CÔNG TY PHÁT TRIỂN CÔNG NGHỆ TIN HỌC THIÊN LONG.
TRUNG TÂM ĐÀO TẠO CHUYÊN VIÊN CÔNG NGHỆ THÔNG TIN.
180 Lê Thanh Nghị - Bách Khoa - Hà Nội.
ĐT: 6280725. Email:thienlongcom@hn.vnn.vn
http://www.thienlongcomputer.com
****

GIÁO TRÌNH ĐÀO TẠO QUẢN TRỊ VIÊN MẠNG WIN 2000 ADVANCE SERVER

Con đường hướn tới tương lai.

Hà Nội, 15/04/2003.

Mở đầu.

Hệ điều hành Windows 2000 Server được phát triển từ nhu cầu cấp thiết của các cơ quan tổ chức muốn có một thế hệ mới các ứng dụng Client/Server, những ứng dụng sẽ cho phép họ xây dựng những ưu thế cạnh tranh mạnh mẽ. Họ đòi hỏi nhiều hơn chứ không phải chỉ đơn thuần là việc nối các máy tính cá nhân lại với nhau hay đưa các ứng dụng từ các máy lớn xuống. Họ cần một nền tảng ổn định với máy chủ quản lý cục bộ, mạng diện rộng với các máy chủ cho các ứng dụng. Xét cho cùng, người sử dụng muốn có ngay lập tức những thông tin mà họ cần và phục vụ những yêu cầu nghiệp vụ riêng biệt.

Với Windows 2K Server: Thông tin ở ngón tay của bạn.

Windows 2K Server kết hợp các khả năng về tệp và in ấn của Novell NetWare với những dịch vụ ứng dụng của UNIX trên một hệ điều hành mạng đa mục đích. Như một máy chủ tệp và in ấn cực kỳ nhanh, W2KS cho phép bạn chia sẻ thông tin cũng như truy cập máy in và các thiết bị khác trên mạng đồng thời cung cấp nền tảng cơ sở hạ tầng ứng dụng cho phép bạn mua hoặc xây dựng các giải pháp nghiệp vụ.

W2KS hỗ trợ hàng loạt các giải pháp nghiệp vụ then chốt của các hãng phần mềm nổi tiếng khác như Oracle, Sybase...Đồng thời nó là thành viên của họ các ứng dụng chủ tích hợp Microsoft BackOffice bao gồm hệ quản trị dữ liệu phân tán SQL Server, Email Server, quản trị các hệ thống, phần cứng, phần mềm trong mạng SMS, hệ kết nối các máy tính lớn và máy Mini của IBM là SNA Server, hệ quản lý các thông tin siêu văn bản - WebServer (IIS), ứng dụng chủ về bảo mật, kiểm soát thông tin, kinh doanh trực tuyến...

Bài 1:

Những nhiệm vụ và các công cụ quản trị của Windows 2K.

Quản trị Windows 2K Server bao gồm những công việc phải tiến hành sau khi cài đặt mạng và các công việc bảo trì hàng ngày. Những nhiệm vụ quản trị bao gồm:

- *Quản trị các khoản mục người sử dụng và khoản mục nhóm.*
  Hoạch định, khởi tạo và duy trì các khoản mục người sử dụng và khoản mục nhóm để bảo đảm cho người sử dụng có thể đăng nhập cũng như truy nhập được vào các tài nguyên cần thiết cho công việc của họ.
- *Quản trị việc bảo mật.*
  Hoạch định, triển khai và áp đặt một số chính sách bảo mật nhằm bảo vệ dữ liệu cũng như các tài nguyên dùng chung trên mạng bao gồm các tệp, thư mục hay máy in...
- *Quản trị máy in.*
  Cài đặt các máy in cục bộ, máy in mạng để đảm bảo cho người sử dụng có thể dễ dàng và nhanh chóng truy nhập và in. Giải quyết các sự cố về in ấn.
- *Quan sát và điều phối các sự kiện, các tài nguyên trên mạng.*
  Hoạch định và triển khai chính sách theo dõi, kiểm soát các sự kiện xảy ra trên mạng liên quan đến các vấn đề bảo mật. Theo dõi và điều khiển việc sử dụng các tài nguyên mạng.
- *Sao lưu và phục hồi dữ liệu.*
  Hoạch định, lập lịch và thực hiện việc sao lưu định kỳ để đảm bảo phục hồi nhanh chóng dữ liệu nếu xảy ra sự cố.

Các công cụ quản trị (Administrative Tools) trong Windows 2KServer sẽ giúp cho người quản trị quản trị hệ thống của họ. Các công cụ quản trị có thể được cài đặt lên máy trạm!

Quản trị vùng.

Việc điều hành, quản lý vùng của người quản trị bao gồm việc quản lý các cá nhân và bảo trì các máy chủ làm việc trong vùng đó. Người quản trị phải đảm bảo cho người sử dụng điều kiện làm việc tốt nhất, dễ dàng truy nhập và khai thác các tài nguyên dùng chung trong khi vẫn bảo mật được các tài nguyên cá nhân, các thông tin quan trọng của cơ quan, tổ chức.
Để làm được việc này, người quản trị phải có sách lược hợp lý trong việc tạo ra môi trường làm việc thích hợp cho từng đối tượng người sử dụng, phân nhóm và quản lý các nhóm, gán quyền và thay đổi quyền cho các nhóm, các cá nhân, đồng bộ và bảo trì máy chủ.

Bài 2.
Quản lý tài nguyên.

Tài nguyên tệp và thư mục:

- *Các hệ thống tệp được Windows 2000 hỗ trợ.*
  + Hệ thống tệp FAT
  + Hệ thống tệp NTFS
- *Bảo mật các tài nguyên mạng thông qua các cho phép chia sẻ.*
  + Chia sẻ các thư mục.
  + Đặt cho phép trên các thư mục được chia sẻ.
  + Nối tới các thư mục được chia sẻ
- *Dùng chế độ bảo mật của NTFS.*
  + Sử dụng các cho phép NTFS..
  + Các mức cho phép truy nhập.
  + Kết hợp các cho phép chia sẻ và cho phép NTFS.

Máy chủ in ấn trên mạng:

- *Thiết lập máy chủ in ấn trên mạng.*
  + In ấn trong môi trường Windows 2000.
  + Thiết lập các máy chủ, máy trạm in ấn.
  + Đặt cấu hình máy in.
- *Quản trị máy chủ in ấn trên mạng.*
  + Những công việc quản trị máy chủ in ấn.
  + Quản lý các tài liệu in.
  + Quản lý máy in.

Bài 3. Các công cụ quản trị

Các công cụ quản trị có thể được cài đặt trên máy chủ hoặc cài đặt trên máy trạm (Cài đặt Administrative Tools).
Các công cụ quản trị có thể không xuất hiện trong nhóm công cụ quản trị. Chúng bao gồm những công cụ thường dùng và những công cụ quản trị nâng cao.

- *Component Services.*
- *Computer Management.*
- *Configure Your Server.*
- *Data Source (ODBC).*
- *Distributed File System.*
- *Event Viewer.*
- *Internet Services Manager.*

Bài 4. Các công cụ quản trị

- *Licensing.*
- *Local Security Policy.*
- *Performance.*
- *Routing And Remote Accsess.*
- *Server Extention Administrator.*
- *Services.*
- *Telnet Server Administrator.*
- *Active Directory User And Computer.*
- *Active Directory Sites And Services*.

Bài 5. Giao thức mạng.

- *Lựa chọn giao thức.*
- *Cài đặt giao thức.*
- *Cấu hình giao thức mạng.*

Bài tập và thực hành.
Bài tập tổng hợp 1.

Bài 6. Windows 2KAV và Internet.

- *Internet.*
- *Intranet.*
- *Bảo mật.*
- *Webserver:*
  + Chức năng.
  + Cài đặt.
  + Cấu hình.
  + Quản trị.

Bài 7. Dịch vụ truy nhập từ xa - RAS.

- *Kết nối mạng diện rộng.*
- *Các giao thức.*
- *Các cổng nối và bộ dẫn đường.*
- *Bảo mật.*
- *Cài đặt RAS.*
- *Cấu hình RAS chủ.*
- *Cấu hình RAS để sử dụng các giao thức riêng biệt.*
- *Cài đặt các cho phép truy nhập từ xa.*

Bài 8. Dịch vụ mạng.

- *Dịch vụ cung cấp địa chỉ động - DHCP.*
  + *Cơ chế hoạt động.*
  + *Cài đặt dịch vụ.*
  + *Cấu hình dịch vụ.*
  + *Cấu hình các địa chỉ IP dự trữ.*
- *Dịch vụ tên Internet WINS.*
  + *Cơ chế hoạt động.*
  + *Cài đặt dịch vụ.*
  + *Cấu hình dịch vụ.*
  + *Kết hợp với DNS.*

Bài 9. Sự cố và giải quyết sự cố.

- *Sự cố đăng nhập.*
- *Không truy nhập được tài nguyên.*
- *Lỗi in ấn qua mạng.*
- *.....*

Bài 10. Một số phương pháp kiểm tra độ an toàn của mạng.

- *Đứng bên trong mạng: Administrator.*
- *Đứng bên ngoài mạng: Hacker.*

QUẢN TRỊ DỊCH VỤ THƯ MỤC.

Sử dụng dịch vụ Active Directory.

Dịch vụ Active Directory là thành phần mấu chốt của Microsoft Windows 2000. Công nghệ Active Directory dựa trên các giao thức Internet chuẩn và có kiểu thiết kế giúp người sử dụng định rõ cấu trúc mạng.

Active Directory ứng dụng DNS, là dịch vụ Internet chuẩn, chịu trách nhiệm tổ chức các nhóm máy tính thành vùng.

Dịch vụ thư mục Active Directory cung cấp cả cấu trúc Logic và cấu trúc vật lý cho các thành phần mạng.

Cấu trúc **Logic** bao gồm:

- **Domain (vùng):** Nhóm các máy tính dùng chung cơ sở dữ liệu thư mục.
- **Domain Tree (Vùng phân cấp):** Một hay nhiều vùng dùng chung không gian tên liên tục.
- **Domain Forest (Tập hợp hệ vùng phân cấp):** Một hay nhiều hệ vùng dùng chung thông tin thư mục.
- **Organizational unit (Đơn vị tổ chức):** Nhóm con gồm những vùng thường phản ánh cấu trúc kinh doanh hoặc cấu trúc chức năng của một công ty.

Cấu trúc V**ật lý** bao gồm:

- **Subnet (mạng con):** Đoạn mạng với dãy địa chỉ IP và mặ nạ mạng cụ thể.
- **Site (địa điểm):** Một hoặc nhiều mạng con dùng để lập cấu hình dịch vụ sao chép và truy cập thư mục.

Quản trị dịch vụ Active Directory.

Công việc quản trị dịch vụ thư mục **Active Directory** tập trung vào những nhiệm vụ chủ yếu được người quản trị thi hành thường kỳ với dịch vụ thư mục **Active Directory**, như mở tài khoản máy tính hoặc kết nạp máy tính vào vùng.

Những công cụ quản lý Active Directory.

Những công cụ quản lý **Active Directory** thường cung cấp ở dạng Snap-in cho MMC (Microsoft Management Console).

- **Active Directory users and Computer:** Quản trị người dùng, nhóm, máy tính, và đơn vị tổ chức.
- **Active Directory and Trusts:** Dùng làm việc với vùng, hệ vùng phân cấp, tập hợp hệ vùng phân cấp.
- **Active Directory Sites and Services :** Quản lý Site và mạng con.

Những công cụ hỗ trợ trong việc quản trị :

- **Active Directory Administration Tool:** Thi hành giao thức LDAP (Lightweight Directory Access Protocol) trên **Active Directory.**
- **Active Directory Replication Monitor:** Quản lý và giám sát hoạt động sao chép thông qua giao diện người sử dụng dạng đồ hoạ.
- **ADSI Edit:** Quản lý đối tượng chứa trong thư mục bao gồm cả sơ đồ thư mục. Ấn định danh sách điều khiển truy nhập.

Công cụ Active Directory Users and Computer.

Active Directory Users and Computer là công cụ quản trị chủ yếu để quản lý Active Directory, cụ thể là thi hành mọi nhiệm vụ quản trị, bao gồm quản trị người sử dụng, máy tính trong vùng,...

Mặc định, Active Directory sẽ làm việc với vùng đang được kết nối, có thể truy cập và quản lý các đối tượng người sử dụng, máy tính trong vùng này thông qua vùng phân cấp. Nếu không tìm thấy máy điều khiển vùng hoặc vùng tham gia không khả dụng, phải kết nối tới máy điều khiển vùng hiện hành hoặc máy điều khiển vùng khác.

Có thể truy cập đến Active Directory Users and Computer bằng nhiều cách khác nhau như:

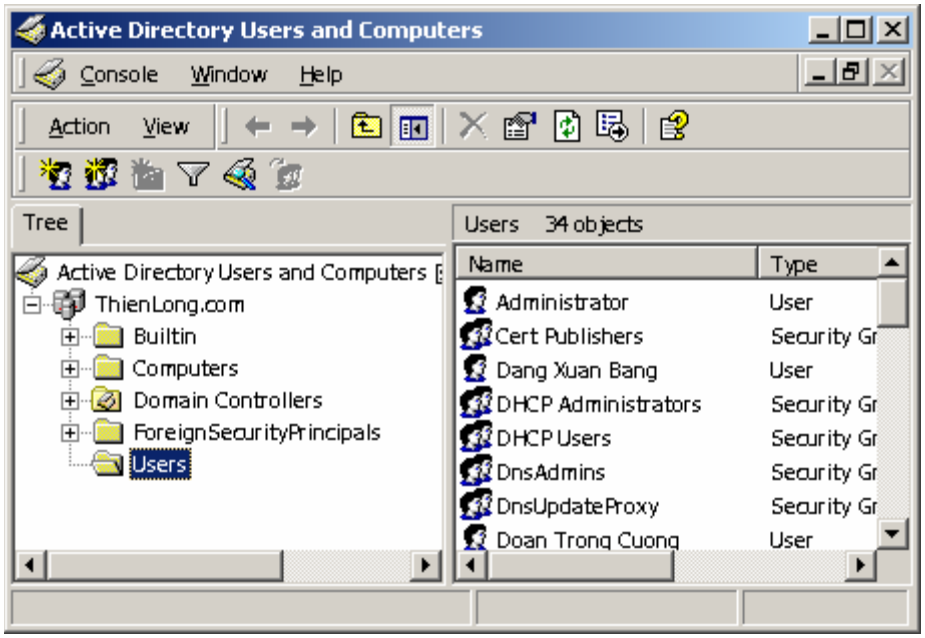
+ Truy nhập thông qua công cụ quản trị như sau:

Trỏ vào Start / Programs / Administrative Tools / Active Directory Users and Computer.

+ Truy nhập thông qua giao diện MMC:

Trỏ tới Start / Run, gõ lệnh mmc. Bổ xung Active Directory Users and Computer vào giao diện.

Sau khi kích hoạt, cửa sổ Active Directory Users and Computer sẽ xuất hiện như sau:



Active Directory có những đặc tính, những tác vụ nâng cao như xem các tuỳ chọn nâng cao hay tìm kiếm đối tượng.
Khi truy cập vùng trong Active Directory Users and Computer, những tập hợp thư mục chuẩn sau đây khả dụng:

- **Builin**: Danh sách tài khoản người dùng cài sẵn.
- **Computers**: Chứa tài khoản máy tính theo mặc định.
- **Domain Controlers**: Chứa máy điều khiển vùng theo mặc định.
- **ForeignSecurityPrincipanls**: Chứa thông tin về đối tượng từ vùng ngoài được uỷ quyền.

*** Kết nối tới máy điều khiển vùng:**
Trong cửa sổ Active Directory Users and Computer, ở khung bên trái bấm chuột phải vào Active Directory Users and Computer, chọn Connect To Domain Conntroler. Vùng hiện hành và máy chủ điều khiển vùng sẽ hiển thị. Chọn tới máy chủ điều khiển vùng cần kết nối.

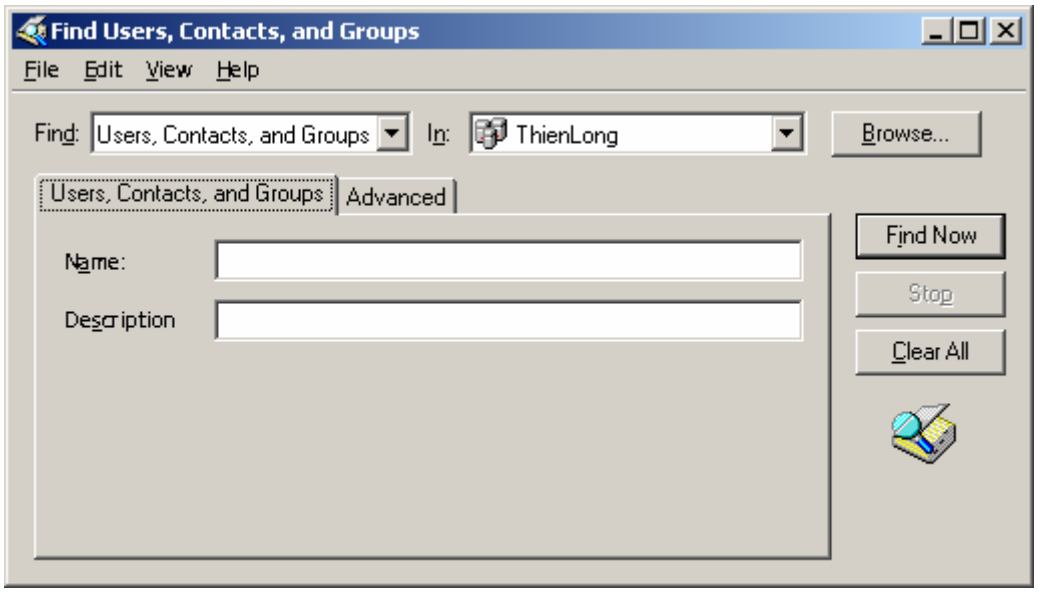
*** Kết nối tới vùng:**
Cũng trong cửa sổ Active Directory Users and Computer, trong ô bên trái, bấm chuột phải vào Active Directory Users and Computer, chọn Connect To Domain.

Tìm kiếm tài khoản và tài nguyên dùng chung.

Active Directory Users and Computer có đặc tính tìm kiếm cài sẵn, cho phép người quản trị tìm ra tài khoản, tài nguyên dùng chung và các đối tượng khác trong thư mục.

Phương pháp tìm kiếm như sau:

- Trong cửa sổ Active Directory Users and Computer, nháy phải chuột vào vùng cần tìm kiếm và chọn Find, Cửa sổ tìm kiếm xuất hiện.
- Trong hộp Find, chọn yêu cầu tìm kiếm:
  - Users, Contacts, and Groups: Tìm kiếm tài khoản người sử dụng, tài khoản nhóm.
  - Computers: Tìm tài khoản máy tính theo tên, loại, chủ sở hữu.
  - Printer: Tìm máy in theo tên, kiểu hoặc đặc tính.
  - Shared Folder: Tìm thư mục dùng chung theo tên hay từ khoá
  - Organization Units: Tìm đơn vị tổ chức theo tên.
  - Custom Search: Thực hiện tìm kiếm nâng cao.



- Trong hộp In, chọn phạm vi tìm kiếm.
- Sau khi nhập xong yêu cầu và phạm vi tìm kiếm, Bấm nút lệnh FindNow.

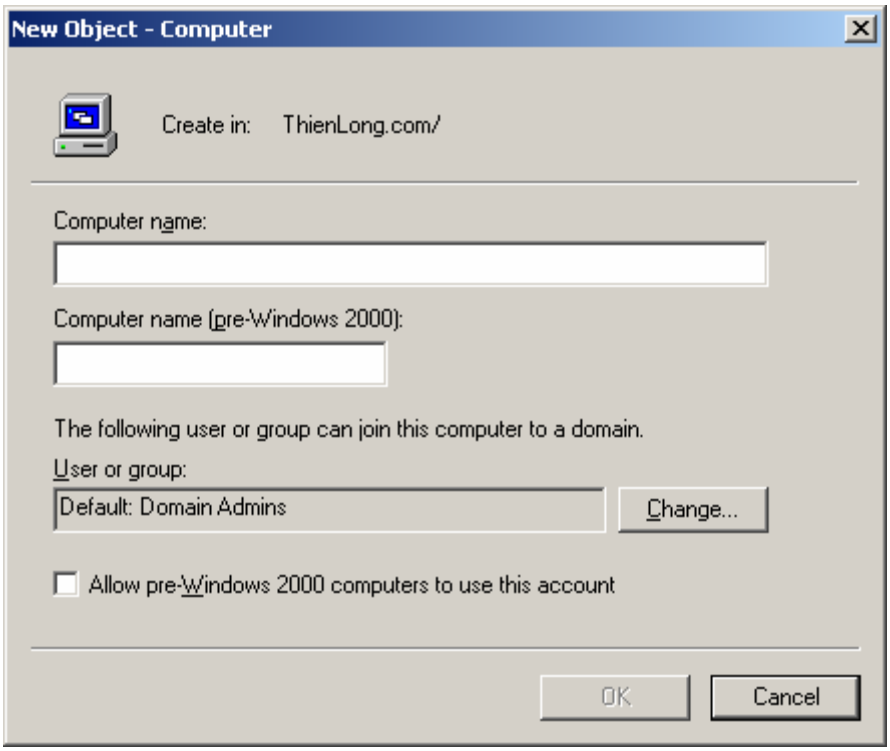
Quản lý tài khoản máy tính.

Tài khoản máy tính được lưu trong Active Directory ở dạng đối tượng, dùng để chi phối hoạt động truy cập mạng và tài nguyên mạng. Người quản trị mạng có thể bổ xung tài khoản vào thư mục bất kỳ hiển thị trong Active Directory Users and Computers.

Tạo tài khoản máy tính trong Active Directory Users and Computers.

Để tạo tài khoản máy tính trong Active Directory Users and Computers, ta cần thực hiện các bước sau:

- Trong cửa sổ Active Directory Users and Computers, ở khung bên phải trong Console Active Directory Users and Computers, nhấp phải chuột vào thư mục sẽ chứa tài khoản máy tính sắp tạo ra.
- Chọn New | Computer để mở hộp thoại New object Computer. Nhập tên cho may khách.
- Theo mặc định, chỉ có thành viên nhóm Domain Admins mới được phép kết nạp (tạo) máy tính vào vùng. Để cho người sử dụng khác hoặc nhóm khác có thể kết nạp máy tính vào vùng, bấm vào nút Change và chọn trong danh sách.



Xoá, vô hiệu hoá và kích hoạt tài khoản máy tính.

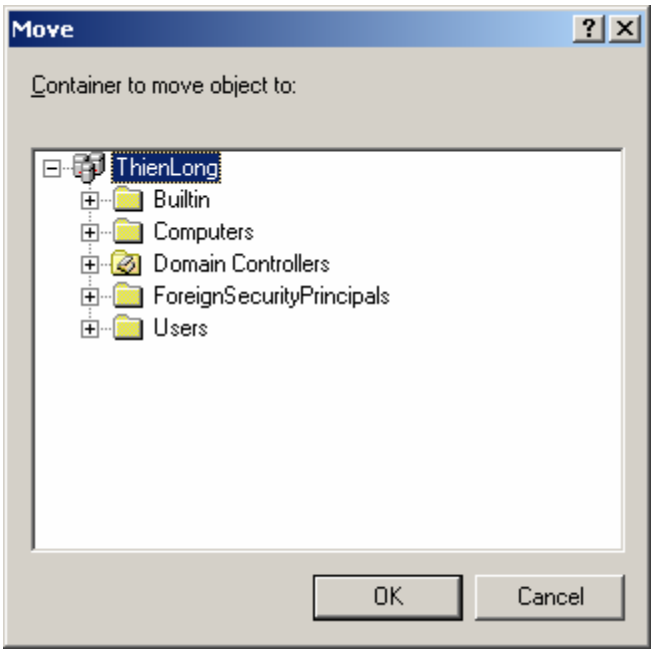
Khi không cần dùng đến tài khoản máy tính nào đó, người quản trị có thể xoá bỏ tài khoản đó trong Active Directory, hoặc vô hiệu hoá một tài khoản máy tính nào đó và cũng có thể sau khi vô hiệu hoá một tài khoản, người quản trị có thể kích hoạt tài khoản đã bị khoá. Để thực hiện được những công việc cụ thể trên, ta thực hiện như sau:

- Trong cửa sổ Active Directory Users and Computers, chuyển đến thư mục chứa tài khoản máy tính cần thao tác, chọn tài khoản máy tính cần thực hiện xoá, vô hiệu hoá, kích hoạt.
- Bấm chuột phải vào tài khoản máy tính đó và chọn Disable Account (Vô hiệu hoá), Enable Account (Kích hoạt), Reset Account (Đặt lại), Delete (Xoá bỏ).

Di dời một tài khoản máy tính.

Nếu muốn di dời một tài khoản máy tính đến một vị trí khác, ta thực hiện như sau:

- Trong cửa sổ Active Directory Users and Computers, chọn thành phần chứa tài khoản máy tính cần di rời.
- Bấm chuột phải, chọn Move, và chọn vị trí mới cần đặt và bấm nút lệnh OK.

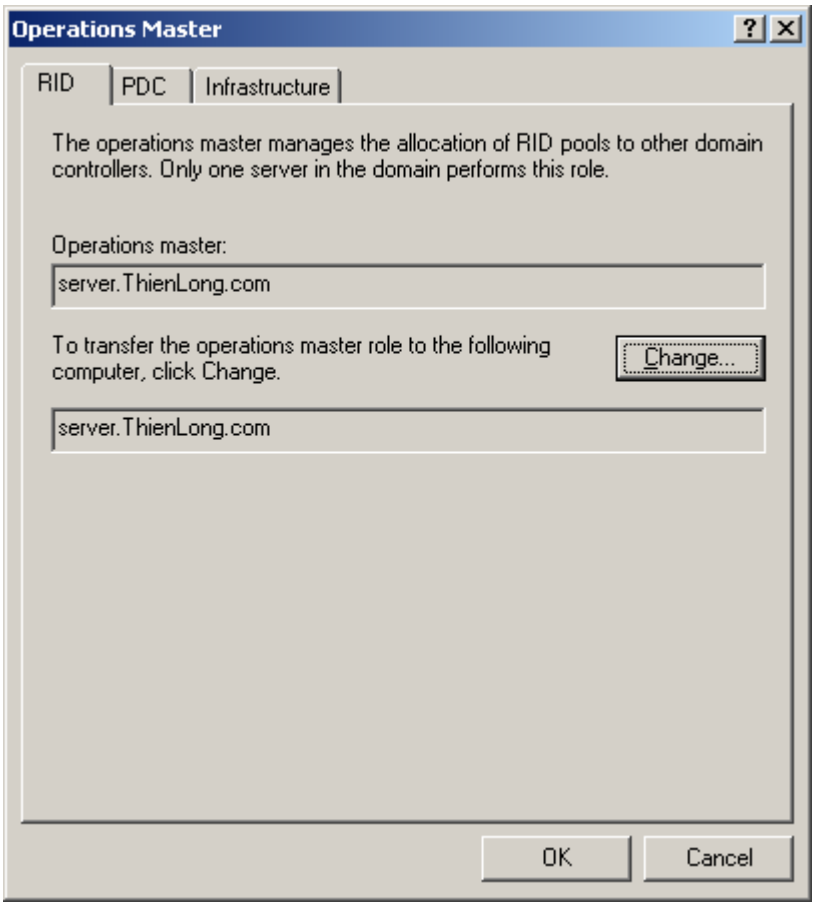


Xem và chuyển giao vai trò trong phạm vi vùng.

Trên cấp độ vùng, người quản trị làm việc với vai trò chủ (Relative ID - RID), máy điều khiển vùng (PDC), và chủ Infrastructure.

Để có thể xem và chuyển giao vai trò trong phạm vi vùng, thực hiện các bước như sau:

- Trong cửa sổ Active Directory Users and Computers, nháy phải chuột vào Active Directory Users and Computers và chọn Operration Master .
- Trong Tab RID chỉ ra vị trí của chủ ID hiện hành, bấm vào nút lệnh Change, chọn máy điều khiển vùng mới sẽ đảm nhận vai trò này.
- Trong Tab PDC, nêu rõ vị trí của máy PDC, bấm vào nút lệnh Change và chỉ ra máy sẽ đảm nhận vai trò mới này.
- Trong Tab Infrastructure, nêu rõ vị trí của máy chủ Infrastructure đặt ở đâu, nếu muốn thay đổi nhấn vào nút lệnh Change và chỉ ra máy nào sẽ đảm nhận vai trò mới này.

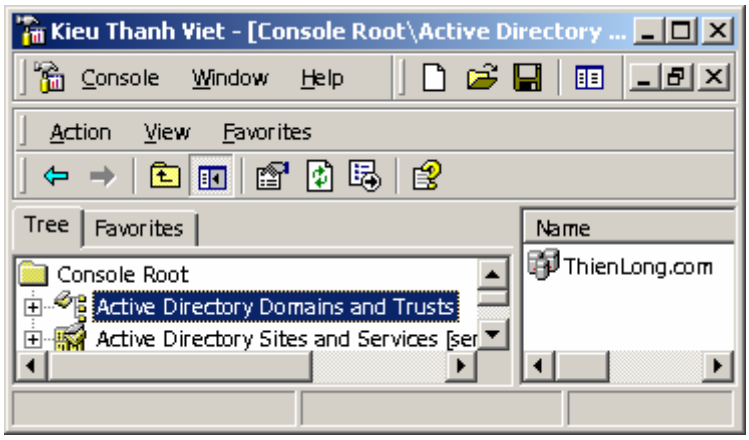


Xem và chuyển giao vai trò chủ tên vùng.

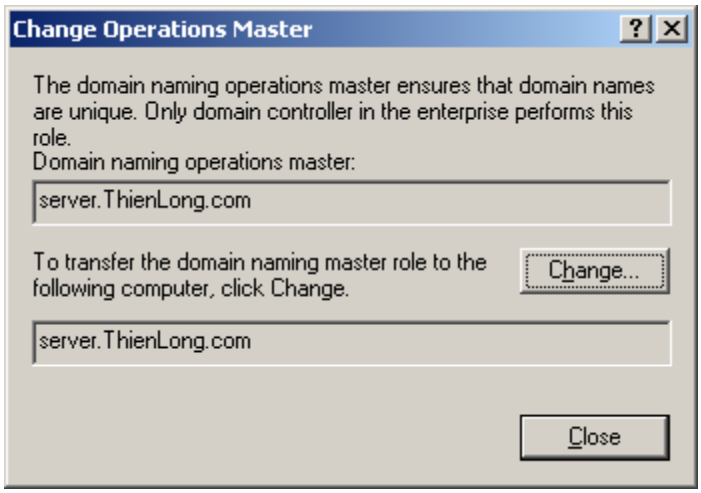
Công cụ Active Directory Domain And Trusts cho phép xem hoặc thay đổi vị trí của chủ tên vùng trong tập hợp hệ vùng. Ở Active Directory Domain And Trusts, cấp cao nhất của hệ vùng chỉ rõ vùng hiện được chọn.

Để thực hiện chuyển giao vai trò chủ tên vùng, thực hiện các thủ tục sau:

- Kích hoạt Active Directory Domain And Trusts.
- Trong cửa sổ Active Directory Domain And Trusts, chọn khung bên trái, bấm chuột phải vào Active Directory Domain And Trusts và chọn Operation Master:



Cửa sổ Change Operation Master xuất hiện như sau:



Trong trường Domain Naming Operation Master hiển thị chủ tên vùng hiện hành.

- Để thay đổi, bấm vào nút lệnh Change và chọn máy điều khiển vùng mới.
- Close.

Quản lý đơn vị tổ chức - Organization Unit - OU.

Organization Unit giúp cho người quản trị mạng sắp xếp đối tượng, ban hành chính sách cho nhóm (Group Policy) trong phạm vi giới hạn.

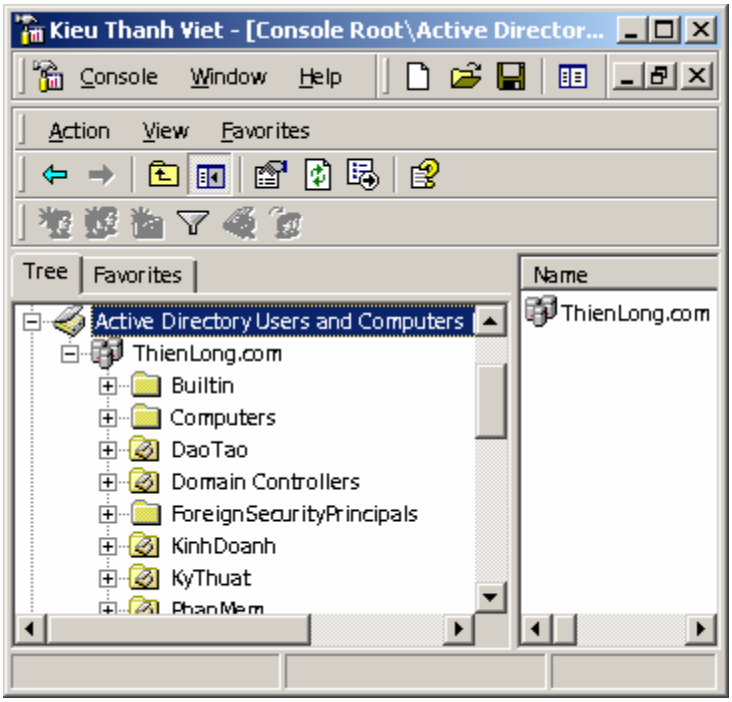
Thiết lập:

Mục đích của việc thiết lập **OU** là phản ánh cấu trúc chức năng hoặc kinh doanh của công ty. Người quản trị thiết lập **OU** ở dạng nhóm con của vùng, hoặc đơn vị con.

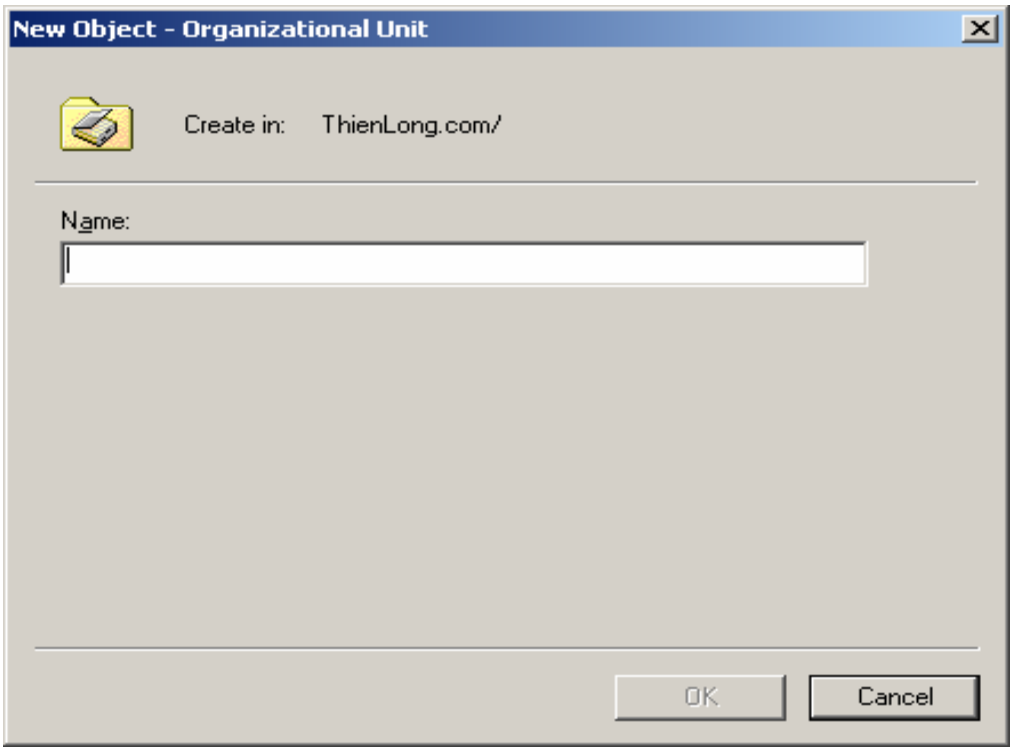
Để thiết lập **OU** cần thực hiện những thư tục sau:

- Khởi động Active Directory Users and Computers.

- Trong khung bên trái, mở rộng tên vùng.
- Bấm chuột phải vào tên vùng hoặc thư mục đơn vị có sẵn nơi muốn bổ xung đơn vị, tổ chức, trên Menu tắt chọn New | OU.



Cửa sổ New Object - Organization Unit xuất hiện như sau:



- Nhập tên cho đơn vị, tổ chức mới rồi bấm OK.

Một OU sau khi được tạo ra có thể được xoá, đổi tên, và di chuyển!!!

Tài khoản người sử dụng và tài khoản nhóm.

Một số khái niệm cơ bản.

*** Mô hình bảo mật của Windows 2K.**

+ Giao thức chứng thực:

Chứng thực trong Windows 2K là quy trình gồm 2 giai đoạn: Đăng nhập tương tác và chứng thực mạng.

Khi người sử dụng đăng nhập máy tính, quy trình đăng nhập tương tác phê chuẩn yêu cầu đăng nhập của người dùng (Xác nhận nhận dạng của nhười sử dụng trước máy tính cục bộ, rồi cấp quyền truy nhập dịch vụ thư mục). Sau đó, mỗi lúc người dùng truy nhập tài nguyên mạng, quy trình chứng thực mạng lại được dùng nhằm xác định xem người dùng có quyền hay không.

Các giao thức chứng thực mạng bao gồm:

- Kerberos V5: Giao thức chuẩn Internet dùng để chứng thực người dùng và hệ thống. (2K)
- NTLM - NT LAN Manager: Chứng thực máy tính trong vùng của Windows NT.
- SSL/TLS - Secure Socket Layer/Transport Layer Security

Kiểm soát hoạt động truy cập:

Active Directory là dịch vụ dựa trên đối tượng. Người dùng, máy tính, nhóm, tài nguyên dùng chung và nhiều thực thể khác đều được định nghĩa ở dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào mô tả bảo mật. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy nhập đối tượng.
- Định rõ quyền truy nhập đã cấp cho người dùng và nhóm.
- Theo dõi các sự kiện phải được kiểm toán cho đối tượng.
- Định rõ quyền sở hữu đối tượng.

Sự khác nhau giữa tài khoản người dùng và tài khoản nhóm.

Windows 2000 cung cấp tài khoản người dùng và tài khoản nhóm. Tài khoản người dùng được thiết kế cho từng cá nhân. Tài khoản nhóm giúp cho người quản trị quản trị được nhiều người dùng hơn. Tuy có thể đăng nhập với tài khoản người dùng, nhưng lại không được đăng nhập với tài khoản nhóm.

Tài khoản người dùng:

- Tài khoản người dùng vùng (Domain User Account): Là tài khoản người dùng được định nghĩa trong Active Directory. Tài khoản người dùng có thể truy cập tài nguyên qua vùng. Tài khoản người dùng được định nghĩa thông qua Active Directory Users And Computer.
- Tài khoản người dùng cục bộ (Local User Account): Là tài khoản người dùng được định nghĩa trên tài khoản người dùng chủ cục bộ. Tài khoản người dùng cục bộ chỉ có quyền truy cập máy tính cục bộ và phải tự chứng thực mình trước khi có thể truy cập mạng. Tài khoản người sử dung cục bộ được tao trong công cụ Local User And Group.

Hoạch định và tạo tài khoản người dùng:

Hoạch định:

Đây là khía cạnh quan trọng nhất của thủ tục tạo tài khoản, hoạch định bao gồm những công việc sau đây:

- Chính sách tên tài khoản: bao gồm tên hiển thị và tên đăng nhập.
- Mật khẩu và chính sách tài khoản: Phương pháp thiết lập chính sách tài khoản.

Tạo tài khoản cho người sử dụng vùng:

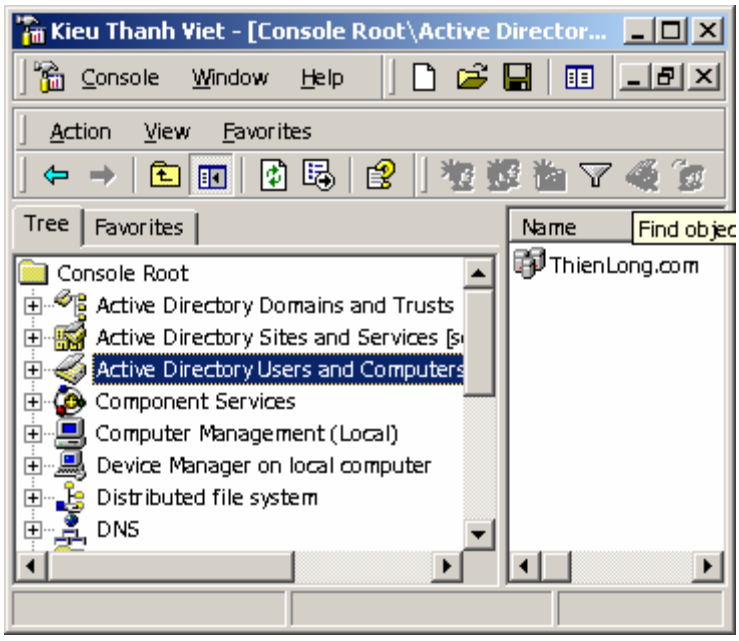
Tài khoản người sử dụng cho phép người quản trị theo dõi và quản lý thông tin về người dùng bao gồm quyền truy nhập và đặc quyền. Khi tạo tài khoản người sử dụng, công cụ quản trị tài khoản sau đây sẽ được sử dụng:

***Active Directory Users And Computer**: Quản trị tài khoản khắp vùng Active Directory.

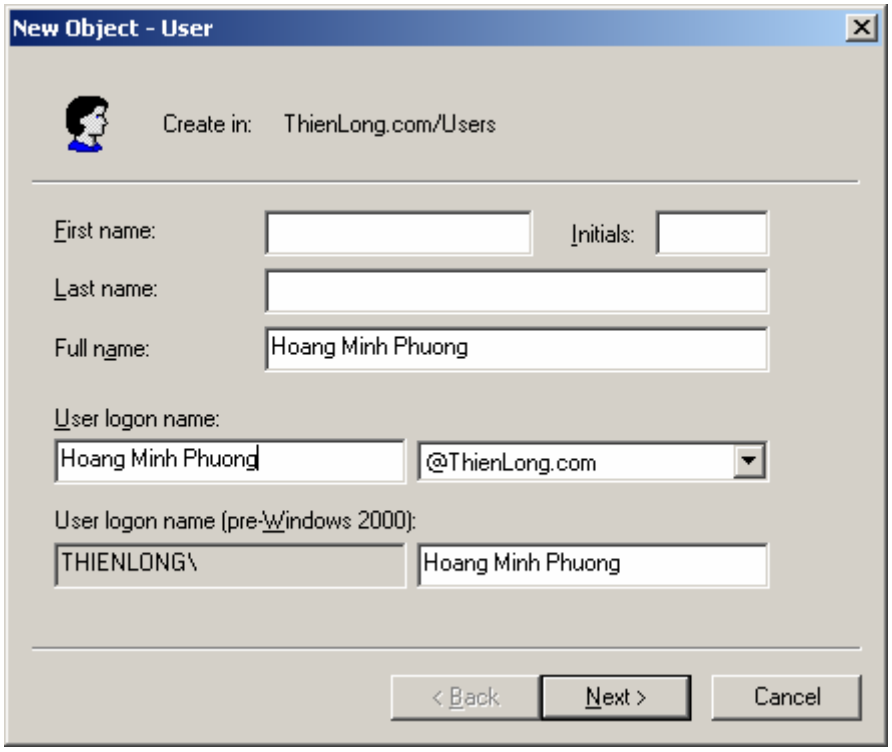
*** Local Users And Group:** Quản trị tài khoản trên máy tính cục bộ.

Để tạo tài khoản người sử dụng trong vùng, ta thực hiện như sau:

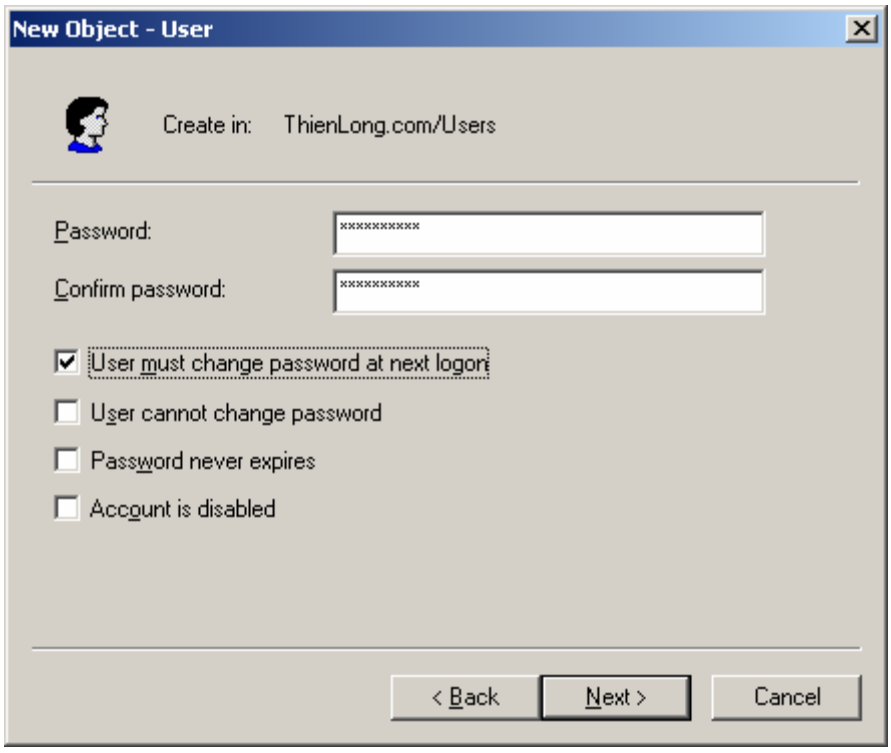
- Kích hoạt công cụ **Active Directory Users And Computer** trong nhóm công cụ quản trị hoặc trong Snapin.



- Nháy phải chuột vào nơi sẽ tiếp nhận tài khoản mới, bấm chuột phải và chọn New User từ Menu tắt.
- Cửa sổ New Object - User sẽ xuất hiện, nhập tên cho người sử dụng sau đó bấm Next.



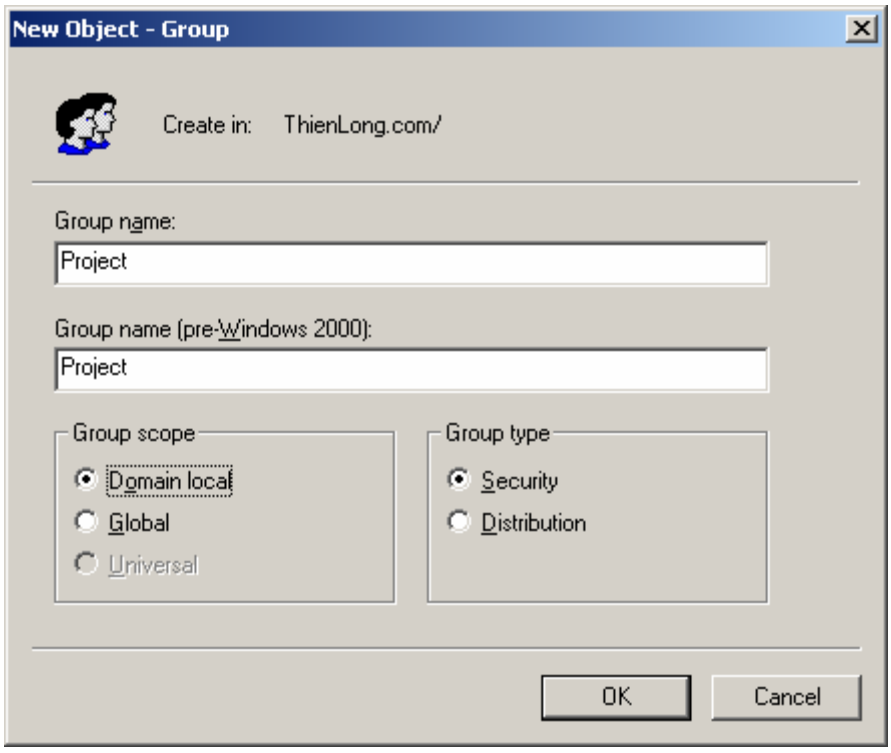
- Sau khi Next, vẫn trong cửa sổ New Object - User, nhập mật khẩu cho người sử dụng. Bấm Next và kết thúc quá trình tạo.



Thiết lập tài khoản nhóm.

Để thiết lập tài khoản nhóm, cân thực hiện các thủ tục sau:

- Kích hoạt công cụ quản trị Active Directory Users And Coputer trong nhóm công cụ quản trị hoặc từ Snapin.
- Bấm chuột phải vào nơi sẽ tiếp nhận tài khoản nhóm mới và chọn New | Group từ Menu tắt.
- Trong cửa sổ New Object - Group vừa xuất hiện, đặt tên cho nhóm, chọn phạm vi cho nhóm và loại nhóm sau đó OK.



Quản lý tài khoản nhóm và tài khoản người dùng hiện có.

Quản lý thông tin liên hệ.

Thông tin liên hệ là thông tin liên hệ cho tài khoản người sử dụng. Đối với mỗi người sử dụng sẽ có thông tin liên hệ riêng. Sau khi tạo ra tài khoản người sử dụng, có thể bổ xung các thông tin liên hệ với người sử dụng đó.

Để ấn định, bổ xung thông tin người sử dụng cần thực hiện những thủ tục sau:

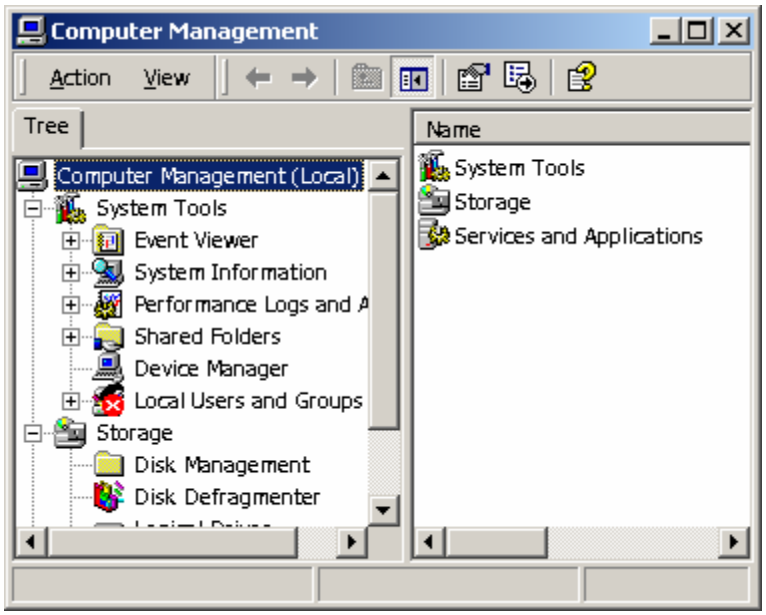
- Kích hoạt công cụ quản trị Active Directory Users And Coputer

Quản lý tài khoản người dùng.

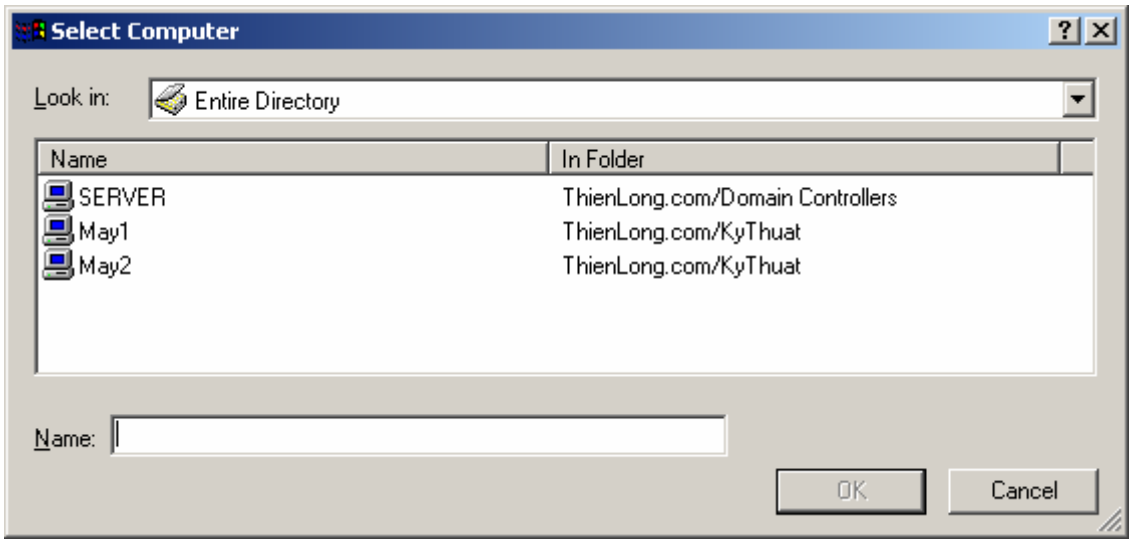
Computer Management - Các tài khoản cục bộ.

Trong những tổ chức, cơ quan nhỏ để đơn giản trong công việc quản trị có thể không dùng AD thì việc tạo các tài khoản người sử dụng cục bộ có thể dùng Computer Management. Tuy nhiên Computer Management có thể tạo ra và quản lý các tài khoản người dùng và nhóm từ xa trong một Server thành viên ở xa trong một Domain.

Cửa sổ Computer Management như sau:



Để có thể tạo và quản lý các tài khoản người dùng và nhóm từ xa trong một Server thành viên ở xa trong một Domain ta thực hiện như sau:
Trong cửa sổ Computer Management | menu Action chọn Connect to another Computer chọn máy cần nói tới để tạo tài khoản, nhóm rồi OK.



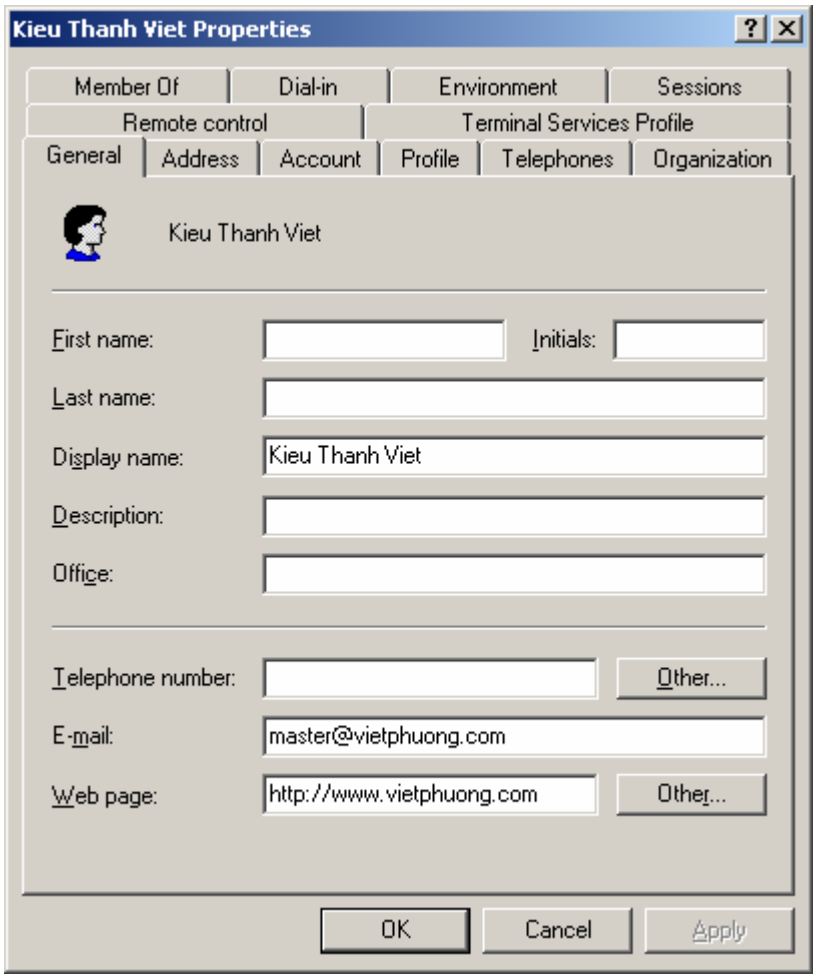
Việc tạo tài khoản người sử dụng trên một Server không cài đặt AD trên Windows 2000 Server sẽ thực hiện bằng công cụ Computer Management.
Trong cửa sổ Computer Management, mở SystemTools, mở Local Users and Groups. Thực hiện công việc tạo tài khoản người sử dụng gần như tạo trong AD.
Các tài khoản cục bộ tạo trên một Server độc lập. Server thành viên được lưu trữ trong cơ sở dữ liệu SAM trong \WINNT\SYSTEM32\CONFIG.

Quản lý tài khoản người sử dụng trong AD.

* Các đặc tính của tài khoản người sử dụng.

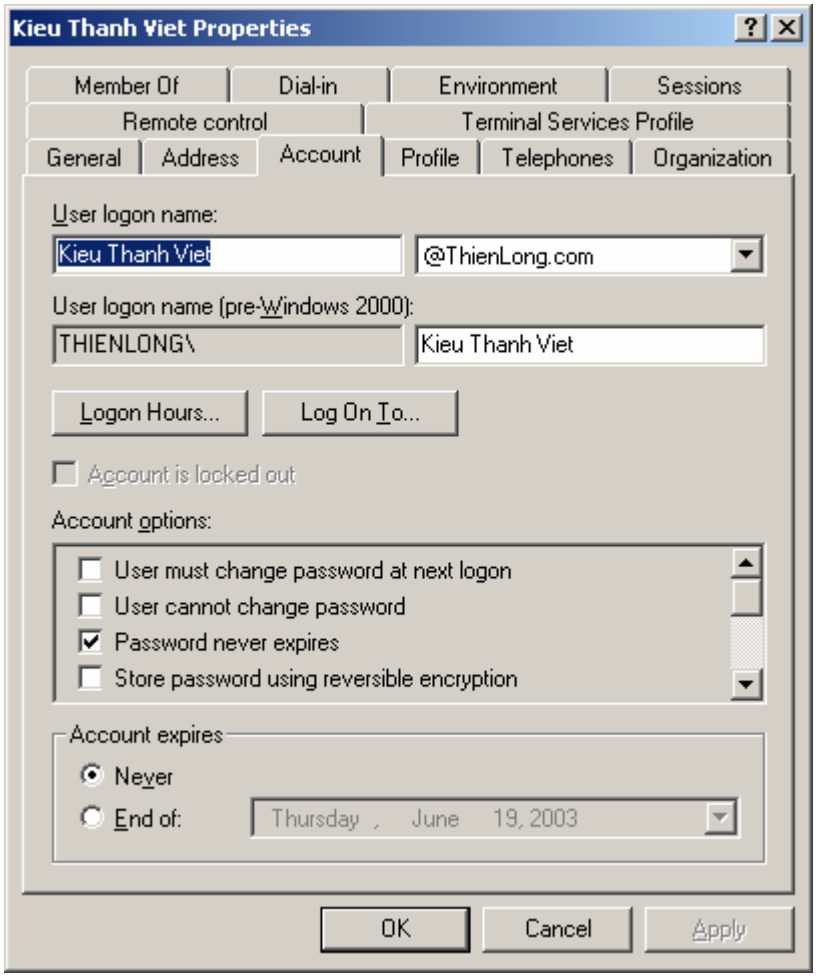
Muốn biết tài khoản của người sử dụng có các đặc tính như thế nào, ta thực hiện như sau:

- Chọn tài khoản người sử dụng muốn xem đặc tính.
- Bấm chuột phải và chọn Properties, cửa sổ Properties xuất hiện. Trong cửa sổ này, ta có thể xem chi tiết về tài khoản đó.



*** Các thiết lập về tài khoản người sử dụng.**

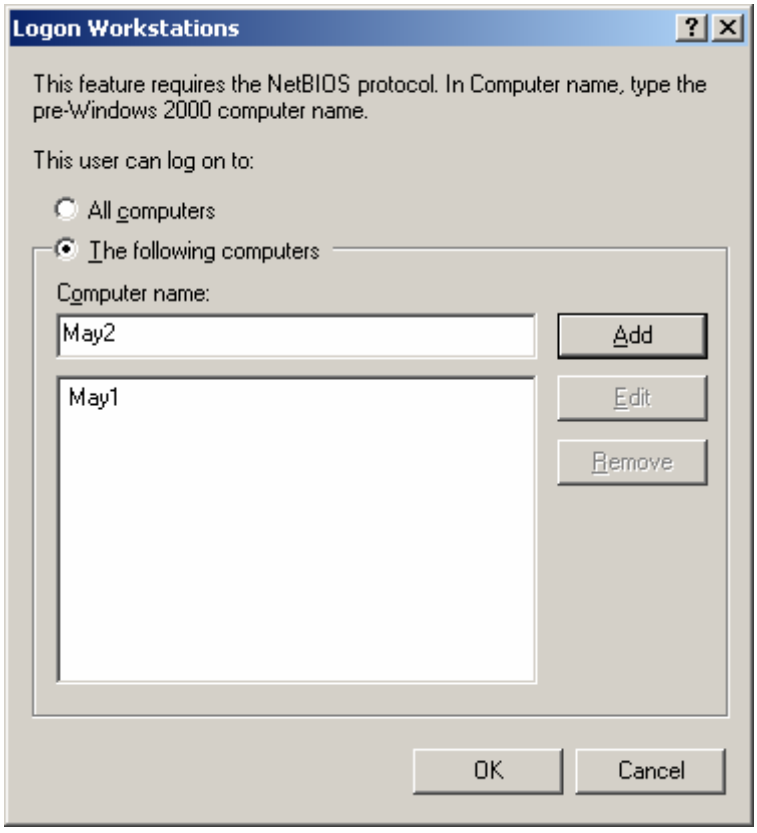
Các thiết lập cho tài khoản người dùng sẽ được đặt trong Tab Account.



Theo mặc định, người sử dụng có thể đăng nhập vào miền từ bất kỳ máy trạm nào, nhưng vẫn có thể chỉ định các máy trạm đăng nhập bằng tên NetBIOS của chúng (Khi đó trên mạng vẫn phải dùng NetBIOS thì chỉ định trên mới có hiệu lực.)

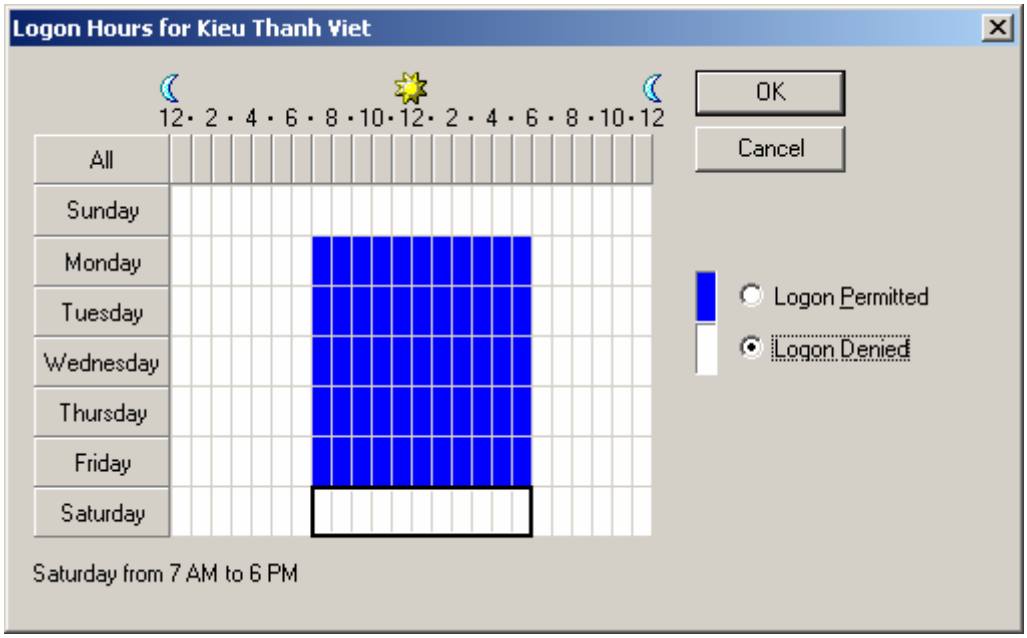
Để chỉ định người sử dụng có thể truy nhập vào mạng từ những máy nào trên mạng ta cần thiết lập lại thuộc tính của tài khoản của người sử dụng đó:

- Chọn tài khoản người sử dụng cần thay đổi thuộc tính, bấm chuột phải chọn Properties.
- Chọn Tab Account.
- Chọn nút lệnh Logon to... và chọn các máy trạm mà người sử dụng có thể đăng nhập.
- Nhập tên cho máy trạm và nhấn Add.



Đặt thời gian truy nhập cho tài khoản người sử dụng:
Theo mặc định, người sử dụng sẽ không bị tự động đăng xuất khi hết giờ đăng nhập. Để đặt thời gian người sử dụng được phép đăng nhập mạng, ta thực hiện như sau:

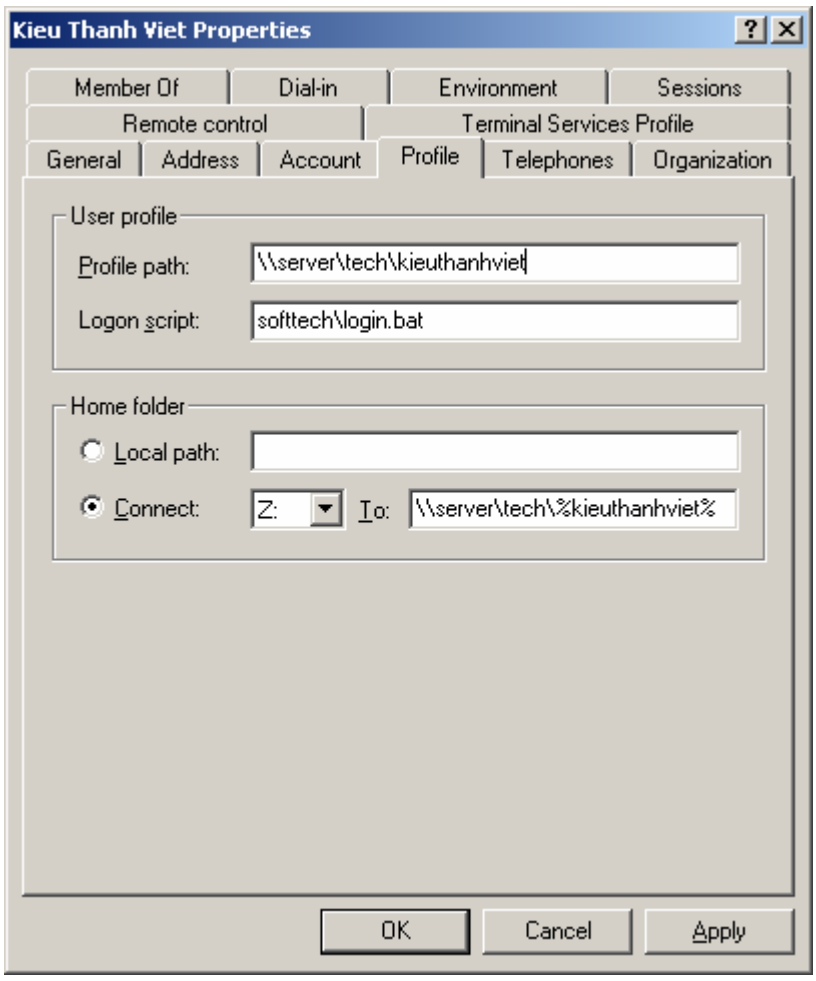
- Trong cửa sổ User Properties chọn Tab Account.
- Bấm chọn nút lệnh Logon Hours...
- Trong cửa sổ Logon Hours chọn ngày và giờ khong cho người sử dụng đăng nhập sau đó bấm chọn Logon Denied.



*** Thông tin biên dạng - Profile.**
Profile là nơi để chỉ định đường dẫn tập tin biên dạng và một kịch bản đăng nhập. Các tuỳ chọn này phần lớn là dành cho các phần mềm máy khách trước Windows 2K (Trong môi trường mạng không thuần nhất).
Các thiết lập cho màn hình **Destop** của người dùng từ nội dung của menu **Start** cho cho tới mầu sắc, cách định hướng chuột có thể lưu trữ ở một nơi nào đó trên mạng để người dùng có thể đăng nhập từ một

máy nào đó trên mạng mà vẫn thấy được màn hình đăng nhập giông nhau.
Profile có nhiều loại: Loại bắt buộc người sử dụng dùng nó và không bắt buộc.
Logon Script là kịch bản được chạy vào lúc đăng nhập để định hình môi trường làm việc cho người sử dụng và cấp phát các tài nguyên mạng mà người sử dụng sẽ được phép truy nhập.

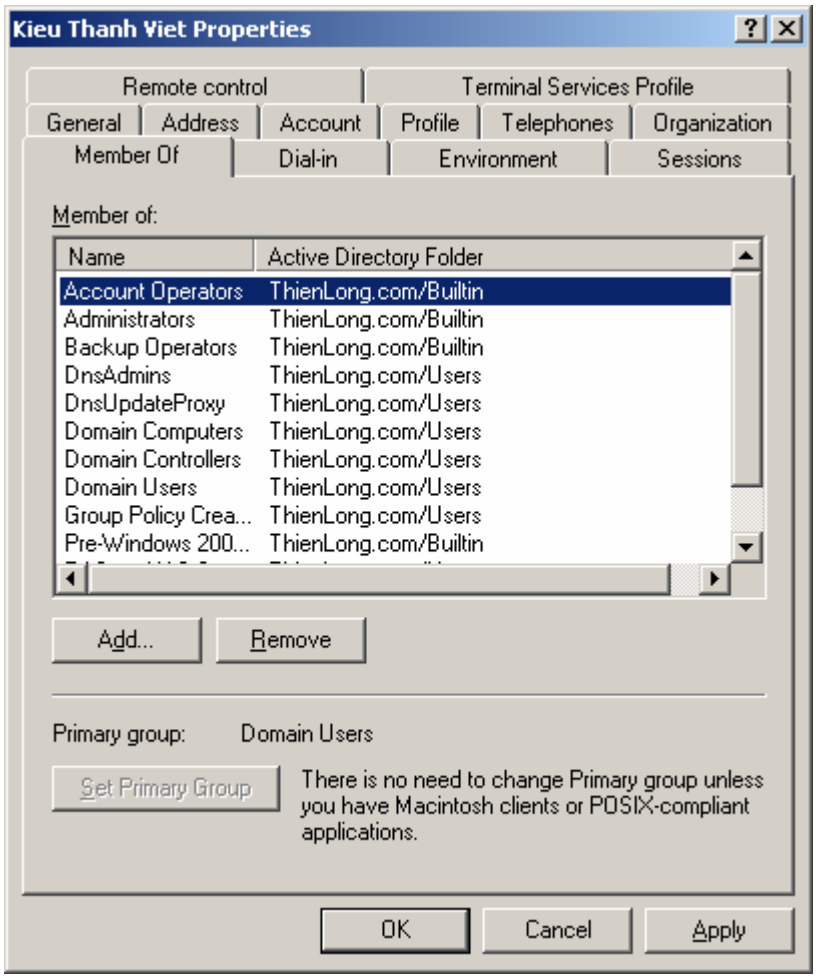
Để nhập vào Profile và Logon Script cần thực hiện những thao tác sau:



Một Home Folder hoặc`Home Directory là một thư mục được cấp cho người sử dụng để họ sử dụng riêng.
Chúng ta có thể chỉ định một thư mục cục bộ làm Home Folder khi người sử dụng đăng nhập trên máy cục bộ.

Khi người sử dụng đăng nhập từ mạng thì người quản trị cần chỉ ra đường dẫn cho Home Folder của người đó.
Một điều quan trọng là người quản trị phải chỉ rõ ràng rằng Home Folder của người sử dụng đó sẽ có dung lượng là bao nhiêu.

Vai trò của người dùng trên mạng.
Trong mạng hiển nhiên là có nhiều người sử dụng, vậy mỗi người dùng trên mạng sẽ có những vai trò như thế nào, họ có những quyền gì trên mạng.
Đối với mỗi người sử dụng trên mạng, người quản trị mạng cần chỉ ra vai trò của họ bằng cách trong cửa sổ User Properties chọn Tab Member of và sau đó có thể bổ xung hoặc loại bỏ vai trò mà người dùng đó thuộc vào.



Các chính sách nhóm - Group Policy

Việc đưa ra một chuẩn mực dành cho mạng là công việc phức tạp, đồng thời việc triển khai các ứng dụng mới ra toàn bộ mạng là công việc rất khó.

Sau khi tạo ra nhóm, người quản trị sẽ dùng công cụ Group Policy để quản lý. Nhưng rất chú ý là Group Policy không quản lý được nhóm mà chỉ có khả năng quản lý OU, Site.

Với Group Policy, người quản trị có thể thực hiện được những công việc sau:

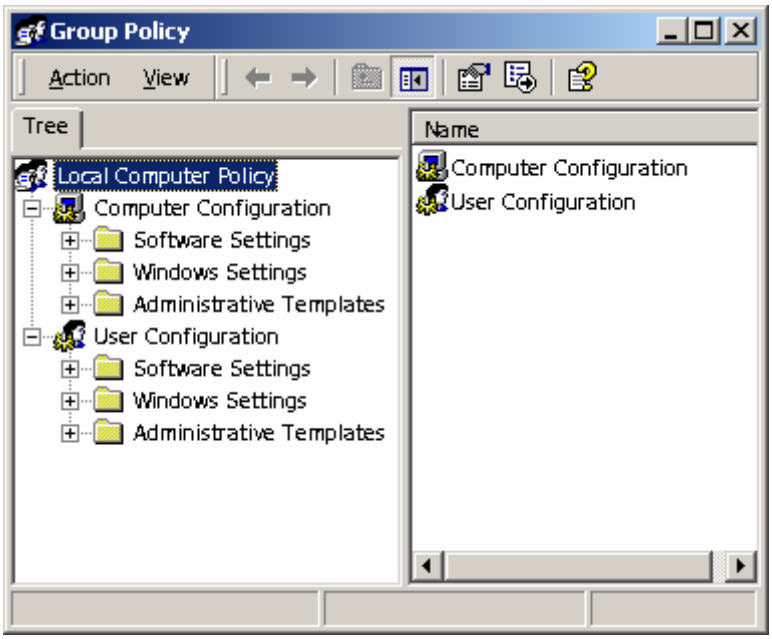
- Phân phối các gói phần mềm tới các máy tính trạm hoặc người sử dụng.
- Phân phối các kịch bản (Đăng nhập, đăng xuất, tắt máy)
- Quy định các chính sách mật khẩu, khoá chặn tài khoản và kiểm soát cho miền.
- Nhân bản một loạt các thiết định bảo mật cho các máy tính ở xa. Áp đặt các tư cách thành viên nhóm và định cấu hình các dịch vụ.
- Quy định, thiết đặt những thông số dành cho Internet Explorer.
- Quy định và thiết đặt những hạn chế trên Destop của máy người sử dụng.
- Định hướng lại một số thư mục trong khái lược người sử dụng.

Thông thường các quản trị viên định cấu hình và triển khai các chính sách nhóm bằng cách xây dựng các đối tượng chính sách nhóm GPO - Group Policy Object.

Các GPO là nơi chứa các thiết định (các chính sách) có thể áp dụng cho các tài khoản người dùng và tài khoản máy trên toàn mạng.

Chỉ cần một GPO là có thể chỉ định cài đặt một mớ ứng dụng trên máy trạm của tất cả người sử dụng như các thiết lập bảo mật, các chính sách tài khoản... trên toàn miền.

Có thể tạo ra một GPO chứa tất cả mọi thiết định hoặc nhiều GPO mỗi cái dành cho một chức năng nào đó.



CHIA SẺ DỮ LIỆU, BẢO MẬT VÀ KIỂM TOÁN.

Cơ chế chia sẻ dữ liệu (data sharing) cho phép người dùng truy cập tài nguyên mạng từ xa, như truy cập tin, thư mục, ổ đĩa. khi chia sẻ thư mục hay ổ đĩa, tất cả các tập tin và thư mục con trực thuộc sẽ khả dụng cho(những) người dùng định rõ. Nếu muốn kiểm soát hoạt động truy cập tin hay thư mục con cụ thể chứa trong thư mục dùng chung, bạn chỉ có thể dựa vào volume NTFS. Trên volume NTFS, bạn cấp hoặc từ chối cấp quyền truy cập tập tin, thư mục thông qua ACL(Access Control List)

Cơ chế bảo mật đối tượng áp dụng cho toàn bộ tài nguyên trên volume NTFS, bao gồm tập tin, thư mục, và các đối tượng của dịch vụ Active Directory. Thường thì chỉ nhà quản trị được phép uỷ quyền cho người dùng quản lý các đối tượng Active Directory. Khi làm thế người dùng được uỷ quyền có thể xem và hiệu chỉnh thông tin trong Active Directory. Bằng cách kiểm soát hoạt động truy cập đối tượng, bạn (tức nhà quản trị) có thể giám sát chặt chẽ hoạt động mạng và đảm bảo rằng chỉ những người có thẩm quyền mới được phép truy cập tài nguyên.

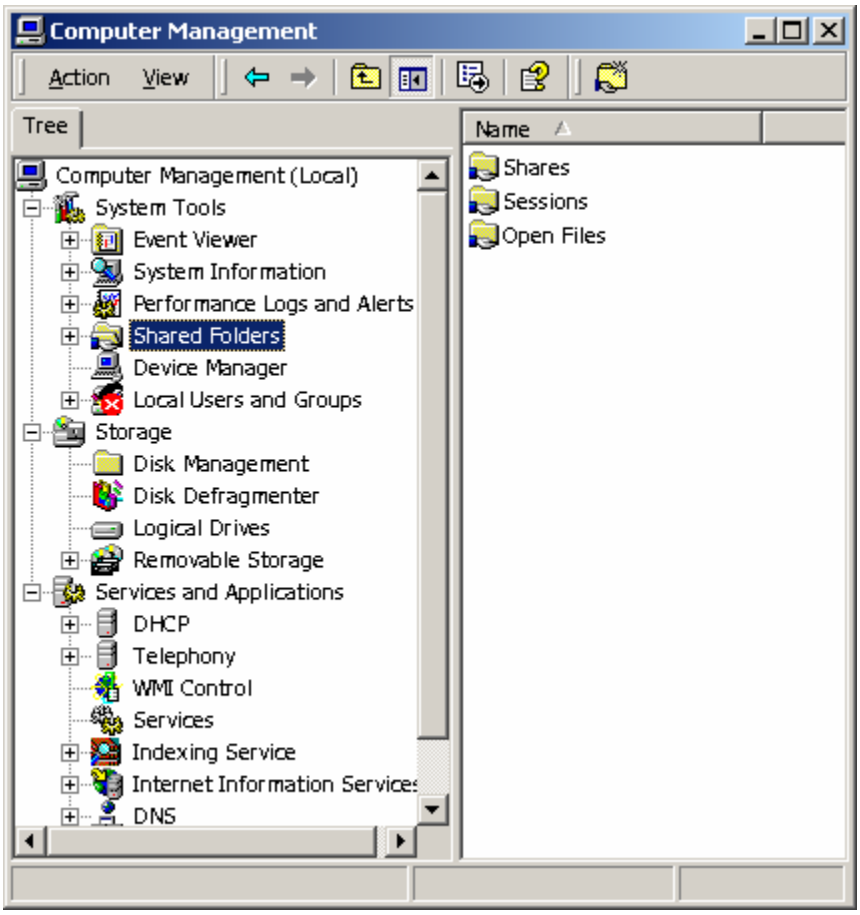
Chia sẻ thư mục trên hệ thống cục bộ và ở xa

Quyền truy cập thư mục dùng chung(tức thư mục được chia sẻ-Sharing folder) không tác động đến những người đang truy cập cục bộ vào trạm làm việc hay máy phục vụ, hiện chứa thư mục dùng chung.

- Bạn cấp quyền truy cập cho người dùng ở xa ngang qua mạng, dựa vào cơ chế chia se thư mục chuẩn.
- Áp dụng cơ chế chia sẻ Web để cấp quyền truy cập tập tin từ Web cho người dùng từ xa. Tuỳ chọn này chỉ khả dụng nếu hệ thống có cài đặt Internet Information Services

bạn có thể xem thư mục dùng chung trên trên máy tính cục bộ hoặc máy tính ở xa, bằng cách:

1. Trong Computer Management, nối kết với máy tính cần làm việc
2. Từ khung bên trái, mở rộng System Tools và Shared Folders, rồi chọn Shares. Các thư mục dùng chung hiện có trên hệ thống sẽ hiển thị.



3. Các cột của thư mục Shares cung cấp thông tin sau đây:

- **Shared Folder**: tên của thư mục dùng chung
- **Shared Path:** Đường dẫn honà chỉnh đẫn đến thư mục trên hệ thống cục bộ
- **Type:** Loại máy tính có thể sử dụng thư mục dùng chung.

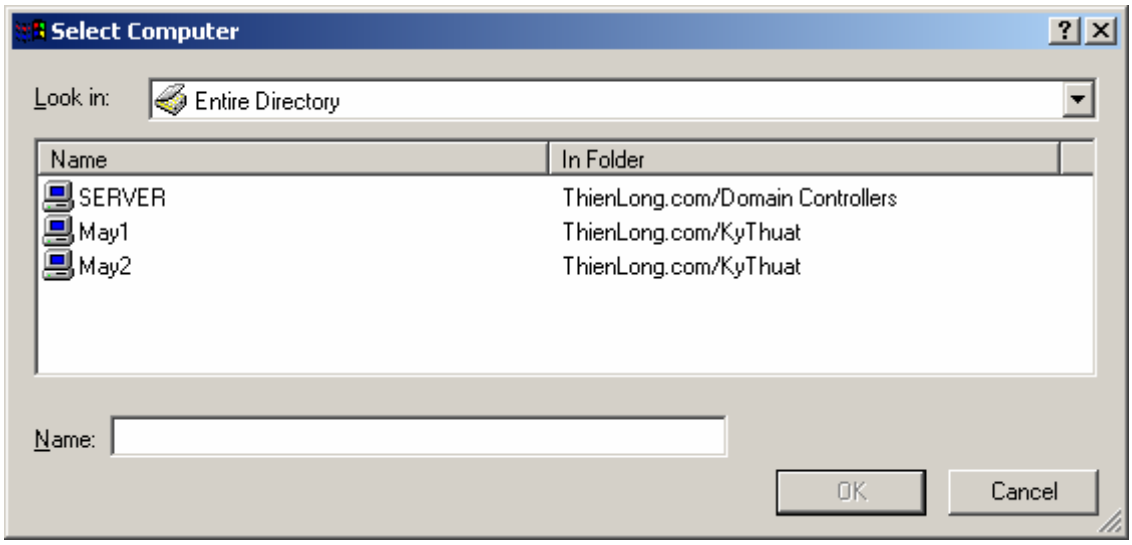
Tạo thư mục dùng chung

Microsoft Windows 2000 cung cấp hai cách chia sẻ thư mục: chia sẻ thư mục cục bộ thông qua Windows Explorer, hoặc chia sẻ thư mục cục bộ và từ xa bằng Computer Management

Do computer Management cho phép bạn làm việc và quản lý tài nguyên dùng chung trên máy tính mạng bất kỳ, nên rõ rằng đây là công cụ rất lý tưởng. Việc chia sẻ thư mục trên máy phục vụ Windows 2000 đòi hỏi bạn phải là thành viên nhóm Administrator hoặc Power Users

Trong computer Management, theo các bước sau để chia sẻ thư mục:

- Nhấp nút phải mouse vào khung bên trái, chọn Connect To Another Computer. Chọn máy



- Từ khung trái mở rộng System Tools và Shared Folder. Sau đó chọn Shares. Các thư mục dùng chung hiện có trên hệ thống hiển thị
- Nhấp nút phải mouse vào Shares, chọn New File Share khởi động Creat Shared Folder Wizard
- Tại trường Folder To Share, gõ đường dẫn tập tin cục bộ đến thư mục cần chia sẻ. đường dẫn phải thật chính xác, như C:\Data\CorpDocuments. Nếu không nhớ rõ đường dẫn, hãy nhấp chuột Browse, duyệt tìm thư mục với hộp thoại Browse For Folder.

- Gõ tên cho thư mục dùng chung. Đây là tên thư mục mà người dùng sẻ kết nối. Tên thư mục dùng chung không được phép trùng lặp đối với từng hệ thống
- Nếu thích, cứ việc gõ thông tin mô tả cho thư mục dùng chung. Sau này khi xem thư mục dùng chung trên máy tính cụ thể, thông tin mô tả sẽ hiển thị trong Computer Management
- Định rõ loại máy tính khách sẽ truy cập , máy tính này(không bắt buộc)
    - Microsoft Windows
    - Novell Netware
    - Apple Macintosh
- Chọn loại máy khách là Apple Macintosh, bạn thay đổi tên dùng chung mặc định cho người dùng Macintosh, bằng cách gõ tên mới vào trường Macintosh Share Name
- Nhấp Next, ấn định cấp độ truy cập cơbản cho thư mục dùng chung. Như minh hoạ ở hình 13.3, những tuỳ chọn khả dụng bao gồm:
    - **All Users Have Full Control**: Cho phép người dùng toàn quyền chi phối như thư mục dùng chung, có nghĩa người dùng có thể thi hành mọi tác vụ cần thiết với tập tin và thư mục dùng chung, như tạo, sửa đổi, xoá bỏ. Trên NTFS, tuỳ chọn này còn cho nfười dùng quyền thay đổi cấp độ truy cập và giành quyền sở hữu tạp tin, thư mục
    - **Administrators Have Full Control:Other users Have Read-Only Access**: Cho phép nhà quản trị có toàn quyền chi phối thư mục dùng chung. Người dùng khác chỉ được phép xem tập tin và đọc dữ liệu, chứ không thể tạo, sửa đổi, hay xoá bỏ tập tin, thư mục
    - **Adminstrators Have Full Control:** Other Users Have no Access Cho phép nhà quản trị có toàn quyền chi phối thư mục dùng chung, nhưngười dùng từ chối cấp quyền truy cập cho người dùng khác. Nhấp chọn tuỳ chọn này nếu muốn tạo thư mục dùng chung và sau đó mới cấp quyền truy cập cho Người dùng hoặc khi bạn định tạo thư mục quản trị dùng chung
    - **Customize Share And Folder Permissions:** Cho phép ấn định quyền truy cập cho Người dùng và nhóm cụ thể. Xem thông tin chi tiết ở mục Management Share Permissions
- Nhấp Finish, và kết thúc công việc.

Tạo thêm thành phần dùng chung trên thư mục dùng chung hiện có

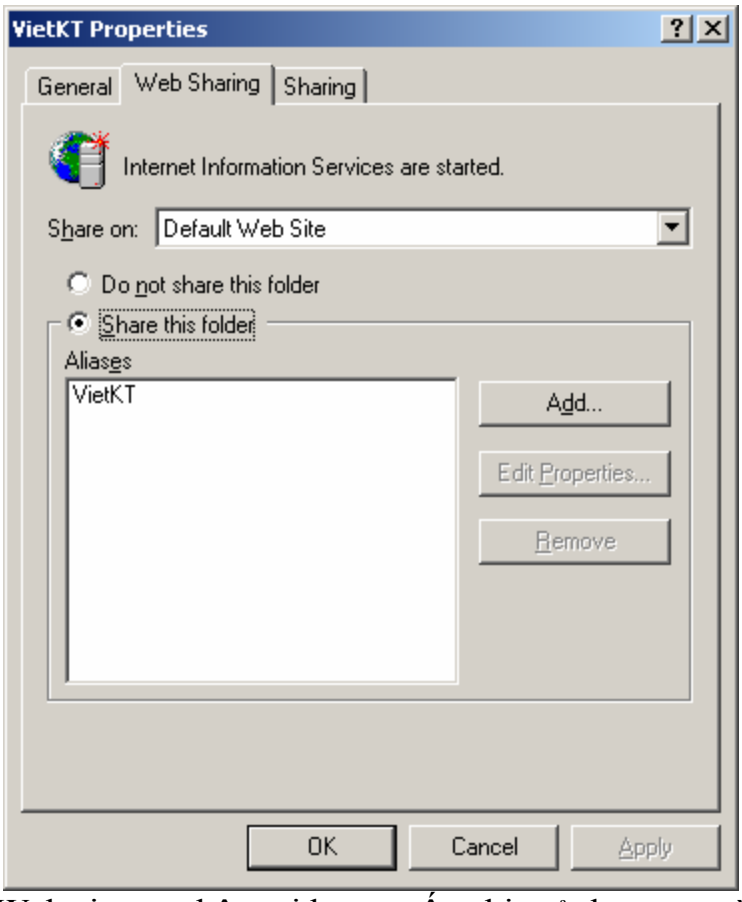
Một thư mục có khả năng chứa nhiều thành phần dùng chung có tên gọi khác nhau và được ấn định tập hợp cấp độ truy cập cũng khác nhau. Để tạo thêm thành phần dùng chung trên thư mục dùng chung hiện có, chỉ việc thực hiện theo thủ tục tạo thư mục dùng chung đã trình bày nay trước đó với một số thay đổi.

- Bước 3: Khi đặt tên thành phần dùng chung nhớ chọn tên hoàn toàn khác.
- Bước 6: Lúc gõ thông tin mô tả, hãy giảI thích mục đích sử dụng thành phần dùng chung đang tạo(và mục đích này khác biệt như thế nào với những thành phần dùng chung còn lại trong cùng thư mục).

Tạo thư mục Web dùng chung.

Nếu hệ thống bạn đang đăng nhập có cài Internet Information Services, bạn có thể tạo thư mục dùng chung truy cập từ trình duyệt Web. Dưới đây là cách tạo thư mục Web dùng chung.

1. Trong Windows Explorer nhấn nút phải mouse vào thư mục cục bộ cần chia sẻ, chọn Properties từ menu tắt.
2. Chuyển sang trang Web Sharing



3. Chọn Web site cục bộ, nơi bạn muốn chia sẻ thư mục, từ danh sách Share On.
4. Nếu đây là thư mục dùng chung đầu tiên, hãy nhất nút Share This Folder mở hộp hội thoại Edit Alias, bằng ngượclại nhấp Add.
5. Gõ bí danh vào trường Alias. *Bí danh* là tên bạn sẽ dùng để truy cập thư mục trên máu phục vụ Web. Trên này không được phép trùng lặp với các thư mục hiện đang được máy phục vụ Web sử dụng. Ví dụ, nếu gõ bí danh MyDir, bạn có thể truy cập thư mục theo đường dẫn http: / / locahost/MyDir.
6. ấn định cấp độ truy cập thư mục: Những tuỳ chọn khả dụng gồm có.

- **Read**: cho phép người dùng Web đọc tập tin chứa trong thư mục.
- **Write**: cho phép người dùng Web ghi dữ liệu vào thư mục.
- **Seript Souree Access:** cho phép người dùng Web truy cập mã nguồn cho kịch bản.
- **Directory Browsing:** Cho phép người dùng Web duyệt thư mục và các thư mục con trực thuộc.

7. ấn định cấp độ truy cập chương trình cho thư mục. Bạn có cả thảy ba tuỳ chọn:

- **None**: Cấm thi hành chương trình và kịch bản.

- **Scripts** Cho hép chạy kịch bản trong thưmục từ Web.
- **Excute** (Includes Scrípt) Cho phép thi hành chương trình và kịch bản trong thư mục từ Web.

8 Nhấp OK khi hoàn tất.

9. Muốn giới hạn truy cập nội dung của thư mục dùng chung trên Volume NTFS, bạn ấn định quyền truy cập tập tin và thư mục như được hướng dẫn ở mục " Quyền truy cập tập tin, thư mục"

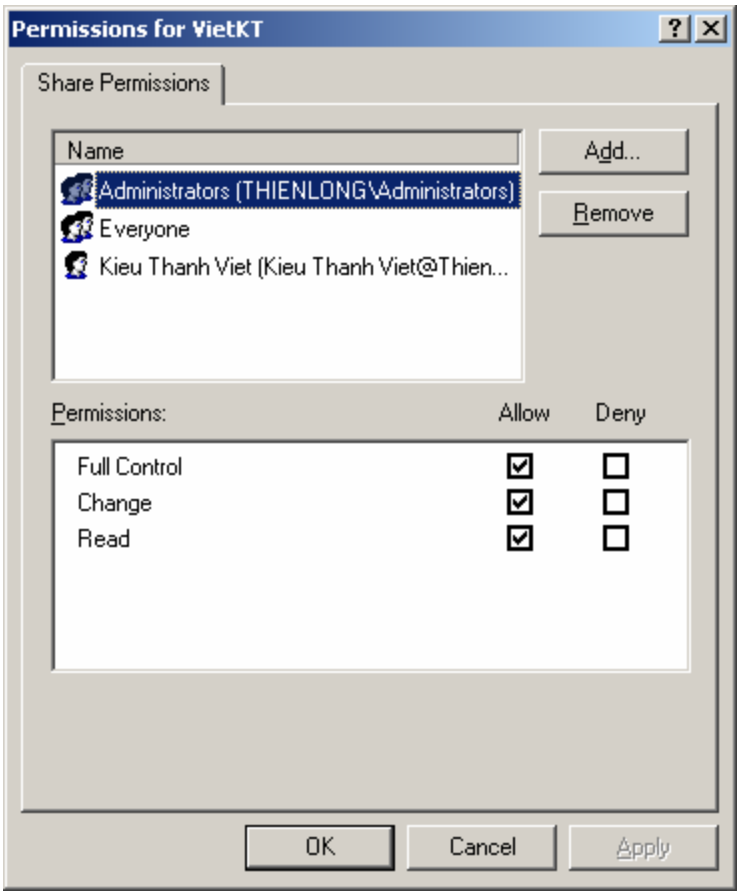
Quản lý cấp độ truy cập thư mục dùng chung.

Cấp độ truy cập thư mục dùng chung ấn định những hành đọng được phép thực hiện trong phạm vi thư mục. Mặc định, khi bạn tạo thư mục dùng chung, hễ ai có thể truy cập mạng là mặc nhiên có toàn quyền truy phối nội dung thư mục này . Với volume NTFS, bạn dựa vào quyền truy vập tập tin và thư mục hầu tăng cường giới hạn những hành động được phép thực hiện trong phạm vi thư mục dùng chung. Còn với volume FAT, quyền truy cập thư mục dùng chung chỉ cho phép kiểm soát hoạt động truy cập.

Những cấp độ truy cập thư mục dùng chung khác nhau

Cấp độ truy cập thư mục dùng chung khả dụng, từ giới hạn nhất định đến tự do nhất, bao gồm:

- **No Access:** không ai có quyền truy cập thư mục đang dùng chung này.
- **Read:** Cho phép người dùng.
- **Change:** Người dùng có quyền truy cập ở cấp độ Read và có thêm khả năng,tạo tập tin và thư mục con, Hiệu chỉnh tập tin, thay đổi thuộc tính của tập tin và thư mục con, xoá bỏ tập tin va thư mục con.
- **Full Control:** Người dùng có quyền Read và Change, cộng thêm những khả năng sau đây trên Volume NTFS.



Quản trị dịch vụ in và máy in mạng.

In ấn là một phần quan trọng trong môt trường mạng, việc dùng chung máy in chỉ là một phần nhỏ.

Tương tự như trong việc dùng chung tập tin, thư mục. Người sử dụng không cần biết là công ty, tổ chức có bao nhiêu máy in, đặt ở đâu và cấu hình ra sao mà họ chỉ cần biết rằng khi họ muốn in là in được ngay và in dễ ràng không chỉ trên một khổ giấy mà là nhiều khổ giấy. Như vậy, người quản trị mạng cần thiết lập môi trường in ấn sao cho phù hợp không chỉ tạo thuận lợi cho người sử dụng khi họ muốn in mà còn đảm bảo tính bảo mật của tài liệu in.

Thông thường trong một công ty, một tổ chức tương đối lớn họ sẽ có một phòng in ấn riêng. Trong đó có các thiết bị in ấn và có các máy chủ in ấn.

Thiết bị in ấn:
Là thiết bị vật lý dùng để thực hiện công việc in ấn. Chúng là các máy in các loại.
Máy chủ in ấn:
Là máy tính chứa trình điều khiển thiết bị in của một hoặc nhiều thiết bị in.
Các trình điều khiển thiết bị in ấn - Printer Driver
Printer Driver là những phần mềm cho phép hệ điều hành liên lạc trao đổi thông tin với máy in.
Bộ tập hợp in - Printer Spooler
Printer Spooler Là một tập hợp các thư viện liên kết động và trình điều khiển thiết bị in. **Printer Spooler** có chức năng nhận và xử lý, lập lịch biểu và phân phối các công việc in ấn. Nó được thực hiện bằng dịch vụ tập hợp in Spooler Service bắt buộc phải có thì mới in ấn được, bao gồm các thành phần sau đây:

- Bộ tiếp vận in - Print Router.
- Bộ cung cấp in tại chỗ.
- Bộ cung cấp in từ xa.
- Các bộ xử lý in.
- Bộ giám sát in.

Quá trình in ấn.
Quá trình in ấn được thực hiện theo những thứ tự sau:

- Người sử dụng chọn in từ một ứng dụng, làm cho ứng dụng đó gọi đến GDI, GDI gọi đến Printer Driver có liên kết với thiết bị in đích.
- Công việc in ấn được chuyển tiếp tới bộ tập hợp in. Thành phần phía máy khách của bộ tập hợp in thực hiện một cuộc gọi thử tục từ xa đến thành phần phía Server của chúng. Thành phần phía Server gọi đến bộ tiếp vận in.
- Bộ tiếp vận in chuyển công việc in ấn đến bộ cung cập in tại chỗ.
- Bộ cung cấp in tại chỗ chuyển giao với các bộ xử lý in.

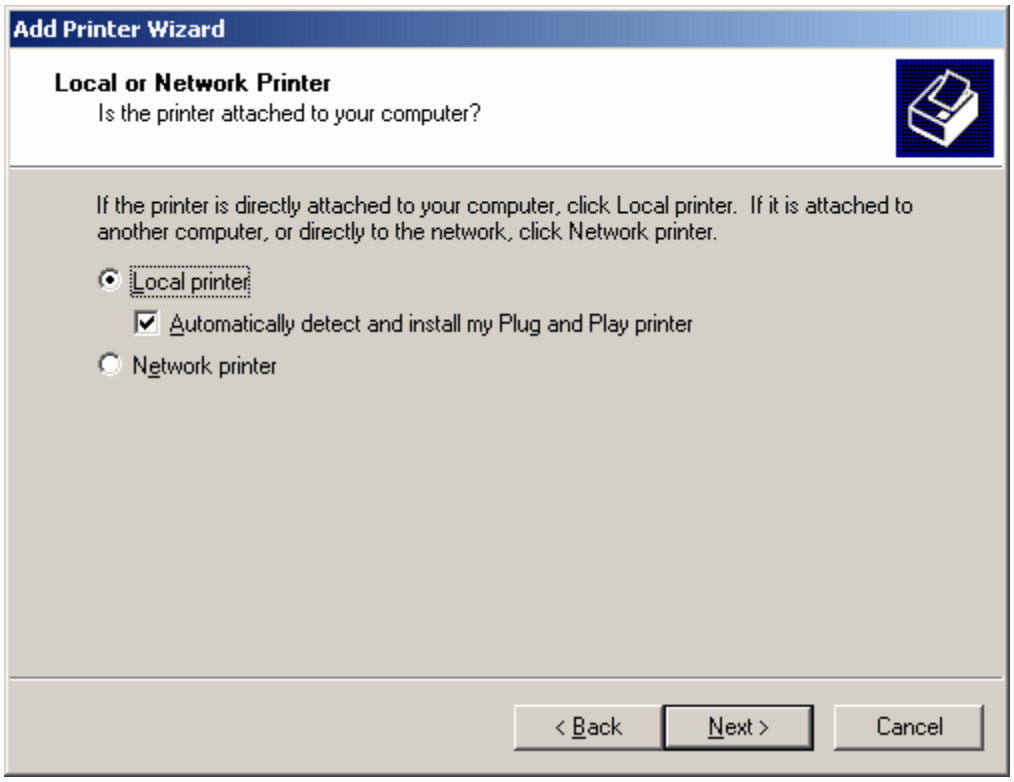
- Triệu gọi trang phân cách.
- Công việc in ấn được bộ giám sát in giám sát.
- Công việc in ấn được chuyển đến thiết bị in và in ra.

Cài đặt máy in.

Để thực hiện cài đặt một máy in ta thực hiện như sau:

* Trỏ vào Start | Setting | Printers để mở cửa sổ Printer.

* Nháy kép vào biểu tượng Add Printer để triệu gọi chương trình Add Printer Wizard. Màn hình Welcome xuất hiện, bấm vào Next.

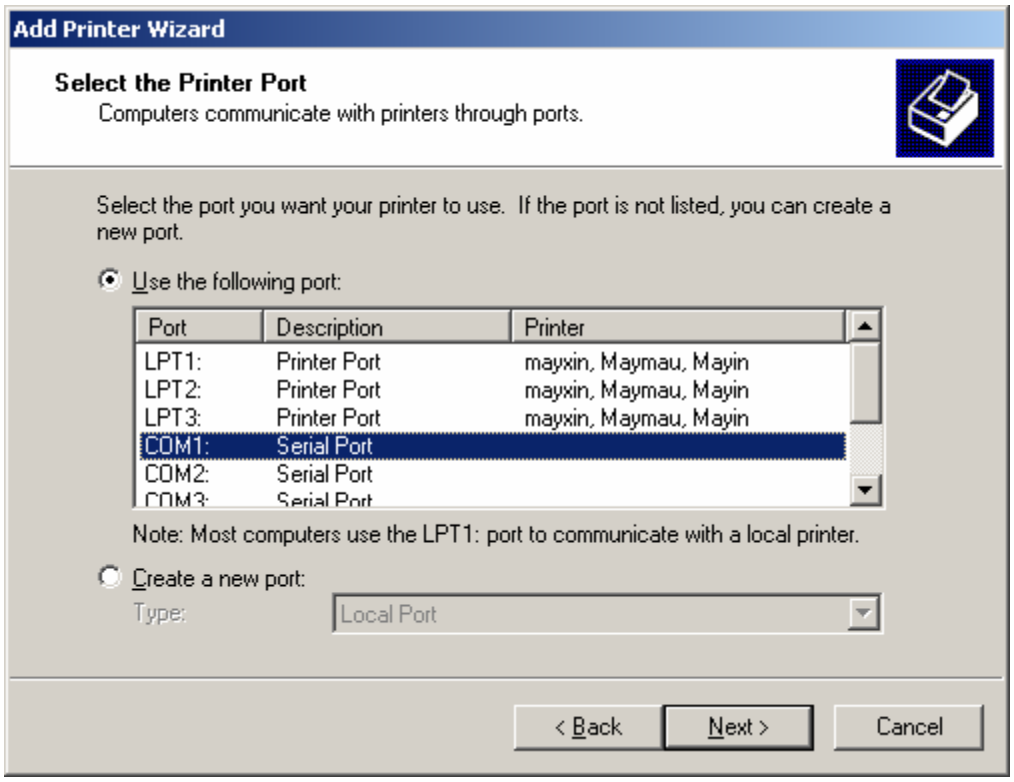


Trong cửa sổ Add Printer Wizard, chọn kết nói với máy in.

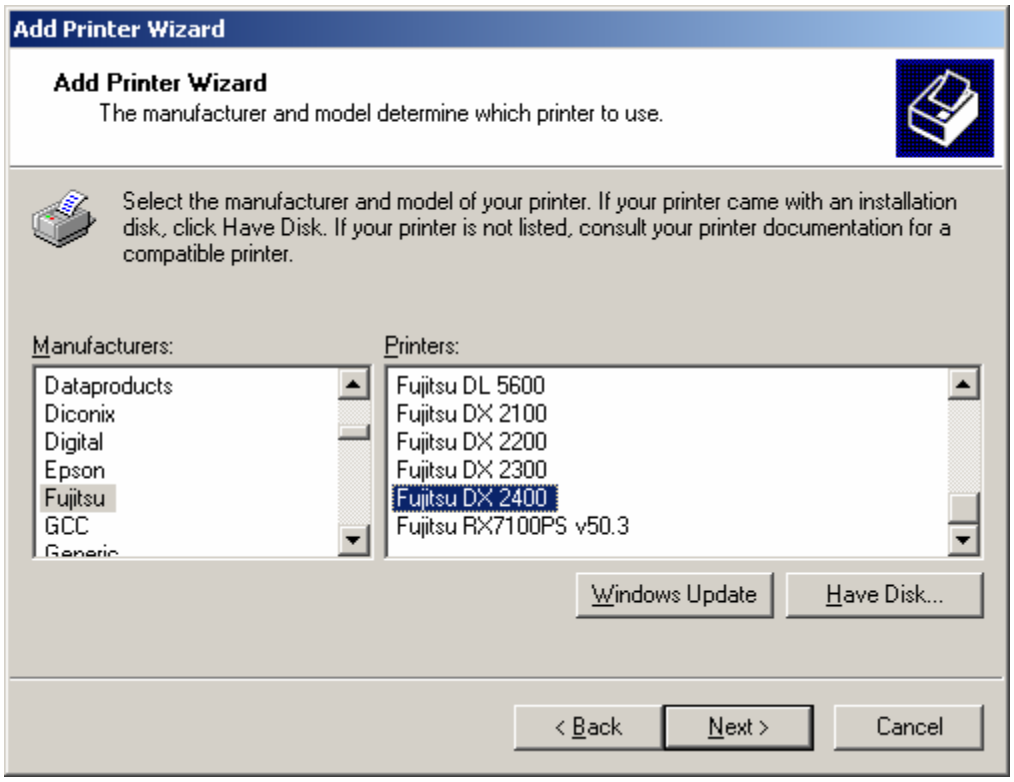
Nếu máy in được nối trực tiếp với máy tính đang được thực hiện cài đặt thì chọn Local Printer. Nếu dùng máy in mạng thì chọn Network Printer. Sau đó Next.

* Máy tính sẽ kiểm tra xem có máy in được kết nối không (Local). Nếu chọn Network Printer thì phải nhập tên hoặc đường dẫn của máy in.

* Chọn cổng kết nối cho máy in rồi Next.



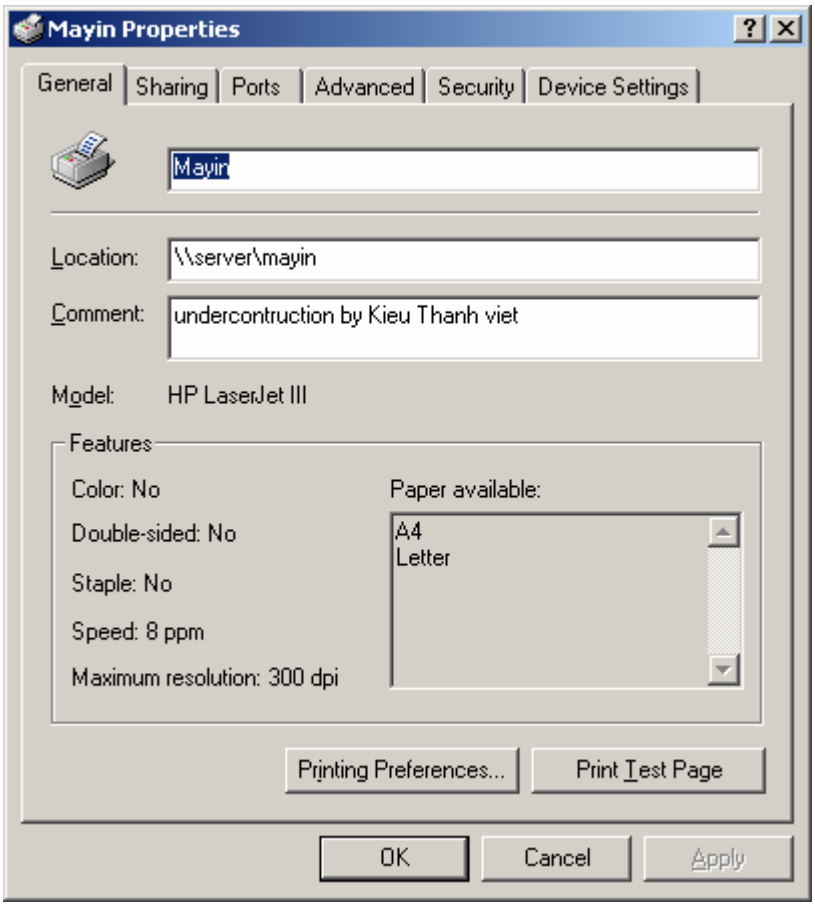
* Chọn nhà sản xuất và đời của máy in nếu có trong danh sách nếu không có, chọn Have Disk... và đưa đường dẫn tới vị trí của Driver.



* Nhập tên cho máy in và quyết định có chọn máy in đang được cài đặt có là máy in mặc định không. Rồi Next.
* Quyết định máy in đang cài đặt có được dùng chung hay không. Nếu không cho dùng chung thì chọn Do not share this Printer.
Nếu cho phép dùng chung máy in thì chọn Share as và nhập tên dùng chung cho máy in. Sau đó bấm Next.
* Nhập thông tin mô tả vị trí và chú thích cho máy in nếu thấy cần thiết. Next.
* Nếu muốn in thử thì chọn Yes và nếu không thì chọn No rồi Next.
Chọn Finish để hoàn tất qúa trình cài đặt.

Định cấu hình máy in.
Để cấu hình một máy in sau khi cài đặt ta làm như sau:

* Trong cửa sổ Printer, chọn máy in cần cấu hình, bấm chuột phải chọn Properties để mở cửa sổ Properties.



Trong cửa sổ này, người quản trị mạng sẽ cấu hình cho máy in như sau:

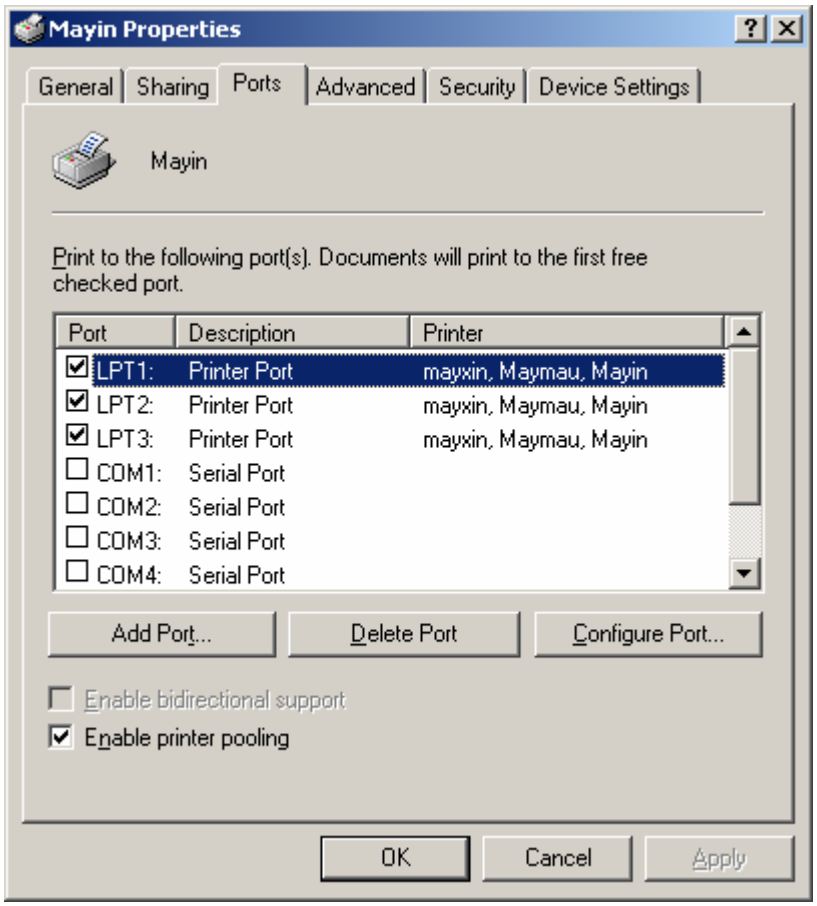
- Tab **Genaral**: Đặt các thông số như khổ giấy, form in, tên máy in, hướng in...
- Tab **Sharing**: Quyết định có cho phép máy in được dùng chung hay không.
- Tab **Port**: Bổ xung thêm cổng in, loại bỏ cổng in, đặt thông số cho cổng in và tạo ra bộ tập hợp in. Nếu không tạo ra bộ tập hợp in thì chỉ có thể chọn riêng biệt cho từng cổng in cho mỗi máy in riêng biệt. Nếu tạo ra bộ tập hợp in ấn, ta có thể tạo ra một tập hợp hàng đợi in, người sử dụng khi in một tài liệu từ một ứng dụng bất kỳ họ không cần biết tài liệu sẽ được in như thế nào khi đó bộ tập hợp in sẽ kiểm tra xem tài liệu in được gửi tới có phù hợp không nếu phù hợp trên máy in nào thì tài liệu sẽ được in trên thiết bị in phù hợp.

Để tạo ra bộ tập hợp in ta làm như sau:

Trong Tab Port, chọn Enable Printer Pooling, khi ta chọn Enable Printer Pooling thì ta có thể chọn đồng thời nhiều thiết bị in trên các cổng riêng biệt.

Điều này có nghĩa như sau:

Khi người sử dụng gửi một lệnh in, tài liệu sẽ được gửi tới bộ tập hợp in. Bộ tập hợp in sẽ kiểm tra xem cổng in nào còn rỗi. Nếu có cổng rỗi phù hợp với tài liệu in thì tài liệu in sẽ được in trên công đó. Nếu có càng nhiều thiết bị in ấn (có nhiều công in - số cổng in sẽ bằng số thiết bị in ấn) thì khả năng sẵn sàng in sẽ cao. Khi đó độ lưu thoát trong mạng sẽ cao và tài liệu sẽ được in nhanh chóng

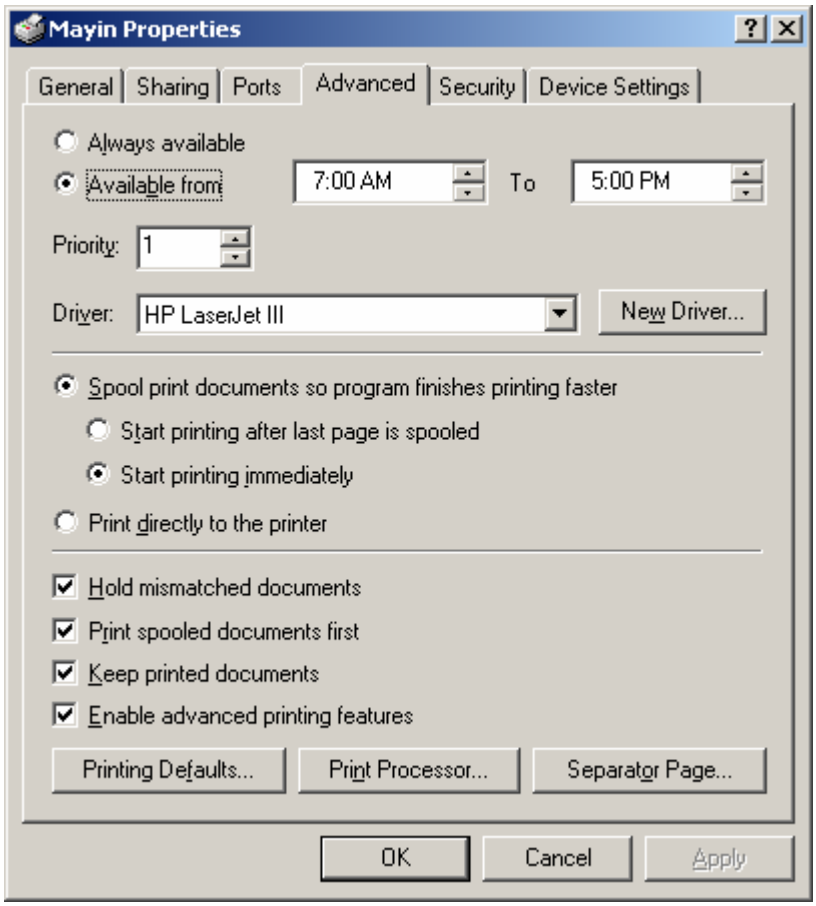


- Tab **Advanced**:

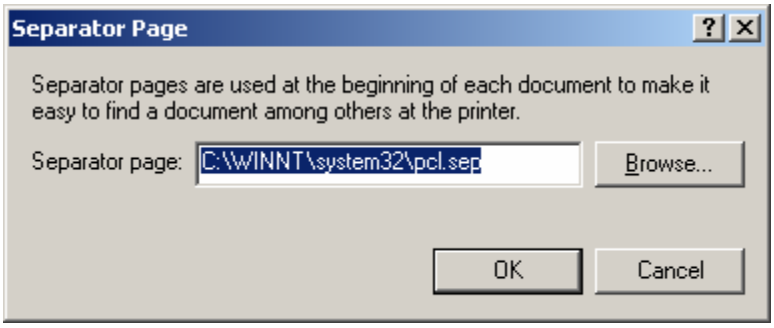
Đây là một tab quan trọng trong các mạng lớn có yêu cầu về in ấn cao. Trong tab Advanced người quản trị mạng sẽ xem xét đặt kế hoạch sao cho tài liệu in sẽ phù hợp với máy in, phù hợp với thời gian in và độ ưu tiên của tài liệu.

Các thông số lựa chọn như sau:

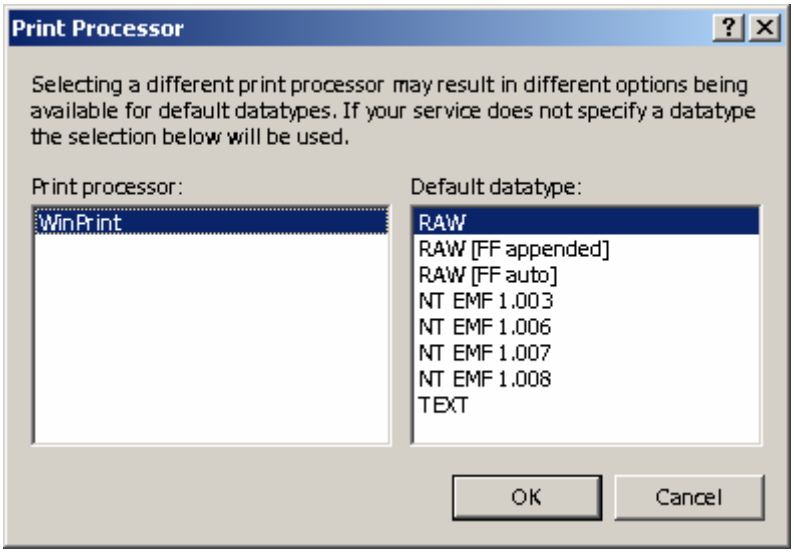
- Always available: Máy in luôn sẵn sàng in (24/24).
- Available from ... To... : Máy in có thể in từ giờ nào tới giờ nào.
- Priority: Độ ưu tiên của tài liệu in. Tài liệu in nào có độ ưu tiên cao hơn sẽ được xử lý trước. Độ ưu tiên được đánh số từ 1 tới 99.



- Spool Print Document so Program Finishes Printing Faster:
  Dùng bộ tập hợp in cho các tài liệu in.
- Print Directly to the Printer:
  In trực tiếp ra máy in, khi đó lựa chọn này sẽ loại bỏ bộ tập hợp in.
-
- Trang phân cách - Serparator Space:
  Khi có nhiều tài liệu của nhiều người sử dụng cùng in thì phải có một cơ chế để phân loại tài liệu in của từng người. Để có thể phân loại tài liệu in của từng người ta dùng trang phân cách Serparator Space. Trong cửa sổ Properites chọn Tab Advanced và chọn nút lệnh Serparator Page.



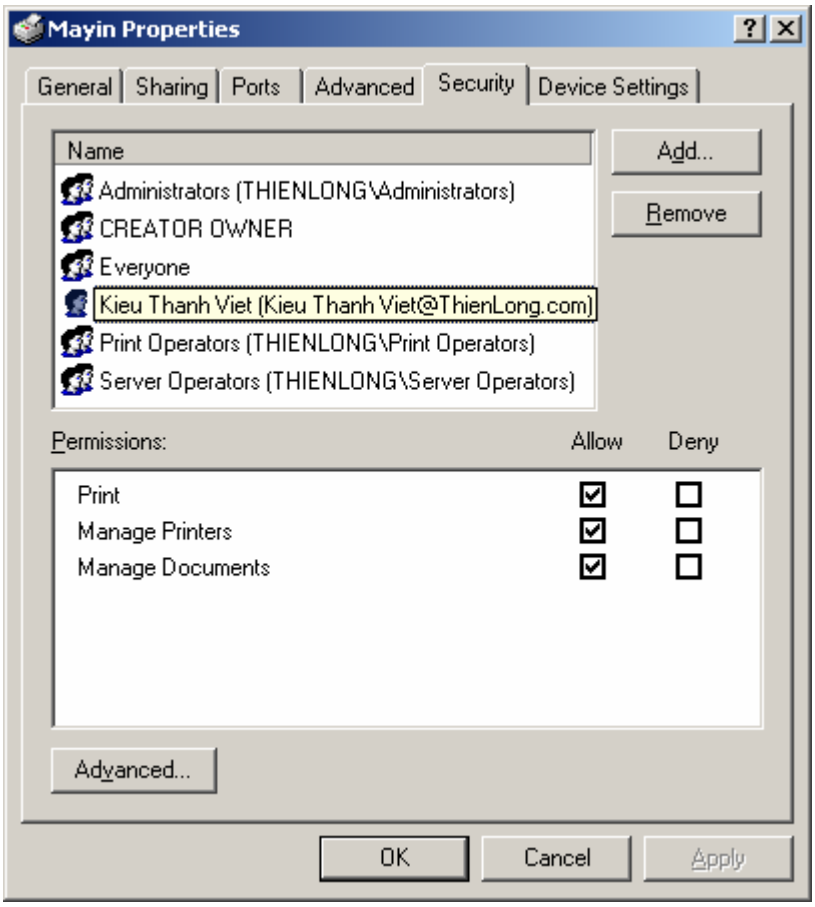
  Trong cửa sổ Separator Page bấm vào nút lệnh Browse chọn trang phân cách cần sửu dụng rồi OK.
- Bộ xử lý in: Print Procceser: Print Procceser sẽ quyết định tài liệu in gửi từ máy khách tới bộ tập hợp in có cần xử lý không. Trong cửa Print Properties chọn tab Advanced và chọn nút lệnh Print Procceser.



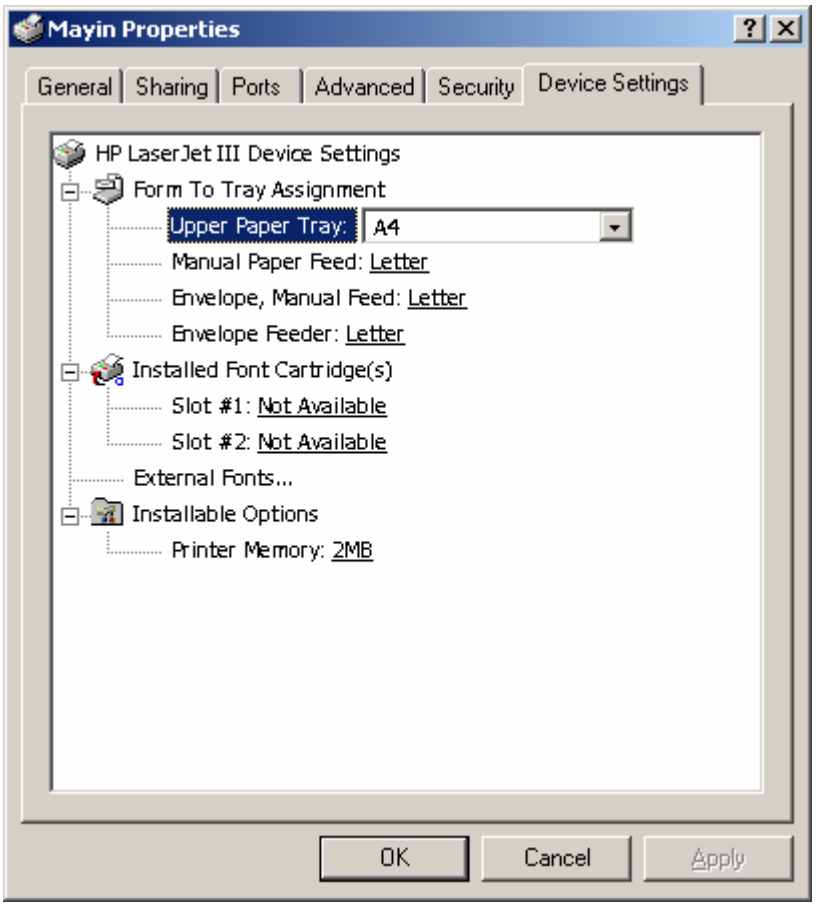
Trong cửa sổ Print Processor chọn kiểu dư liệu và OK.

- Tab Security: Đây là tab rất quan trọng về bảo mật. Trong Tab này người quản trị sẽ chỉ rõ ràng vai trò của người sử dụng trong mạng. Người nào là người có quyền quản lý tài liệu in, quản lý thiết bị in, và quản lý máy in.
  Để bổ xung người sử dụng hoặc nhóm nào đó vào trong danh sách ta bấm vào nút lệnh Add, và để loại bỏ người sử dụng, nhóm nào đó ta chọn trong danh sách và nhấn vào nút Remove.

  Trong khung Permission:
  Có hai lựa chọn: Allow: Cho phép và Deny: Không cho phép
  Muốn cấp quyền hay không cấp quyền nào đó cho người sử dụng, nhóm người sử dụng ta đánh dấu vào người sử dụng và trong khung Permission ta cấp quyền cho người sử dụng hoặc nhóm người sử dụng đó.



Tab Device Setting:



Windows Terminal Services

Vận hành một mạng Windows 2K lớn.

Trong phần này, chúng ta sẽ đề cập những khái niệm về Win 2K rộng hơn mức một server và vài máy trạm, đến phạm vi mạng dành cho toàn bộ một danh nghiệp lớn. Tức là, cho đến nay bạn đã đọc về Active Directory, các chính sách nhóm site, và việc sao chép folder SYSVOL..., thế nhưng những khái niệm về Win 2K trong phần trước sẽ thay đổi ra sao khi bắt đầu mở rộng các dịch vụ đó ra? Thực ra, Win 2K nói chung và Active Directory nói riêng, đã được thiết kế chủ yếu dành cho các nhà doanh nghiệp lớn. Do số lượng của các cơ sở hạ tầng mới quá nhiều,

nên chương trình này chỉ bàn về một số điều cần suy nghĩ khi muốn triển khai rộng khắp Win 2K trong môi trường mạng doanh nghiệp.

Các vấn đề về thiết kế Active Directory.

Khi bắt đầu suy nghĩ về cách triển khai Win 2K và Active Directory, những mối quan tâm đầu tiên hẳn là xung quanh việc hoạch định NameSpace AD . Người quản trị sẽ phải dự trù có bao nhiêu miền Win 2K, bao nhiêu cây, bao nhiêu rừng. Tiêu chuẩn để bổ sung thêm miền, cây, và rừng mới là gì? Khó có thể nhấn mạnh đầy đủ tầm quan trọng của việc hoạch định cẩn thận những gì bạn sẽ có được khi bạn chuyển từ môi trường mạng hiện tại của bạn - có thể là NT 4, NDS, hay một thứ gì đó hoàn toàn khácsang một cơ sở hạ tầng dựa trên Win 2K. Đây đòi hỏi không chỉ phải suy tính về mục tiêu tối hậu (chẳng hạn: cuối cùng phải hợp nhất lại thành một miền duy nhất), mà còn phải suy nghĩ về cách thức để được điều đó, quá trình đó sẽ diễn ra trong bao lâu, và làm cách nào để bạn chấp nhận được những trường hợp ngoại lệ đối với cách thiết lập AD .

Rừng của toàn doanh nghiệp

Để bắt đầu, chúng ta hãy làm quen một số vấn đề mà người quản trị chắc chắn sẽ gặp khi xây dựng cơ sở hạ tầng AD lớn. Chúng ta bắt đầu từ phần trên cùng: *gốc của rừng* (forest root). Khi xây dựng máy DC Win 2K đầu tiên trong miền Win 2K đầu tiên, người quản trị được hỏi rằng đây có phải là DC đầu tiên trong cây có miền đó (gọi tắt là *cây miền*-domain tree), và cây này có phải là cây đầu tiên trong rừng hay không. Nếu trả lời Yes cho hai câu hỏi này, người quản trị đã vô tình thực hiện vài quyết định quan trọng về tương lai Active Directory mạng. Bất luận người quản trị đưa bao nhiêu cây miễn vào trong rừng, miền đầu tiên này, được gọi là gốc rừng, cũng đóng vai trò đặc biệt trong cơ sở hạ tầng AD.

Với Active Directory trong Win 2K, người quản trị không thể gỡ bỏ hoặc đổi tên gốc của rừng bên trong AD. Do đó bởi vai trò quan trọng của nó, nó phải được giữ nguyên như thế trong suốt cuộc đời của rừng. Vì vậy, hãy xem miền gốc của rừng này như một "khoảng chứa nền tảng" đối với tổ chức AD. Tức là, người quản trị chỉ nên dùng miền này để chứa các phần tử nền tảng thôi. Để chứa những đối tượng làm việc của người quản trị, chẳng hạn như User, các Computer, các Printer, và v.v..., Hãy xây dựng các miền con dưới các miền đó. Trong miền gốc đó, người quản trị chỉ dữ lại một nhóm quản trị viên có quyền hành trên toàn mạng, được quyền trực hiện những thay đổi với các phần tử nền

tảng, như các site và *giản đồ* (schema) của AD chẳng hạn, và bổ sung thêm các cây miền khác.

Việc sửa đổi giản đồ, hợp nhất các rừng

Khi bành trướng môi trường AD, một vấn đề khác không thể không quan tâm là *giản đồ tổ chức*(schema) của nó. Schema của một AD là kiến trúc và mối quan hệ giữa các lớp và thuộc tính của cơ sở dữ liệu này.Win 2K được bán ra với một schema kèm sẵn, nhưng người quản trị có thể mở rộng nó ra để đáp ứng nhu cầu của mình. Bằng cách dùng công cụ snap-in Schema AD MMC, hoặc thông qua Active Directory Sevices Interface (ADSI)- một bộ các API để truy cập vào Active Directory và các hệ dịch vụ danh bạ khác bằng cách lập trình, người quản trị có thể tự do đưa các lớp và thuộc tính theo ý muốn của riêng mình vào Active Directory của cơ quan . Ý tưởng này rất có ích nếu người quản trị có toàn quyền kiểm soát môi trường AD , nhưng nó gây ra không ít vấn đề khi cơ quan bạn phình to lên hoặc teo nhỏ lại. Đó là vì , hiện giờ, đối với mỗi rừng, người quản trị chỉ có áp dụng một Schema mà thôi. Khi người quản trị định rõ rừng của mình, Schema đặt tại miền đầu tiên sẽ được sao chép vào tất cả các miền khác trong cây và tất cả các cây sau đó tham gia vào vùng ấy.

Bây giờ, chúng ta thử xem xét một kịch bản, trong đó cơ quan bạn vừa mua lại một công ty mới, hoặc một chi nhánh có sẵn trong cơ quan bạn vừa xây dựng cơ sở hạ tầng AD riêng của họ. Trong cả hai trường hợp ấy, hẳn là phải có một rừng có sẵn nhưng riêng biệt với rừng (cũ hoặc chính) của cơ quan bạn (bởi vì công ty mua được kia khi cài đặt miền AD đầu tiên của họ, hẳn cũng đã xây dựng rừng riêng của họ rồi). Hơn nữa, mỗi thứ rừng riêng biệt nay có thể thực hiện nhưng thay đổi schema dối với nó, khiến nó không tương thích với rừng của bạn nữa. Trong phiên bản Win 2K hiện tại, không có công cụ nào có thể dùng để hợp nhất các rừng hoặc các schema cả . Điều đó có nghĩa là, người quản trị chỉ có hai điều để chọn. Chọn lựa thứ nhất là , người quản trị có thể tạo ra những mối quan hệ uỷ quyền không bắc cầu(Nontranstive Trus Relationship) tường minh giữa các miền trong rừng để cho các truy cập trong 1 vùng để cho phép truy cập các miền trong rừng kia (theo kiểu các quan hệ uỷ quyền của NT 4). Trong trường hợp này, người quản trị có thể duy trì nhiều rừng bên trong mạng của cơ quan.

Giải pháp này có những ưu và khuyết điểm của nó, thực ra không có giải pháp nào tối ưu để quản trị nhiều rừng cả. Trong một môi trường đa rừng, không có quyền lực quản trị chung đâu. Các thành viên của

Enterprise Admins từ một rừng không có quyền lực gì trên mỗt rừng khác, trừ khi được chỉ định một cách tường minh thông qua các mối quan hệ uỷ quyền.
Một chọn lựa khác để giải quyết vấn đề nhiều rừng là người quản trị có thể quyết định giữ lại một rừng trong số đó, rồi dùng các công cụ được Microsoft (hoặc một hãng khác) cung cấp để chuyển (Migrate) các đối tượng từ các đối tượng từ các rừng còn lại. Trong các trường hợp sau này, người quản trị sẽ có thể hành xử với các rừng khác "ngoại lai" ấy như thể chúng là các miền NT 4 đời cũ cần được chuyển vào các miền Win2K vậy. Dĩ nhiên, tất cả những thay đổi về Schema đã được thực hiện trong các vùng ngoại lai ấy sẽ bị mất đi khi người quản trị chuyển đổi đối tượng đó vào rừng của cơ quan.

Các site

Các site là các danh giới đối với ba *khung cảnh định danh* (naming context) được mô tả bên dưới. Bên trong một site, sự sao chép các khung cảnh định danh này là tự động, và theo mặc định sẽ diễn ra năm phút một lần. Người ta có thể tạo ra site để liên kết các nhóm các mạng con (subnet), nhằm đại diện cho một nhóm các mối nối liên kết có bandwidth cao. Các site cũng có thể băng ngang qua các ranh giới miền - người quản trị có thể nhóm hai DC từ những miền khác nhau vào trong cùng một site. Các site còn có một vai trò khác, chứ không phải chỉ để kiểm soát và sao chép thông tin định danh. Ví dụ, người quản trị có thể tạo ra các đối tượng chính nhóm (GPO) trên các site, cho phép người quản trị liên kết việc quản lý các máy trạm với một mạng con cụ thể trên mạng. Khi mạng Win2K n tăng trưởng, việc duy trì bảo quản các site cũng tăng theo.
Các site được tự tay người quản trị mạng xây dựng lên. Nhưng chú ý rằng, người quản trị chỉ có thể quy định các site khi ở bên trong miền gốc của rừng. Cho dù bạn có thể nạp công cụ snap-in của MMC tên là AD Sites và Services với trọng tâm đặt tên máy DC của một miền con, nhưng người quản trị không thể quy định các site ở đó được đâu. Điều này ngăn không cho các quản trị viên trong các miền con ngẫu nhiên quy định các site ảnh hưởng không tốt đến Topology sao chép của người quản trị.
Đi đôi với các site là các đối tượng mạng con. Người quản trị phải tự tay quy định mỗi mạng con IP luận lý bên trong cơ sở hạ tầng Active Directory, rồi liên kết các mạng con đó với đối tượng site phù hợp. Hơn nữa, người quản trị phải liên kết các site mà họ quy định với một *liên kết site* (site link) đã đinh. Các site link cho phép người quản trị n nhóm các site có cùng *chi phí* hay *giá* (cost) theo quan điểm truyền dữ liệu trên mạng. Quá trình vừa tự tay quy định các site và site link, vừa tự tay liên kết các mạng con với chúng trong một cơ sở hạ tầng AD lớn có thể

rất nặng nhọc! Mỗi site link và mỗi đối tượng mối nối kết NTDS giữa các server trong mỗi site còn đòi hỏi người quản trị phải quy định lịch biểu sao chép nữa.
Khi người quản trị bành chướng cơ sở hạ tầng AD của họ ra hàng trăm site và hàng chục site link, công việc chăm sóc bảo trì lịch biểu đồ sộ này có thể nhanh chóng chiếm hết thời gian làm việc của người quản trị. Hiện nay, công cụ duy nhất mà người quản trị có thể tuỳ ghi sử dụng là công cụ snap-in cho MMC tên là AD sites and Servicer. Rõ ràng Microsoft phải mau mau cung cấp một giao điện tốt hơn để quản lý các site trong một cơ sở hạ tầng Win2K lớn.

Các Organizational Unit - OU.

Đối với các OU trong một co sở hạ tầng AD lớn, nguyên tắc cần chú ý là: Giữ cho chúng đơn giản thôi! sự kiện có thể xây dựng các OU trong AD và có được một chỗ tiện lợi để uỷ thác quyền quản trị có thể bị lạm dụng quá đáng. Microsoft khuyến cáo rằng không nên nhiều hơn 10 cấp OU, nhưng thực ra mà nói, khó mà kiểm soát được sự phức tạp của một hệ thống cấp bậc sâu đến vậy. Căn cứ vào mô hình kế thừa (inheritance) bên trong AD, nếu người quản trị quản lý 10 cấp OU lồng nhau mỗi cấp thường đi kèm một mức độ bảo mật, một kiểu cách được quản trị được uỷ quyền, và các GPO của nó, hẳn người quản trị sẽ gặp nhiều khó khăn! Cách tiếp cận tốt nhất khi cơ sở hạ tầng AD của bạn tăng trưởng là bắt đầu bằng một cấu trúc OU càng phẳng càng tốt. (Phẳng có nghĩa là có ít tầng lớp thôi).
Sau đó, lúc nào bạn cũng có thể dời các đối tượng từ chỗ này sang chỗ khác bên trong ,khi bạn tìm ra những kiểu cách tốt hơn để tập hợ người dùng.
Trong khi thiết kế AD, bạn thường phải cân nhắc, chọn lựa giữa các yếu tố mâu thuẫn (trale-off) như sau: trong nhiều trường hợp người quản trị có thể nhóm các đối tượng lại bằng các OU hoặc bằng các nhóm bảo mật (security group) đều được. Ví dụ, người quản trị có thể ràng buộc một nhóm người dùng trong bộ phận tài chính của cơ quan bằng cách tạo ra một OU tên là Finance hoặc bằng cách tạo ra một nhóm bảo mật tên là Finance bên trong một OU lớn hơn. Chọn con đường nào là tuỳ mục tiêu của người quản trị. Khi trói buộc một nhóm người bên trong một OU, người quản trị làm cho việc tách riêng những người dùng đó để uỷ thác quyền kiểm soát và áp đặt các chính sách nhóm trở nên dễ dàng hơn. Tuy nhiên, nếu những người dùng trong OU đó cũng nhận được chính sách nhóm giống y như bốn hay năm OU khác, với những nhu cầu tương tự thôi, khi đó chia OU chỉ là chuyện vô ích. Trong trường hợp đó người quản trị phải hoặc tạo thêm những GPO khác, hoặc liên kết những GPO có sẵn từ một OU khác vào GPO mới của họ.

Nếu phân chia người bảo mật thông qua các nhóm người bảo mật bên trong cấu trúc OU chung hơn, lớn hơn, người quản trị có thể thấy rằng khi đến lúc phải quản lý nhu cầu đặc biệt của những người dùng nào đó, sẽ khó hơn để chon lọc được họ ra khỏi đám đông một cách êm xuôi. Rốt cuộc, nhằm có được mức độ kiểm soát cấu hình và quản trị thích hợp đối với người dùng của mình, chắc hẳn phải chọn một sự kết hợp nào đó của các nhóm OU và các nhóm bảo mật để quản lý và cách ly họ.

Các GPO

Sử dụng các đối tượng chính sách nhóm (GPO) là một tính năng mạnh mẽ trong Win2K, nhưng nó cũng là tính năng dễ gây ra cho người quản trị những cơn ác mộng quản trị nhất khi người quản trị mở rộng hạ tầng cơ sở AD của họ. Một phần do người quản trị có thể quy định các GPO ở quá nhiều cấp khác nhau, và một phần là do Microsoft cung cấp quá ít những công cụ giải quyết trục trặc để xác định những gì đang diễn ra trong quá trính xử lý các GPO. Xin nhắc lại, các GPO có thể được quy định ở các cấp: máy tại chỗ, site, miền, và OU; chúng được *truyền* hay *thừa hưởng* (inherit) từ cấp trên xuống cấp dưới, và tác dụng của chúng có thể được lọc chắn thông qua các nhóm bảo mật. Ngoài ra, các GPO chỉ được sử lý bằng các đối tượng máy hoặc đối tượng người dùng thôi. Người quản trị có thể quy định nhiều GPO ở mỗi cấp trong hệ thống cấp bậc của AD. Người quản trị có thể để cho một số GPO phủ quyết (override) một cách thô bạo các GPO khác, hoặc ngược lại, người quản trị có thể ngăn chặn việc phủ quyết một GPO nào đó. Cuối cùng, mỗi GPO chứa một số *đốt* (node) chức năng khác nhau, mỗi đốt đó cung cấp một mức độ kiểm soát đôi khi chẳng có liên quan gì với nhau cả đối với người dùng và máy tính được áp dụng chính sách đó. Tất cả những chuyện này được tạo ra nhằm có được một môi trường nhiều khả năng và phức tạp đối với người kiểm soát đối với người dùng và máy thông qua các GPO. Vậy thì, người quản trị có thể làm gì trong việc quản lý các GPO để thu được lợi ích từ những khả năng quan trọng của chúng ? Câu trả lời cũng như câu trả lời đối với việc quản lý nhiều khái niệm của cơ sở hạ tầng AD - giữ cho nó càng đơn giản càng tốt. Chuyện có thể quy định nhiều GPO ở nhiều cấp trong hệ thống bậc AD không có nghĩa người quản trị phải làm như thế? Ví dụ, mỗi GPO có chứa nhiều đốt chức năng chẳng hạn, Software Installation, Security, Logon/Logoff Scripts, Folder Redirection, Administrative Templates, …; tại sao chúng ta không nhóm một số đốt ấy lại trong GPO cho dễ quản lý và sử dụng? Ví dụ, người quản trị có thể quy định một GPO " security", chỉ có chức năng duy nhất là triển khai các nhóm chọn lựa và bảo mật đối với người dùng và máy thôi . Bằng cách này, người quản trị có thể dễ dàng

uỷ quyền quản trị GPO đó cho những quản trị viên chuyên về bảo mật và phần mềm khiến không khai triển được Microsoft Word ra toàn xí nghiệp .

Tương tự, ngoài việc quy định các GPO có chức năng duy nhất hoặc hạn chế, người quản trị nên tính tới việc hạn chế số lượng GPO được quy định bởi các cấp site, miền, và OU. Việc quy định các GPO ở cấp miền chỉ nên dành cho chính sách nào có ảnh hưởng trên toàn miền thôi, như chính sách bảo mật chẳng hạn. Hãy để lại các chính sách cài đặt phần mềm hoặc khuôn mẫu quản trị cho các OU. Lợi ích của chiến lược này sẽ trở nên rõ ràng khi tính tới bộ *chính sách tổng hợp* (Resultant Set of Policy_ RSOP).

RSOP thực chất là *chính sách hiệu dụng* (tức là hiệu quả thực tế khi áp dụng nhiều chính sách) trên một người dùng hoặc một máy tính bên trong container đã định trong cơ sở hạ tầng AD. về lĩnh vực này, Microsoft chỉ cung cấp ít công cụ trợ giúp. Tuy nhiên, một số hãng phần mềm quản trị khác, nhu Full Armor chẳng hạn (www. full armor. com) dự dịnh cung cấp các công cụ RSOP để giúp người quản trị quản lý việc triển khai các GPO trên mạng. Nếu dự định triển khai các GPO một cách quy mô trong Win2K, người quản trị nên tìm cách có được các công cụ này.

Một điểm khác cần quan tâm là thời gian tiêu tốn cho việc sử dụng các GPO vào lúc người dùng đăng nhập hoặc máy khởi động. Người dùng hoặc máy phải xử lý nhiều GPO, thì thời gian trì hoãn lúc đăng nhập hoặc khởi động. Điều này đáng chú ý vào lúc người dùng đăng nhập, bởi vì các GPO bình thường được xử lý trước lúc shell cuả người dùng được nạp . Người quản trị có thể sửa đổi kiểu này thông qua một chính sách khuôn mẫu quản trị, như trong nhiều trường hợp, có thể người quản trị không muốn làm như vậy.

Căn cứ theo kiểu hành sự này, người quản trị nên làm bất cứ điều gì có thể làm được nhằm tối thiểu hoá thời gian xử lý các GPO. Microsoft đã cố gắng sắp xếp hợp lý hoá việc xử lý các GPO theo nhiều cách. Trước hết, họ cho phép người quản trị chọn vô hiệu hoá các thiét định cấu hình của người dùng hoặc các thiết định cấu hình của máy trong GPO cụ thể. Nếu người quản trị đã quy định một GPO có chức năng duy nhất là ấn định chính sách trên một đối tượng nào đó, thì bạn nên duyệt vào ô thích hợp trong trang đặc tính Group Poliry để vô hiệu hoá việc xử lý đối với phần đó của GPO. Như thế sẽ làm giảm một cách đáng kể thời gian tiêu tôn cho việc xử lý các GPO. Ngoài ra, phiên bản của GPO cũng sẽ được theo dõi sát sao vào mỗi lúc xử lý. Nếu không có thay đổi nào đã xẩy ra vào khoảng thời gian giữa các người dùng đăng nhập hoặc máy khởi động, thì GPO sẽ không được xử lý. Có một khuôn mẫu quản

trị có thể dùng được để phủ quyết lối hành xử này, nhưng nó sẽ làm tăng thêm thời gian xử lý một cách đáng kể.

Việc sửa đổi các GPO

Một vấn đề nữa cần để ý khi triển khai các GPO: bởi vì các GPO cũng là một đối tượng trong Active Directory, nên chúng cũng phải chịu tác động của nhiều quá trình sao chép multimaster (nghĩa là sao chép từ DC này sang DC khác, khắp các miền trong mạng) nhưng các đối tượng AD khác. Vì thế, vào một lúc nào đấy, rất có thể có hai người chỉnh sửa một GPO. Dĩ nhiên, hậu quả có thể rất nghiêm trọng nếu như những sửa đổi của họ đối nghịch lẫn nhau vào lúc sao chép. Để ngăn ngừa viễn cảnh này, công cụ snap-in Group Policy theo mặc định sẽ luôn luôn đặt trọng tâm tác động (focus) vào DC nào hiện đóng vai trò PDC của miền AD đã định để chỉnh sửa GPO. Người quản trị có thể thấy được điều này bằng cách chọn menu **View** trong khi đang làm nổi bật một GPO từ bên trong snap-in **Group Policy** của cửaổ **MMC**. Bạn sẽ thấy một mục chọn tên là **DC Options**.

Đ ể mặc chọn lựa đó ở vị trí mặc định của nó sẽ bảo đảm rằng các thay đổi GPO luôn luôn được thực hiện ở cùng một server, và làm giảm nguy cơ có hai người cùng chỉnh sửa một GPO trên hai máy khác nhau.

Những vấn đề về sao chép trong Win2K

Việc sao chép (replication) các bộ phận của cơ sở hạ tầng đữ liệu Win2K có một ảnh hưởng lớn đối với tính khả thi (reliability) và tính sẵn dùng (availability) khi mở rộng mạng. Việc sao chép Active Directory, danh mục toàn rừng (global catalog), dữ liệu SYSVOL, và Dfs tất cả đều ảnh hưởng đối với hiệu năng hoạt động, tính sẵn dùng và kinh nghiệm sử dụng mạng. Trong mục này, chúng ta sẽ bàn về một số thử thách chính người quản trị sẽ gặp phải khi triển khai những dịch vụ đa dạng đó.

Tuy nhiên, trước hết, chúng ta làm rõ khái niệm *khung cảnh định danh* (naming context).Trong Win2K, có ba naming context được sao chép: miền (donain), giản đồ tổ chức AD (AD schema), và cấu hình (configuration). Người quản trị có thể xem các naming context

như là các lộ trình (path) hoặc vòng (loop) sao chép đi xuyên qua môi trường mạng Win2k của . Domain naming cotext là lộ trình sao chép mà chỉ đi qua các máy DC bên trong trong một miền. Nó chịu rách nhiệm về việc sao chép những thay đổi về cơ sở dữ liệu AD đối với một miền nhất định.

Thư mục dùng chung Sysvol

sysvol được sao chép ra tất cả các máy DC trong một miền. Bên dưới sysvol có hầu hết những dữ liệu liên kết với các GPO.

sysvol dùng dịch vụ sao chép tập tin để sao chép nội dung của nó giữa tất cả các DC trong một miền. Bên dưới SYSYVOL có hầu hết các dữ liệu liên kết với các GPO, cũng như mọi thông tin theo kiểu NETLOGON cũ kỹ dành cho các máy đời cũ NT 4 hoặc Win 9x. SYSVOL đùng dịch vụ sao chép tập tin (File Replication Server _ FRS) mới mẻ của NT để sao chép nội dung của nó giữa tất cả cácmáy DC trong một miền. Theo mặc định FRS sao chép theo cùng một lịch biểu như Active Directory, và tôn trọng các danh giới site giống hệt như việc so chép của AD vậy.

Người quản trị có thể thay đổi lịch biểu sao chép của FRS. Từ công cụ snap-in **AD Users and Computer**, chọn mục lệnh **View/ AD advanced Features** rồi tìm đến tính năng **System\ File Replication Service.** Từ đó, nếu làm nổi bật **Domain System Volume** (tức share SYSVOL), nhắp phải, chọn **Properties** từ menu ngữ cảnh, rồi nhắp nút **Change schedule** trong khung thoại đặc tính hiện ra lúc đó người quản trị sẽ có việc sao chép qua danh giới site sẽ mất nhiều thời gian hơn là sao chép chỉ bên trong site; ví dụ, nếu người quản trị đã đưa một kịch bản đăng nhập mới vào GPO vốn được đặt trọng tâm tác động trên một máy DC cụ thể thì có thể mất nhiều thời gian để kịch bản đó được sao chép ra hết tất cả các share SYSVOL trên tất cả các DC bên trong miền .

Hệ thống tập tin phân tán (Dfs)

Hệ thống tập tin phân tán (Ditributed File System_ tức Dfs) tượng trưng cho một loạt thư thách khác biệt nhau như đều quan trọng SYSVOL. Chúng ta nghiên cứu thử một số khả năng của Dfs trong Win2K, để xem bạn có thể gặp rắc rối như thể nào trong việc triển khai nó ra trong một cơ sở hạ tầng lớn.

Với Dfs, người quản trị có thể quy định một share *gốc chịu lỗi* (fault-tolerat root gọi tắt là FT *root),* tức là Dfs root, bên trong một miền đã định. chú ý rằng chỉ có thể quy định cho mỗi server một dfs root được tham chiếu theo tên miền chứ không phải theo tên server.Ví dụ, nếu tên miền của là **vn. mycomputer**, người quản trị có thể ánh xạ một ổ đĩa đến share \ **\vn. mycomputer. com\dfs root.** Bên dưới một Dfs root cụ thể, có một số liên kết Dfs (Dfs link) nào đó. Các Dfs link

xuất hiện dưới dạng như các thư mục con lý luận đối với Dfs root, như thực chất thì trỏ đến một số share nào đó nằm trên các server khác (Win2K, NT 4, và thậm chí cả các server NetWare và Unix nữa). Mỗi Dfs link cũng có một bản sao (replica) liên kết với nó.
Ví dụ, bên dưới một share Dfs root tên **dfsroot** (giả dụ như vậy), có thể tạo ra một Dfs link tên là **apps, n**ơi bạn lưu giữ cất gói chương trình cài đặt ứng dụng trên mạng của bạn. Bên dưới mỗi Dfs root, người quản trị có thể đưa vào các thành viên bản sao. Các bản sao này đại diện cho các share nằm trên các server khác nhưng có nội dung giống nhau. người quản trị. Ví dụ, Dfs link tên **apps** chúng ta có thể có hai thành viên bản sao là các share cùng có tên **apps** nhưng nằm trên \ \servera và\ \serverb. Các thành viên bản sao thông thường đượ dùng khi bạn có những nội dung read only nào đó, như các tập tin nhị phân của một ứng dụng chẳng hạn, và người quản trị muốn chúng có thể được truy cập từ nhiều server trong mạng. Trong ví dụ này, giả sử servera nằm trong site X và serverb nằm trong site Y. Các khách hàng trong site X nối kết vào share \ **mycompany.com\ dfsroot\ apps** sẽ được chuyển hướng tới \ \servera\apps, còn các khách hàng trong Site Y nối kết vào cùng share đó sẽ được chuyển hướng tới \ \ serverb \apps. Như vậy, Dfs mang lại một mức độ *hấp lực server* (server affinity) nào đó, dựa theo topology của các site.
Một đặc điểm khác của Dfs là cung cấp khả năng sao chép tập tin (file replication, nếu hiểu rộng hơn thì là directory replication) đối với tất cả các thành viên bản sao đó. việc sao chép của Dfs thực chất là dùng dịch vụ FileReplication Service của NT, nhưng nó tạo ra topology sao chép riêng của nó mà người quản trị không kiểm soát được. Theo mặc định Dfs tạo ra một topology hình sao giữa tất cả những thành viên bản sao mà người quản trị chỉ định. Không có cách nào dễ dàng để biết khi nào thì các bản sao của Dfs đã 'đồng quy" (converge, tức là những thay đổi về nội dung đã được sao chép đến tất cả những bản sao). Đối với những mạng lớn, với nhiều thành viên bản sao khác đặt rải rác trong các site, ngang qua các đường liên kết WAN đa dạng, chắc hẳn người quản trị sẽ thấy rằng cơ chế sao chép của Dfs quả là không thoả đáng. Cơ chế sao chép có trong dfs thực ra chỉ có ý nghĩa đối với mạng nhỏ hơn, nội dung của read- only được sao chép ra một ít server thôi. Thực tế, nếu người quản trị chọn sử dụng cơ chế sao chép tự động có trong dfs, là người quản trị bị hạn chế chỉ được phép có 32 thành viên bản sao đối với một đốt liên kêt con!!!. Còn nếu khi chọn Dfs link mà người quản trị chọn phương án sao chép thủ công (manual replication), thì người quản trị có thể an toàn yểm trợ đến 1000 thành viên bản sao. chú ý rằng khi chọn sao chép thủ công là người quản trị đang cho dfs biết rằng người quản trị dự định cung cấp

cơ chế riêng của mình để sao chép nội dung ra mỗi thành viên bản sao ngoài phạm vi cơ sở hạ tầng Dfs.
Ngoài ra, cũng có thể người quản trị bị cám dỗ bởi ý nghĩ là dùng cơ chế sao chép của dfs để sao chép những dữ liệu không read- only, như các home folder của người dùng chẳng hạn. Nên biết rằng, bản Dfs hiện nay không thực sự phù hợp với kiểu tiếp cận như thế đâu. Điều này chủ yếu là vì ,bạn thực sự không có cách nào để kiểm soát được khi nào dfs sẽ"quy đồng" các bản sao cả. (Nếu một người dung thực hiện một thay đổi với home folder của mình trên một bản sao sau khi thực hiện một thay đổi khác trên một bản sao khác, thì thay đổi trước có thể bị mất đi, do nó chưa kịp phổ biến rộng rãi). Với Dfs, người quản trị chỉ nên dùng tính năng chịu lỗi như một cách để tìm tìm ra vị trí thực (vật lý) từ các tên share luận lý . Hãy để Dfs tạo ra một cây tập tin phân tán mà việc sao chép lệ thuộc vào topology của cacsite . Nếu phải dùng cơ chế sao chép của Dfs, người quản trị chỉ nên áp dụng Dfs với những nội dung read- only, còn không thì phải sắm một phần mềm sao chép *near-real- time* (nghĩa là việc sao chép ra khắp mạng được thực hầu như tức thời, hầu như không có trì hoãn nào cả) nào đó để thực hiện việc sao chép nội dung thực sự.

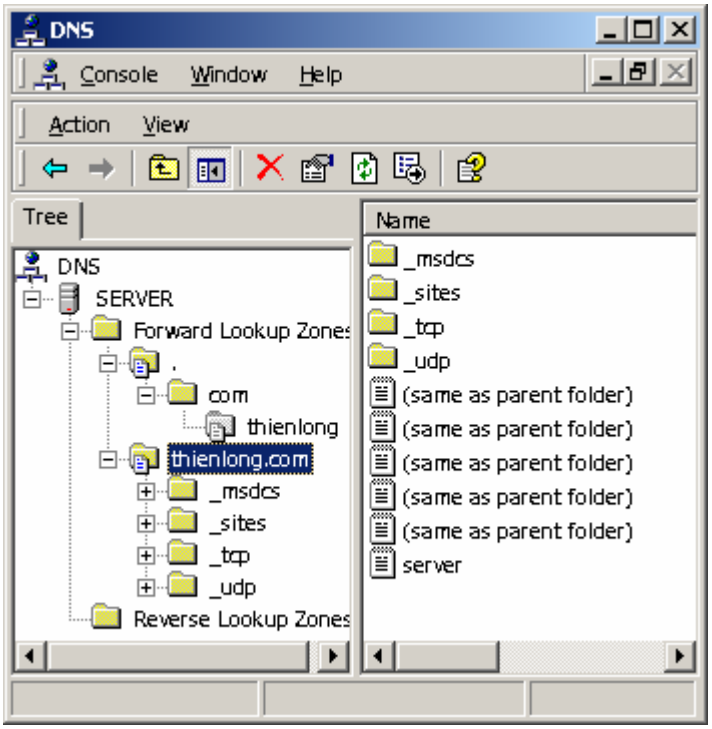
Việc sao chép GPO

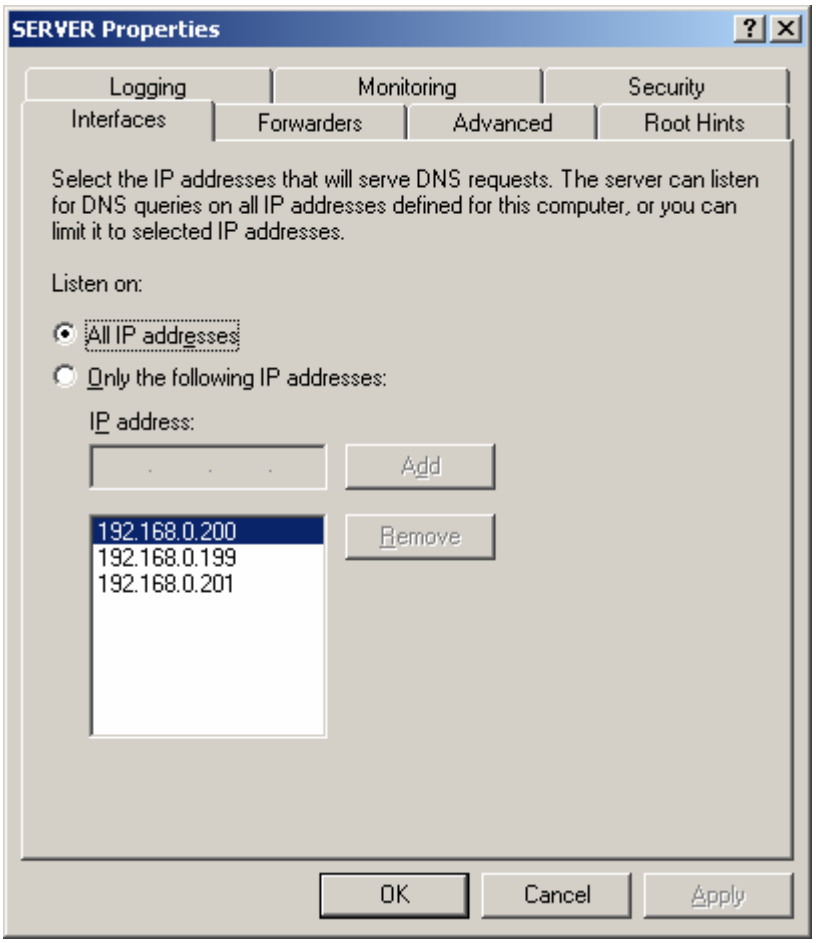
Trường hợp đặc biệt của các GPO và cách thức sao chép chúng bên trong cơ sở hạ tầng mạng Win2K. Kiểu cách sao chép này có thể trở thành một vấn đề quan trong trong những môi trường mạng lớn, có nhiều GPO được triển khai khắp các site với những đương liên kết WAN có tốc độ khác nhau. Nên biết rằng mỗi GPO thực ra được tạo lên bởi hai thành phần: Group Policy Container (GPC) và Group Policy Template (GPT). GPC là một đối tượng bên trong Active Directory, chứa thông tin tham chiếu đến một GPO cụ thể. GPC được sao chép giống hệt như những đối tượng AD khác, theo kiểu *multimaster,*trên cơ sở từng đặc tính một. Thành phần GPT thực ra mới là thành phần chính của GPO. Nó là các tập tin thực sự tạo nên một GPO. Các kịch bản tắt máy và khởi động, kịch bản đăng nhập và đăng xuất, các khuôn mẫu quản trị và tập tin hệ quả của nó là **registry.pol** và các khuôn mẫu bảo mật dều được chứa trong GPT, vốn được sao chép bên trong share SYSYVOL.
Do hai thành phần này là những thực thể phân biệt, có kiểu cách sao chép hoàn toàn khác biệt, nên có khả năng là một GPC được sao chép trước khi GPT liên kết với nó được sao chép nhất là trong một mạng lớn.

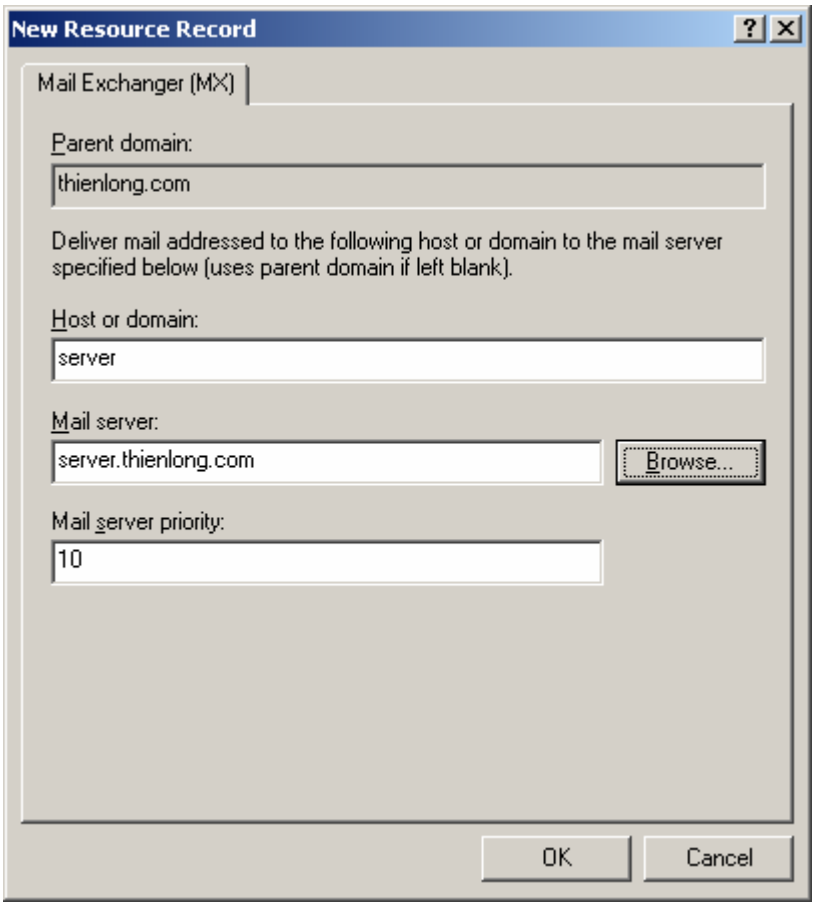
Triển khai các dịch vụ cơ sở hạ tầng.

Khi đã sẵn sàng việc triển khai một cơ sở hạ tầng mạng Win2K cỡ lớn, người quản trị cần cài đặt và cấu hình một số dịch vụ cơ sở hạ tầng để cho phép AD và các phần mềm máy khách có thể làm việc. Các dịch vụ cơ sở hạ tầng làm nền tảng cho việc phát triển một mạng máy tính.

DNS

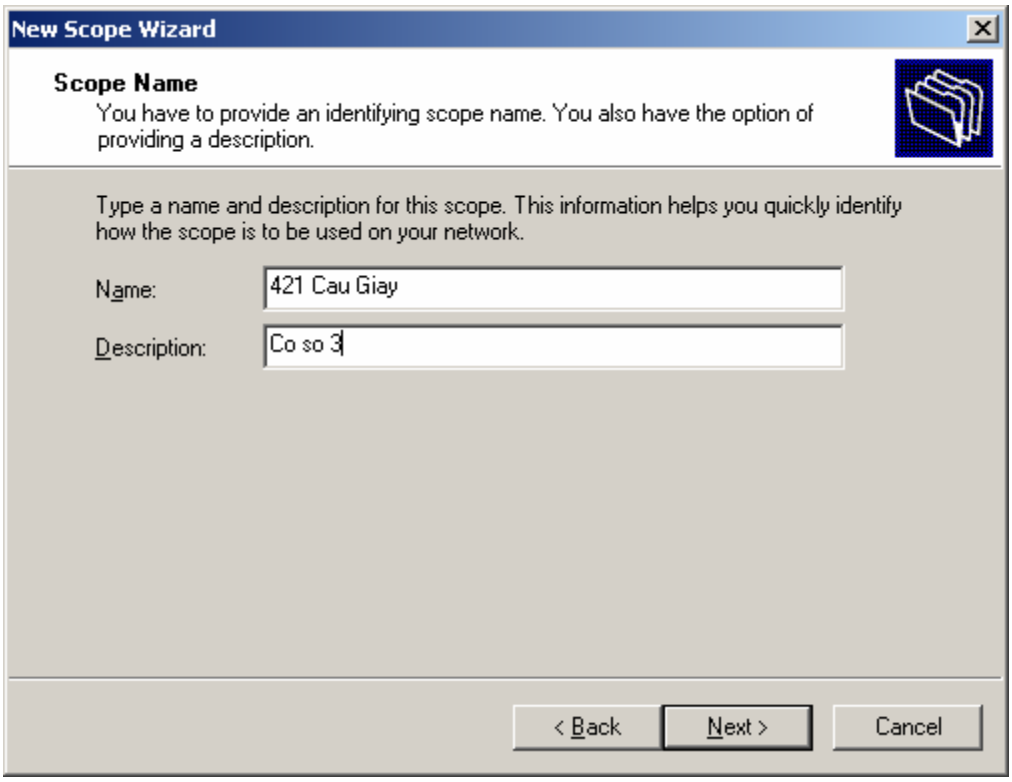


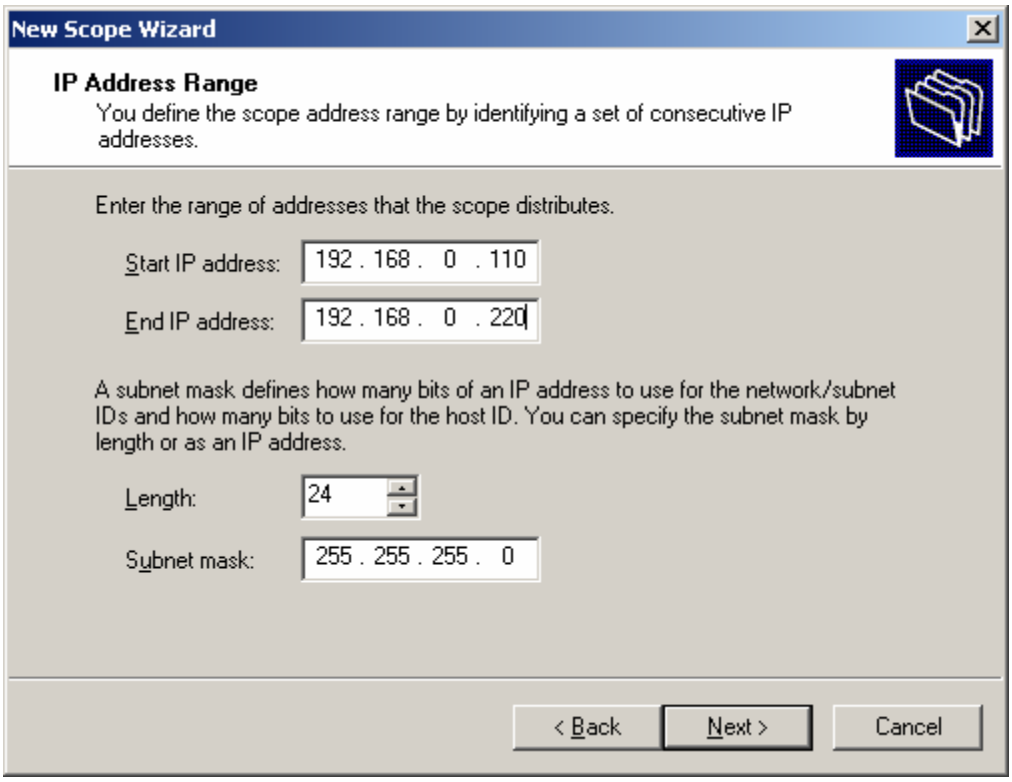

SERVER Properties
Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.
Listen on:
All IP addresses
Only the following IP addresses:
IP address:
Add
192.168.0.200
192.168.0.199
192.168.0.201
Remove
OK
Cancel
Apply

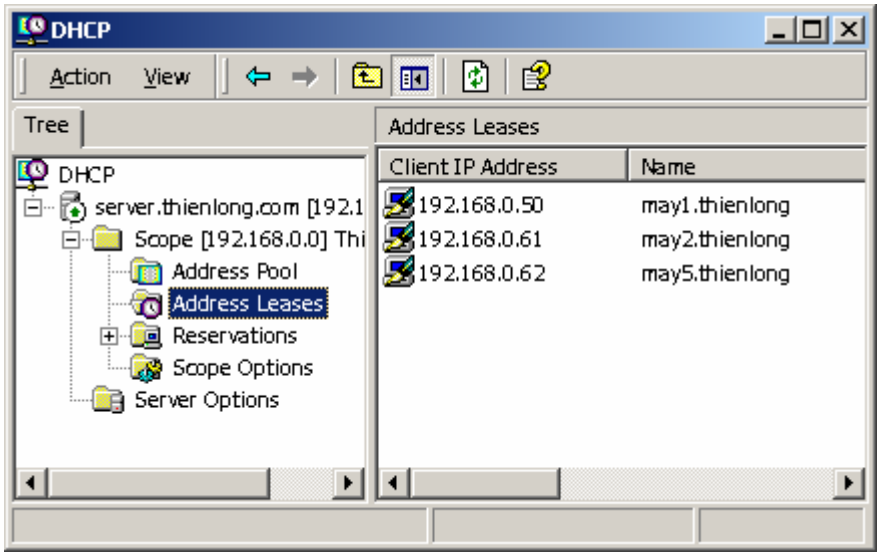


DHCP.

*** Nguyên tắc hoạt động.**
*** Cài đặt:**
*** Cấu hình:**
- Tạo một Scope:


New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
421 Cau Giay
Description:
Co so 3
< Back
Next >
Cancel


New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address: 192 . 168 . 0 . 110
End IP address: 192 . 168 . 0 . 220
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length: 24
Subnet mask: 255 . 255 . 255 . 0
< Back
Next >
Cancel


DHCP
Action
View
Tree
Address Leases
DHCP
server.thienlong.com [192.1
Scope [192.168.0.0] Thi
Address Pool
Address Leases
Reservations
Scope Options
Server Options
Client IP Address
Name
192.168.0.50
may1.thienlong
192.168.0.61
may2.thienlong
192.168.0.62
may5.thienlong

Giao thức mạng.

*** Các khái niệm cơ bản:**

- Định nghĩa:

Giao thức mạng là tập hợp các quy tắc, quy ước sao cho các thực thể tham gia truyền thông trên mạng có thể liên lạc được với nhau. Hay nói cách khác, giao thức mạng là ngôn ngữ chung để cho các máy tính làm việc được với nhau.

- Lớp mạng:
- Mạng con:
- Giao thức dẫn đường.

*** Lựa chọn:**

Việc lựa chọn giao thức mạng phụ thuộc vào mục đích sử dụng cụ thể trong từng mạng. Đối với mỗi tiêu chuẩn đưa ra ta có thể có các lựa chọn giao thức mạng khác nhau:

- Giao thức NetBEUI - NetBIOS Extention User Interface:
- Giao thức TCP/ IP.
- Giao thức IPX/SPX…

*** Cài đặt:**

*** Cấu hình:**

Các lệnh được dùng trong Windows 2K

A

Append

Arp

Assoc

At

Atmadm

Attrib

B

Batch commands

Break

Buffers

C

Cacls

Call

Chcp

Chdir (cd)

Chkdsk

Chkntfs

Cipher

Cls

Cluster

Cluster commands overview

Cluster group

D

E

F

Net localgroup

Net name

Net pause

Net print

Net send

Net session

Net share

Net start

Net start Alerter

Net start Client Service for NetWare

Net start ClipBook Server

Net start Computer Browser

Net start DHCP Client

Net start Directory Replicator

Net start Eventlog

Net start File Server for Macintosh

Net start FTP Publishing Service

Net start Gateway Service for NetWare

Net start Lpdsvc

Net start Messenger

Net start Microsoft DHCP Service

Net start Net Logon

Net start Network DDE

Net start NT LM Security Support Provider

Net start OLE

Net start Print Server for Macintosh

Net start Remote Access Connection Manager

Net start Remote Access ISNSAP Service

Net start Remote Procedure Call (RPC) Locator

Net start Remote Procedure Call (RPC) Service

Net start Schedule

Net start Server

Net start Simple TCP/IP Services

Net start Site Server LDAP Service

Net start SNMP

Net start Spooler

Net start TCP/IP NetBIOS Helper

Net start UPS

Net start Windows Internet Name Service

Net start Workstation

Net statistics

Net stop

Net time

Net use

Net user

Net view

Netsh

Netstat

Nlsfunc

Nslookup