



NETWORK INFORMATION SECURITY VIETNAM

Backup phục hồi dữ liệu và phục hồi hệ thống trong Windows XP Pro/ Server 2003

Backup dữ liệu là một trong những công việc rất cơ bản từ những người sử dụng bình thường sao lưu dữ liệu cá nhân đến các Network Admin sao lưu hàng GB dữ liệu của doanh nghiệp. Đây cũng là tác vụ bắt buộc nhằm đảm bảo an toàn dữ liệu khi xảy ra các sự cố như Virus phá hoại dữ liệu, hư hỏng phần cứng, bất cẩn dẫn đến xóa nhầm data, thay đổi Server cần chuyển data từ Server cũ sang...nhờ backup đầy đủ theo thời gian được sắp đặt (scheduling), cũng như chọn kiểu backup phù hợp mà chúng ta có thể phục hồi kịp thời các dữ liệu này một khi xảy ra các sự cố kể trên.

Tóm lại kỹ năng backup là một trong số các kỹ năng cơ bản không thể thiếu của Admin.

Trước hết hãy xem xét tiện ích backup trên Windows XP Pro/ Server 2003

Windows XP Professional / Server 2003 bao gồm tiện ích được xây dựng sẵn Windows Backup, giúp sao lưu và phục hồi dữ liệu trên máy của bạn (local) hoặc một máy ở xa (remote Windows systems). Windows Backup lưu trữ dữ liệu trên nhiều loại phương tiện lưu trữ (media) khác nhau như hard disk, floppy disks, CD-ROMs ghi, ổ đĩa băng từ (tape), và các thiết bị đĩa nén khác như Iomega Jaz® drives. Backup cho phép xác lập được lưu trữ vào các file đơn hoặc có thể lưu giữ dữ liệu trải dài vào nhiều băng từ (tapes). Windows Backup hỗ trợ nhiều loại backup khác nhau, sau đây chúng ta hãy làm quen với 3 kiểu backup phổ biến nhất.

Loại Backup	Mô tả	Ưu điểm	Nhược điểm
Full backup	Backup toàn bộ các Files trong Folder mà bạn xác định để backup. Tóm lại đây là kiểu backup thông thường	Dễ dàng xác định dữ liệu để backup và phục hồi	Tốn thời gian và tốn không gian lưu trữ dữ liệu.
Incremental backup	Một xác lập để backup những files có sự thay đổi kể từ lần backup cuối cùng (thuộc bất cứ loại backup nào).	Mất ít thời gian và không gian lưu trữ nhất.	Tuy nhiên khi phục hồi lại khá mất thời gian do bạn cần restore bản full backup lần cuối cùng trước, sau đó theo trình tự tìm các incremental backups của những ngày sau đó để phục hồi.
Differential backup	Một xác lập để backup những files có sự thay đổi kể từ lần backup	Mất ít thời gian và không gian lưu trữ hơn so với một full	Thông tin backup còn bị lập lại. Backup tốn nhiều thời gian hơn so

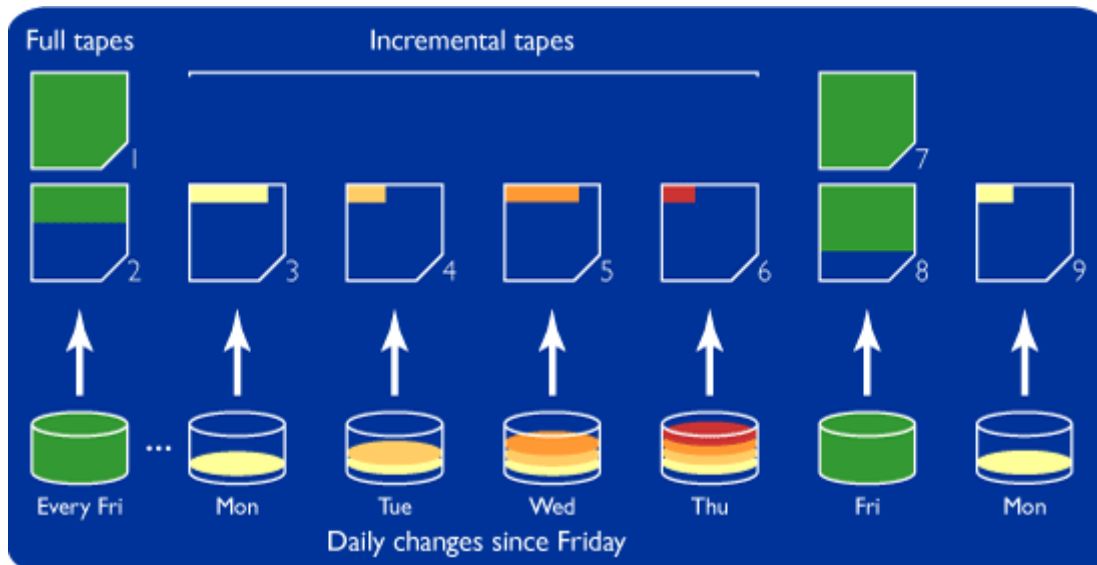


NETWORK INFORMATION SECURITY VIETNAM

	cuối cùng full backup.	backup; Khi phục hồi lại khá nhanh so với Incremental backup	với Incremental.
--	------------------------	--	------------------

Hãy theo dõi một ví dụ trong thực tế của một Backup Administrator để hiểu rõ hơn về các loại backup này.

Hoàng là một Backup Admin của cty A, nhiệm vụ của anh là backup các dữ liệu quan trọng nằm tại thư mục **Data** của Server. Anh dùng tiện ích Windows Backup để thực hiện.



Hãy xem hình minh họa **Incremental backup**

Lần đầu tiên anh ấy backup thư mục Data là vào **ngày thứ 6 (Friday)**, vì là lần đầu tiên backup nên anh ấy chọn **Normal backup** (hay còn gọi là **Full backup**).

Ngày thứ 7 và chủ nhật, cty nghỉ

Ví dụ 1: Admin bắt đầu chọn kiểu Backup Incremental Vào ngày thứ 2 cho đến các ngày kế tiếp

Qua **ngày thứ 2 (Mon)** cty làm việc và User đã cập nhật thêm dữ liệu vào Data (**màu Vàng nhạt**)





NETWORK INFORMATION SECURITY VIETNAM

Và Admin sẽ chỉ backup incremental phần màu vàng nhạt này

Qua **ngày thứ 3 (Tue)** cty làm việc và User đã cập nhật thêm dữ liệu vào Data **(màu Vàng đậm)**



Và Admin sẽ chỉ backup incremental phần màu vàng đậm này

Qua **ngày thứ 4 (Wed)** cty làm việc và User đã cập nhật thêm dữ liệu vào Data **(màu cam)**



Và Admin sẽ chỉ backup incremental phần màu Cam này

Qua **ngày thứ 5 (Thu)** cty làm việc và User đã cập nhật thêm dữ liệu vào Data **(màu Đỏ)**



Và Admin sẽ chỉ backup incremental phần màu Đỏ này

Đến ngày làm việc **cuối cùng ngày thứ 6 (Fri)**, Admin lại tổng hợp và backup một bản Full Backup toàn bộ từ thứ 6 tuần trước đến thứ 6 tuần này.



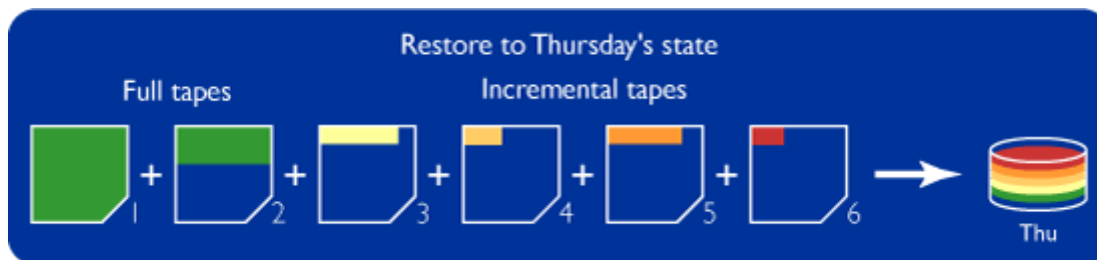


NETWORK INFORMATION SECURITY VIETNAM

Đến vấn đề phục hồi khi xảy ra sự cố mất dữ liệu

Giả sử như chưa kịp backup full tổng hợp này và có sự cố mất mát dữ liệu vào ngày thứ 5 (Thu) thì anh Hoàng sẽ giải quyết thế nào. Chúng ta hãy suy luận và tìm cách giải quyết đơn giản nhé

Đơn giản chỉ cần phục hồi bản full backup thứ 6 tuần trước (**Fri**) + **Inc Mon** + **Inc Tue** + **Inc Wed** + **Inc Thu** = Phục hồi đầy đủ dữ liệu vừa mất



Như vậy các bạn rút ra được 2 điểm chú ý quan trọng sau khi tiến hành Incremental backup:

Thời gian backup nhanh vì chỉ backup dữ liệu tăng thêm những ngày sau đó kể từ sau full backup vào ngày đầu tiên.

Tuy nhiên lại mất nhiều thời gian cho việc phục hồi, cần phục hồi bản Full backup đầu tiên trước và sau đó tìm lần lượt các bản Incre backup từ các ngày kế tiếp

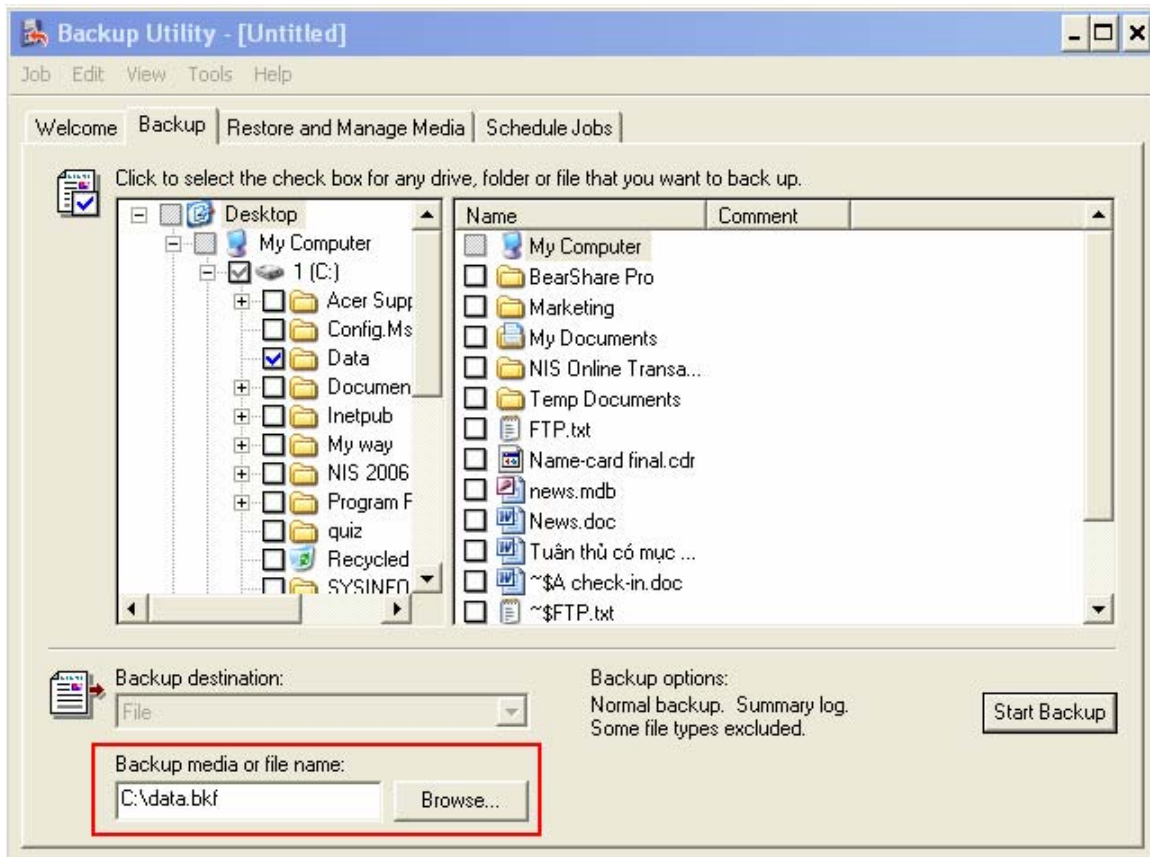
Thực hành: Hướng dẫn từng bước của Ví dụ 1

Tại **Run** đánh lệnh **NTBACKUP.EXE**

Chương trình Windows Backup sẽ được mở và bạn chọn tab **Backup**



NETWORK INFORMATION SECURITY VIETNAM



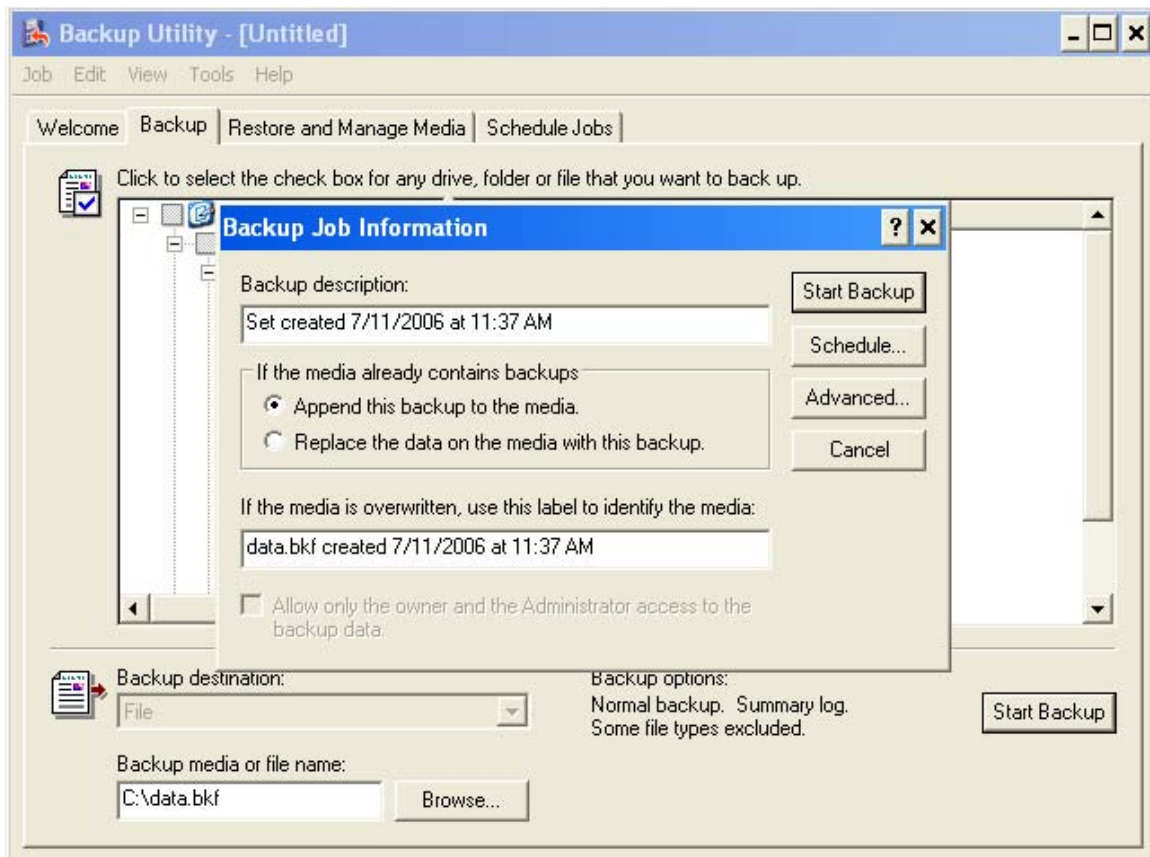
Các bạn chọn folder cần backup, trong ví dụ này là **Data** nằm tại **C:**

Và chọn tên của backup File và nơi lưu trữ sau backup, chúng ta chọn lưu file với tên là **data.bkf** cũng đặt tại C: khung màu Đỏ (hoặc ghi vào các Zip disk, Floppy disk hoặc tapes...)

Sau đó click vào **Start Backup**



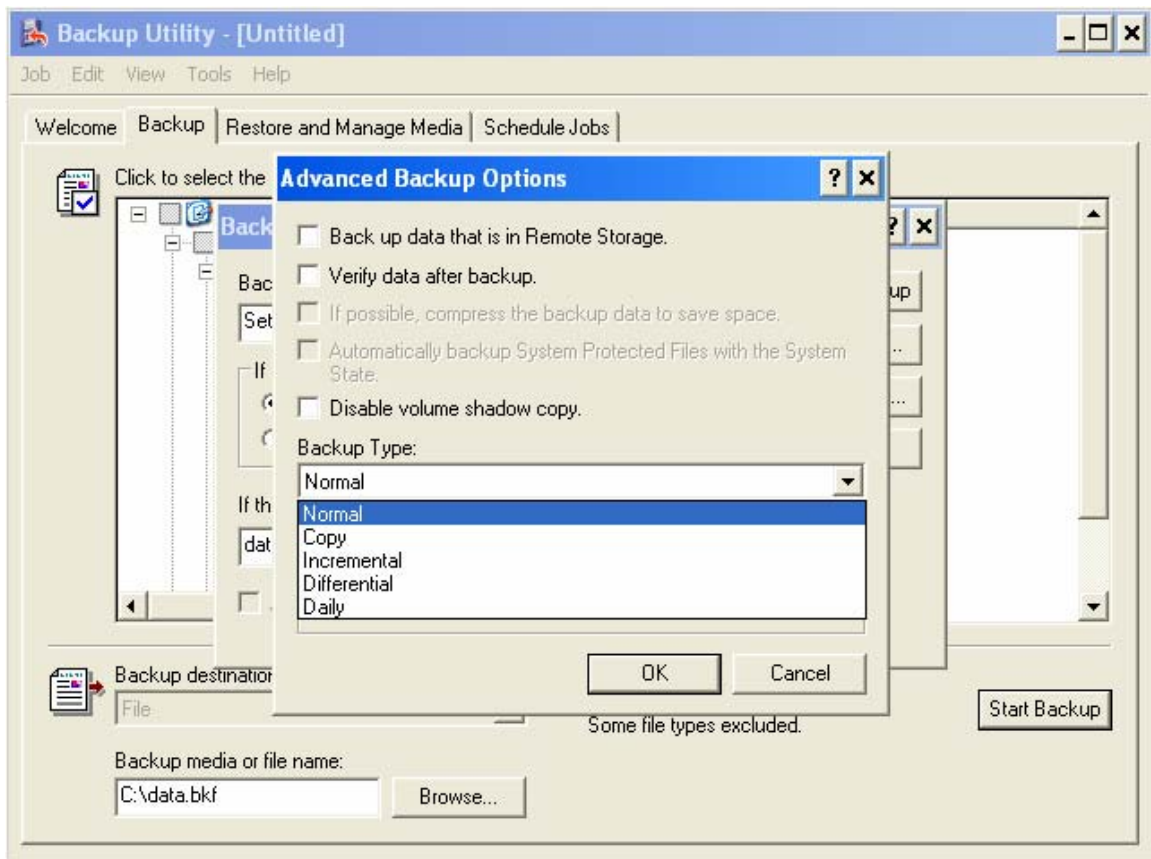
NETWORK INFORMATION SECURITY VIETNAM



Tại đây có một số thông tin về backup ví dụ như ngày tạo ra bản backup này, có thể chọn tab **Advanced**, để xem có những loại backup nào và vì đây là lần đầu tiên backup thư mục **Data** nên đương nhiên là chọn **Normal** backup, chọn Ok và chọn **Start Backup** để thi hành



NETWORK INFORMATION SECURITY VIETNAM

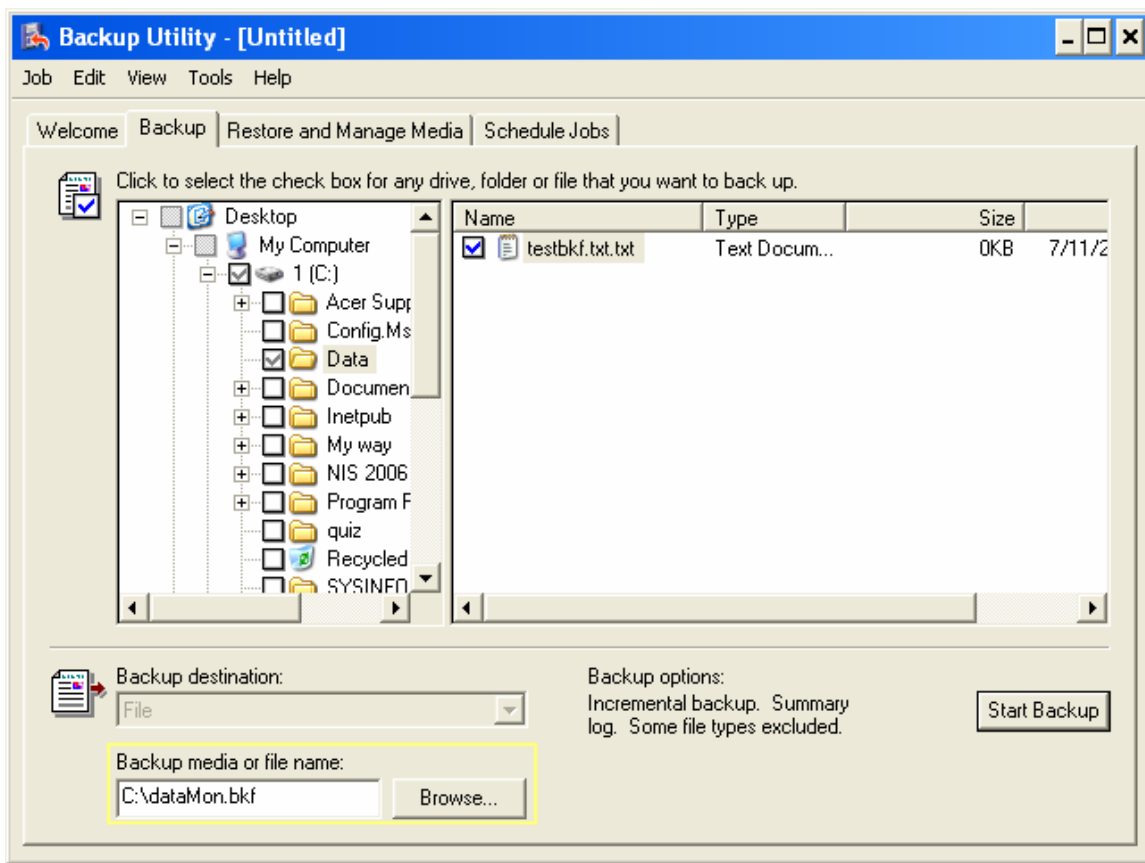


Như vậy đến đây bạn đã tiến hành Normal Backup (Full backup) cho **C:\Data**, thời gian diễn ra việc này là ngày thứ Sáu (Fri) và đây cũng là bản backup đầu tiên .

Tiếp đến qua tuần sau vào cuối ngày thứ Hai, chúng ta thực hiện kiểu backup Incremental cho dữ liệu tăng thêm vào ngày thứ Hai. Chú ý khung màu Vàng nhạt các bạn chọn file lưu trữ là **C:\DataMon.bkf**



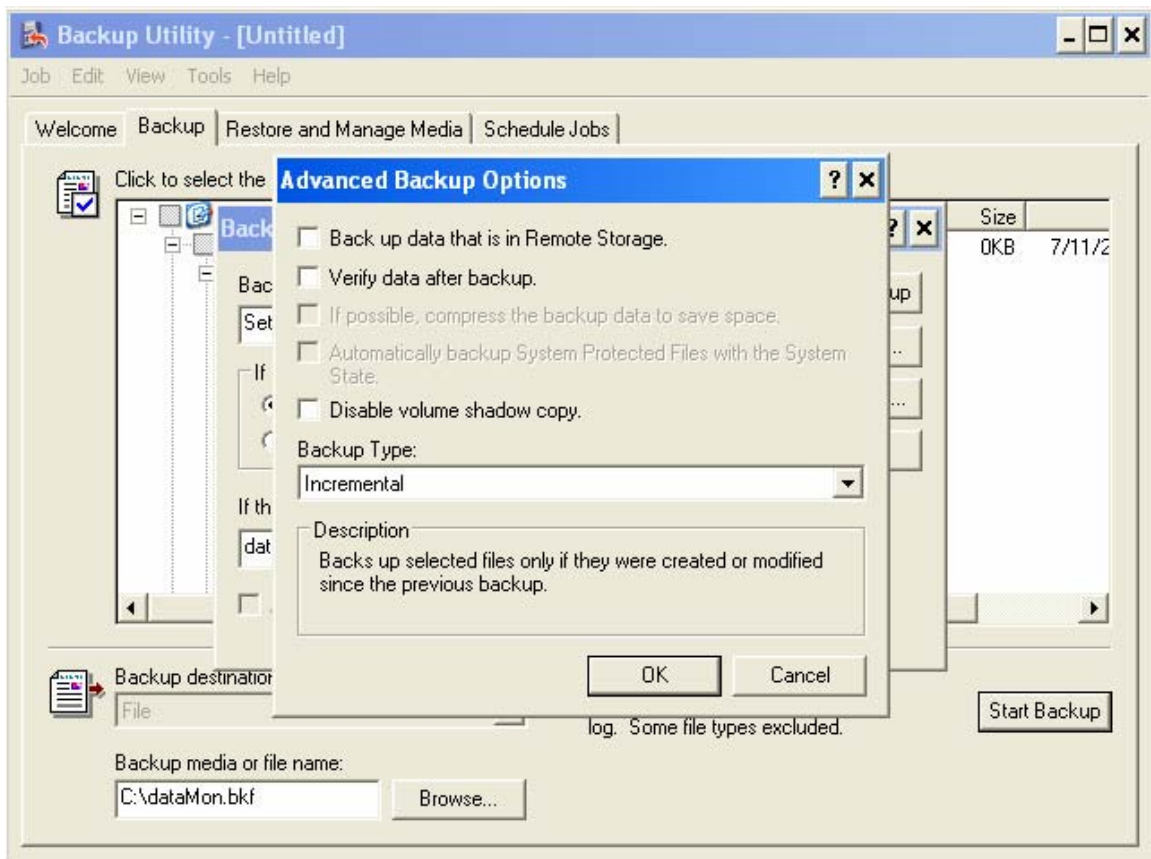
NETWORK INFORMATION SECURITY VIETNAM



Chọn **Start backup**, Chọn tab **Advanced** và chọn Backup Type là **Incremental**



NETWORK INFORMATION SECURITY VIETNAM



Như vậy Windows backup chỉ backup phần dữ liệu tăng thêm (incremental) của ngày thứ Hai kể từ sau Full backup thứ Sáu tuần trước.

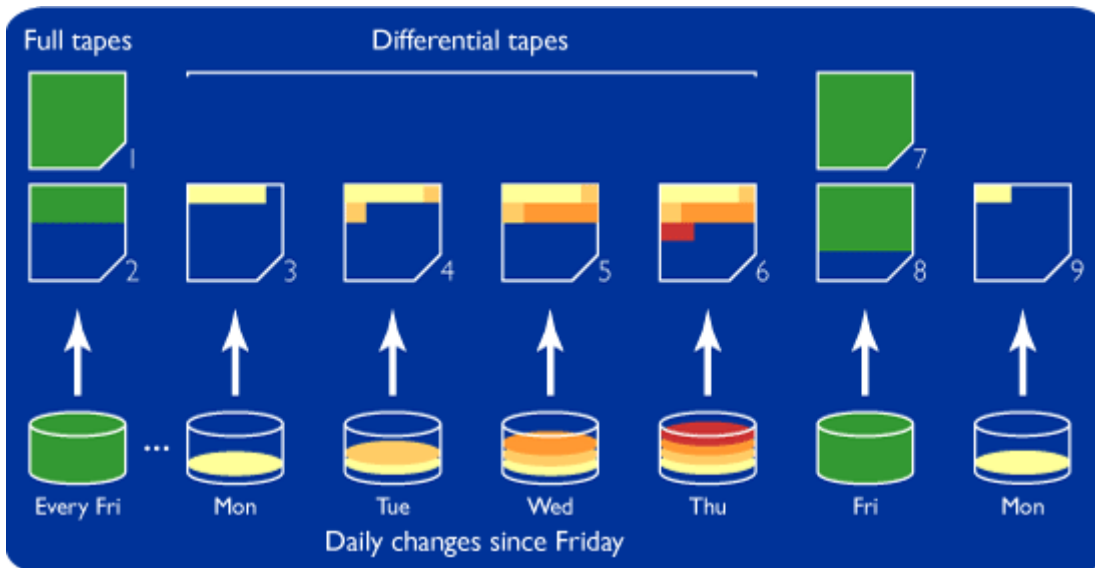
Vào ngày thứ ba (Tue) làm tương tự ngày thứ Hai và đặt Incremental file là **C:\dataTue.bkf**

Cứ thế tiếp tục cho đến ngày thứ Năm (Thu) C:\dataThu.bkf, trước khi Full backup tổng hợp vào ngày Thứ Sáu để bắt đầu làm nền cho tuần mới tiếp theo..

Ví dụ 2: Admin chọn kiểu backup Differential vào ngày thứ 2 và các ngày kế tiếp



NETWORK INFORMATION SECURITY VIETNAM



Hãy xem hình minh họa **Differential backup**

Đối với kiểu backup này cũng bắt đầu **Normal (full backup)** thư mục Data vào **ngày thứ sáu (Fri)**

Qua tuần đến **ngày làm việc thứ Hai (Mon)**, User đã cập nhật thêm dữ liệu vào Data (**phần màu Vàng nhạt**)



Admin sẽ backup Differential phần màu vàng nhạt này

Đến **ngày làm việc thứ Ba (Tue)**, User đã cập nhật thêm dữ liệu vào Data (**phần màu Vàng đậm**)



Admin sẽ backup Differential phần màu vàng đậm này + phần màu vàng nhạt ngày 2 thứ Hai trước đó

Đến **ngày làm việc thứ Tư (Wed)**, User đã cập nhật thêm dữ liệu vào Data (**phần màu Cam**)



NETWORK INFORMATION SECURITY VIETNAM



Admin sẽ backup Differential phần màu Cam này + phần màu vàng đậm ngày thứ Ba + phần màu vàng nhạt ngày thứ Hai trước đó

Đến **ngày làm việc thứ Năm (Thu)**, User đã cập nhật thêm dữ liệu vào Data **(phần màu Đỏ)**



Admin sẽ backup Differential phần màu Đỏ này + phần màu Cam + phần màu vàng đậm ngày thứ Ba + phần màu vàng nhạt ngày thứ Hai trước đó

Đến ngày làm việc **cuối cùng ngày thứ 6 (Fri)**, Admin lại tổng hợp và backup một bản Full Backup toàn bộ từ thứ 6 tuần trước đến thứ 6 tuần này.



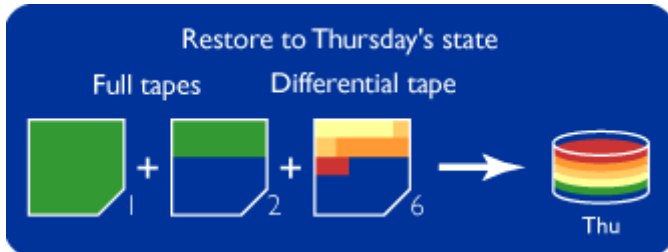
Đến vấn đề phục hồi khi xảy ra sự cố mất dữ liệu

Giả sử như chưa kịp backup full tổng hợp này và có sự cố mất mát dữ liệu vào ngày thứ 5 (Thu) thì anh Hoàng sẽ giải quyết thế nào. Chúng ta hãy suy luận và tìm cách giải quyết đơn giản nhé

Đơn giản chỉ cần phục hồi bản full backup thứ 6 tuần trước **(Fri) + Differential Backup vào ngày thứ Năm (Thu)** = Phục hồi đầy đủ dữ liệu vừa mất



NETWORK INFORMATION SECURITY VIETNAM



Như vậy các bạn rút ra được 2 điểm chú ý quan trọng sau khi tiến hành Incremental backup:

Thời gian backup nhanh hơn so với Normal backup nhưng lại lâu hơn Incremental backup vì phải backup lại các dữ liệu lập lại sau Full backup ngày đầu tiên.

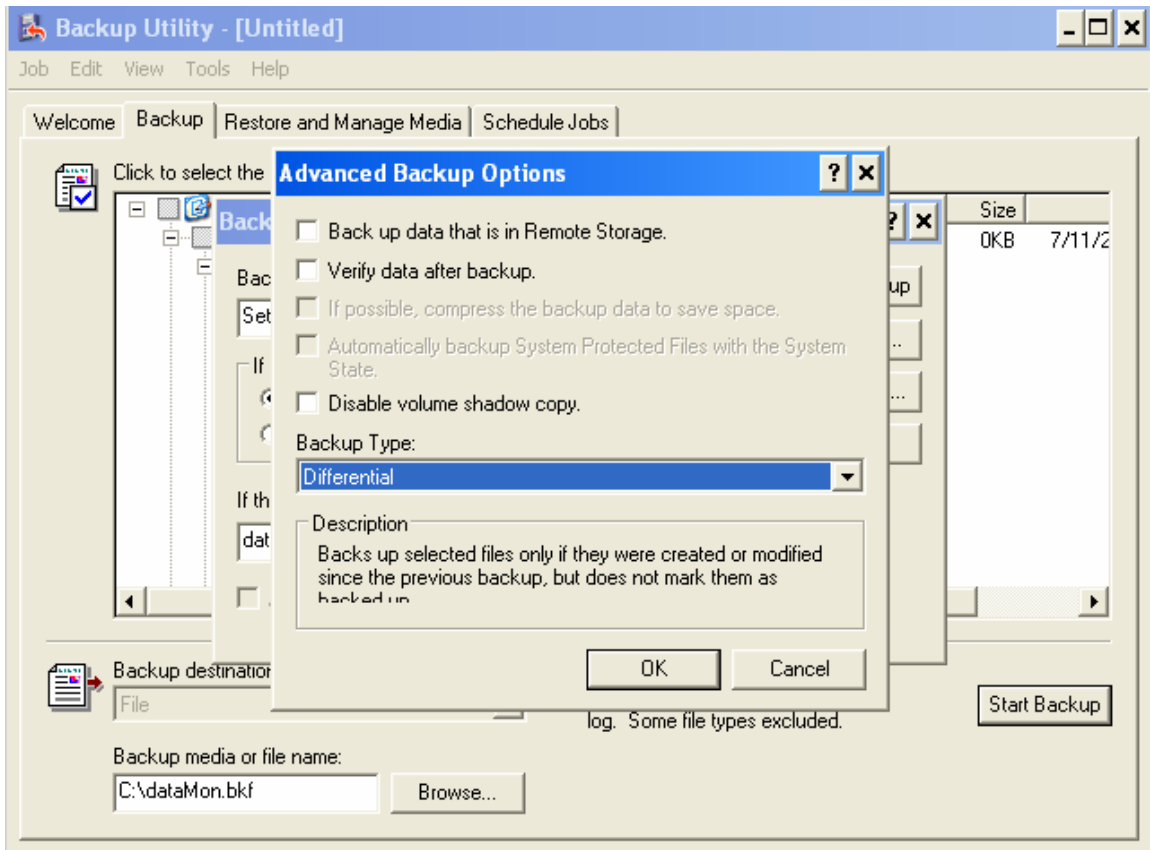
Tuy nhiên lại mất rất ít thời gian cho việc phục hồi, cần phục hồi bản Full backup đầu tiên trước và sau đó tìm bản Differential backup của ngày cần phục hồi dữ liệu

Thực hành: Hướng dẫn từng bước của Ví dụ 2

Làm từng bước tương tự Ví dụ 1, Sau Normal (Full backup) vào thứ Sáu đến các ngày thứ Hai, Ba, Tư của tuần mới thay lựa chọn **Incremental** bằng **Differential**



NETWORK INFORMATION SECURITY VIETNAM



Vừa rồi các bạn đã xem xét vấn đề Backup dữ liệu thông thường trên máy tính dùng tiện ích Windows backup, tiếp theo là các vấn đề backup file quan trọng thuộc hệ thống (system Files), thiếu các System Files này hoặc hư hỏng bất kỳ thành phần nào của hệ thống như các lớp COM+, Registry, System32..có thể khiến máy tính Crash và không khởi động vào làm việc được..

Backup System State data (Backup registry & các thành phần cốt lõi hệ thống)

System state data là những thành phần quan trọng của Hệ thống cần Backup theo định kỳ nhằm có cơ sở để phục hồi HĐH một khi hỏng hóc rơi vào các thành phần sau khiến hệ thống Computer của chúng ta không làm việc hoặc bị thay đổi chỉnh sửa sai lệch gây ảnh hưởng đến cấu hình hệ thống và hoạt động của Hardware , Software đang vận hành

- Boot files (Các Files liên quan đến quá trình khởi động hệ thống như Boot.ini, Ntldr..)



NETWORK INFORMATION SECURITY VIETNAM

- Các files hệ thống cần được bảo vệ (Windows có WFP -Windows File Protection, tính năng tự động backup và phục hồi khi xảy ra hỏng hóc hay bị xóa các file hệ thống như *SYS, DLL, TTF, FON, OCX, và EXE*)

- Registry

- COM+ object một cơ sở dữ liệu của các thành phần chương trình được chia sẻ giữa các Ứng dụng

Chú ý: System state data của Server hay Workstation thông thường chỉ chứa những thành phần này, nếu các Server như Domain Controller (máy chủ điều khiển hoạt động Domain) sẽ chứa thêm các thành phần liên quan đến Domain ví dụ như:

Active Directory Database

Tất cả các thành phần trong System State data được tích hợp với nhau và khi backup không thể chọn tách rời từng thành phần để backup

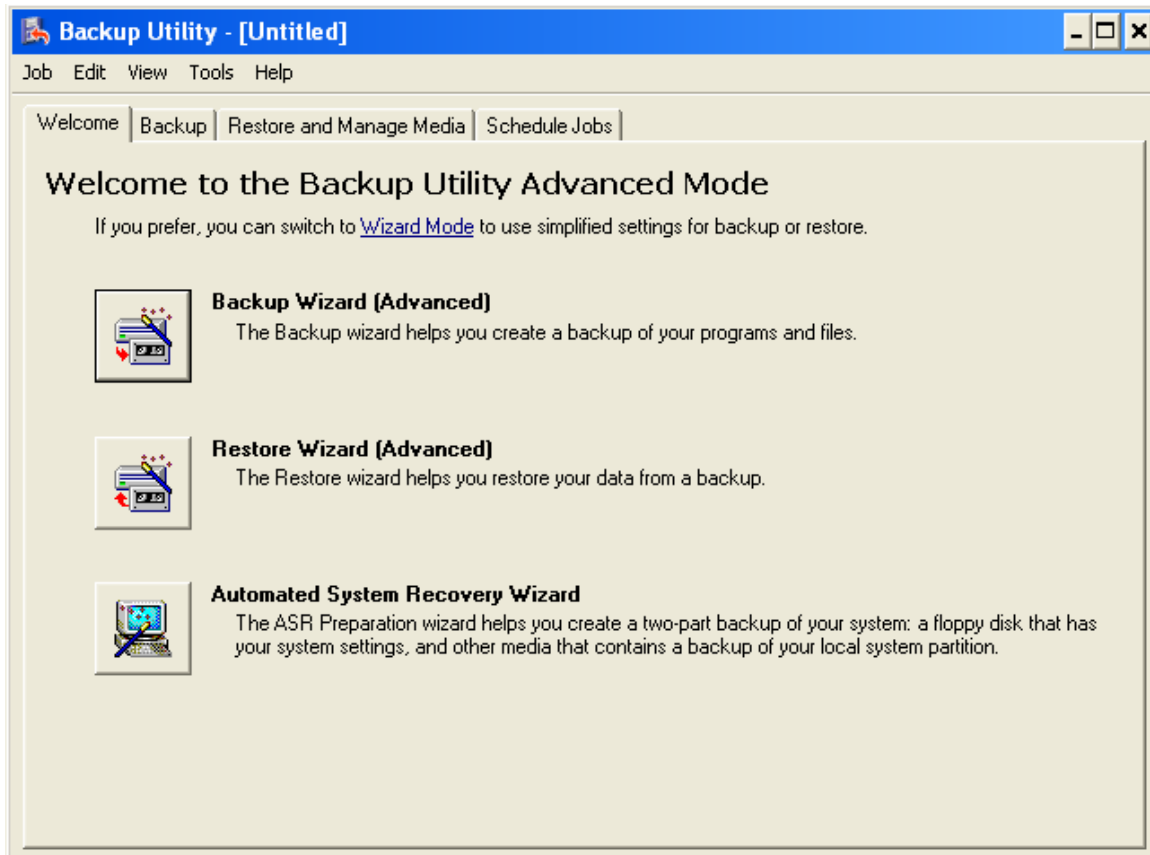
*Như vậy ví dụ nếu bạn muốn backup toàn bộ **Registry**, thì cũng cần backup System state data..không thể chọn đơn lẻ Registry trong SSD để backup.*

Thực hành:

1. Mở Windows Backup.
2. Chọn **Back Up Wizard** và click **Next**.



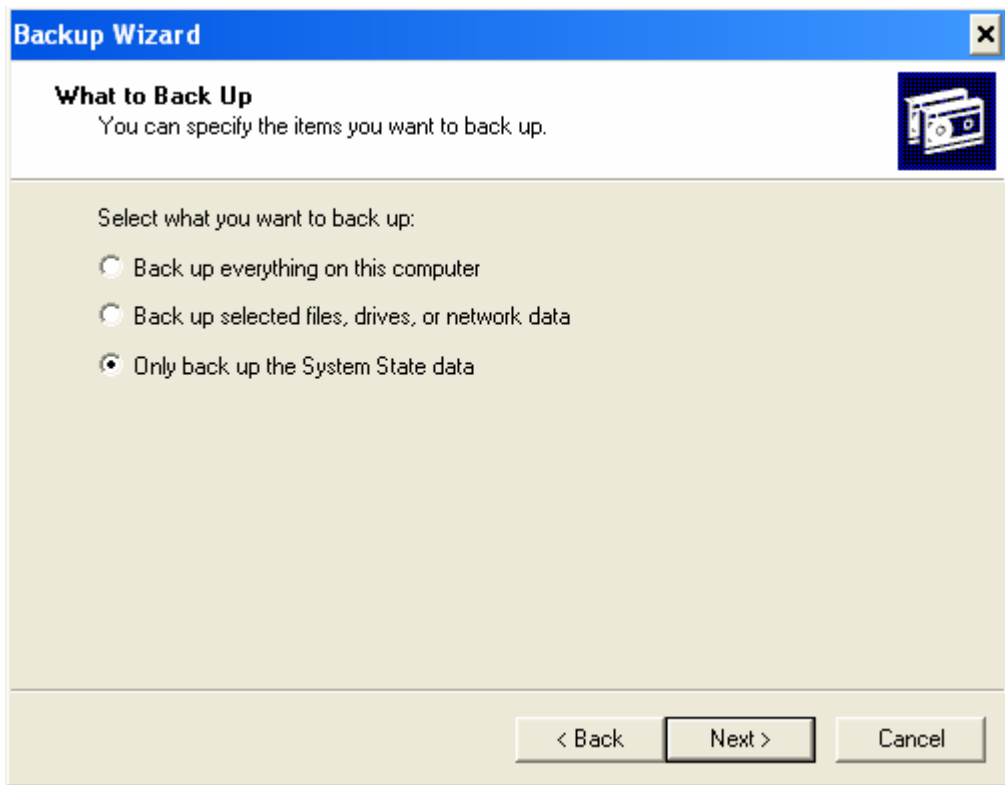
NETWORK INFORMATION SECURITY VIETNAM



3. Select **Only Backup the System State Data** và click **Next**.



NETWORK INFORMATION SECURITY VIETNAM

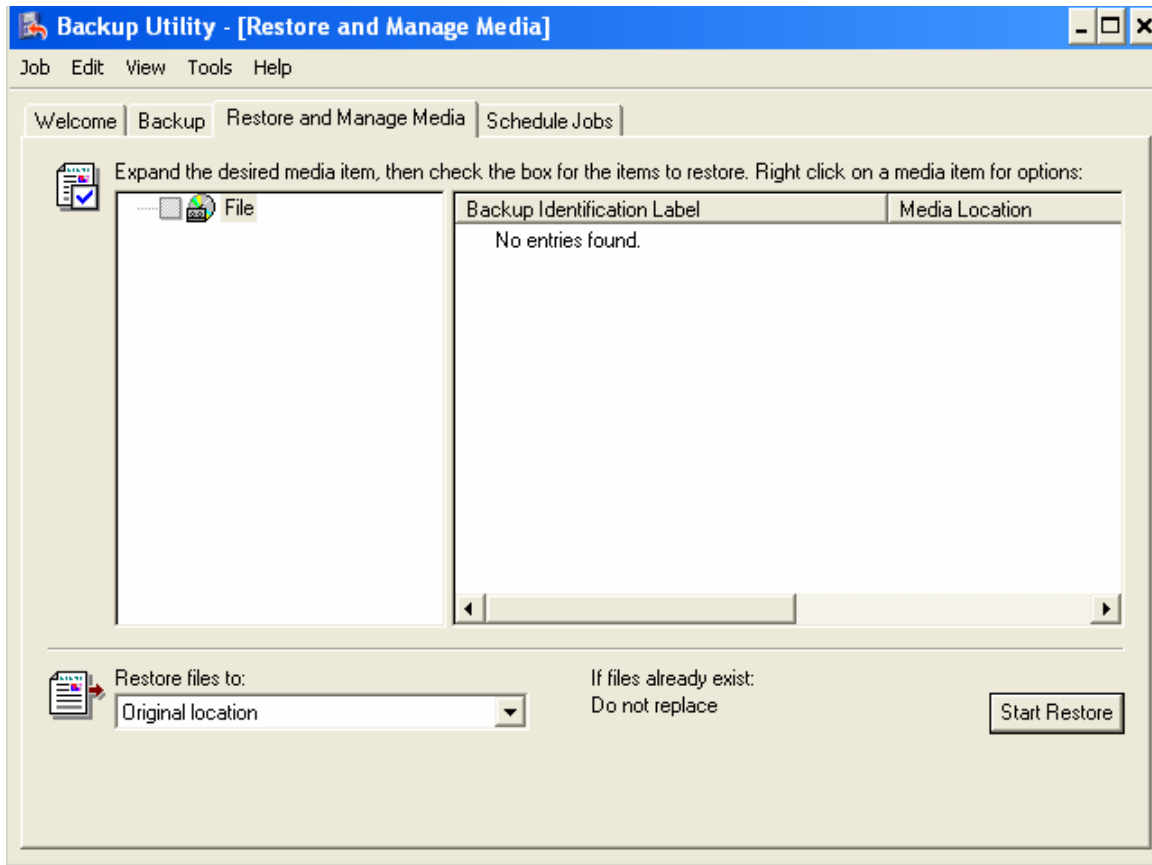


4. Xác định nơi lưu trữ bản backup , chọn các tùy chọn tại **advanced** Backup options, hoặc lập lịch biểu (schedule) cho việc này diễn ra tự động.

Khi hệ thống gặp sự cố hay các File/Registry bị thay đổi có thể chọn Restore để phục hồi



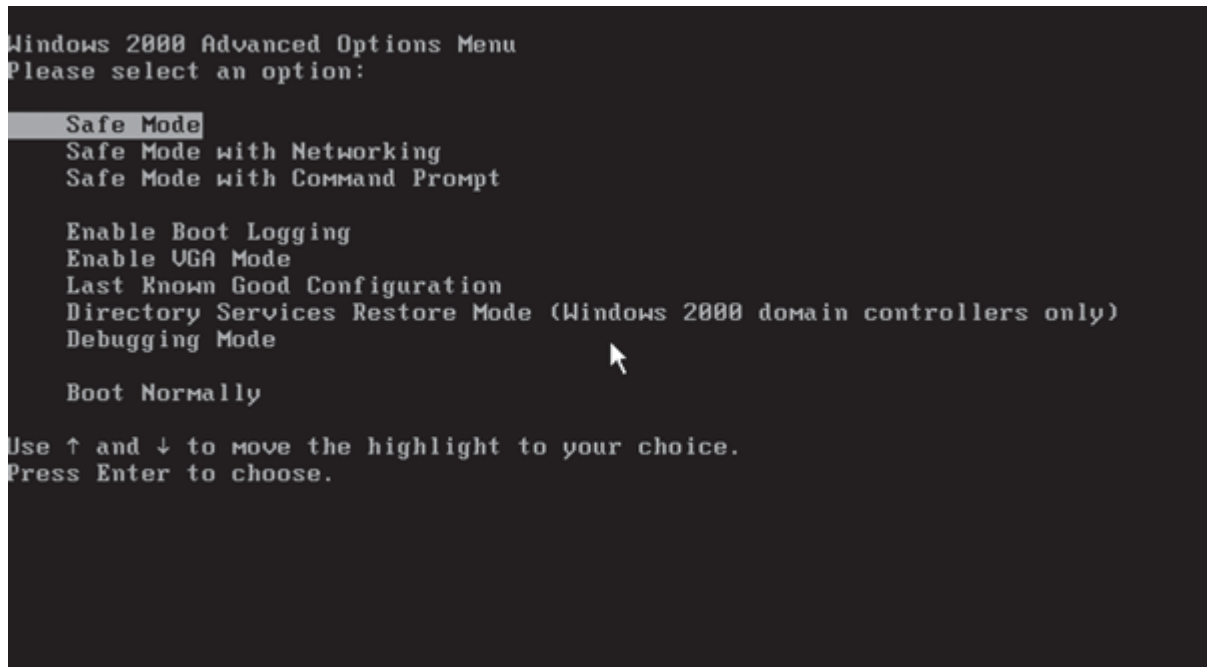
NETWORK INFORMATION SECURITY VIETNAM



Khi hệ thống gặp sự cố nặng không vào HĐH được, khởi động lại Computer chọn **F8** và chọn **Safe Mode**, vào chế độ này tiên hành hoạt động phục hồi System State data tương tự



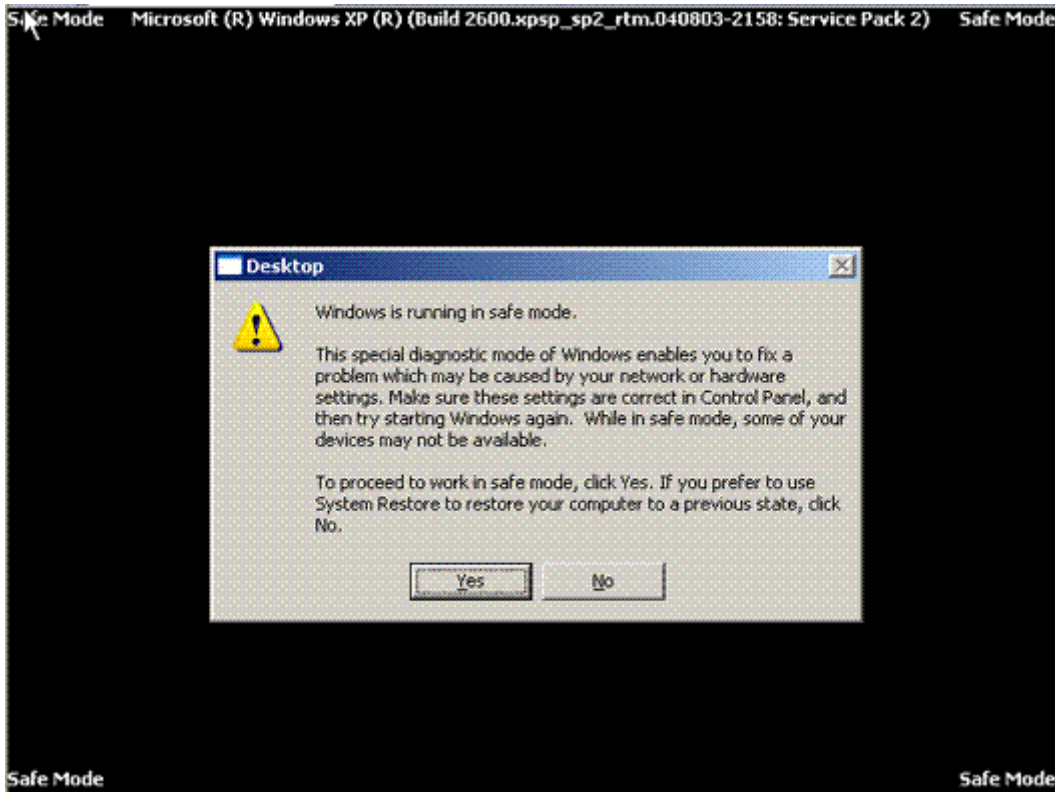
NETWORK INFORMATION SECURITY VIETNAM



Khởi động vào **Safe Mode..** Sau đó chúng ta mở chương trình Backup và tiến hành phục hồi System state data bình thường.



NETWORK INFORMATION SECURITY VIETNAM



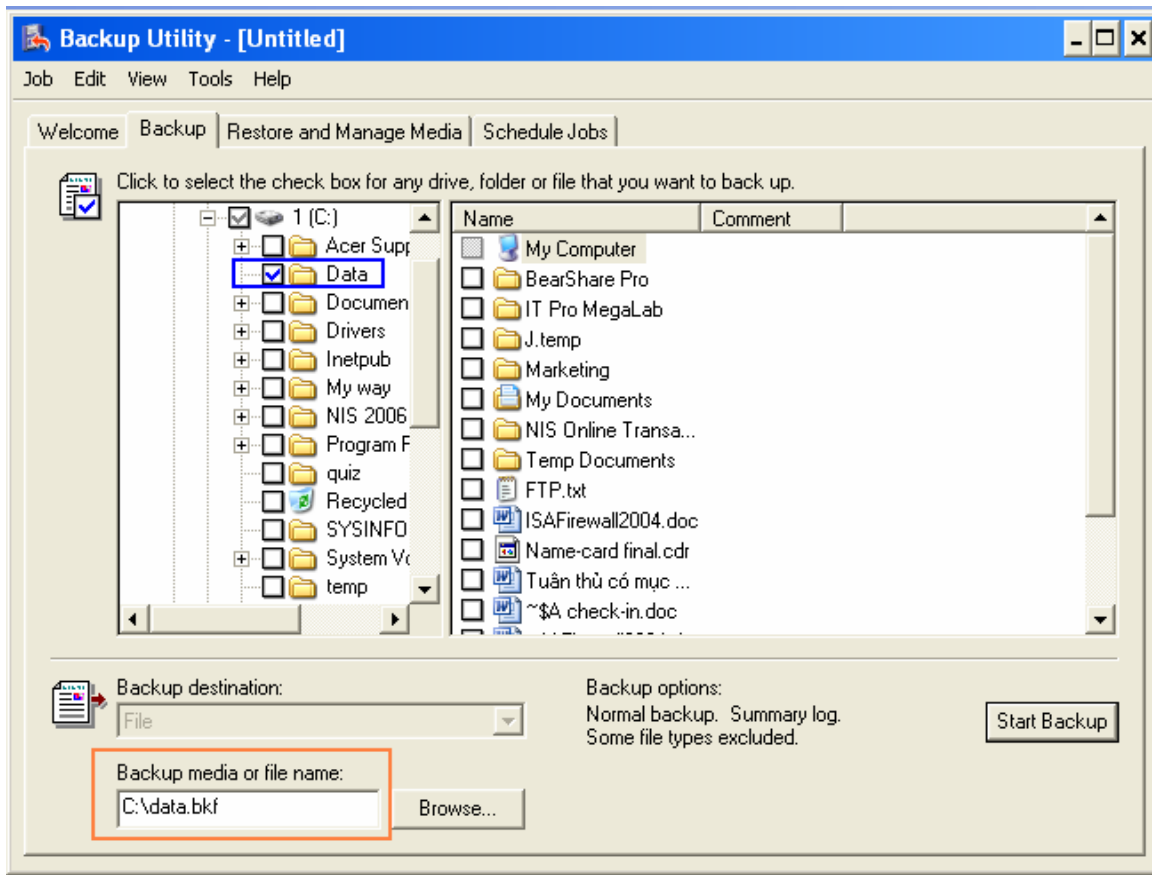
Lập lịch biểu cho việc backup diễn ra tự động

Backup dữ liệu thông thường của Computer (data) và dữ liệu hệ thống như System State data là công việc quan trọng phải làm, nhưng hãy tượng tượng ngày nào cũng làm hoặc làm ngẫu nhiên, chắc chắn sẽ gây nhầm chán, hoặc thiếu sót. Bất kỳ phần mềm backup nào cũng đều có tính năng lập lịch để backup tự động vào thời điểm xác định. Tính năng này gọi là **Scheduling Backup**

Tiến hành các bước bình thường, chọn dữ liệu cần backup, trong ví dụ này là C:\Data, khung màu xanh và file được backup .bkf được lưu tại đâu, khung màu hồng



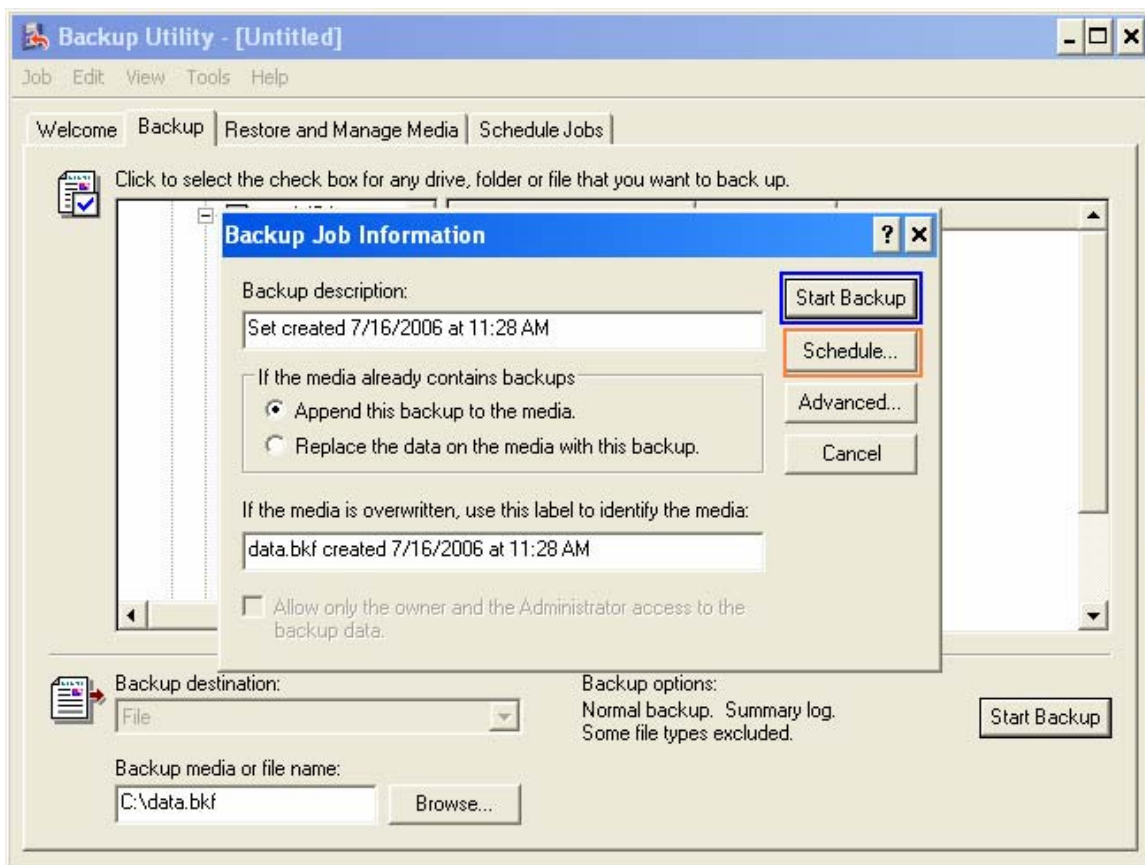
NETWORK INFORMATION SECURITY VIETNAM



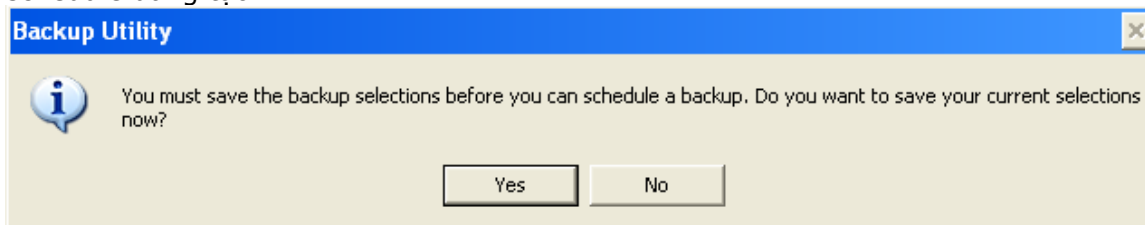
Chọn **Start Backup**, sau đó nếu chúng ta click vào nút Start Backup, màu xanh công việc sẽ tiến hành bình thường. Để lập schedule các bạn click vào nút **Schedule**, khung màu hồng



NETWORK INFORMATION SECURITY VIETNAM



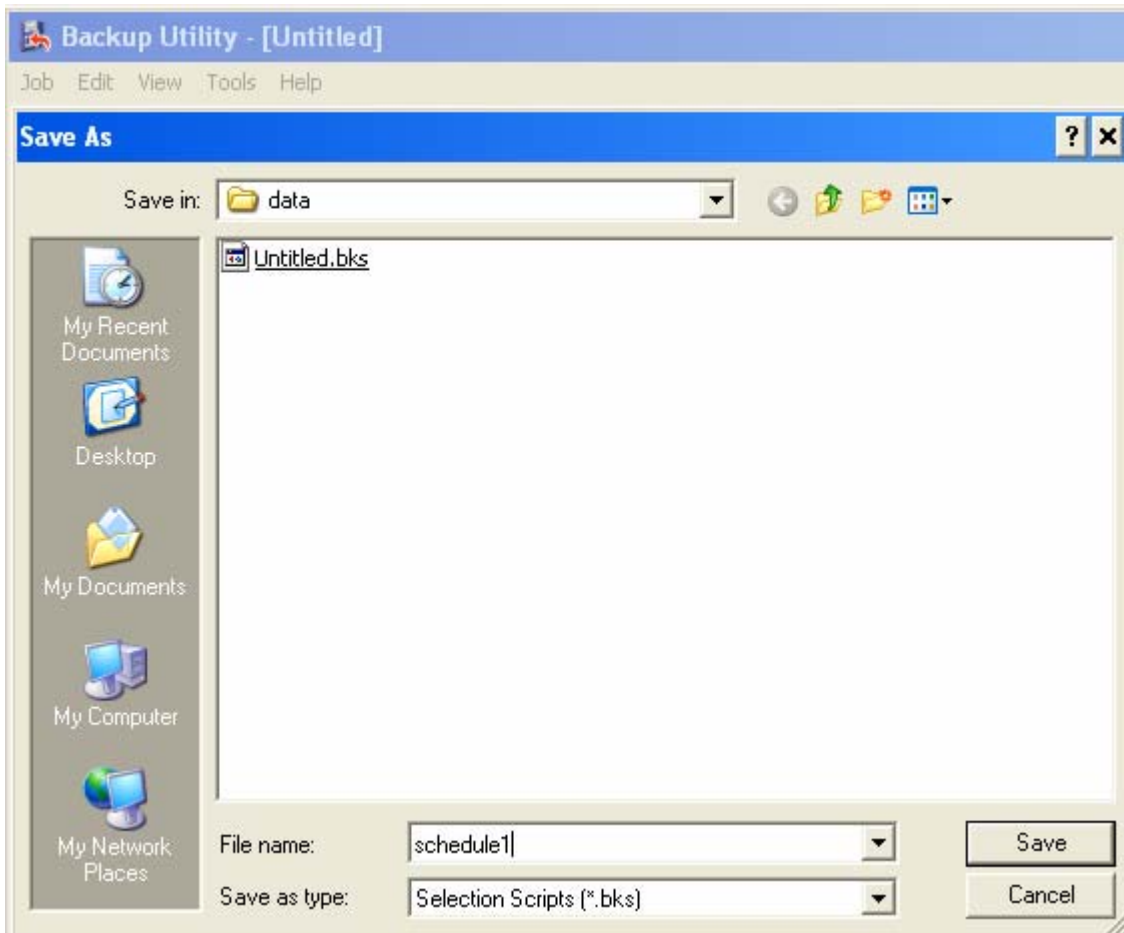
Chúng ta có thể lập hàng loạt lịch biểu để backup các dữ liệu khác nhau, thế nên các bạn phải xác nhận cho từng schedule này. Chọn **Yes**, để hệ thống lưu lại chọn lựa schedule đang tạo



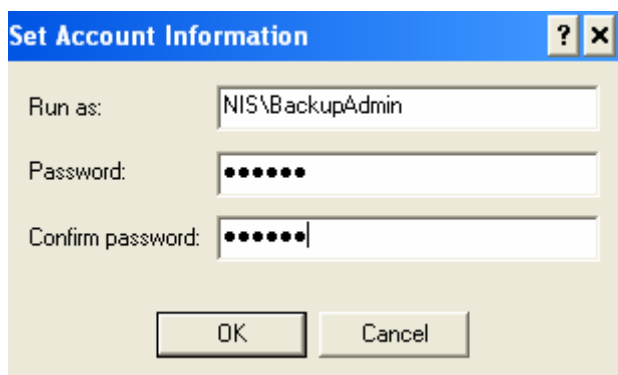
Trong ví dụ này chúng ta đặt tên file là **schedule1.bks**



NETWORK INFORMATION SECURITY VIETNAM



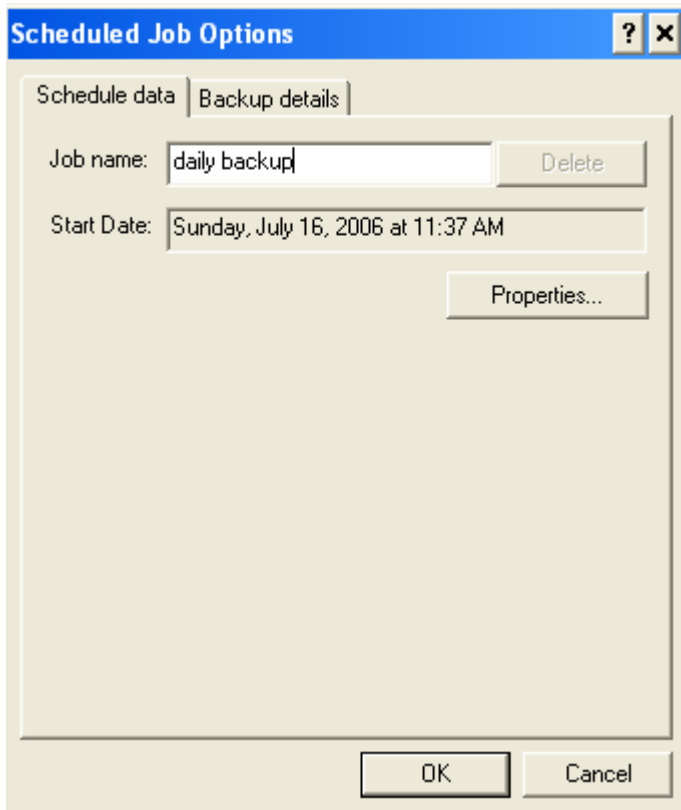
Sau đó xác định tài khoản được dùng để chạy backup tự động theo lịch. Trong ví dụ này tôi dùng User là **BackupAdmin (password là 123456)**, tài khoản này thuộc nhóm **Backup Operators**. Trên hệ thống thì mặc định chỉ có 2 Groups là có thể chạy các chương trình Backup/Restore là **Administrators** và **Backup Operators**.





NETWORK INFORMATION SECURITY VIETNAM

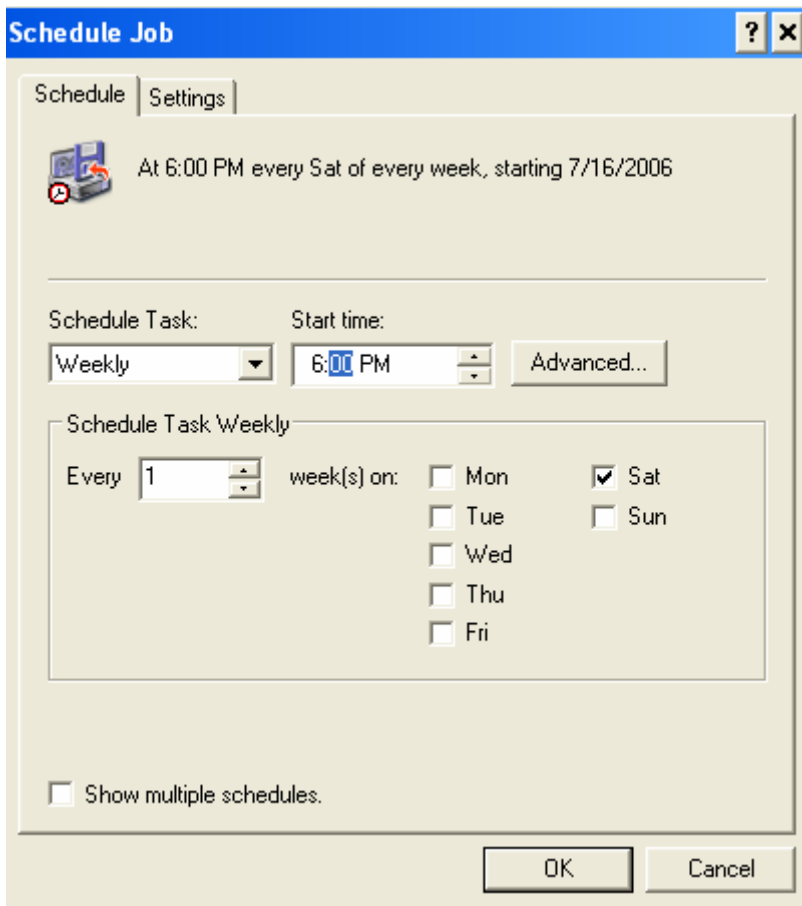
Tiếp theo đặt tên schedule backup này là **daily backup** (đặt tên này tùy ý bạn)



Chọn tiếp **properties**, và xác lập các thông số như Daily (backup hàng ngày), Once (chỉ một lần duy nhất), Weekly (hàng tuần)...**Start Time** (bắt đầu backup thời điểm nào). Trong ví dụ này tôi sẽ chọn backup vào ngày thứ 7 hàng tuần, vào 6 giờ chiều, vì đây là thời điểm thích hợp cho backup khi Mạng cty không giao dịch nhiều (ngày nghỉ)..



NETWORK INFORMATION SECURITY VIETNAM



Như vậy cứ đến thời điểm này hàng tuần nbackup sẽ tự động chạy và backup theo đúng những lịch đã tạo.

Dùng System Restore Point phục hồi hệ thống trên Windows XP Pro.

Nếu như backup System State Data khiến cho người sử dụng cảm thấy yên tâm hơn về hệ thống của mình, vì các thành phần lõi của hệ thống đã được "save", và nếu như sự cố xảy ra có liên quan đến system, registry v.vv khiến HĐH không thể làm việc, lúc này bạn có thể khởi động Computer từ chế độ an toàn Safe Mode và bắt đầu tiến trình phục hồi. Cơ hội để máy tính vận hành bình thường trở lại là rất lớn Tuy nhiên không phải lúc nào chúng ta cũng cần một quy trình xử lý công phu như vậy. Có những sự cố nhỏ xảy ra trên hệ thống, khiến hệ thống không còn vận hành trơn tru như lúc đầu, có những xung đột hệ thống, xung đột giữa hệ thống và new Applications, .. khiến hệ thống chạy có vẻ "chập chờn", chậm chạp. Bạn cài thêm một số ứng dụng mới hôm nay, cài một số thiết bị phần cứng mới, chỉnh sửa các thông số hệ thống..và những hành động này có thể là nguyên nhân. Bạn ước gì Computer của bạn quay trở lại trạng thái hoạt động tốt như hôm thứ 6 vừa rồi, Windows XP Pro có thể giúp bạn điều này không. Microsoft có vẻ như rất hiểu người



NETWORK INFORMATION SECURITY VIETNAM

dùng chuyên nghiệp và tích hợp vào HDH này tính năng **System Restore Point**, một tính năng hay, có thể đưa Computer quay trở lại những thời điểm được cho là tốt nhất vào những ngày trước đó.

*Một khi hệ thống Failed, một khi hệ thống hoạt động làm bạn không hài lòng, có thể dùng **System Restore Point** đưa hệ thống trở về một thời điểm hoạt động tốt nhất. Tất nhiên thời điểm này đã được System Restore Point "save" lại, và vấn đề duy nhất bạn cần làm là: Trong nhiều thời điểm đã được "save", hãy xác định thời điểm cần phục hồi. Thứ 6 hay thụ tuần trước máy hoạt động ổn định, System Restore Point hãy giúp tôi phục hồi về thời điểm ấy..*

Nếu System Restore Point có thể làm được điều này, hẳn là kỳ diệu vì đã giúp bạn bỏ qua hàng loạt vấn đề đau đầu khi chẩn đoán và khắc phục nguyên nhân của các sự cố. Và các thủ tục phiền hà khi tiến hành phục hồi.

System Restore Point hoạt động thế nào ? Hãy tưởng tượng như một máy ảnh, nó ghi lại cấu hình hệ thống vào thời điểm mà bạn muốn chụp (snapshot), và như vậy nó sẽ quan sát và ghi lại được những thay đổi của những thành phần hệ thống tại các thời điểm khác nhau như: sự thay đổi các System files: EXE, SYS, DLL, và COM files...sau đó lưu lại tất cả thay đổi này vào Hard disk. Tuy nhiên cũng chú ý rằng, nó không có trách nhiệm lưu những dữ liệu thông thường của bạn tại những thời điểm này như các file .doc, .xls và các dữ liệu khác chứa trong My Documents folder. Đây là những dữ liệu cá nhân thông thường, không phải là dữ liệu hệ thống (bạn phải tự backup theo cách thông thường thôi).

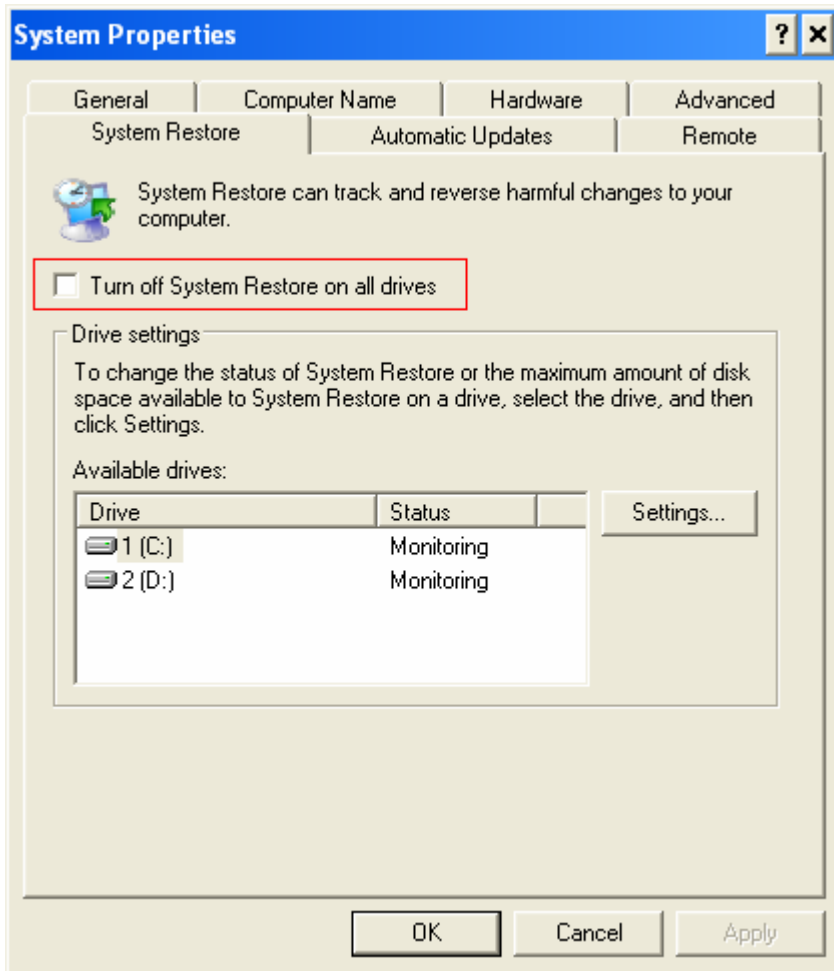
Và cũng chú ý một điều quan trọng là, khi phục hồi hệ thống về quá khứ, System Restore Point cũng không hoàn toàn remove những ứng dụng bạn mới cài đặt, bạn cứ yên tâm về điều này...

Cấu hình một System Restore Point

Trước khi cấu hình một System Restore Point, thì bạn cần phải bật tính năng này lên Right-click vào **My Computer**, chọn **Properties** và chọn **System Restore** như hình minh họa



NETWORK INFORMATION SECURITY VIETNAM



Bỏ không check vào khung màu Đỏ (như vậy bạn đã kích hoạt System Restore Point), chờ trong giây lát để hệ thống kích hoạt tính năng này.

Cần chú ý một điều về không gian đĩa cứng phải dành cho hoạt động của System Restore, ít nhất là 200MB nếu đĩa cứng dung lượng nhỏ. Thường đĩa cứng nhỏ hơn 4 GB, cần ít nhất 400 MB, trên 4 GB cần 12% dung lượng dành cho System Restore để lưu dữ liệu. VÀ tất nhiên nếu bạn không dùng tính năng System Restore thì hãy tắt (Turn Off) nó, để dành space lưu trữ cho các mục đích khác.

Tiếp theo sau khi đã bật System Restore, hãy chạy System Restore từ **Start** menu, chọn **All Programs, Accessories, System Tools, System Restore**. Hãy xem cách thức hoạt động

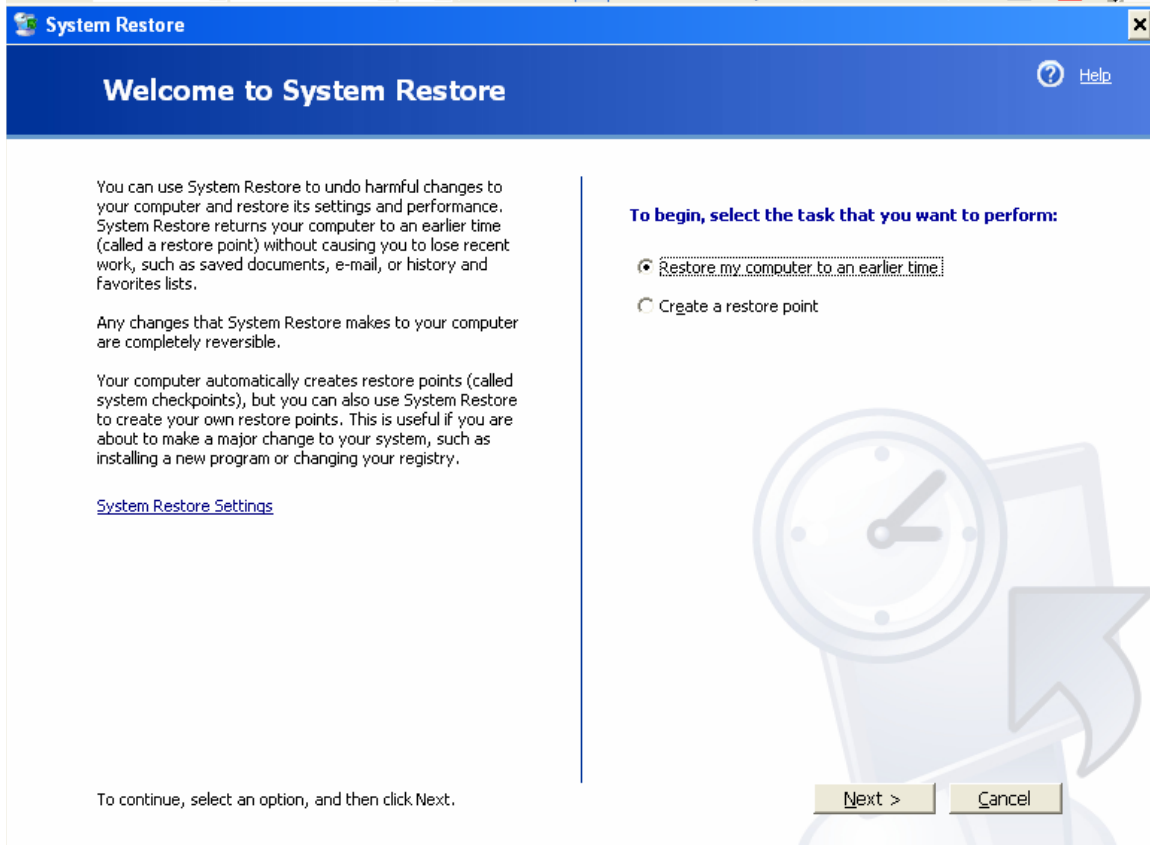
Trước hết, ngay sau khi bạn bật System Restore lên, thì hệ thống sẽ tạo ra ngay **System Checkpoint**, nó sẽ giám sát ngay toàn bộ những thay đổi hệ thống và lưu vào đĩa cứng. Cứ khoảng 24h một System Checkpoint mới sẽ được tạo, tất nhiên ngày nào bạn không dùng Computer ngày ấy System Restore sẽ không tạo System Checkpoint, ngày khi bạn mở máy vào ngày kế tiếp nó sẽ được tạo.



NETWORK INFORMATION SECURITY VIETNAM

Như vậy nếu System Checkpoint được tạo ra lần đầu tiên vào hôm nay, thì ngay ngày mai nếu không hài lòng với hoạt động của hệ thống, bạn có thể dùng chức năng phục hồi để chọn và quay trở lại System Checkpoint hôm qua.

Ví dụ tôi muốn quay trở lại thời điểm hôm qua, khi System Restore đã được "save"



Tôi chọn **Restore my computer to an earlier time** và chọn System checkpoint



NETWORK INFORMATION SECURITY VIETNAM

System Restore

Select a Restore Point

The following calendar displays in bold all of the dates that have restore points available. The list displays the restore points that are available for the selected date.

Possible types of restore points are: system checkpoints (scheduled restore points created by your computer), manual restore points (restore points created by you), and installation restore points (automatic restore points created when certain programs are installed).

1. On this calendar, click a bold date. 2. On this list, click a restore point.

July, 2006						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

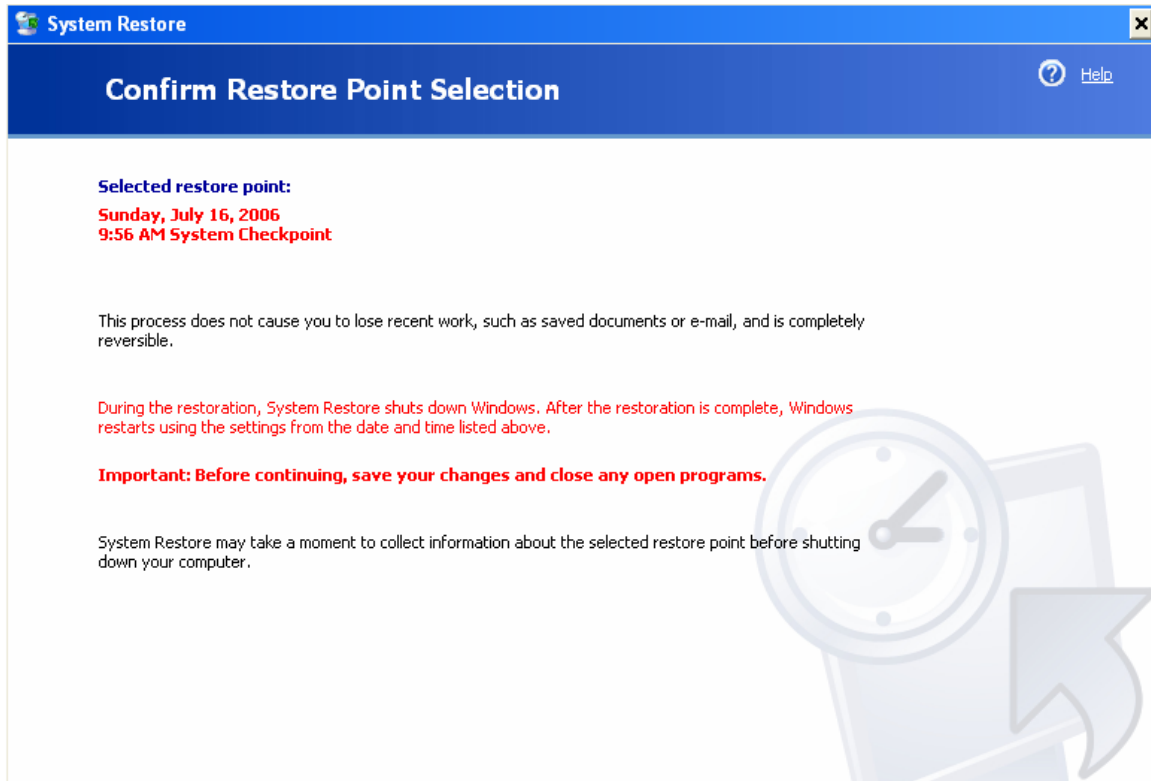
Sunday, July 16, 2006	
9:56:57 AM	new drivers
9:56:34 AM	System Checkpoint

< Back Next > Cancel

Đây là System checkpoint được hệ thống tạo ra lần đầu tiên vào thời điểm kích hoạt chức năng System Restore.
Click **Next** và thấy bảng thông báo



NETWORK INFORMATION SECURITY VIETNAM



*"Quy trình phục hồi không làm mất dữ liệu gần đây như e-mail, và có thể quay trở lại trạng thái vừa rồi nếu bạn muốn...
Trong suốt quá trình phục hồi System Restore sẽ shutdown Windows, sau khi khởi động Windows sẽ dùng lại các xác lập hệ thống đã lưu trước đó của ngày hôm qua lúc 9h56 AM..". xem hình.*

Như vậy System checkpoint từ khi được kích hoạt đã theo dõi sát sao hệ thống, và tạo ra các System checkpoint mới sau mỗi 24h (1 day), quá trình theo dõi và sao lưu từng ngày hoàn toàn tự động.

Tuy nhiên quá trình một ngày như vậy có lẽ là hơi dài, và đôi khi bạn tiến hành một việc gì đó can thiệp vào hệ thống như cài Application mới, cài Drivers cho thiết bị mới, bạn muốn tự mình tạo ngay các Restore Point tại thời điểm ấy, để nếu xảy ra trục trặc ngay sau khi cài những App và Drivers, bạn có thể phục hồi hệ thống quay lại thời điểm gần nhất khi bạn vừa lưu lại Restore point chứ không phải quay lại thời điểm ngày hôm trước

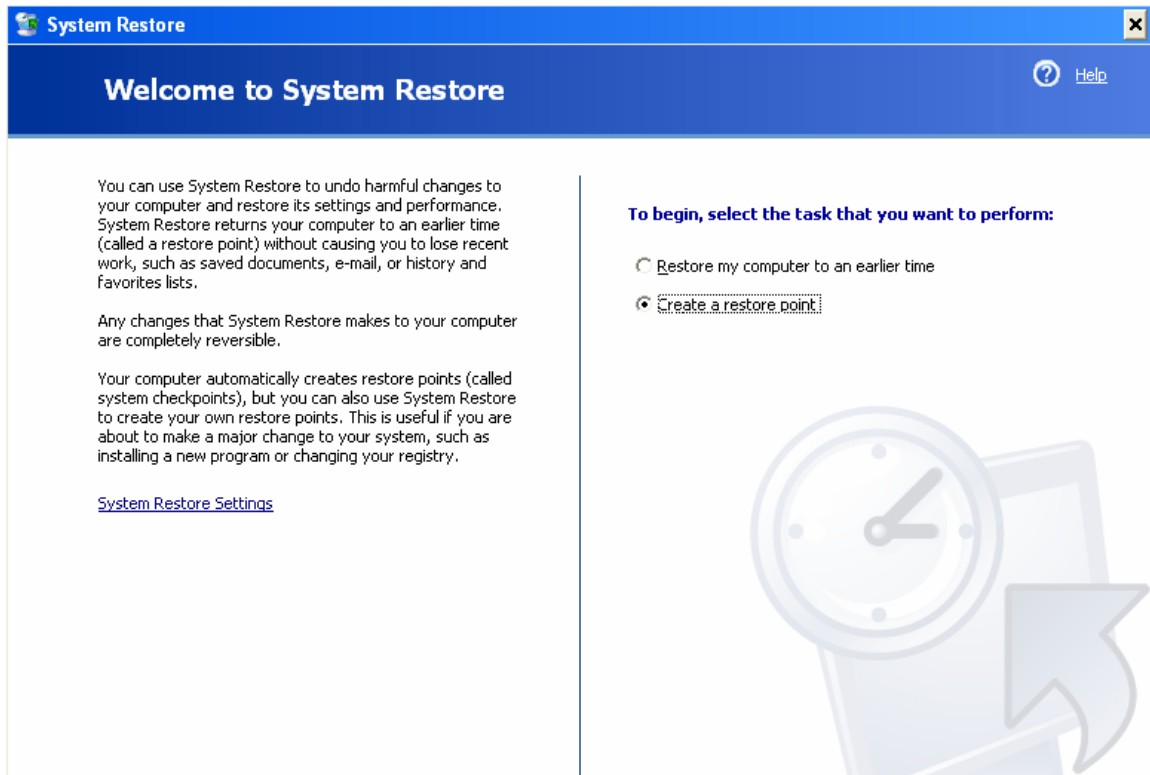
Như vậy đến đây có lẽ bạn đã hiểu cơ bản sự khác nhau giữa **System Checkpoint** do hệ thống tự tạo ngay lần đầu và sau mỗi 24h khác với một **Restore Point** do bạn tạo bất kỳ lúc nào bạn muốn (thường tiến hành sau khi cài Applications hoặc thay đổi Registry hoặc cài Drivers thiết bị mới..)

Cách tạo một Restore Point như sau:



NETWORK INFORMATION SECURITY VIETNAM

1. Tại **Help and Support Center**, click **Undo Changes To Your Computer With System Restore**.
2. Chọn **Create A Restore Point** và click **Next**.



3. Đặt tên cho **restore point** này ví dụ như **new drivers** và click **Create**.
Và khi muốn phục hồi bạn chỉ cần chọn **Restore my computer to an earlier time**
Và chọn Restore Point có tên **new drivers** bạn đã tạo



NETWORK INFORMATION SECURITY VIETNAM

System Restore

Select a Restore Point

The following calendar displays in bold all of the dates that have restore points available. The list displays the restore points that are available for the selected date.

Possible types of restore points are: system checkpoints (scheduled restore points created by your computer), manual restore points (restore points created by you), and installation restore points (automatic restore points created when certain programs are installed).

1. On this calendar, click a bold date. 2. On this list, click a restore point.

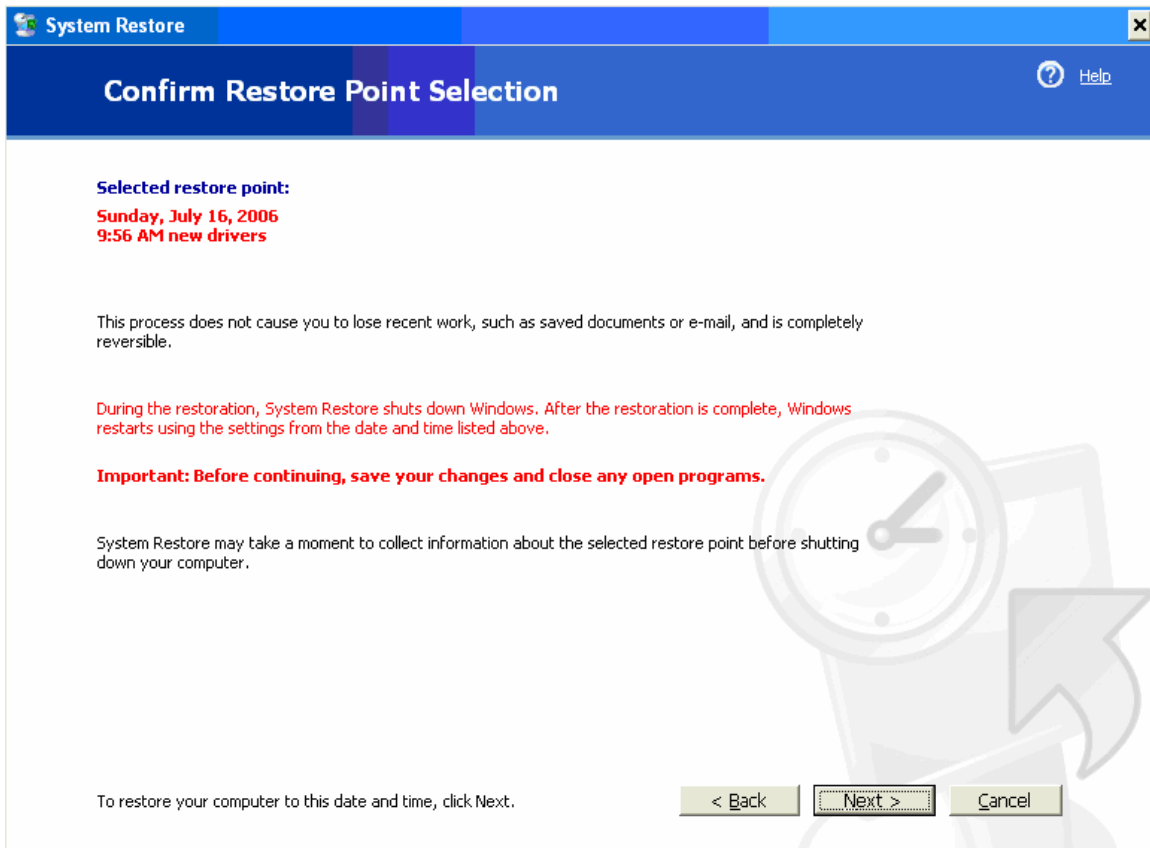
July, 2006						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Sunday, July 16, 2006	
9:56:57 AM	new drivers
9:56:34 AM	System Checkpoint

Xuất hiện thông báo như giải thích phần System checkpoint..



NETWORK INFORMATION SECURITY VIETNAM



Phục hồi toàn bộ hệ thống dùng ASR (Automated System Recovery – Phục hồi hệ thống tự động)

Trong các phần trước, chúng ta đã đề cập đến các vấn đề đảm bảo an toàn hệ thống thông qua việc:

- Backup toàn bộ System State Data (bao gồm Boot files, Com+ components, Registry..), để nếu có xảy ra hỏng hóc những File hệ thống này, có sự can thiệp làm hỏng Registry, hoặc các thành phần hệ thống khác. Chúng ta có thể dễ dàng phục hồi lại (Khởi động Computer vào HĐH chính và Restore, nếu HĐH chính không khởi động, hoàn toàn có thể vào chế độ an toàn Safe-mode để tiến hành phục hồi. Quy trình phục hồi đơn giản chỉ là xác định file đã backup của System state data đã lưu tại Partition hoặc thiết bị lưu trữ nào đó và phục hồi về nguyên trạng – Original Location...)
- Bạn cũng đã học qua cách sử dụng System Restore Point, sau khi được kích hoạt nó sẽ giám sát và lưu thông tin hệ thống tại những thời điểm khác nhau, nếu hiện tại chúng ta không hài lòng với hoạt động củ hệ thống (hệ thống ận hành chậm, treo máy, có xung đột ứng dụng hoặc drivers không tương thích .., có thể dùng System checkpoint hoặc Restore Point để mang hệ thống quay trở lại thời điểm hoạt động trơn tru mà bạn hài lòng nhất.



NETWORK INFORMATION SECURITY VIETNAM

- Các bạn đã nhận thấy rằng, Hệ thống đã trở nên an toàn hơn với những tính năng rất hay này. Tuy nhiên còn một nguy cơ khác, nguy cơ lớn nhất, một điều gì đó có thể khiến toàn bộ hệ thống "down". Nếu điều đó xảy ra, là thảm họa "disaster" cho Computer. Không thể khởi động lại Computer, cho dù bạn có khởi động từ safe-mode, màn hình xanh chết chóc "blue-death" xuất hiện. Đây là mối đe dọa nguy hiểm nhất, và người dùng cũng "sợ" nó nhất, thường thì họ sẽ cài lại toàn bộ máy (cái duy nhất giữ lại được có lẽ là Data của họ còn đâu đó trên C:, D:, E:...), tất cả mọi ứng dụng, cấu hình hệ thống sau bao năm tháng triển khai đã không còn..

Tóm lại là bạn đang đối mặt với một hệ thống hoàn toàn bị "failed". Tuy nhiên bạn không nên quá lo lắng, Windows XP Pro đã chuẩn bị cho bạn một vũ khí mạnh, và nếu sử dụng đúng cách, nó sẽ đem hệ thống hoạt động bình thường trở lại, đó là hệ thống phục hồi tự động **ASR**

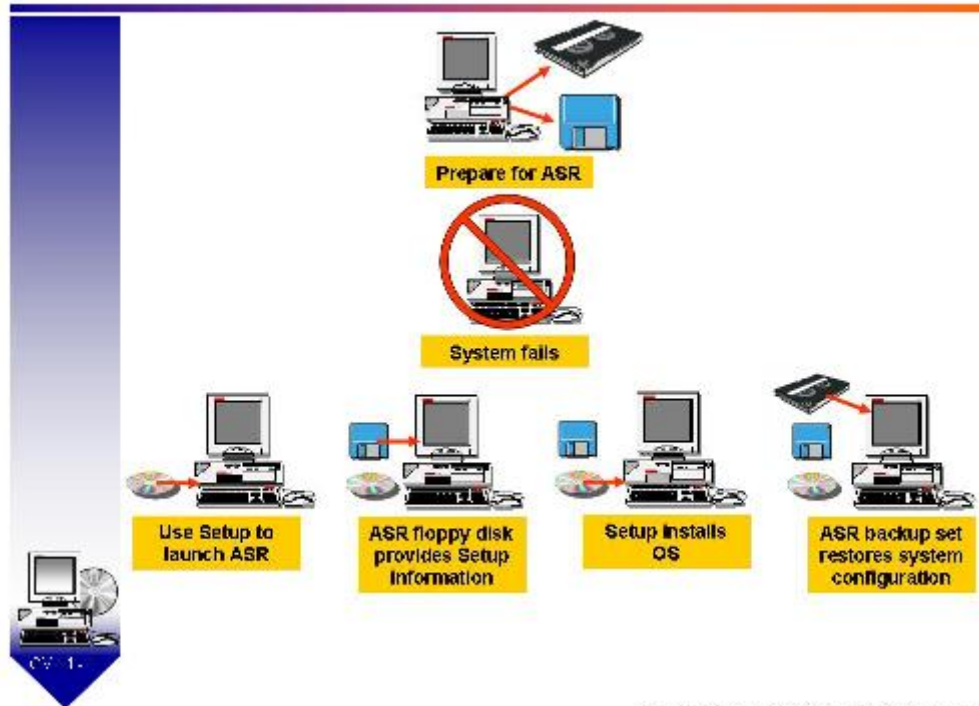
Automated System Recovery (ASR) là một quy trình dùng các dữ liệu đã backup và toàn bộ source files của Windows XP Professional installation (các source files cài đặt này chính là CD cài đặt Windows XP Pro) để xây dựng lại "rebuild" một hệ thống máy tính đã hỏng. Để tiến hành ASR, cần những bước chuẩn bị sau:

- Đĩa CD-ROM cài đặt Windows XP Professional (cái này chúng ta đã có)
- Một đĩa mềm ASR (ASR floppy disk), đĩa này chứa các file thông tin cài đặt gọi là *Setup Information Files (SIF)* đây là những thông tin cơ sở cần để Windows Setup có thể chạy phục hồi ASR.
- Một tập *ASR backup set*, được tạo với chương trình Windows Backup mà bạn đã biết, ASR backup set này là một bản copy toàn bộ files hệ thống (system files) của Windows XP Professional và tất cả thông tin về cấu hình hệ thống.

Đây là 3 bước cần chuẩn bị trước khi bắt tay vào phục hồi hệ thống.
Hãy xem kỹ hình minh họa sau về quy trình từng bước phục hồi



The ASR Process



Như vậy các bạn nhận thấy trình tự diễn ra như sau:

1. Administrator sẽ dùng Windows Backup để tạo một **ASR backup set** trước (ASR backup set có dung lượng khá lớn, vài trăm MB, vì lưu lại toàn bộ cấu hình hệ thống và ASR backup set bắt buộc phải lưu trữ trên các thiết bị lưu trữ cục bộ của máy bạn như: Ổ ghi CD, usb disk, HDD thứ 2, Iomega Zip disk.. chứ không phải lưu tại một thiết bị hay một ổ đĩa Mạng của server Mạng nào đó) . Các bạn cũng chú ý rằng ASR backup set lưu thông tin cấu hình hệ thống (system files, Registry, System components, System Policy, User Accounts..) chứ không lưu dữ liệu cá nhân của bạn như music, video, documents, email,..sau ASR backup set cần chọn thêm backup là **backup everything on this computer** , mà chúng tôi sẽ đề cập sau. *Để sau này ngoài việc phục hồi cấu hình hệ thống từ ASR backup set , các bạn không để đánh mất bất kỳ dữ liệu gì trên Computer của mình. Chú ý thêm nữa là ASR backup set cũng không được lưu trên đĩa cứng HDD có chứa thư mục cài đặt Windows XP , ví dụ như C:\Windows của bạn, vì nếu HDD của bạn bị hư hỏng hoàn toàn, thì không thể lấy lại ASR backup set để phục vụ cho quá trình phục hồi..*

Ngay sau bước này ASR sẽ yêu cầu bạn tạo một đĩa mềm **ASR floppy disk**.



NETWORK INFORMATION SECURITY VIETNAM

2. Một hệ thống đã failed hoàn toàn, không khởi động được. Ví dụ như Computer của bạn hư hỏng hoàn toàn đĩa cứng.
3. Administrator thay đĩa cứng mới vào hoặc chọn một Computer khác dùng cho quá trình phục hồi.
4. Administrator sẽ chạy chương trình cài đặt Windows Setup từ CD-ROM Windows XP và bắt đầu khởi hoạt cho tiến trình phục hồi ASR.
5. Administrator cung cấp đĩa mềm ASR floppy disk vào.
6. Hệ thống sau khi xem và lấy các thông tin từ ASR floppy disk phục vụ cho tiến trình Windows Setup tiếp theo.
7. Windows Setup sẽ cài HĐH như các xác lập đã ghi trên ASR floppy disk.
8. Administrator cung cấp đĩa (CD, Usb, Iomega Zip) đã lưu trữ **ASR backup set** vào để tiến trình tiếp tục (lúc này các bạn đã hiểu vì sao ASR backup set không lưu trên ổ đĩa mạng mà phải là local)
9. ASR sẽ cấu hình hệ thống theo thông tin trong **ASR backup set**.
10. Và sau bước này các bạn có thể khởi động lại hệ thống cũ trên Computer mới. Và nếu lo ngại những dữ liệu cá nhân trước đó bị mất, thì bước **backup everything on this computer** (đã chuẩn bị trước theo lịch biểu trong quá trình backup định kỳ của Computer) sẽ là bước cuối cùng giúp chúng ta có một hệ thống bảo toàn trọn vẹn .

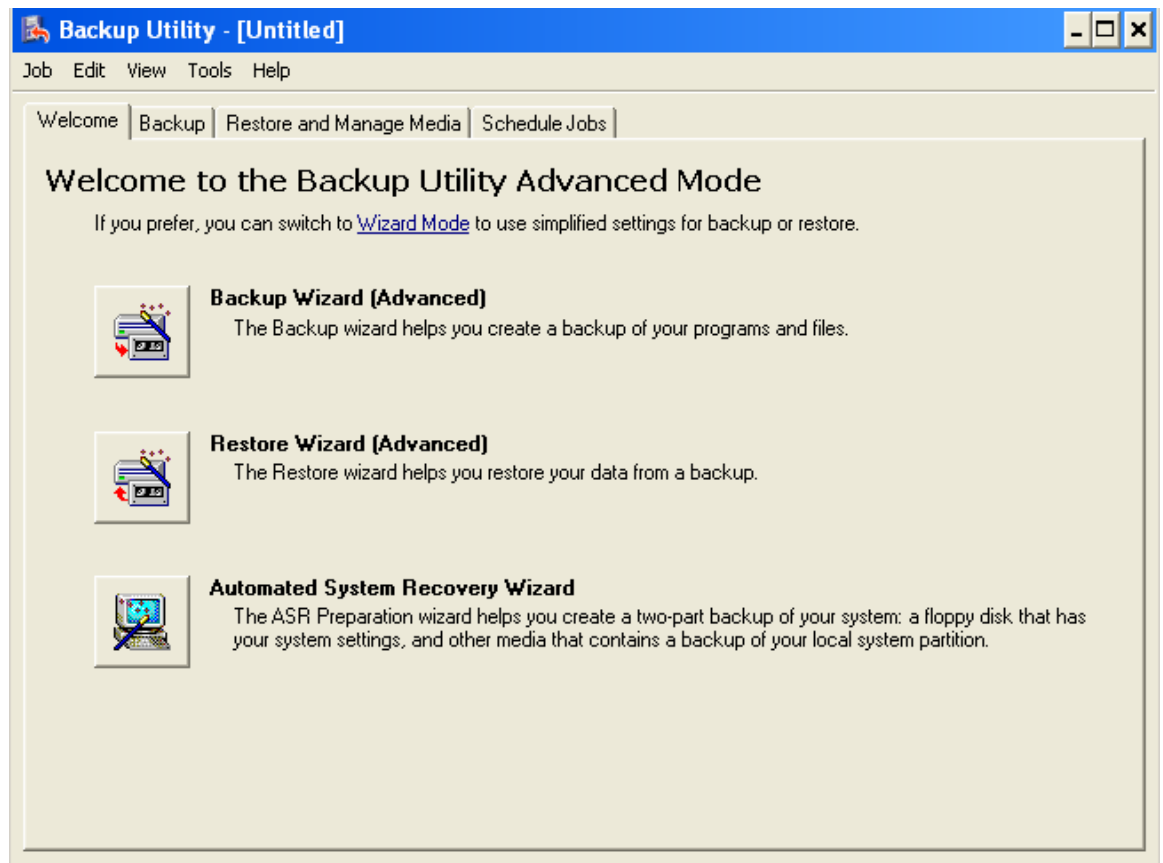
Và sau đây là các bước thực hành, Steps by Steps:

1. Backup toàn bộ dữ liệu trên Computer là công việc nên làm theo định kỳ, để bất cứ tình huống nào xảy ra (như hư toàn bộ HDD), dữ liệu cá nhân của bạn vẫn không bị mất. Chúng ta có thể lập lịch biểu vào những giờ nghỉ ngơi "idle", để hệ thống tự động backup toàn bộ dữ liệu trên computer. Ví dụ anh Hùng sẽ thường **backup everything on this computer**, vào 12h PM thứ 7 hàng tuần. Lần đầu tiên **backup everything on this computer** đương nhiên là anh ấy sẽ chọn **Normal** (hay còn gọi Full backup) và thứ 7 các tuần tiếp theo, để giảm thời gian backup, anh ấy có thể chọn các kiểu như **Incremental** hoặc **Differential**. Và các bạn cũng chú ý một điều quan trọng là nếu dữ liệu Computer càng quan trọng, tần suất chỉnh sửa thay đổi nhiều, thì số lần backup cũng tăng theo, có thể một tuần phải backup nhiều lần.

Mở **Ntbackup.exe, Backup Wizard**, chọn **Next**



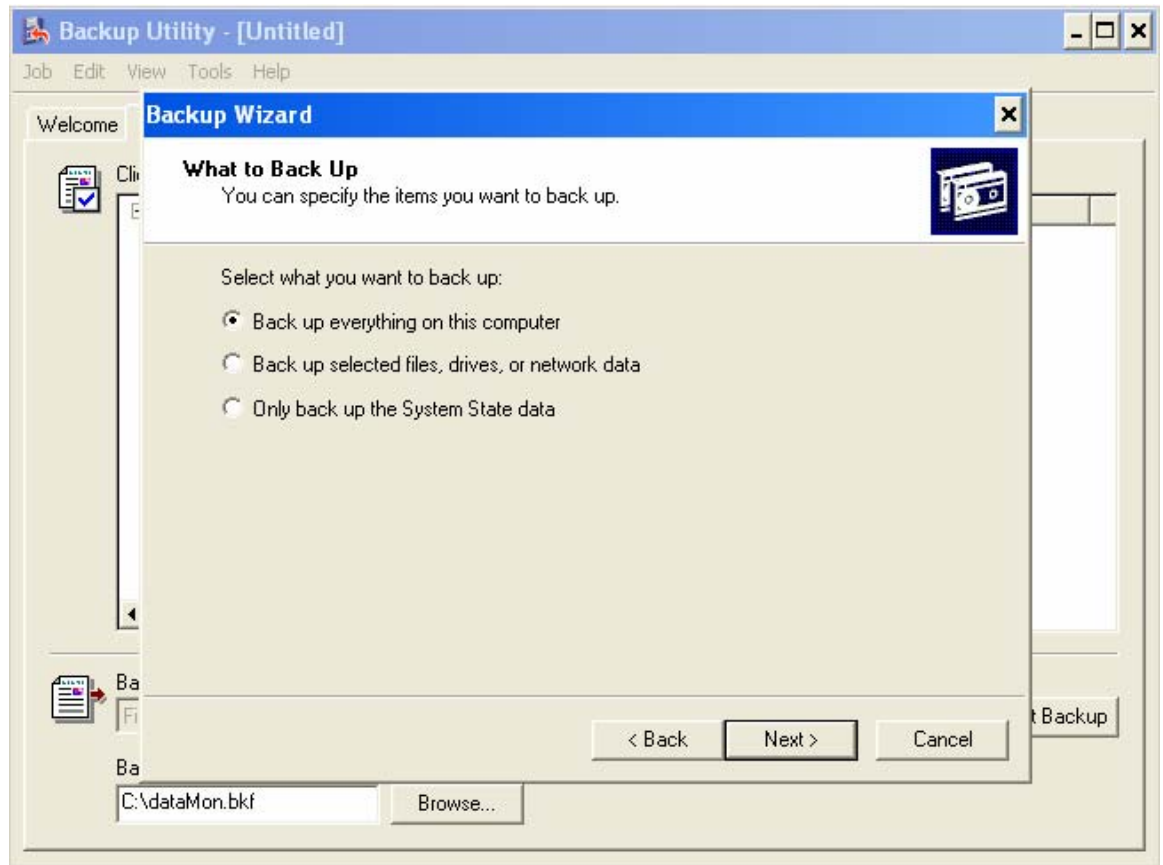
NETWORK INFORMATION SECURITY VIETNAM



Chọn tiếp **backup everything on this computer**, chọn **Next**



NETWORK INFORMATION SECURITY VIETNAM




Lúc này cần chú ý toàn bộ data trên Computer bạn cần ổ chứa lớn tương xứng (chọn partition/HDD, tape, các loại đĩa lưu trữ khác đủ lớn), trong ví dụ này tôi chọn lưu dữ liệu lên ổ D: (trong thực tế nếu có kinh phí các bạn nên trang bị các loại thiết bị lưu trữ chuyên dụng à bảo quản cẩn thận, lưu trữ trên cùng là giải pháp không tốt chút nào)

Chọn D: và file backup toàn bộ dữ liệu là FullBackup.pkf



NETWORK INFORMATION SECURITY VIETNAM

Backup Wizard ✕

Backup Type, Destination, and Name 

Your files and settings are stored in the destination you specify.

Select the backup type:

File

Choose a place to save your backup:

D:\ Browse...

Type a name for this backup:

FullData.bkf

< Back **Next >** Cancel

Chọn **Next**, và trước khi click **Finish**, chọn tab **Advanced**, để kiểm tra lần đầu backup là **Normal**



NETWORK INFORMATION SECURITY VIETNAM

Backup Wizard [X]

Type of Backup
You can choose the type of backup that fits your needs.

Select the type of backup:

Normal

Description
Backs up selected files, and marks each file as backed up.

< Back Next > Cancel

Backup Wizard [X]

Completing the Backup Wizard

You have created the following backup settings:

Description: Set created 7/17/2006 at 3:03 AM
Contents: Back up all files on my local drive(s)
Location: File
Media: C:\dataMon.bkf
When: Now
Verify off, Do not use hardware compression,
Append to my media, Normal backup.

To close this wizard and start the backup, click Finish.
To specify additional backup options,
click Advanced.

Advanced...

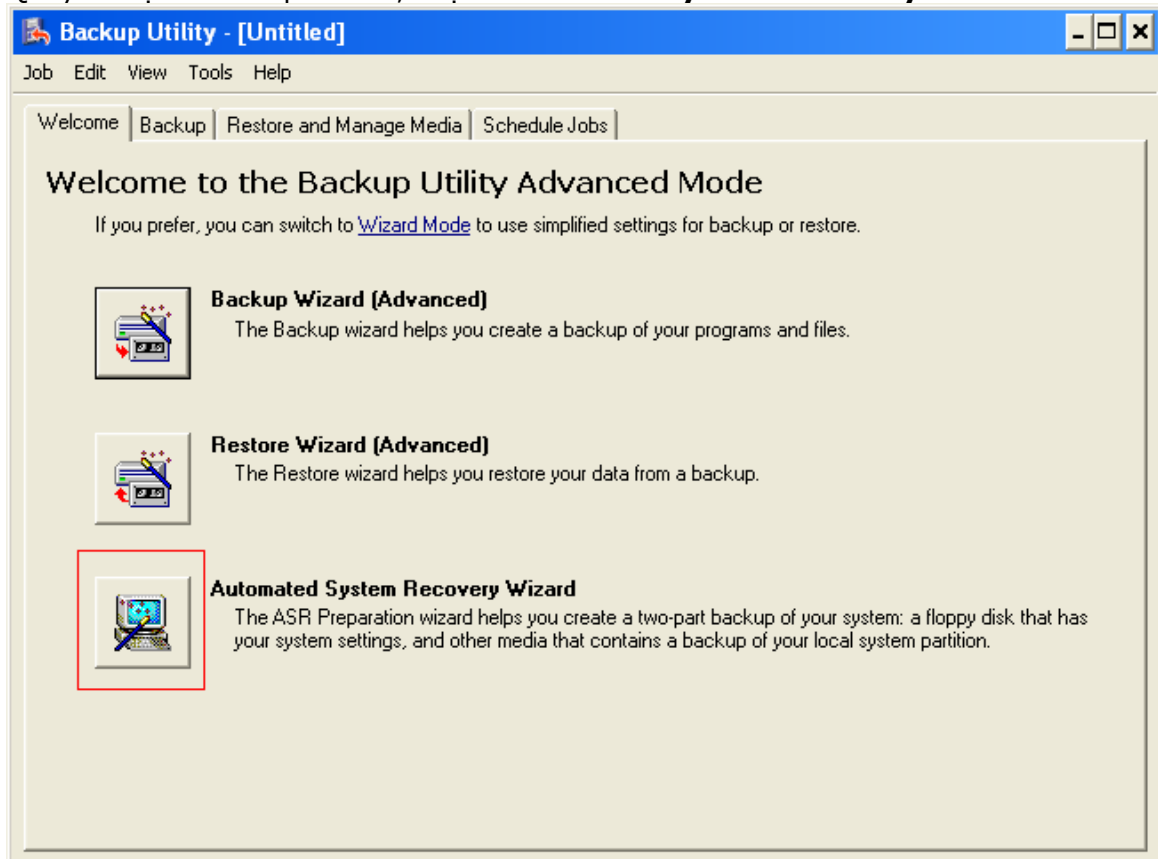
< Back Finish Cancel



NETWORK INFORMATION SECURITY VIETNAM

2. Tạo **ASR Backup Set**

Quay trở lại Ntbackup wizard, chọn **Automated System Recovery Data**




Trong ví dụ này, **ASR backup set** sẽ được lưu tại D: với filename **ASR.bkf**, click **Next**



NETWORK INFORMATION SECURITY VIETNAM

Automated System Recovery Preparation Wizard ✕

Backup Destination 

Where would you like the system backup to be saved?

Select a media type for your system backup, and then enter the name of the media to store the backup data.

Backup media type:

Backup media or file name:

The wizard will also require a floppy disk to create a recovery disk. This disk will contain information necessary to recover your system.

Sau đó click **finish**, để hoàn thành **ASR backup set**. Tiến trình này kéo dài khoảng 30'.

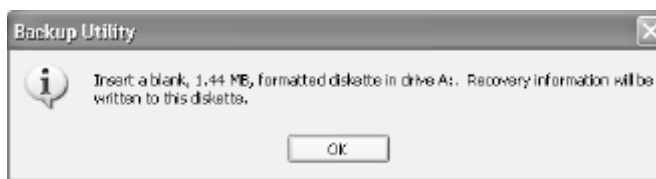


NETWORK INFORMATION SECURITY VIETNAM



3. Tạo đĩa mềm **ASR floppy disk**

Ngay sau tiến trình này các bạn sẽ tạo đĩa mềm ASR, chèn FDD 1.44' theo như hướng dẫn



Ngay sau khi tiến trình ghi hoàn thành, rút đĩa mềm ra và dán nhãn (label) ghi rõ **ASR** để nhớ mà dùng cho quá trình phục hồi.





NETWORK INFORMATION SECURITY VIETNAM

Click **close** 2 lần và đóng Windows backup lại.

4. Hệ thống hư hỏng và tiến hành các bước phục hồi trên Computer mới hoặc đã thay đĩa cứng mới

a. Chèn đĩa cài đặt Windows XP Professional CD-ROM vào ổ CD-ROM

b. Restart lại computer.

c. Được nhắc nhở nhấn một phím.

d. Chọn nhấn [**F2**] để chạy **Automated System Recovery (ASR)** và nhận thấy thông báo message xuất hiện dưới thanh trạng thái, nhấn [**F2**].

e. Khi được nhắc nhở chèn đĩa mềm ASR floppy disk, nhấn bất kỳ phím nào tiếp theo. Nếu tiến trình phục hồi không nhận ra ASR floppy, để nguyên nó trong ổ đĩa mềm và khởi động lại Computer từ CD-ROM

f. Tiếp theo, nhấn **C** khi được nhắc nhở và xác nhận xóa toàn bộ các partition trên đĩa cứng, để ASR tái tạo lại cấu hình Basic Disk.
Sau bước cấu hình Disk này, Windows sẽ tự động cài HĐH, thời gian khoảng 45'.

g. Restart lại Computer và **Automated System Recovery Wizard** xuất hiện, click **Next**. Khi được nhắc, chèn thiết bị lưu trữ **ASR backup Set** (chú ý bạn đã backup nó vào HDD thứ 2, hoặc CD write, Zip, USB....chọn đúng thiết bị)

h. **verify the location of the backup set..** chọn **Next**

i. Click **Finish** hoàn tất tiến trình phục hồi, mất khoảng 30' nữa.

ii. Khởi động lại Computer, và log-on với tài khoản Administrator hoặc các tài khoản Admin khác của bạn lúc trước. Cần thận dùng các công cụ quản trị hệ thống (**Administrative tools**) kiểm tra lại các tài khoản User accounts vẫn đầy đủ, kiểm tra xem Computer vẫn là thành viên domain....

iii. Nếu muốn, bây giờ bạn có thể phục hồi các dữ liệu cá nhân của mình với **FullBackup.bkf** đã thực hiện tại bước 1

 **Network Information Security Vietnam.**

www.Nis.com.vn

Securitytraining@Nis.com.vn