24). Nhánh văn phòng Y sử dụng địa chỉ mạng 192.168.4.0 với một mặt nạ mạng 255.255.255.0 (192.168.4.0/24)

Để đơn giản hoá việc cấu hình, các kết nối mạng riêng ảo là một kết nối được khởi tạo một chiều, đó là luôn được khởi tạo bởi Router tại nhánh văn phòng. Điều này thích hợp hơn kết nối được khởi tạo 2 chiều vì nhánh văn phòng không phải sử dụng một kết nối Internet liên tục và vì vậy tiết kiệm được chi phí (Trong nhiều trường hợp ngày nay. một nhánh văn phòng có thể sử dụng ADSL hoặc Modem cho kết nối và như vậy duy trì trạng thái kết nối liên tục, như vậy xem những tuỳ chọn nào là sẵn có cho kịch bản của ta và các kết nối văn phòng chi nhánh).

Sơ đồ kịch bản kết nối được mô tả như trong hình 7.1



7.3.1.2. Các công việc cài đặt

7.3.1.2.1. Cấu hình cho máy chủ mạng riêng ảo

Để triển khai máy chủ mạng riêng ảo tại mạng trung tâm của Tổng công ty, ta cần thực hiện các công việc sau:

- Cấu hình mạng

- Cấu hình Domain

- Cấu hình bảo mật

1. Cấu hình mạng

Việc cấu hình mạng xác định tất cả thông tin liên lạc cốt yếu, chẳng hạn mạng và địa chỉ Node, định tuyến, mạng con và thông tin mạng WAN khác. Những phần cốt yếu của cấu hình mạng là:

- Intranet của tổng công ty sử dụng địa chỉ mạng riêng 172.16.0.0 với một subnetmask 255.254.0.0 (172.16.0.0/12)

- Máy chủ mạng riêng ảo kết nối trực tiếp với Internet sử dụng một liên kết WAN chuyên dụng T3. Tại mạng chính, VPN Router phải phân phối tất các các kết nối hiện tại.

- Cấu hình địa chỉ IP của card mạng WAN trên Internet, chẳng hạn là 207.209.68.1 Địa chỉ này được cấp phát bởi ISP, địa chỉ IP của card mạng WAN được tham chiếu trên Internet bằng một tên miền(Chẳng hạn vpn.coA.com)

- Máy chủ mạng riêng ảo kết nối trực tiếp tới mạng Intranet chứa một bộ định tuyến kết nối phần còn lại của mạng Intranet. Cấu hình phân mạng Intranet có định danh mạng là 172.31.0.0 với subnetmask 255.255.0.0 (172.31.0.0/16)

- Máy chủ mạng riêng ảo được cấu hình với một vùng địa chỉ IP tĩnh để cấp phát tới các bộ định tuyến là một tập con của phân mạng Intranet

Bước đầu tiên trong việc triển khai máy chủ mạng riêng ảo là cài đặt cấu hình vật lý và lôgic cho máy chủ mạng riêng ảo. Dựa trên cấu hình mạng Intranet của tổng công ty, máy chủ này được cấu hình như sau:

Cài đặt phần cứng trên máy chủ mạng riêng ảo

Card mạng dùng để kết nối tới phân mạng Intranet và card mạng kết nối tới Internet được cài đặt đúng. Ta giả định sử dụng T3 để kết nối máy chủ mạng riêng ảo với Internet. Chúng ta sẽ xem nó như một card mạng WAN

Cấu hình TCP/IP trên card mạng LAN và WAN

Xác định địa chỉ IP cho card mạng LAN, chẳng hạn sử dụng địa chỉ IP là 172.31.0.1 với một subnetmask là 255.255.0.0.

Xác định địa chỉ IP cho card mạng WAN, chẳng hạn là 207.209.68.1 với mặt nạ mạng là 255.255.255.255

DNS cũng được cấu hình và nên hướng vào dịch vụ DNS bên trong của Công ty. Trình phân giải địa chỉ bên ngoài nên được chuyển tiếp bởi máy chủ DNS bên trong tới một người có thẩm quyền bên ngoài

Cấu hình dịch vụ định tuyến

Để cấu hình dịch vụ định tuyến trên máy chủ mạng riêng ảo sử dụng các thiết lập sau:

- Kết nối mạng riêng ảo, xem xét đến kết nối tương ứng với giao diện được kết nối tới Internet

- Gán địa chỉ IP, thông thường xác định một phạm vi địa chỉ, chẳng hạn từ 172.31.255.1 tới 172.31.255.254, nghĩa là tạo ra một vùng địa chỉ tĩnh cho 254 Client VPN, hoặc sử dụng giao thức cấu hình Host động(DHCP) để phân phối địa chỉ IP cho các Client

Cấu hình đường định tuyến tĩnh trên máy chủ để kết nối liên lạc giữa Intranet và Internet

Không có các đường định tuyến tĩnh, chỉ mạng con cục bộ sẽ được coi như các Client VPN. Máy chủ VPN cần biết về tất cả các mạng con mà Client có thể cần kết nối đến và vì vậy đòi hỏi phải có các đường định tuyến tĩnh.

Để kết nối được tới các vị trí trong Intranet, một đường định tuyến tĩnh được tạo với các thiết lập cho:

- Giao diện mạng: Card mạng LAN kết nối với Intranet

- Địa chỉ dích: Chẳng hạn, 172.16.0.0

- Mặt nạ mạng: Chẳng hạn, 255.240.0.0

- Gateway: Chẳng hạn, 172.31.0.2

Đường định tuyến tĩnh làm đơn giản hoá việc định tuyến bằng cách tổng kết tất cả các đích trên mạng Intranet của tổng công ty. Kỹ thuật này được biết như là bộ tổng hợp định tuyến. Đường định tuyến tĩnh này được sử dụng mà máy chủ mạng riêng ảo không cần được cấu hình với một giao thức định tuyến.

Để kết nối tới được các vị trí trên Internet, một đường định tuyến được tạo với các thiết lập cho:

- Giao diện mạng trên Card mạng WAN kết nối tới Internet

- Địa chỉ đích

- Mặt nạ mạng

- Gateway

Đường định tuyến này tổng hợp tất cả các đích trên Internet và sẽ cho máy chủ mạng riêng ảo gửi bất kỳ đích nào "chư biết" được yêu cầu ra Internet cho trình phân giải tên. Đường định tuyến này cho phép máy chủ mạng riêng ao phản hồi một Client từ xa hoặc một Router yêu cầu quay số từ bất kỳ nơi nào trên Internet. Việc sử dụng các đường định tuyến tĩnh thay cho Default Gateway thiết lập trên các giao diện, nên có thể bỏ trống. Các đường định tuyến tĩnh sẽ không bị đè bởi bất kỳ cấu hình tự động nào

Cấu hình một đường định tuyến tĩnh trên Router Intranet để kết nối được với các văn phòng chi nhánh.

Để kết nối được với các văn phòng chi nhánh từ Router Intranet, một đường định tuyến tĩnh được tạo theo các thiết lập theo các thông số cần thiết:

- Giao diện mạng LAN kết nối tới Intranet

- Địa chỉ đích, chẳng hạn 192.168.0.0

- Mặt nạ mạng, chẳng hạn 172.31.0.1

Đường định tuyến tĩnh này làm đơn giản hoá việc định tuyến bằng cách tổng hợp tất cả các đích tại văn phòng chi nhánh của Tổng công ty. Router Intranet phân phối đường định tuyến tĩnh này tới các Router lân cận của nó, và như vậy một đường định tuyến tới các văn phòng chi nhánh tồn tại trên mỗi Router của Intranet. Đây là cách tất cả các tài nguyên bên trong sẽ biết cách tìm các nhánh văn phòng ở xa. Bằng cách phân phối đường định tuyến này, máy chủ mạng riêng ảo có thể kiểm soát tất cả luồng lưu lượng tới các văn phòng ở xa.

2. Cấu hình Domain

Để thuận tiện cho việc áp dụng các thiết lập kết nối khác nhau với các kiểu kết nổi mạng riêng ảo khác nhau, với kết nối mạng riêng ảo tới văn phòng A, trên máy chủ Domain ta thực hiện

- Tạo tài khoản người dùng, chẳng hạn VPN_A

- Với các thuộc tính quay số trên tài khoản VPN_A, mức cho phép truy cập từ xa được thiết lập và đường định tuyến tĩnh 192.168.28.0 với một mặt nạ mạng 255.255.255.0 được thêm vào.

- Các tài khoản nên được tạo theo nhóm

3. Cấu hình bảo mật

Để cho phép các kết nối L2TP/IPSec, Domain tổng công ty được cấu hình đê tự động nạp các chứng chỉ tới tất cả các thành viên của Domain

4. Cấu hình chính sách truy cập từ xa

Để định nghĩa các thiết lập mã hoá và xác thực cho các Router mạng riêng ảo, ta tạo chính sách truy cập từ xa với các thông tin cần quan tâm:

- Tên chính sách

- Phương pháp truy cập, chẳng hạn VPN

- Người dùng hoặc nhóm truy cập

- Phương pháp xác thực

- Mức mã hoá chính sách, thường chọn mức mã hoá mạnh hoặc mạnh nhất

Những mô hình ở phần trên, ta mô tả một kết nối văn phòng chi nhánh dựa trên PPTP cho nhánh văn phòng X và một kết nối văn phòng chi nhánh dựa trên L2TP/IPSec cho văn phòng Y. Qua mô tả kịch bản này, chúng ta có thể bao trùm tất cả cơ sở cho việc triển khai. Muốn an toàn nhất, L2TP/IPSec với các chứng chỉ số là giải pháp được khuyến cáo. Nhiều nhà cung cấp đề xuất chế độ đường hầm IPSec cho hoạt động này nhưng nó bị từ chối vì lý do an toàn bởi IETF

7.3.1.2.2. Kết nối văn phòng chi nhánh dựa trên PPTP

Nhánh văn phòng X là một nhánh văn phòng dựa trên PPTP, kết nối tới máy chủ mạng riêng ảo tại tổng công ty.

Để triển khai một PPTP, khởi tạo một chiều, tại Router trên nhánh văn phòng A ta thực hiện cấu hình:

1. Cấu hình giao diện cho kết nối tới ISP

Để kết nối Router tại văn phòng A tới Internet qua một ISP cục bộ, một giao được thiết lập như sau:

- Tên giao diện: chẳng hạn ISP

- Kiểu kết nối: Sử dụng Modem, ISDN hoặc thiết bị vật lý khác

- Lựa chọn một thiết bị: Chọn một thiết bị ISDN thích hợp

- Số điện thoại: Số điện thoại của ISP cho nhánh văn phòng A

- Các đường định tuyến tĩnh cho mạng ở xa

+ Để tạo kết nối tới ISP của nhánh văn phòng A lúc kết nối mạng riêng ảo cần được thiết lập, ta tạo ra đường định tuyến tĩnh tại Router văn phòng A

- Giấy uỷ nhiệm quay số ra ngoài, bao gồm các thông tin

+ Username: là tên tài khoản mà ISP cấp cho nhánh văn phòng A

+ Password: Mật khẩu tương ứng

+ Xác minh lại mật khẩu tương ứng

2. Cấu hình giao diện cho kết nối mạng riêng ảo

Để kết nối Router nhánh văn phòng A tới máy chủ mạng riêng ảo tại trung tâm sử dụng kết nối mạng riêng ảo qua Internet, người quản trị mạng trung tâm phải tạo một giao diện quay số với các tham số thông thường như:

- Tên giao diện

- Kiểu kết nối: Kết nối sử dụng VPN

- Kiểu mạng riêng ảo, do đây là kết nối dựa trên PPTP nên chọn giao thức phải là PPTP

- Địa chỉ đích, là giao diện mạng thứ 2 kết nối với Internet tại máy chủ VPN trên trung tâm

- Xác định giao thức và tính an toàn được dùng

- Các đường định tuyến tĩnh cho các mạng từ xa

Để làm cho tất cả các vị trí trên Intranet tổng công ty có thể kết nối tới được, ta tạo ra đường định tuyến tĩnh. Trong đó có các tham số cần quan tâm như:

+ Địa chỉ đích phải là định danh mạng của tổng công ty, chẳng hạn 172.16.0.0

+ Mặt nạ mạng, chẳng hạn là 255.240.0.0

Để là cho tất cả các vị trí trên các nhánh văn phòng có thể kết nối tới được, ta cũng tạo ra đường định tuyến tĩnh, với địa chỉ đích phải là địa chỉ mạng của các nhánh văn phòng, chẳng hạn 192.168.0.0; mặt nạ mạng là 255.255.0.0

- Giấy uỷ quyền quay số ra ngoài, sử dụng cho tài khoản trên Domain của tổng công ty

7.3.1.2.3. Kết nối chi nhánh văn phòng dựa trên L2TP/IPSec

Nhánh văn phòng Y là một kết nối dựa trên L2TP/IPSec, kết nối mạng riêng ảo với mãy chủ mạng riêng ảo tại tổng công ty.

Để triển khai một kết nối mạng riêng ảo khởi tạo một chiều dựa trên L2TP/IPSec tới văn phòng trung tâm dựa trên cấu hình thiết lập máy chủ mạng riêng ảo như phần 7.2.1, ta thực hiện cấu hình trên nhánh văn phòng A như sau:

1. Cấu hình chứng chỉ

Bộ định tuyến trên nhánh văn phòng Y được cấu hình bởi người quản trị mạng của tổng công ty trong khi nó được kết nối vật lý với Intranet của tổng công ty. Sau đó nó được vận chuyển tới nhánh mạng văn phòng Y. Trong khi bộ định tuyến tại nhánh văn phòng Y được kết nối tới Intranet của tổng công ty, một chứng chỉ số được cài đặt. Đây là điểm quan trọng cần nhớ, đặc biệt nếu ta đang thực hiện các kết nối khởi tạo hai chiều trên mỗi phần cấu hình bộ định tuyến từ xa, trong khi nó vẫn còn kết nối tới Intranet trung tâm, đồng bộ hoá toàn bộ người dùng trên mỗi Domain, sau đó vận chuyển máy chủ mạng riêng ảo tới nhánh mạng từ xa.

2. Cấu hình giao diện cho kết nối tới ISP

Để kết nối bộ định tuyến trên nhánh văn phòng Y tới Internet qua một ISP cục bộ, người quản trị phải thiết lập giao diện mạng thích hợp với các tham số:

- Tên giao diện, thường lấy tên của ISP

- Kiểu kết nối, dùng một Modem, Card ISDN hay thiết bị vật lý khác

- Lựa chọn một thiết bị thích hợp, chẳng hạn thiết bị ISDN

- Số điện thoại, số điện thoại của ISP cho nhánh văn phòng Y

- Các giao thức và tính năng an toàn

- Các đường định tuyến tĩnh cho các mạng từ xa: Để tạo kết nối cho nhánh văn phòng Y tới ISP lúc kết nối mạng riêng ảo cần được tạo, ta phải tạo ra các đường định tuyến tĩnh tới mạng trung tâm với các tham số cần quan tâm như:

+ Mạng đích: chính là mạng trung tâm ở tổng công ty, chẳng hạn trong ví dụ trên là 207.209.68.1

+ Mặt nạ mạng, chẳng hạn 255.255.255.255 tuỳ thuộc vào địa chỉ của mạng đích

- Các giấy uỷ quyền quay số ra ngoài, liên quan đến tài khoản người dùng do ISP cung cấp

3. Cấu hình giao diện cho kết nối mạng riêng ảo

Để kết nối bộ định tuyến tại nhánh văn phòng Y tới máy chủ mạng riêng ảo dùng kết nối mạng riêng ảo qua Internet, người quản trị phải tạo một giao diện kết nối thích hợp với các tham số cơ bản như sau:

- Tên giao diện: Có thể lấy thêm của tổng công ty, để phân biệt và tránh nhầm lẫn khi dùng

- Kiểu kết nối: chọn kiểu VPN

- Kiểu mạng riêng ảo: Đây đang là kết nối mạng riêng ảo dựa trên L2TP nên ta chọn là L2TP

- Địa chỉ đích: là địa chỉ giao diện mạng kết nối với Internet của máy chủ mạng riêng ảo, chẳng hạn 207.209.68.1

- Các đường định tuyến tĩnh cho mạng từ xa:

+ Để làm cho tất cả các vị trí trên mạng Intranet của Tổng công ty có thể kết nối tới được, ta phải tạo ra các đường định tuyến tĩnh thích hợp với các tham số cần được quan tâm như sau:

* Địa chỉ mạng đích, đây chính là định danh mạng Intranet tại tổng công ty, trong mô hình kết nối của ta thì đó là 172.16.0.0

* Mặt nạ mạng tương ứng của mạng đích, chẳng hạn 255.240.0.0

+ Để làm cho tất cả các vị trính trên nhánh văn phòng Y có thể kết nối tới được, ta phải tạo đường định tuyến tĩnh đến chúng, Cụ thể:

* Mạng đích, là mạng Intranet của nhánh văn phòng Y, trong ví dụ trên là 192.168.0.0

* Mặt nạ mạng: chẳng hạn là 255.255.0.0

- Giấy uỷ quyền quay số ra ngoài, với các thông tin liên quan đến người dùng của nhánh văn phòng Y

7.3.2. Các văn phòng chi nhánh kết nối thường xuyên

Các văn phòng chi nhánh X và Y của tổng công ty A được kết nối với văn phòng trung tâm bằng các kết nối mạng riêng ảo thường xuyên, 24/24 mỗi ngày. Các bộ định tuyến trên các nhánh văn phòng X và Y tương đương với các Card mạng WAN T1 kết nối thường trực tới một ISP cục bộ để truy cập tới Internet. Trong thị trường liên lạc ngày nay, nhiều công ty sử dụng ADSL hoặc hoặc Modem điện thoại cho những chức năng này vì 2 lý do: chi phí rẻ hơn nhiều bởi vì chi phí của kết nối Internet với ADSL và Modem điện thoại rẻ hơn so với đường thuê riêng T1, và chúng cung cấp lượng băng thông tối thiểu tương đối tốt, tương đương băng thông một kênh kép ISDN 128-kb/s.

Nhánh văn phòng X sử dụng địa chỉ IP có định danh mạng là 192.168.9.0 với một mặt nạ mạng là 255.255.255.0(192.168.9.0/24). Router tại nhánh văn phòng này sử dụng địa chỉ IP công cộng là 131.107.0.1 cho giao diện kết nối Internet của nó. Nhánh văn phòng Y sử dụng một địa chỉ IP có phầm mạng là 192.168.14.0 với một mặt nạ mạng 255.255.255.0 (192.168.14.0/24). Router tại nhánh văn phòng Y sử dụng địa chỉ IP công cộng là 157.60.0.1 cho giao diện kết nối tới Internet

Kết nối mạng riêng ảo là một kết nối được khởi tạo 2 chiều, được khởi tạo hoặc từ các nhánh văn phòng hoặc từ máy chủ mạng riêng ảo. Các kết nối được khởi tạo 2 chiều yêu cầu tạo các giao diện mạng, chính sách truy cập từ xa và vùng địa chỉ IP tĩnh trên các Router ở cả 2 phía của kết nối

7.3.2.1. Cấu hình máy chủ mạng riêng ảo

Để triển khai các kết nối mạng riêng ảo đối tác để kết nối Công ty X, Y với mạng mở rộng của Tổng công ty A với kết nối cố định, máy chủ mạng riêng ảo được thiết lập theo cấu hình cơ bản như trong mục 7.3.1.2.1 của chương VII. Ngoài ra cần phải cấu hình thêm như sau:

1. Cấu hình Domain

Tạo 3 tài khoản người dùng trên máy chủ mạng riêng ảo và đưa vào cùng một nhóm. Cụ thể:

Với kết nối mạng riêng ảo của nhánh văn phòng X được khởi tạo bởi Router của nó, tài khoản người dùng được tạo với các thiết lập về: mật khẩu; mức cho phép truy cập được thiết lập để kiểm soat truy cập qua chính sách truy cập từ xa; tài khoản này được thêm vào nhóm thích hợp

Với kết nối mạng riêng ảo của nhánh văn phòng Y được khởi tạo bởi Router của nó, ta cũng tạo tài khoản người dùng với các thiết lập về: mật khẩu, mức cho phép truy cập từ xa được thiết lập để kiểm soát truy cập qua chính sách truy cập từ xa; tài khoản này cũng được thêm vào nhóm thích hợp

Với kết nối mạng riêng ảo tới nhánh văn phòng X và Y được khởi tạo bởi Server VPN, ta cũng tạo tà khoản với các thiết lập về: mật khẩu, mức cho phép truy cập từ xa để kiểm soát truy cập qua chính sách truy cập từ xa; tài khoản này cũng được thêm vào nhóm thích hợp

2. Cấu hình chính sách truy cập từ xa

Vì có các kết nối 2 chiều, các chính sách truy cập từ xa phải được cấu hình tại máy chủ VPN, Router trên nhánh văn phòng X và Y, các chính sách này có tên giống nhau

Cấu hình chính sách truy cập từ xa trên máy chủ VPN:

Việc cấu hình này giống với trong các nhánh văn phòng kết nối không thường xuyên

Cấu hình chính sách truy cập từ xa trên Router của nhánh văn phòng X và Y:

Để định nghĩa các thiết lập mã hoá và xác thực cho các kết nối mạng riêng ảo, chính sách truy cập từ xa được tạo trên các nhánh văn phòng với các tham số cần lưu ý như sau:

- Tên chính sách

- Phương pháp truy cập

- Người dùng hoặc nhóm được truy cập: ta chọn nhóm mà 3 tài khoản đã tạo ở trên là thành viên

- Các phương pháp xác thực

- Mức mã hoá: Thường chọn mã hoá mạnh hoặc mạnh nhất

3. Cấu hình vùng địa chỉ IP

Các vùng địa chỉ IP phải được cấu hình tại máy chủ VPN, Router trên nhánh văn phòng X và Y như sau:

Cấu hình vùng địa chỉ IP tại máy chủ VPN:

Việc cấu hình vùng địa chỉ IP cho máy chủ VPN hoàn toàn giống như trong phần 7.3.1.2.1

Cấu hình vùng địa chỉ IP trên Router của nhánh văn phòng X:

Một vùng địa chi IP tĩnh, chẳng hạn từ 192.168.9.248 đến 192.168.9.253 được cấu hình

Cấu hình vùng địa chỉ IP trên Router của nhánh văn phòng Y:

Một vùng địa chi IP tĩnh, chẳng hạn từ 192.168.14.248 đến 192.168.14.253 được cấu hình

7.3.2.2. Cấu hình kết nối dựa trên PPTP

Nhánh văn phòng X là một nhánh văn phòng dựa trên PPTP sử dụng một Router VPN để tạo một kết nối mạng riêng ảo cố định với máy chủ mạng riêng ảo ở văn phòng trung tâm

Để triển khai một kết nối mạng riêng ảo PPTP được khởi tạo một chiều ta cấu hình trên máy chủ mạng riêng ảo và trên Router tại nhánh X như sau:

7.3.2.2.1. Cấu hình máy chủ mạng riêng ảo

Máy chủ mạng riêng ảo được cấu hình với một giao diện, các đường định tuyến tính và các bộ lọc gói PPTP

Cấu hình giao diện cho kết nối mạng riêng ảo: