Mục lục

GIỚI THIỆU

Sau khi hoàn tất khoá học, học viên có khả năng:

- Hiểu được các khái niệm, lý thuyết về mạng máy tính như: **OSI, TCP/IP**.
- Hiểu được các chức năng và mô hình hoạt động của các thiết bị mạng như: Hub, Switch, Router, Modem, Network Card…
- Sử dụng được các tiện ích mạng thông dụng như: web, mail, ftp…
- Cài đặt và quản trị hệ điều hành **Windows Server 2003**.
- Tổ chức và quản lý người dùng trên môi trường **Windows Server 2003**.
- Tổ chức phân quyền NTFS và quản lý tài nguyên dùng chung trên mạng như: thư mục, máy in, tập tin…
- Quản lý đĩa theo công nghệ **Dynamic Storage**.
- Xây dựng được hệ thống mạng kết nối từ xa (**Remote Access Services**).
- Xây dựng và quản trị được các dịch vụ cơ sở như: DNS, FTP, Web, Mail...
- Chia sẻ kết nối internet thông qua các kỹ thuật như: ICS, NAT, Proxy trên môi trường Windows Server 2003.
- Bảo mật hệ thống mạng thông qua phần mềm ISA 2004.

Với thời lượng 108 tiết LT và 180 tiết TH được phân bổ như sau :

STT	Bài học	Số tiết LT	Số tiết TH
1	Giới thiệu về mạng	4	5
2	Mô hình tham chiếu OSI	4	0
3	Địa chỉ IP	5	5
4	Phương tiện truyền dẫn và các thiết bị mạng	6	10
5	Các kiến trúc và công nghệ mạng LAN	5	10
6	Khảo sát các lớp trong mô hình OSI	6	10
7	Các dịch vụ mạng cơ sở	6	20
8	Giới thiệu và cài đặt Windows Server 2003	4	3
9	Active Directory	4	8
10	Quản lý tài khoản người dùng và nhóm	4	10
11	Chính sách hệ thống	5	6
12	Chính sách nhóm	3	3

13	Quản lý đĩa	3	5
14	Tạo và quản lý thư mục dùng chung	4	10
15	Dịch vụ DHCP	2	3
16	Quản lý in ấn	2	2
17	Dịch vụ truy cập từ xa	5	10
18	Dịch vụ DNS	6	12
19	Dịch vụ FTP	3	6
20	Dịch vụ WEB	5	10
21	Dịch vụ MAIL	8	16
22	Dịch vụ Proxy	8	16
23	Giới thiệu về hai phần mềm Mdaemon và Wingate	6	0
	Tổng số tiết :	108	180

GIÁO TRÌNH LÝ THUYẾT

Sử dụng giáo trình **Mạng Máy Tính** của tác giả Trần Văn Thành, tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

Sử dụng giáo trình **Quản trị Windows Server 2003** của tác giả Trần Văn Thành, tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

Sử dụng giáo trình **Dịch Vụ Mạng Windows 2003** của tác giả Tiêu Đông Nhơn tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

TÀI LIỆU THAM KHẢO

Giáo Trình **Windows Server 2003** của Sybex.

Các giáo trình MCSE của Microsoft.

Các tài liệu trên website http://support.microsoft.com/winsrv2003

Bài 1
GIỚI THIỆU VỀ MẠNG

Tóm tắt

Lý thuyết 4 tiết - Thực hành 5 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức tổng quát về mạng máy tính, các loại mạng, các mô hình xử lý mạng…	I. Các kiến thức cơ sở. II. Các loại mạng máy tính. III. Các mô hình xử lý mạng. IV. Các mô hình ứng dụng mạng. V. Các lợi ích thực tế của mạng	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

Bài 1
GIỚI THIỆU VỀ MẠNG

I. CÁC KIẾN THỨC CƠ SỞ

Mạng máy tính là một nhóm các máy tính, thiết bị ngoại vi được nối kết với nhau thông qua các phương tiện truyền dẫn như cáp, sóng điện từ, tia hồng ngoại... giúp cho các thiết bị này có thể trao đổi dữ liệu với nhau một cách dễ dàng.

Các thành phần cơ bản cấu thành nên mạng máy tính:

- Các loại máy tính: **Palm, Laptop, PC, MainFrame**...
- Các thiết bị giao tiếp: Card mạng (**NIC** hay **Adapter**), **Hub, Switch, Router**...
- Môi trường truyền dẫn: cáp, sóng điện từ, sóng vi ba, tia hồng ngoại...
- Các protocol: **TCP/IP, NetBeui, Apple Talk, IPX/SPX...**
- Các hệ điều hành mạng: **WinNT, Win2000, Win2003, Novell Netware, Unix...**
- Các tài nguyên: file, thư mục
- Các thiết bị ngoại vi: máy in, máy fax, **Modem**, **Scanner**...
- Các ứng dụng mạng: phần mềm quản lý kho bãi, phần mềm bán vé tàu...

Server (máy phục vụ): là máy tính được cài đặt các phần mềm chuyên dụng làm chức năng cung cấp các dịch vụ cho các máy tính khác. Tùy theo dịch vụ mà các máy này cung cấp, người ta chia thành các loại **server** như sau: **File server** (cung cấp các dịch vụ về file và thư mục), **Print server** (cung cấp các dịch vụ về in ấn). Do làm chức năng phục vụ cho các máy tính khác nên cấu hình máy server phải mạnh, thông thường là máy chuyên dụng của các hãng như: Compaq, Intel, IBM...

Client (máy trạm): là máy tính sử dụng các dịch vụ mà các máy server cung cấp. Do xử lý số công việc không lớn nên thông thường các máy này không yêu cầu có cấu hình mạnh.

Peer: là những máy tính vừa đóng vai trò là máy sử dụng vừa là máy cung cấp các dịch vụ. Máy peer thường sử dụng các hệ điều hành như: **DOS, WinNT Workstation, Win9X, Win Me, Win2K Professional, WinXP...**

Media (phương tiện truyền dẫn): là cách thức và vật liệu nối kết các máy lại với nhau.

Shared data (dữ liệu dùng chung): là tập hợp các tập tin, thư mục mà các máy tính chia sẻ để các máy tính khác truy cập sử dụng chúng thông qua mạng.

Resource (tài nguyên): là tập tin, thư mục, máy in, máy Fax, Modem, ổ CDROM và các thành phần khác mà người dùng mạng sử dụng.

User (người dùng): là người sử dụng máy trạm (**client**) để truy xuất các tài nguyên mạng. Thông thường một user sẽ có một username (**account**) và một password. Hệ thống mạng sẽ dựa vào username và password để biết bạn là ai, có quyền vào mạng hay không và có quyền sử dụng những tài nguyên nào trên mạng.

Administrator: là nhà quản trị hệ thống mạng.

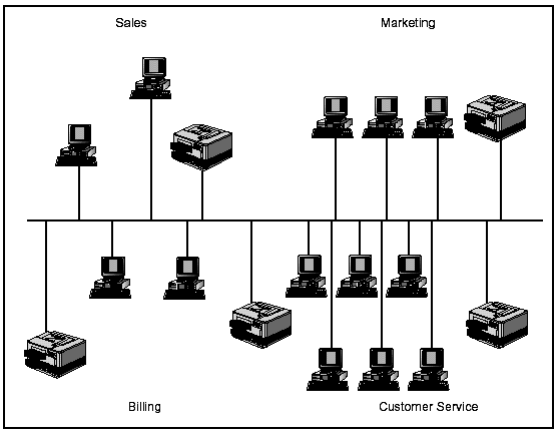
II. CÁC LOẠI MẠNG MÁY TÍNH

II.1. Mạng cục bộ LAN (Local Area Network)

Mạng LAN là một nhóm máy tính và các thiết bị truyền thông mạng được nối kết với nhau trong một khu vực nhỏ như một toà nhà cao ốc, khuôn viên trường đại học, khu giải trí ...

Các mạng LAN thường có đặc điểm sau:

- Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng.
- Kích thước mạng bị giới hạn bởi các thiết bị.
- Chi phí các thiết bị mạng LAN tương đối rẻ.
- Quản trị đơn giản.



Hình 1.1 – Mô hình mạng cục bộ (LAN)

II.2. Mạng đô thị MAN (Metropolitan Area Network)

Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng...) và các phương thức truyền thông khác nhau.

Đặc điểm của mạng MAN:

- Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...
- Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó khăn hơn.
- Chi phí các thiết bị mạng MAN tương đối đắt tiền.

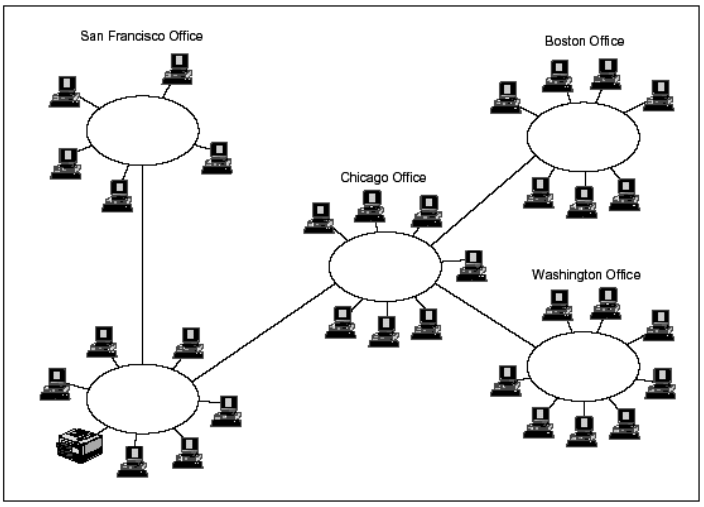
II.3. Mạng diện rộng WAN (Wide Area Network)

Mạng WAN bao phủ vùng địa lý rộng lớn có thể là một quốc gia, một lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu, điển hình là mạng Internet. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (**satellites**), sóng viba (**microwave**), cáp quang, cáp điện

thoại...

Đặc điểm của mạng WAN:

- Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp ...
- Phạm vi hoạt động rộng lớn không giới hạn.
- Do kết nối của nhiều LAN, MAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên thường là có tổ chức quốc tế đứng ra quản trị.
- Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.



Hình 1.2 – Mô hình mạng diện rộng (WAN)

II.4. Mạng Internet

Mạng Internet là trường hợp đặc biệt của mạng WAN, nó cung cấp các dịch vụ toàn cầu như mail, web, chat, ftp và phục vụ miễn phí cho mọi người.

III. CÁC MÔ HÌNH XỬ LÝ MẠNG

Cơ bản có ba loại mô hình xử lý mạng bao gồm:

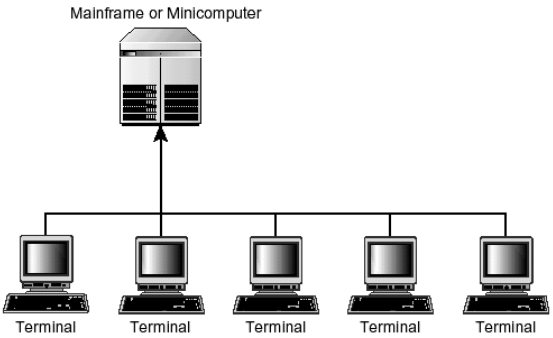
- Mô hình xử lý mạng tập trung
- Mô hình xử lý mạng phân phối
- Mô hình xử lý mạng cộng tác.

III.1. Mô hình xử lý mạng tập trung

Toàn bộ các tiến trình xử lý diễn ra tại máy tính trung tâm. Các máy trạm cuối (**terminals**) được nối mạng với máy tính trung tâm và chỉ hoạt động như những thiết bị nhập xuất dữ liệu cho phép người dùng xem trên màn hình và nhập liệu bàn phím. Các máy trạm đầu cuối không lưu trữ và xử lý dữ liệu. Mô hình xử lý mạng trên có thể triển khai trên hệ thống phần cứng hoặc phần mềm được cài đặt trên server.

Ưu điểm: dữ liệu được bảo mật an toàn, dễ backup và diệt virus. Chi phí cho các thiết bị thấp.

Khuyết điểm: khó đáp ứng được các yêu cầu của nhiều ứng dụng khác nhau, tốc độ truy xuất chậm.



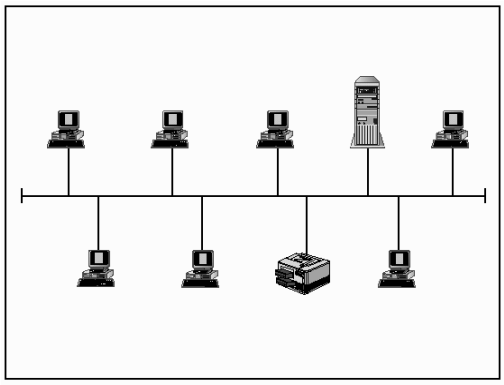
Hình 1.3 – Mô hình xử lý mạng tập trung

III.2. Mô hình xử lý mạng phân phối

Các máy tính có khả năng hoạt động độc lập, các công việc được tách nhỏ và giao cho nhiều máy tính khác nhau thay vì tập trung xử lý trên máy trung tâm. Tuy dữ liệu được xử lý và lưu trữ tại máy cục bộ nhưng các máy tính này được nối mạng với nhau nên chúng có thể trao đổi dữ liệu và dịch vụ.

Ưu điểm: truy xuất nhanh, phần lớn không giới hạn các ứng dụng.

Khuyết điểm: dữ liệu lưu trữ rời rạc khó đồng bộ, backup và rất dễ nhiễm virus.



Hình 1.4 – Mô hình xử lý mạng phân phối

III.3. Mô hình xử lý mạng cộng tác.

Mô hình xử lý cộng tác bao gồm nhiều máy tính có thể hợp tác để thực hiện một công việc. Một máy tính có thể mượn năng lực xử lý bằng cách chạy các chương trình trên các máy nằm trong mạng.

Ưu điểm: rất nhanh và mạnh, có thể dùng để chạy các ứng dụng có các phép toán lớn.

Khuyết điểm: các dữ liệu được lưu trữ trên các vị trí khác nhau nên rất khó đồng bộ và backup, khả năng nhiễm virus rất cao.

IV. CÁC MÔ HÌNH QUẢN LÝ MẠNG

IV.1. Workgroup

Trong mô hình này các máy tính có quyền hạn ngang nhau và không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình. Đồng thời các máy tính cục bộ này cũng tự chứng thực cho người dùng cục bộ.

IV.2. Domain

Ngược lại với mô hình Workgroup, trong mô hình Domain thì việc quản lý và chứng thực người dùng mạng tập trung tại máy tính **Primary Domain Controller**. Các tài nguyên mạng cũng được quản lý tập trung và cấp quyền hạn cho từng người dùng. Lúc đó trong hệ thống có các máy tính chuyên dụng làm nhiệm vụ cung cấp các dịch vụ và quản lý các máy trạm.

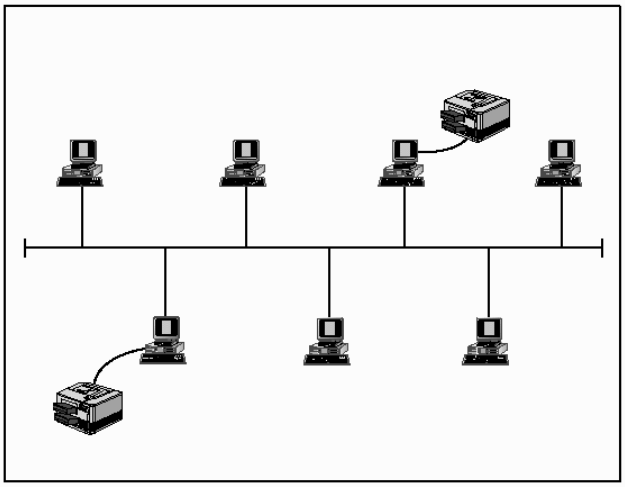
V. CÁC MÔ HÌNH ỨNG DỤNG MẠNG

V.1. Mạng ngang hàng (peer to peer)

Mạng ngang hàng cung cấp việc kết nối cơ bản giữa các máy tính nhưng không có bất kỳ một máy tính nào đóng vai trò phục vụ. Một máy tính trên mạng có thể vừa là **client**, vừa là **server**. Trong môi trường này, người dùng trên từng máy tính chịu trách nhiệm điều hành và chia sẻ các tài nguyên của máy tính mình. Mô hình này chỉ phù hợp với các tổ chức nhỏ, số người giới hạn (thông thường nhỏ hơn 10 người), và không quan tâm đến vấn đề bảo mật. Mạng ngang hàng thường dùng các hệ điều hành sau: **Win95, Windows for workgroup, WinNT Workstation, Win2000 Proffessional, OS/2...**

Ưu điểm: do mô hình mạng ngang hàng đơn giản nên dễ cài đặt, tổ chức và quản trị, chi phí thiết bị cho mô hình này thấp.

Khuyết điểm: không cho phép quản lý tập trung nên dữ liệu phân tán, khả năng bảo mật thấp, rất dễ bị xâm nhập. Các tài nguyên không được sắp xếp nên rất khó định vị và tìm kiếm.



Hình 1.5 – Mô hình ứng dụng mạng ngang hàng (**Peer-to-Peer**)

V.2. Mạng khách chủ (client- server)

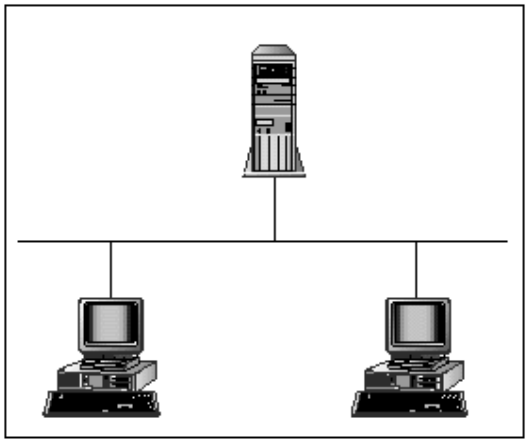
Trong mô hình mạng khách chủ có một hệ thống máy tính cung cấp các tài nguyên và dịch vụ cho cả hệ thống mạng sử dụng gọi là các máy chủ (**server**). Một hệ thống máy tính sử dụng các tài nguyên và dịch vụ này được gọi là máy khách (**client**). Các server thường có cấu hình mạnh (tốc độ xử lý nhanh, kích thước lưu trữ lớn) hoặc là các máy chuyên dụng. Dựa vào chức năng có thể chia thành các loại server như sau:

- **File Server**: phục vụ các yêu cầu hệ thống tập tin trong mạng.
- **Print Server**: phục vụ các yêu cầu in ấn trong mạng.
- **Application Server**: cho phép các ứng dụng chạy trên các server và trả về kết quả cho client.
- **Mail Server**: cung cấp các dịch vụ về gởi nhận e-mail.
- **Web Server**: cung cấp các dịch vụ về web.
- **Database Server**: cung cấp các dịch vụ về lưu trữ, tìm kiếm thông tin.
- **Communication Server**: quản lý các kết nối từ xa.

Hệ điều hành mạng dùng trong mô hình client - server là **WinNT, Novell NetWare, Unix, Win2K...**

Ưu điểm: do các dữ liệu được lưu trữ tập trung nên dễ bảo mật, backup và đồng bộ với nhau. Tài nguyên và dịch vụ được tập trung nên dễ chia sẻ và quản lý và có thể phục vụ cho nhiều người dùng.

Khuyết điểm: các server chuyên dụng rất đắt tiền, phải có nhà quản trị cho hệ thống.



Hình 1.6 – Mô hình ứng dụng mạng khách chủ (**Client-Server**)

VI. CÁC DỊCH VỤ MẠNG

Các dịch vụ mạng phổ biến nhất là:

- Dịch vụ tập tin.
- Dịch vụ in ấn.
- Dịch vụ thông điệp.
- Dịch vụ thư mục.
- Dịch vụ ứng dụng.
- Dịch vụ cơ sở dữ liệu.

- Dịch vụ Web.

VI.1. Dịch vụ tập tin (Files Services)

Dịch vụ tập tin cho phép các máy tính chia sẻ các tập tin, thao tác trên các tập tin chia sẻ này như: lưu trữ, tìm kiếm, di chuyển...

Truyền tập tin: không có mạng, các khả năng truyền tải tập tin giữa các máy tính bị hạn chế. Ví dụ như chúng ta muốn sao chép một tập tin từ máy tính cục bộ ở Việt Nam sang một máy tính server đặt tại Pháp thì chúng ta dùng dịch vụ FTP để sao chép. Dịch vụ này rất phổ biến và đơn giản.

Lưu trữ tập tin: phần lớn các dữ liệu quan trọng trên mạng đều được lưu trữ tập trung theo nhiều cách khác nhau:

Lưu trữ trực tuyến (**online storage**): dữ liệu được lưu trữ trên đĩa cứng nên truy xuất dễ dàng, nhanh chóng, bất kể thời gian. Nhưng phương pháp này có một khuyết điểm là chúng không thể tháo rời để trao đổi hoặc lưu trữ tách rời, đồng thời chi phí lưu trữ một MB dữ liệu tương đối cao.

Lưu trữ ngoại tuyến (**offline storage**): thường áp dụng cho dữ liệu ít khi cần truy xuất (lưu trữ, backup). Các thiết bị phổ biến dùng cho phương pháp này là băng từ, đĩa quang.

Lưu trữ cận tuyến (**near- line storage**): phương pháp này giúp ta khắc phục được tình trạng truy xuất chậm của phương pháp lưu trữ ngoại tuyến nhưng chi phí lại không cao đó là chúng ta dùng thiết bị **Jukebox** để tự động quản lý các băng từ và đĩa quang.

Di trú dữ liệu (**data migration**) là công nghệ tự động dời các dữ liệu ít dùng từ kho lưu trữ trực tuyến sang kho lưu trữ cận tuyến hay ngoại tuyến. Nói cách khác đây là quá trình chuyển các tập tin từ dạng lưu trữ này sang dạng lưu trữ khác.

Đồng bộ hóa việc cập nhật tập tin: dịch vụ này theo dõi các thay đổi khác nhau lên cùng một tập tin để đảm bảo rằng tất cả mọi người dùng đều có bản sao mới nhất của tập tin và tập tin không bị hỏng.

Sao lưu dự phòng (**backup**) là quá trình sao chép và lưu trữ một bản sao dữ liệu từ thiết bị lưu trữ chính. Khi thiết bị lưu trữ chính có sự cố thì chúng ta dùng bản sao này để phục hồi dữ liệu.

VI.2. Dịch vụ in ấn (Print Services)

Dịch vụ in ấn là một ứng dụng mạng điều khiển và quản lý việc truy cập các máy in, máy fax mạng. Các lợi ích của dịch vụ in ấn:

Giảm chi phí cho nhiều người có thể chia nhau dùng chung các thiết bị đắt tiền như máy in màu, máy vẽ, máy in khổ giấy lớn.

Tăng độ linh hoạt vì các máy tính có thể đặt bất kỳ nơi nào, chứ không chỉ đặt cạnh PC của người dùng.

Dùng cơ chế hàng đợi in để ấn định mức độ ưu tiên nội dung nào được in trước, nội dung nào được in sau.

VI.3. Dịch vụ thông điệp (Message Services)

Là dịch vụ cho phép gởi/nhận các thư điện tử (**e-mail**). Công nghệ thư điện tử này rẻ tiền, nhanh chóng, phong phú cho phép đính kèm nhiều loại file khác nhau như: phim ảnh, âm thanh... Ngoài ra dịch vụ này còn cung cấp các ứng dụng khác như: thư thoại (**voice mail**), các ứng dụng nhóm làm việc (**workgroup application**).

VI.4. Dịch vụ thư mục (Directory Services)

Dịch vụ này cho phép tích hợp mọi thông tin về các đối tượng trên mạng thành một cấu trúc thư mục dùng chung nhờ đó mà quá trình quản lý và chia sẻ tài nguyên trở nên hiệu quả hơn.

VI.5. Dịch vụ ứng dụng (Application Services)

Dịch vụ này cung cấp kết quả cho các chương trình ở **client** bằng cách thực hiện các chương trình trên **server**. Dịch vụ này cho phép các ứng dụng huy động năng lực của các máy tính chuyên dụng khác trên mạng.

VI.6. Dịch vụ cơ sở dữ liệu (Database Services)

Dịch vụ cơ sở dữ liệu thực hiện các chức năng sau:

- Bảo mật cơ sở dữ liệu.
- Tối ưu hóa tiến trình thực hiện các tác vụ cơ sở dữ liệu.
- Phục vụ số lượng người dùng lớn, truy cập nhanh vào các cơ sở dữ liệu.
- Phân phối dữ liệu qua nhiều hệ phục vụ CSDL.

VI.7. Dịch vụ Web

Dịch vụ này cho phép tất cả mọi người trên mạng có thể trao đổi các siêu văn bản với nhau. Các siêu bản này có thể chứa hình ảnh, âm thanh giúp các người dùng có thể trao đổi nhanh thông tin và sống động hơn.

VII. CÁC LỢI ÍCH THỰC TẾ CỦA MẠNG.

VII.1. Tiết kiệm được tài nguyên phần cứng.

Khi các máy tính của một phòng ban được nối mạng với nhau thì chúng ta có thể chia sẻ những thiết bị ngoại vi như máy in, máy FAX, ổ đĩa CDROM... Thay vì trang bị cho từng máy PC thì thông qua mạng chúng ta có thể dùng chung các thiết bị này.

Ví dụ 1: trong một phòng máy thực hành có khoảng 30 máy, nếu trang bị cho tất cả các máy trạm có đĩa cứng thì rất phí mà chúng ta lại không tận dụng được hết năng suất của các đĩa cứng đó. Giải pháp tập trung tất cả các ứng dụng vào server và dùng công nghệ mạng bootrom để chạy các máy trạm sẽ làm giảm chi phí phần cứng đồng thời tiện dụng cho công tác quản trị phòng máy hạn chế được tình trạng các học viên vô tình làm hỏng các máy trạm.

Ví dụ 2: Một công ty muốn rằng tất cả các phòng ban đều được sử dụng Internet thông qua modem và đường điện thoại. Nếu chúng ta trang bị cho mỗi phòng ban 1 modem và 1 đường điện thoại thì không khả thi vì vậy chúng ta phải tận dụng cơ sở hạ tầng mạng để chia sẻ 1 modem và đường điện thoại cho cả công ty đều có thể truy cập Internet.

VII.2. Trao đổi dữ liệu trở nên dễ dàng hơn.

Theo phương pháp truyền thống muốn chép dữ liệu giữa hai máy tính chúng ta dùng đĩa mềm hoặc dùng cáp **link** để nối hai máy lại với nhau sau đó chép dữ liệu. Chúng ta thấy rằng hai giải pháp trên sẽ không thực tế nếu một máy đặt tại tầng trệt và một máy đặt tại tầng 5 trong một tòa nhà. Việc trao đổi dữ liệu giữa các máy tính ngày càng nhiều hơn, đa dạng hơn, khoảng cách giữa các phòng ban trong công ty ngày càng xa hơn nên việc trao đổi dữ liệu theo phương thức truyền thống không còn được áp dụng nữa, thay vào đó là các máy tính này được nối với nhau qua công nghệ mạng.

VII.3. Chia sẻ ứng dụng.

Các ứng dụng thay vì trên từng máy trạm chúng ta sẽ cài trên một máy server và các máy trạm dùng chung ứng dụng đó trên **server**. Lúc đó ta tiết kiệm được chi phí bản quyền và chi phí cài đặt, quản trị.

VII.4. Tập trung dữ liệu, bảo mật và backup tốt.

Đối với các công ty lớn dữ liệu lưu trữ trên các máy trạm rời rạc dễ dẫn đến tình trạng hư hỏng thông tin và không được bảo mật. Nếu các dữ liệu này được tập trung về server để tiện việc bảo mật, backup và quét virus.

VII.5. Sử dụng các phần mềm ứng dụng trên mạng.

Nhờ các công nghệ mạng mà các phần mềm ứng dụng phát triển mạnh và được áp dụng vào nhiều lĩnh vực như hàng không (phần mềm bán vé máy bay tại các chi nhánh), đường sắt (phần mềm theo dõi đăng ký vé và bán vé tàu), cấp thoát nước (phần mềm quản lý công ty cấp thoát nước thành phố)...

VII.6. Sử dụng các dịch vụ Internet.

Ngày nay Internet rất phát triển, tất cả mọi người trên thế giới đều có thể trao đổi E-mail với nhau một cách dễ dàng hoặc có thể trò chuyện với nhau mà chi phí rất thấp so với phí viễn thông. Đồng thời các công ty cũng dùng công nghệ Web để quảng cáo sản phẩm, mua bán hàng hóa qua mạng (thương mại điện tử) ...

Dựa trên cơ sở hạ tầng mạng chúng ta có thể xây dựng các hệ thống ứng dụng lớn như chính phủ điện tử, thương mại điện tử, điện thoại Internet nhằm giảm chi phí và tăng khả năng phục vụ ngày càng tốt hơn cho con người.

Bài 2
MÔ HÌNH THAM CHIẾU OSI

Tóm tắt

Lý thuyết 4 tiết - Thực hành 0 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về giao thức, mô hình OSI, TCP/IP và quá trình xử lý, vận chuyển của một gói tin …	I. Mô hình OSI. II. Quá trình xử lý và vận chuyển của một gói dữ liệu. III. Mô hình tham chiếu TCP/IP.	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

I. MÔ HÌNH OSI.

I.1. Khái niệm giao thức (protocol).

Là quy tắc giao tiếp (tiêu chuẩn giao tiếp) giữa hai hệ thống giúp chúng hiểu và trao đổi dữ liệu được với nhau.

Ví dụ: **Internetwork Packet Exchange** (**IPX**), **Transmission control protocol/ Internetwork Protocol** (**TCP/IP**), **NetBIOS Extended User Interface** (**NetBEUI**)…

I.2. Các tổ chức định chuẩn.

ITU (**International Telecommunication Union**): Hiệp hội Viễn thông quốc tế.

IEEE (**Institute of Electrical and Electronic Engineers**): Viện các kĩ sư điện và điện tử.

ISO (**International Standardization Organization**): Tổ chức Tiêu chuẩn quốc tế, trụ sở tại Geneve, Thụy Sĩ. Vào năm 1977, ISO được giao trách nhiệm thiết kế một chuẩn truyền thông dựa trên lí thuyết về kiến trúc các hệ thống mở làm cơ sở để thiết kế mạng máy tính. Mô hình này có tên là OSI (**Open System Interconnection** - tương kết các hệ thống mở)

I.3. Mô hình OSI.

Mô hình OSI (**Open System Interconnection**): là mô hình được tổ chức ISO đề xuất từ 1977 và công bố lần đầu vào 1984. Để các máy tính và các thiết bị mạng có thể truyền thông với nhau phải có những qui tắc giao tiếp được các bên chấp nhận. Mô hình OSI là một khuôn mẫu giúp chúng ta hiểu dữ liệu đi xuyên qua mạng như thế nào đồng thời cũng giúp chúng ta hiểu được các chức năng mạng diễn ra tại mỗi lớp.

Trong mô hình OSI có bảy lớp, mỗi lớp mô tả một phần chức năng độc lập. Sự tách lớp của mô hình này mang lại những lợi ích sau:

- Chia hoạt động thông tin mạng thành những phần nhỏ hơn, đơn giản hơn giúp chúng ta dễ khảo sát và tìm hiểu hơn.
- Chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà cung cấp sản phẩm.
- Ngăn chặn được tình trạng sự thay đổi của một lớp làm ảnh hưởng đến các lớp khác, như vậy giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.

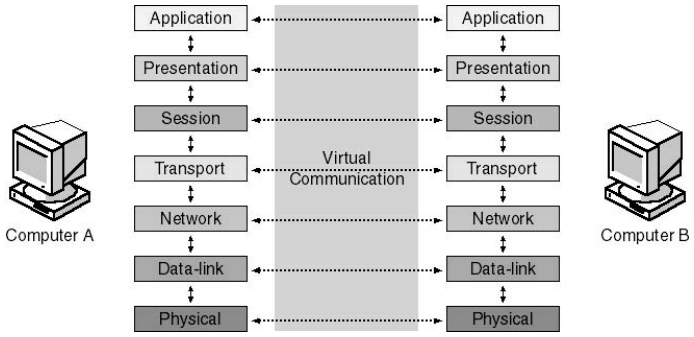
Mô hình tham chiếu OSI định nghĩa các qui tắc cho các nội dung sau:

- Cách thức các thiết bị giao tiếp và truyền thông được với nhau.
- Các phương pháp để các thiết bị trên mạng khi nào thì được truyền dữ liệu, khi nào thì không được.
- Các phương pháp để đảm bảo truyền đúng dữ liệu và đúng bên nhận.
- Cách thức vận tải, truyền, sắp xếp và kết nối với nhau.
- Cách thức đảm bảo các thiết bị mạng duy trì tốc độ truyền dữ liệu thích hợp.
- Cách biểu diễn một bit thiết bị truyền dẫn.

Mô hình tham chiếu OSI được chia thành bảy lớp với các chức năng sau:

- **Application Layer** (lớp ứng dụng): giao diện giữa ứng dụng và mạng.

- **Presentation Layer** (lớp trình bày): thoả thuận khuôn dạng trao đổi dữ liệu.
- **Session Layer** (lớp phiên): cho phép người dùng thiết lập các kết nối.
- **Transport Layer** (lớp vận chuyển): đảm bảo truyền thông giữa hai hệ thống.
- **Network Layer** (lớp mạng): định hướng dữ liệu truyền trong môi trường liên mạng.
- **Data link Layer** (lớp liên kết dữ liệu): xác định việc truy xuất đến các thiết bị.
- **Physical Layer** (lớp vật lý): chuyển đổi dữ liệu thành các bit và truyền đi.



Hình 2.1 – Mô hình tham chiếu OSI

I.4. Chức năng của các lớp trong mô hình tham chiếu OSI

Lớp ứng dụng (**Application Layer**): là giao diện giữa các chương trình ứng dụng của người dùng và mạng. Lớp **Application** xử lý truy nhập mạng chung, kiểm soát luồng và phục hồi lỗi. Lớp này không cung cấp các dịch vụ cho lớp nào mà nó cung cấp dịch vụ cho các ứng dụng như: truyền file, gởi nhận E-mail, Telnet, HTTP, FTP, SMTP…

Lớp trình bày (**Presentation Layer**): lớp này chịu trách nhiệm thương lượng và xác lập dạng thức dữ liệu được trao đổi. Nó đảm bảo thông tin mà lớp ứng dụng của một hệ thống đầu cuối gởi đi, lớp ứng dụng của hệ thống khác có thể đọc được. Lớp trình bày thông dịch giữa nhiều dạng dữ liệu khác nhau thông qua một dạng chung, đồng thời nó cũng nén và giải nén dữ liệu. Thứ tự byte, bit bên gởi và bên nhận qui ước qui tắc gởi nhận một chuỗi byte, bit từ trái qua phải hay từ phải qua trái. Nếu hai bên không thống nhất thì sẽ có sự chuyển đổi thứ tự các byte bit vào trước hoặc sau khi truyền. Lớp **presentation** cũng quản lý các cấp độ nén dữ liệu nhằm giảm số bit cần truyền. Ví dụ: **JPEG, ASCCI, EBCDIC....**

Lớp phiên (**Session Layer**): lớp này có chức năng thiết lập, quản lý, và kết thúc các phiên thông tin giữa hai thiết bị truyền nhận. Lớp phiên cung cấp các dịch vụ cho lớp trình bày. Lớp **Session** cung cấp sự đồng bộ hóa giữa các tác vụ người dùng bằng cách đặt những điểm kiểm tra vào luồng dữ liệu. Bằng cách này, nếu mạng không hoạt động thì chỉ có dữ liệu truyền sau điểm kiểm tra cuối cùng mới phải truyền lại. Lớp này cũng thi hành kiểm soát hội thoại giữa các quá trình giao tiếp, điều chỉnh bên nào truyền, khi nào, trong bao lâu. Ví dụ như: **RPC, NFS**,... Lớp này kết nối theo ba cách: **Haft-duplex, Simplex, Full-duplex.**

Lớp vận chuyển (**Transport Layer**): lớp vận chuyển phân đoạn dữ liệu từ hệ thống máy truyền và tái thiết lập dữ liệu vào một luồng dữ liệu tại hệ thống máy nhận đảm bảo rằng việc bàn giao các thông điệp giữa các thiết bị đáng tin cậy. Dữ liệu tại lớp này gọi là **segment**. Lớp này thiết lập, duy trì và kết

thúc các mạch ảo đảm bảo cung cấp các dịch vụ sau:

- Xếp thứ tự các phân đoạn: khi một thông điệp lớn được tách thành nhiều phân đoạn nhỏ để ban giao, lớp vận chuyển sẽ sắp xếp thứ tự các phân đoạn trước khi ráp nối các phân đoạn thành thông điệp ban đầu.
- Kiểm soát lỗi: khi có phân đoạn bị thất bại, sai hoặc trùng lắp, lớp vận chuyển sẽ yêu cầu truyền lại.
- Kiểm soát luồng: lớp vận chuyển dùng các tín hiệu báo nhận để xác nhận. Bên gửi sẽ không truyền đi phân đoạn dữ liệu kế tiếp nếu bên nhận chưa gởi tín hiệu xác nhận rằng đã nhận được phân đoạn dữ liệu trước đó đầy đủ.

Lớp mạng (**Network Layer**): lớp mạng chịu trách nhiệm lập địa chỉ các thông điệp, diễn dịch địa chỉ và tên logic thành địa chỉ vật lý đồng thời nó cũng chịu trách nhiệm gởi packet từ mạng nguồn đến mạng đích. Lớp này quyết định đường đi từ máy tính nguồn đến máy tính đích. Nó quyết định dữ liệu sẽ truyền trên đường nào dựa vào tình trạng, ưu tiên dịch vụ và các yếu tố khác. Nó cũng quản lý lưu lượng trên mạng chẳng hạn như chuyển đổi gói, định tuyến, và kiểm soát sự tắc nghẽn dữ liệu. Nếu bộ thích ứng mạng trên bộ định tuyến (router) không thể truyền đủ đoạn dữ liệu mà máy tính nguồn gởi đi, lớp **Network** trên bộ định tuyến sẽ chia dữ liệu thành những đơn vị nhỏ hơn, nói cách khác, nếu máy tính nguồn gởi đi các gói tin có kích thước là 20Kb, trong khi **Router** chỉ cho phép các gói tin có kích thước là 10Kb đi qua, thì lúc đó lớp **Network** của **Router** sẽ chia gói tin ra làm 2, mỗi gói tin có kích thước là 10Kb. Ở đầu nhận, lớp **Network** ráp nối lại dữ liệu. Ví dụ: một số giao thức lớp này: IP, IPX,... Dữ liệu ở lớp này gọi packet hoặc datagram.

Lớp liên kết dữ liệu (**Data link Layer**): cung cấp khả năng chuyển dữ liệu tin cậy xuyên qua một liên kết vật lý. Lớp này liên quan đến:

- Địa chỉ vật lý.
- Mô hình mạng.
- Cơ chế truy cập đường truyền.
- Thông báo lỗi.
- Thứ tự phân phối frame.
- Điều khiển dòng.

Tại lớp **data link**, các bít đến từ lớp vật lý được chuyển thành các frame dữ liệu bằng cách dùng một số nghi thức tại lớp này. Lớp **data link** được chia thành hai lớp con:

- Lớp con LLC (**logical link control**).
- Lớp con MAC (**media access control**).

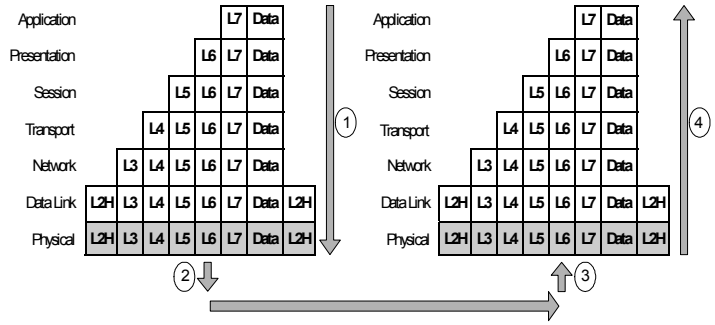
Lớp con LLC là phần trên so với các giao thức truy cập đường truyền khác, nó cung cấp sự mềm dẻo về giao tiếp. Bởi vì lớp con LLC hoạt động độc lập với các giao thức truy cập đường truyền, cho nên các giao thức lớp trên hơn (ví dụ như IP ở lớp mạng) có thể hoạt động mà không phụ thuộc vào loại phương tiện LAN. Lớp con LLC có thể lệ thuộc vào các lớp thấp hơn trong việc cung cấp truy cập đường truyền.

Lớp con MAC cung cấp tính thứ tự truy cập vào môi trường LAN. Khi nhiều trạm cùng truy cập chia sẻ môi trường truyền, để định danh mỗi trạm, lớp cho MAC định nghĩa một trường địa chỉ phần cứng, gọi là địa chỉ MAC address. Địa chỉ MAC là một con số đơn nhất đối với mỗi giao tiếp LAN (card mạng).

Lớp vật lý (**Physical Layer**): định nghĩa các qui cách về điện, cơ, thủ tục và các đặc tả chức năng để kích hoạt, duy trì và dừng một liên kết vật lý giữa các hệ thống đầu cuối. Một số các đặc điểm trong lớp vật lý này bao gồm:

- Mức điện thế.
- Khoảng thời gian thay đổi điện thế.
- Tốc độ dữ liệu vật lý.
- Khoảng đường truyền tối đa.
- Các đầu nối vật lý.

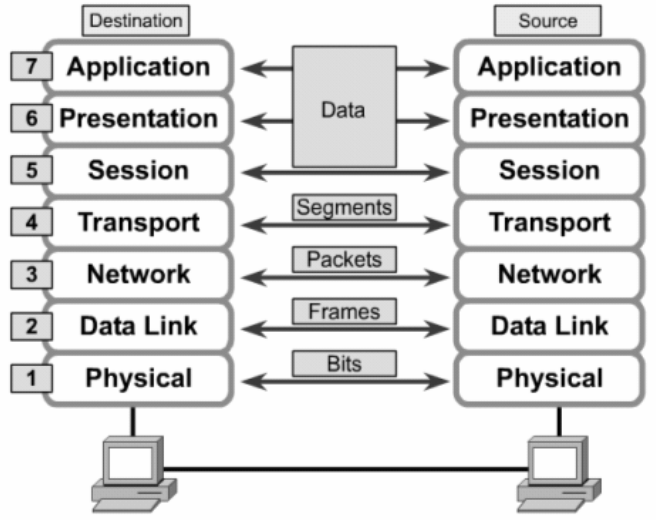
II. QUÁ TRÌNH XỬ LÝ VÀ VẬN CHUYỂN CỦA MỘT GÓI DỮ LIỆU.



Hình 2.2 – Quá trình xử lý và vận chuyển của gói tin

II.1. Quá trình đóng gói dữ liệu (tại máy gửi)

Đóng gói dữ liệu là quá trình đặt dữ liệu nhận được vào sau **header** (và trước **trailer**) trên mỗi lớp. Lớp **Physical** không đóng gói dữ liệu vì nó không dùng **header** và **trailer**. Việc đóng gói dữ liệu không nhất thiết phải xảy ra trong mỗi lần truyền dữ liệu của trình ứng dụng. Các lớp 5, 6, 7 sử dụng **header** trong quá trình khởi động, nhưng trong phần lớn các lần truyền thì không có **header** của lớp 5, 6, 7 lý do là không có thông tin mới để trao đổi.



Hình 2.3 – Tên gọi dữ liệu ở các tầng trong mô hình OSI

Các dữ liệu tại máy gửi được xử lý theo trình tự như sau:

- Người dùng thông qua lớp **Application** để đưa các thông tin vào máy tính. Các thông tin này có nhiều dạng khác nhau như: hình ảnh, âm thanh, văn bản…
- Tiếp theo các thông tin đó được chuyển xuống lớp **Presentation** để chuyển thành dạng chung, rồi mã hoá và nén dữ liệu.
- Tiếp đó dữ liệu được chuyển xuống lớp **Session** để bổ sung các thông tin về phiên giao dịch này.
- Dữ liệu tiếp tục được chuyển xuống lớp **Transport**, tại lớp này dữ liệu được cắt ra thành nhiều **Segment** và bổ sung thêm các thông tin về phương thức vận chuyển dữ liệu để đảm bảo độ tin cậy khi truyền.
- Dữ liệu tiếp tục được chuyển xuống lớp **Network**, tại lớp này mỗi **Segment** được cắt ra thành nhiều **Packet** và bổ sung thêm các thông tin định tuyến.
- Tiếp đó dữ liệu được chuyển xuống lớp **Data Link**, tại lớp này mỗi **Packet** sẽ được cắt ra thành nhiều **Frame** và bổ sung thêm các thông tin kiểm tra gói tin (để kiểm tra ở nơi nhận).
- Cuối cùng, mỗi **Frame** sẽ được tầng Vật Lý chuyển thành một chuỗi các bit, và được đẩy lên các phương tiện truyền dẫn để truyền đến các thiết bị khác.

II.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.

Bước 1: Trình ứng dụng (trên máy gửi) tạo ra dữ liệu và các chương trình phần cứng, phần mềm cài đặt mỗi lớp sẽ bổ sung vào header và trailer (quá trình đóng gói dữ liệu tại máy gửi).

Bước 2: Lớp **Physical** (trên máy gửi) phát sinh tín hiệu lên môi trường truyền tải để truyền dữ liệu.

Bước 3: Lớp **Physical** (trên máy nhận) nhận dữ liệu.

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ **header** và **trailer** và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận).

Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng **MAC Table** của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng **MAC Table** để lớp **Datalink** sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gởi gói tin đi (giao thức ARP sẽ được nói thêm trong chương 6).
- Nếu khác địa chỉ mạng thì máy gửi sẽ kiểm tra xem máy có được khai báo **Default Gateway** hay không.
    + Nếu có khai báo **Default Gateway** thì máy gửi sẽ gởi gói tin thông qua **Default Gateway**.
    + Nếu không có khai báo **Default Gateway** thì máy gởi sẽ loại bỏ gói tin và thông báo "**Destination host Unreachable**"

II.3. Chi tiết quá trình xử lý tại máy nhận

Bước 1: Lớp **Physical** kiểm tra quá trình đồng bộ bit và đặt chuỗi bit nhận được vào vùng đệm. Sau đó thông báo cho lớp **Data Link** dữ liệu đã được nhận.

Bước 2: Lớp **Data Link** kiểm lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ. Sau đó kiểm tra địa chỉ lớp **Data Link** (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

Bước 3: Địa chỉ lớp **Network** được kiểm tra xem có phải là địa chỉ máy nhận hay không (địa chỉ IP) ? Nếu đúng thì dữ liệu được chuyển lên cho lớp **Transport** xử lý.

Bước 4: Nếu giao thức lớp **Transport** có hỗ trợ việc phục hồi lỗi thì số định danh phân đoạn được xử lý. Các thông tin **ACK, NAK** (gói tin **ACK, NAK** dùng để phản hồi về việc các gói tin đã được gởi đến máy nhận chưa) cũng được xử lý ở lớp này. Sau quá trình phục hồi lỗi và sắp thứ tự các phân đoạn, dữ liệu được đưa lên lớp **Session**.

Bước 5: Lớp **Session** đảm bảo một chuỗi các thông điệp đã trọn vẹn. Sau khi các luồng đã hoàn tất, lớp Session chuyển dữ liệu sau header lớp 5 lên cho lớp **Presentation** xử lý.

Bước 6: Dữ liệu sẽ được lớp **Presentation** xử lý bằng cách chuyển đổi dạng thức dữ liệu. Sau đó kết quả chuyển lên cho lớp **Application**.

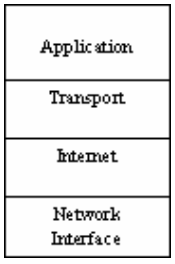
Bước 7: Lớp **Application** xử lý **header** cuối cùng. **Header** này chứa các tham số thoả thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

III. MÔ HÌNH THAM CHIẾU TCP/IP.

III.1. Vai trò của mô hình tham chiếu TCP/IP.

Các bộ phận, văn phòng của Chính phủ Hoa Kỳ đã nhận thức được sự quan trọng và tiềm năng của kĩ thuật Internet từ nhiều năm trước, cũng như đã cung cấp tài chánh cho việc nghiên cứu, để thực sự có được một mạng Internet toàn cầu. Sự hình thành kĩ thuật Internet là kết quả nghiên cứu dưới sự tài trợ của **Defense/Advanced Research Projects Agency** (**ARPA/DARPA**). Kĩ thuật **ARPA** bao gồm một tập hợp của các chuẩn mạng, đặc tả chi tiết cách thức mà các máy tính thông tin liên lạc với nhau, cũng như các quy ước cho các mạng **interconnecting** và định tuyến giao thông. Tên chính thức là **TCP/IP Internet Protocol Suite** và thường được gọi là **TCP/IP**, có thể dùng để thông tin liên lạc qua tập hợp bất kỳ các mạng **interconnected**. Nó có thể dùng để liên kết mạng trong một công ty, không nhất thiết phải nối kết với các mạng khác bên ngoài.

III.2. Các lớp của mô hình tham chiếu TCP/IP.

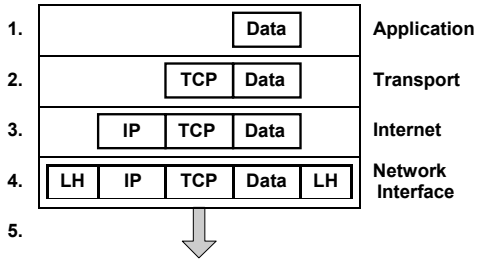


Hình 2.4 – Mô hình tham chiếu TCP/IP

Mô hình tham chiếu TCP/IP tương tự như kiến trúc OSI, sau đây là một số tính chất của các lớp trong mô hình tham chiếu TCP/IP:

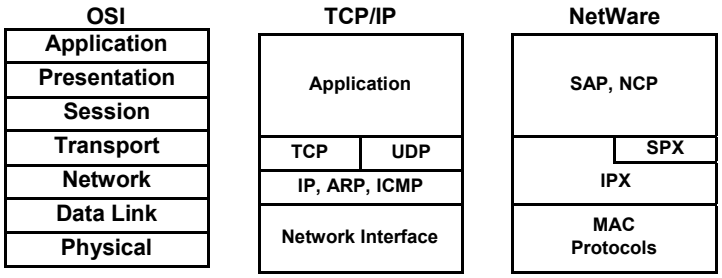
- Lớp **Application**: quản lý các giao thức, như hỗ trợ việc trình bày, mã hóa, và quản lý cuộc gọi. Lớp **Application** cũng hỗ trợ nhiều ứng dụng, như: FTP (**File Transfer Protocol**), HTTP (**Hypertext Transfer Protocol**), SMTP (**Simple Mail Transfer Protocol**), DNS (**Domain Name System**), TFTP (**Trivial File Transfer Protocol**).
- Lớp **Transport**: đảm nhiệm việc vận chuyển từ nguồn đến đích. Tầng **Transport** đảm nhiệm việc truyền dữ liệu thông qua hai nghi thức: TCP (**Transmission Control Protocol**) và UDP (**User Datagram Protocol**).
- Lớp **Internet**: đảm nhiệm việc chọn lựa đường đi tốt nhất cho các gói tin. Nghi thức được sử dụng chính ở tầng này là nghi thức IP (**Internet Protocol**).
- Lớp **Network Interface**: có tính chất tương tự như hai lớp **Data Link** và **Physical** của kiến trúc OSI.

III.3. Các bước đóng gói dữ liệu trong mô hình TCP/IP.



Hình 2.5 – Các bước đóng gói trong mô hình TCP/IP

III.4. So sánh mô hình OSI và TCP/IP.



Hình 2.6 – So sánh mô hình OSI và mô hình TCP/IP

Các điểm giống nhau:

- Cả hai đều có kiến trúc phân lớp.
- Đều có lớp **Application**, mặc dù các dịch vụ ở mỗi lớp khác nhau.
- Đều có các lớp **Transport** và **Network**.
- Sử dụng kĩ thuật chuyển packet (**packet-switched**).
- Các nhà quản trị mạng chuyên nghiệp cần phải biết rõ hai mô hình trên.

Các điểm khác nhau:

- Mô hình TCP/IP kết hợp lớp **Presentation** và lớp **Session** vào trong lớp **Application**.

- Mô hình TCP/IP kết hợp lớp **Data Link** và lớp **Physical** vào trong một lớp.

- Mô hình TCP/IP đơn giản hơn bởi vì có ít lớp hơn.
- Nghi thức TCP/IP được chuẩn hóa và được sử dụng phổ biến trên toàn thế giới.

Tóm tắt

Lý thuyết 5 tiết - Thực hành 5 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về cấu trúc của một địa chỉ IP, các lớp địa chỉ, kỹ thuật chia mạng con, kỹ thuật NAT…	I. Tổng quan về địa chỉ IP. II. Giới thiệu các lớp địa chỉ. III. Các ví dụ khi tính toán trên địa chỉ mạng.	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

I. TỔNG QUAN VỀ ĐỊA CHỈ IP

Là địa chỉ có cấu trúc, được chia làm hai hoặc ba phần là: **network_id&host_id** hoặc **network_id&subnet_id&host_id**.

Là một con số có kích thước 32 bit. Khi trình bày, người ta chia con số 32 bit này thành bốn phần, mỗi phần có kích thước 8 bit, gọi là **octet** hoặc **byte**. Có các cách trình bày sau:

- Ký pháp thập phân có dấu chấm (**dotted-decimal notation**). Ví dụ: 172.16.30.56.
- Ký pháp nhị phân. Ví dụ: 10101100 00010000 00011110 00111000.
- Ký pháp thập lục phân. Ví dụ: AC 10 1E 38.

Không gian địa chỉ IP (gồm 2^{32} địa chỉ) được chia thành nhiều lớp (class) để dễ quản lý. Đó là các lớp: A, B, C, D và E; trong đó các lớp A, B và C được triển khai để đặt cho các host trên mạng **Internet**; lớp D dùng cho các nhóm **multicast**; còn lớp E phục vụ cho mục đích nghiên cứu.

Địa chỉ IP còn được gọi là địa chỉ **logical**, trong khi địa chỉ **MAC** còn gọi là địa chỉ vật lý (hay địa chỉ **physical**).

II. MỘT SỐ KHÁI NIỆM VÀ THUẬT NGỮ LIÊN QUAN.

Network_id: là giá trị để xác định đường mạng. Trong số 32 bit dùng địa chỉ IP, sẽ có một số bit đầu tiên dùng để xác định network_id. Giá trị của các bit này được dùng để xác định đường mạng.

Host_id: là giá trị để xác định host trong đường mạng. Trong số 32 bit dùng làm địa chỉ IP, sẽ có một số bit cuối cùng dùng để xác định host_id. Host_id chính là giá trị của các bit này.

Địa chỉ **host**: là địa chỉ IP, có thể dùng để đặt cho các interface của các host. Hai host nằm thuộc cùng một mạng sẽ có **network_id** giống nhau và **host_id** khác nhau.

Mạng (**network**): một nhóm nhiều host kết nối trực tiếp với nhau. Giữa hai host bất kỳ không bị phân cách bởi một thiết bị layer 3. Giữa mạng này với mạng khác phải kết nối với nhau bằng thiết bị layer 3.

Địa chỉ mạng (**network address**): là địa chỉ IP dùng để đặt cho các mạng. Địa chỉ này không thể dùng để đặt cho một **interface**. Phần **host_id** của địa chỉ chỉ chứa các bit 0. Ví dụ 172.29.0.0 là một địa chỉ mạng.

Mạng con (**subnet network**): là mạng có được khi một địa chỉ mạng (thuộc lớp A, B, C) được phân chia nhỏ hơn (để tận dụng số địa chỉ mạng được cấp phát). Địa chỉ mạng con được xác định dựa vào địa chỉ IP và mặt nạ mạng con (**subnet mask**) đi kèm (sẽ đề cập rõ hơn ở phần sau).

Địa chỉ **broadcast**: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần **host_id** chỉ chứa các bit 1. Địa chỉ này cũng không thể dùng để đặt cho một host được. Ví dụ 172.29.255.255 là một địa chỉ **broadcast**.

Các phép toán làm việc trên bit:

Phép AND			Phép OR		
A	B	A and B	A	B	A or B
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	0	1	1
0	0	0	0	0	0

Ví dụ sau minh hoạ phép AND giữa địa chỉ 172.29.14.10 và mask 255.255.0.0

172.29.14.10 = 10101100000111010000111000001010AND

255.255.0.0 = 11111111111111110000000000000000

172.29.0.0 = 10101100000111010000000000000000

Mặt nạ mạng (**network mask**): là một con số dài 32 bit, là phương tiện giúp máy xác định được địa chỉ mạng của một địa chỉ IP (bằng cách AND giữa địa chỉ IP với mặt nạ mạng) để phục vụ cho công việc routing. Mặt nạ mạng cũng cho biết số bit nằm trong phần **host_id**. Được xây dựng theo cách: bật các bit tương ứng với phần **network_id** (chuyển thành bit 1) và tắt các bit tương ứng với phần **host_id** (chuyển thành bit 0).

Mặt nạ mặc định của lớp A: sử dụng cho các địa chỉ lớp A khi không chia mạng con, mặt nạ có giá trị 255.0.0.0.

Mặt nạ mặc định của lớp B: sử dụng cho các địa chỉ lớp B khi không chia mạng con, mặt nạ có giá trị 255.255.0.0.

Mặt nạ mặc định của lớp C: sử dụng cho các địa chỉ lớp C khi không chia mạng con, mặt nạ có giá trị 255.255.255.0.

III. GIỚI THIỆU CÁC LỚP ĐỊA CHỈ.

III.1. Lớp A.

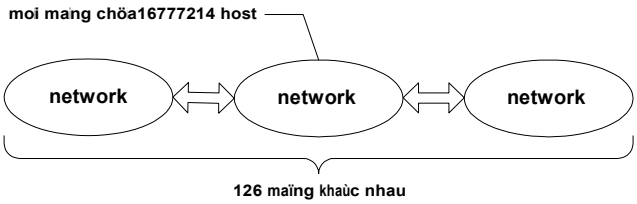
Dành một byte cho phần **network_id** và ba byte cho phần **host_id**.

network_id		host_id	

Để nhận diện ra lớp A, bit đầu tiên của byte đầu tiên phải là bit 0. Dưới dạng nhị phân, byte này có dạng 0xxxxxxx. Vì vậy, những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (00000000) đến 127 (01111111) sẽ thuộc lớp A. Ví dụ địa chỉ 50.14.32.8 là một địa chỉ lớp A (50 < 127).

Byte đầu tiên này cũng chính là **network_id**, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại bảy bit để đánh thứ tự các mạng, ta được 128 (2^7) mạng lớp A khác nhau. Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 (2^7-2) địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

Phần host_id chiếm 24 bit, tức có thể đặt địa chỉ cho 16.777.216 (2^{24}) host khác nhau trong mỗi mạng. Bỏ đi một địa chỉ mạng (phần **host_id** chứa toàn các bit 0) và một địa chỉ **broadcast** (phần **host_id** chứa toàn các bit 1) như vậy có tất cả 16.777.214 (2^{24}-2) host khác nhau trong mỗi mạng lớp A. Ví dụ, đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.



Hình 3.1 – Mô tả các mạng lớp A kết nối với nhau

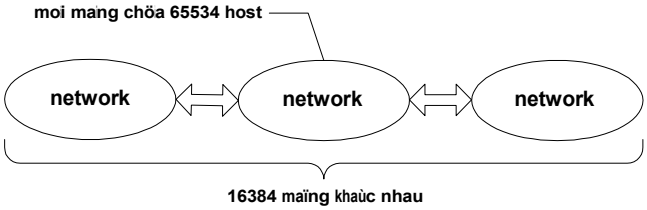
III.2. Lớp B.

Dành hai byte cho mỗi phần **network_id** và **host_id**.

Dấu hiệu để nhận dạng địa chỉ lớp B là byte đầu tiên luôn bắt đầu bằng hai bit 10. Dưới dạng nhị phân, octet có dạng 10xxxxxx. Vì vậy những địa chỉ nằm trong khoảng từ 128 (10000000) đến 191 (10111111) sẽ thuộc về lớp B. Ví dụ 172.29.10.1 là một địa chỉ lớp B (128 < 172 < 191).

Phần **network_id** chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16.384 (2^{14}) mạng khác nhau (128.0.0.0 đến 191.255.0.0)

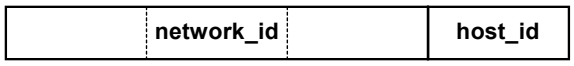
Phần **host_id** dài 16 bit hay có 65536 (2^{16}) giá trị khác nhau. Trừ 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B. Ví dụ, đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.



Hình 3.2 – Mô tả các mạng lớp B kết nối với nhau

III.3. Lớp C.

Dành ba byte cho phần **network_id** và một byte cho phần **host_id**.



Byte đầu tiên luôn bắt đầu bằng ba bit 110 và dạng nhị phân của octet này là 110xxxxx. Như vậy những địa chỉ nằm trong khoảng từ 192 (**110**00000) đến 223 (**110**11111) sẽ thuộc về lớp C. Ví dụ một địa chỉ lớp C là 203.162.41.235 (192 < 203 < 223).

Phần **network_id** dùng ba byte hay 24 bit, trừ đi 3 bit làm ID của lớp, còn lại 21 bit hay 2.097.152 (2^{21})

địa chỉ mạng (từ **192.0.0**.0 đến **223.255.255**.0).

Phần **host_id** dài một byte cho 256 (2^8) giá trị khác nhau. Trừ đi hai trường hợp đặc biệt ta còn 254 host khác nhau trong một mạng lớp C. Ví dụ, đối với mạng 203.162.41.0, các địa chỉ host hợp lệ là từ 203.162.41.1 đến 203.162.41.254.

III.4. Lớp D và E.

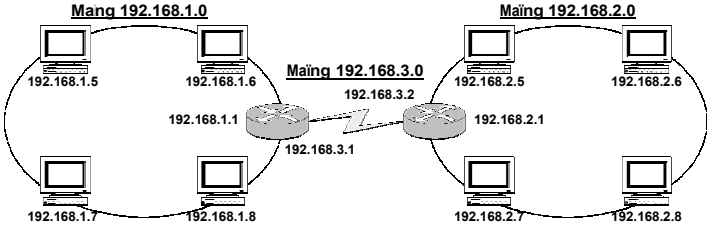
Các địa chỉ có byte đầu tiên nằm trong khoảng 224 đến 255 là các địa chỉ thuộc lớp D hoặc E. Do các lớp này không phục vụ cho việc đánh địa chỉ các host nên không trình bày ở đây.

III.5. Bảng tổng kết.

	Lớp A	Lớp B	Lớp C
Giá trị của byte đầu tiên	0 – 127	128 – 191	192 – 223
Số byte phần Network_id	1	2	3
Số byte phần Host_id	3	2	1
Network mask	255.0.0.0	255.255.0.0	255.255.255.0
Broadcast	XX.255.255.255	XX.XX.255.255	XX.XX.XX.255
Network Address	XX.0.0.0	XX.XX.0.0	XX.XX.XX.0
Số đường mạng	128	16.384	2.097.152
Số host trên mỗi đường mạng	16.777.214	65.534	254

* Ghi chú: XX là số bất kỳ trong miền cho phép.

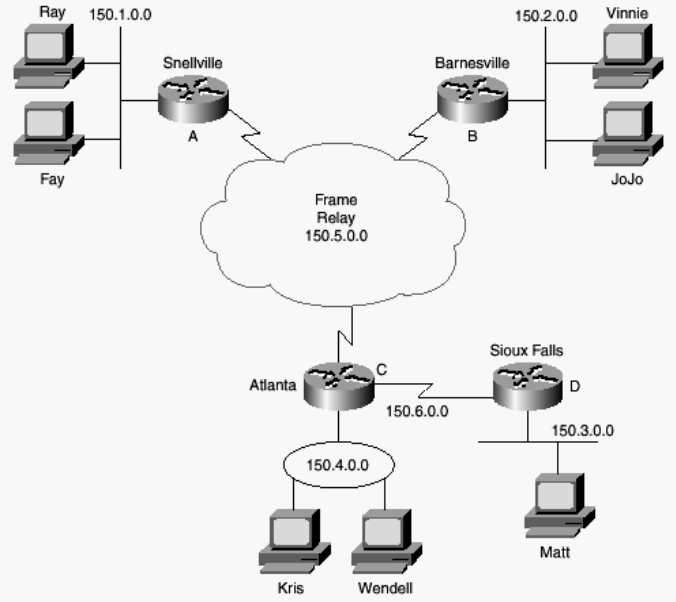
III.6. Ví dụ cách triển khai đặt địa chỉ IP cho một hệ thống mạng.



Hình 3.3 – Minh họa một hệ thống mạng

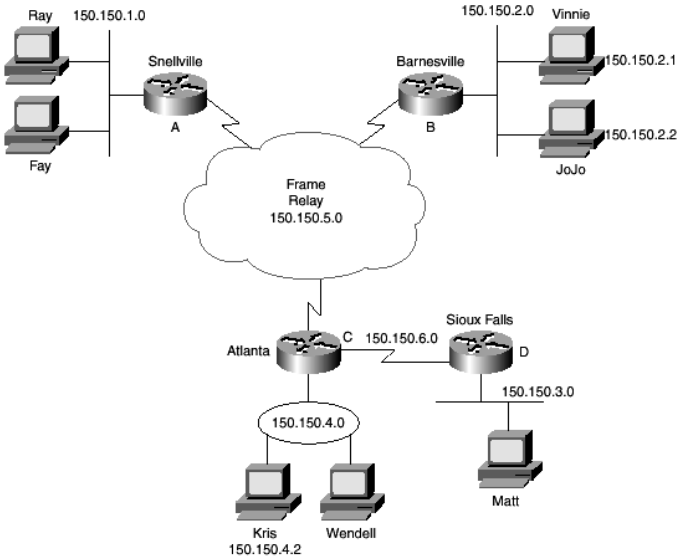
III.7. Chia mạng con (subnetting).

Giả sử ta phải tiến hành đặt địa chỉ IP cho hệ thống có cấu trúc như sau:



Hình 3.4 – Hệ thống mạng có 6 đường mạng

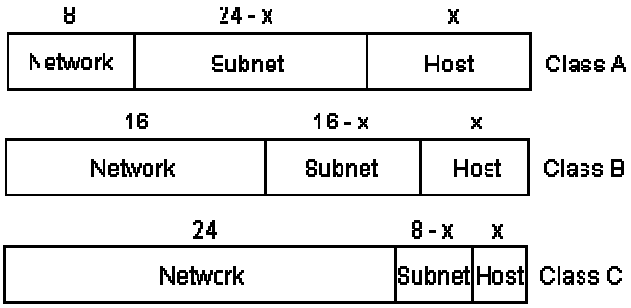
Theo hình trên, ta bắt buộc phải dùng đến tất cả là sáu đường mạng riêng biệt để đặt cho hệ thống mạng của mình, mặc dù trong mỗi mạng chỉ dùng đến vài địa chỉ trong tổng số 65534 địa chỉ hợp lệ, đó là một sự phí phạm to lớn. Thay vì vậy, khi sử dụng kỹ thuật chia mạng con, ta chỉ cần sử dụng một đường mạng 150.150.0.0 và chia đường mạng này thành sáu mạng con theo hình bên dưới:



Hình 3.5 – Hệ thống mạng có 6 đường mạng (sau khi chia Subnet)

Rõ ràng khi tiến hành cấp phát địa chỉ cho các hệ thống mạng lớn, người ta phải sử dụng kỹ thuật chia mạng con trong tình hình địa chỉ IP ngày càng khan hiếm. Ví dụ trong hình trên hoàn toàn chưa phải là chiến lược chia mạng con tối ưu. Thật sự người ta còn có thể chia mạng con nhỏ hơn nữa, đến một mức độ không bỏ phí một địa chỉ IP nào khác.

Xét về khía cạnh kỹ thuật, chia mạng con chính là việc mượn một số bit trong phần **host_id** ban đầu để đặt cho các mạng con. Lúc này, cấu trúc của địa chỉ IP gồm có ba phần: ***network_id***, ***subnet_id*** và ***host_id***. Số bit dùng cho phần **subnet_id** bao nhiêu là tuỳ thuộc vào chiến lược chia mạng con của người quản trị, có thể là một con số tròn byte (8 bit) hoặc một số bit lẻ vẫn được. Tuy nhiên **subnet_id** không thể chiếm trọn số bit có trong **host_id** ban đầu, cụ thể là (số bit làm **subnet_id**) ≤ (số bit làm host_id)-2.



Hình 3.6 – Số lượng **Subnet** tối đa được phép

Số lượng host trong mỗi mạng con được xác định bằng số bit trong phần host_id; $2^x - 2$ là số địa chỉ hợp lệ có thể đặt cho các host trong mạng con. Tương tự, số bit trong phần **subnet_id** xác định số lượng mạng con. Giả sử số bit là y ⇨ $2^y - 2$ là số lượng mạng con có được (trường hợp đặc biệt thì có thể sử dụng được 2^y mạng con).

Một số khái niệm mới:

- *Địa chỉ mạng con (địa chỉ đường mạng)*: bao gồm cả phần **network_id** và **subnet_id**, phần **host_id** chỉ chứa các bit 0. Theo hình bên trên thì ta có các địa chỉ mạng con sau: 150.150.1.0, 150.150.2.0, …
- *Địa chỉ **broadcast** trong một mạng con:* Giữ nguyên các bit dùng làm địa chỉ mạng con, đồng thời bật tất cả các bit trong phần **host_id** lên 1. Ví dụ địa chỉ **broadcast** của mạng con 150.150.1.0 là 150.150.1.255.
- *Mặt nạ mạng con (**subnet mask**):* giúp máy tính xác định được địa chỉ mạng con của một địa chỉ host. Để xây dựng mặt nạ mạng con cho một hệ thống địa chỉ, ta bật các bit trong phần **network_id** và **subnet_id** lên 1, tắt các bit trong phần **host_id** thành 0. Ví dụ mặt nạ mạng con dùng cho hệ thống mạng trong hình trên là 255.255.255.0.

Vấn đề đặt ra là khi xác định được một địa chỉ IP (ví dụ 172.29.8.230) ta không thể biết được host này nằm trong mạng nào (không thể biết mạng này có chia mạng con hay không, và nếu có chia thì dùng bao nhiêu bit để chia). Chính vì vậy khi ghi nhận địa chỉ IP của một host, ta cũng phải cho biết **subnet mask** là bao nhiêu (**subnet mask** có thể là giá trị thập phân, cũng có thể là số bit dùng làm **subnet mask**).

+ Ví dụ địa chỉ IP ghi theo giá trị thập phân của **subnet mask** là 172.29.8.230/255.255.255.0
+ Hoặc địa chỉ IP ghi theo số bit dùng làm **subnet mask** là 172.29.8.230/24.

III.8. Địa chỉ riêng (private address) và cơ chế chuyển đổi địa chỉ mạng (Network Address Translation - NAT)

Tất cả các IP host khi kết nối vào mạng Internet đều phải có một địa chỉ IP do tổ chức IANA (**Internet Assigned Numbers Authority**) cấp phát – gọi là địa chỉ hợp lệ (hay là được đăng ký). Tuy nhiên số lượng host kết nối vào mạng ngày càng gia tăng dẫn đến tình trạng khan hiếm địa chỉ IP. Một giải pháp đưa ra là sử dụng cơ chế NAT kèm theo là RFC 1918 qui định danh sách địa chỉ riêng. Các địa chỉ này sẽ không được IANA cấp phát - hay còn gọi là địa chỉ không hợp lệ. Bảng sau liệt kê danh sách các địa chỉ này:

Nhóm địa chỉ	Lớp	Số lượng mạng
10.0.0.0 đến 10.255.255.255	A	1
172.16.0.0 đến 172.31.255.255	B	16
192.168.0.0 đến 192.168.255.255	C	256

III.9. Cơ chế NAT

NAT được sử dụng trong thực tế là tại một thời điểm, tất cả các host trong một mạng **LAN** thường không truy xuất vào Internet đồng thời, chính vì vậy ta không cần phải sử dụng một số lượng tương ứng địa chỉ IP hợp lệ. **NAT** cũng được sử dụng khi nhà cung cấp dịch vụ Internet (ISP) cung cấp số lượng địa chỉ IP hợp lệ ít hơn so với số máy cần truy cập Internet. **NAT** được sử dụng trên các router đóng vai trò là gateway cho một mạng. Các host bên trong mạng **LAN** sẽ sử dụng một lớp địa chỉ riêng thích hợp. Còn danh sách các địa chỉ IP hợp lệ sẽ được cấu hình trên **Router NAT**. Tất cả các packet của các host bên trong mạng **LAN** khi gửi đến một host trên Internet đều được router **NAT** phân tích và chuyển đổi các địa chỉ riêng có trong packet thành một địa chỉ hợp lệ trong danh sách rồi mới chuyển đến host đích nằm trên mạng Internet. Sau đó nếu có một packet gửi cho một host bên trong mạng **LAN** thì **Router NAT** cũng chuyển đổi địa chỉ đích thành địa chỉ riêng của host đó rồi mới chuyển cho host ở bên trong mạng **LAN**.

Một cơ chế mở rộng của **NAT** là **PAT** (**Port Address Translation**) cũng dùng cho mục đích tương ứng. Lúc này thay vì chỉ chuyển đổi địa chỉ IP thì cả địa chỉ cổng dịch vụ (port) cũng được chuyển đổi (do **Router NAT** quyết định).

IV. MỘT SỐ CÂU HỎI THƯỜNG ĐẶT RA KHI LÀM VIỆC VỚI ĐỊA CHỈ IP.

IV.1. Ví dụ 1.

Người ta ghi nhận được địa chỉ IP của một host như sau: 172.29.32.30/255.255.240.0, hãy trả lời các câu hỏi sau:

- Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?

- Hãy cho biết host nằm trong mạng có địa chỉ là gì?

- Hãy cho biết địa chỉ broadcast dùng cho mạng đó?
- Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên.

Hướng dẫn trả lời:

Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?

1. Xác định lớp địa chỉ ⇨ xác định mặt nạ mặc định của lớp, so khớp với mặt nạ của địa chỉ ⇨ kết luận có chia mạng con hay không?
2. Xác định số bit trong subnet_id = ***x*** ⇨ số mạng con = 2^x-2.
3. Xác định số bit trong host_id = ***y*** ⇨ số host trong mạng con = 2^y-2.

   ⇨ Như vậy, Host này có địa chỉ IP thuộc lớp B, trong khi subnet mask của Host lại là 255.255.240.0 (khác với subnet mask mặc định của lớp B) ⇨ nên host trên nằm trong mạng có chia mạng con.

Subnet mask mặc định của lớp B	255.255.0.0	=	11111111	11111111	00000000	00000000
Subnet mask của Host	255.255.240.0	=	11111111	11111111	**1111**0000	00000000

   ⇨ So sánh số bit dùng làm subnet mask của Host với số bit dùng làm subnet mask mặc định của lớp B, sẽ có được số bit dùng làm subnet_id là 4 bit. Nên số bit dùng làm host_id sẽ là (16-4) = 12 bit.

   ⇨ Số mạng con tương tự là 14.

   ⇨ Số host trong mỗi mạng con là 4094.

Hãy cho biết host nằm trong mạng có địa chỉ là gì?

1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.
   + Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP.
   + Byte nào của subnet mask là 0 thì ghi lại byte tương ứng ở địa chỉ IP là 0.
   + Nếu giá trị của byte nào ở subnet mask khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**.
2. Tìm số cơ sở = 256-số khó chịu.
3. Tìm bội số lớn nhất của số cơ sở nhưng bội số này phải bé hơn hoặc bằng số tương ứng trong địa chỉ IP và ghi lại số này.

   ⇨ 172.29.___.0. **Số khó chịu** = 240.

   ⇨ **Số cơ sở** = 256 – 240 = 16.

   ⇨ Bội số của 16 lớn nhất nhưng bé hơn hoặc bằng 32 là 32

   ⇨ địa chỉ đường mạng cần tìm là 172.29.32.0.

Hãy cho biết địa chỉ broadcast dùng cho mạng đó?

1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.

+ Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP,
+ Byte nào của subnet mask là 0 thì ghi vào byte tương ứng của địa chỉ IP là 255
+ Nếu byte của subnet mask có giá trị khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**.

2. Tìm số cơ sở = 256 - số khó chịu.
3. Tìm bội số nhỏ nhất của **số cơ sở** nhưng bội số này phải lớn hơn số tương ứng trong địa chỉ IP, đem số này trừ đi 1 thì được kết quả.

   - 172.29.___.255. **Số khó chịu** = 240.
   - **Số cơ sở** = 256 – 240 = 16.
   - Bội số nhỏ nhất của 16 nhưng lớn hơn 32 là 48. 48 – 1 =47
   - Địa chỉ broadcast cần tìm là 172.29.47.255.

Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên?

Các địa chỉ host hợp lệ có thể đặt cho các host nằm chung mạng con với host ở trên là: các địa chỉ sau địa chỉ mạng và trước địa chỉ broadcast.

- Các địa chỉ từ 172.29.32.1 đến 172.29.47.254.

IV.2. Ví dụ 2.

Cho host có địa chỉ 10.8.100.49/19. Hãy trả lời các câu hỏi trên cho host này.

- **Subnet mask** là 19 bit hay 255.255.224.0 ⇨ có chia mạng con. Số bit trong subnet_id là 11 ⇨ số subnet = 2^{11}-2 = 2046. Số bit trong host_id là 13 ⇨ số host hợp lệ = 2^{13} – 2 = 8190.
- Địa chỉ mạng: 10.8.___.0. **Số khó chịu** = 224 ⇨ **Số cơ sở** = 256 – 224 = 32. Bội số lớn nhất của 32 nhưng bé hơn 100 là 96 ⇨ địa chỉ mạng là 10.8.96.0.
- Địa chỉ broadcast: 10.8.127.255.
- Các địa chỉ hợp lệ của mạng con: 10.8.96.1 đến 10.8.127.254

Tóm tắt

Lý thuyết 6 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về các môi trường truyền dẫn, chức năng và mô hình hoạt động của các thiết bị mạng…	I. Giới thiệu về môi trường truyền dẫn. II. Các loại cáp mạng. III. Đường truyền vô tuyến. IV. Các thiết bị mạng	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

I. GIỚI THIỆU VỀ MÔI TRƯỜNG TRUYỀN DẪN

I.1. Khái niệm

Trên một mạng máy tính, các dữ liệu được truyền trên một môi trường truyền dẫn (**transmission media**), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị. Có hai loại phương tiện truyền dẫn chủ yếu:

- Hữu tuyến (**bounded media**)
- Vô tuyến (**boundless media**)

Thông thường hệ thống mạng sử dụng hai loại tín hiệu là: digital và analog.

I.2. Tần số truyền thông

Phương tiện truyền dẫn giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân (bật/tắt). Các tín hiệu truyền thông giữa các máy tính và các thiết bị là các dạng sóng điện từ trải dài từ tần số radio đến tần số hồng ngoại.

Các sóng tần số radio thường được dùng để phát tín hiệu LAN. Các tần số này có thể được dùng với cáp xoắn đôi, cáp đồng trục hoặc thông qua việc truyền phủ sóng radio.

Sóng viba (**microware**) thường dùng truyền thông tập trung giữa hai điểm hoặc giữa các trạm mặt đất và các vệ tinh, ví dụ như mạng điện thoại cellular.

Tia hồng ngoại thường dùng cho các kiểu truyền thông qua mạng trên các khoảng cách tương đối ngắn và có thể phát được sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Chúng ta có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

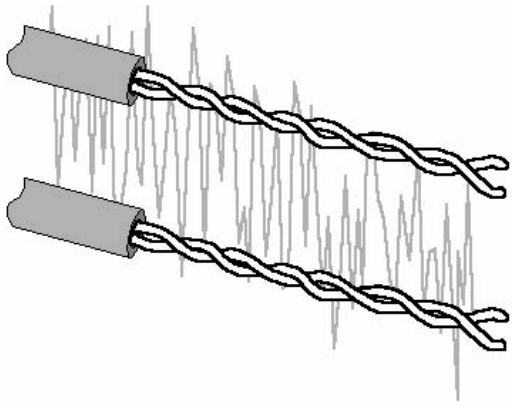
I.3. Các đặc tính của phương tiện truyền dẫn

Mỗi phương tiện truyền dẫn đều có những tính năng đặc biệt thích hợp với mỗi kiểu dịch vụ cụ thể, nhưng thông thường chúng ta quan tâm đến những yếu tố sau:

- Chi phí
- Yêu cầu cài đặt
- Độ bảo mật
- Băng thông (**bandwidth**): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:

+ Bps (**Bits per second**-số bit trong một giây): đây là đơn vị cơ bản của băng thông.
+ KBps (**Kilobits per second**): 1 KBps=10^3 bps=1000 Bps
+ MBps (**Megabits per second**): 1 MBps = 10^3 KBps
+ GBps (**Gigabits per second**): 1 GBps = 10^3 MBps
+ TBps (**Terabits per second**): 1 TBps = 10^3 GBPS.

- Thông lượng (**Throughput**): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.
- Băng tầng cơ sở (**baseband**): dành toàn bộ băng thông cho một kênh truyền, băng tầng mở rộng (**broadband**):cho phép nhiều kênh truyền chia sẻ một phương tiện truyền dẫn (chia sẻ băng thông).
- Độ suy giảm (**attenuation**): độ đo sự suy yếu đi của tín hiệu khi di chuyển trên một phương tiện truyền dẫn. Các nhà thiết kế cáp phải chỉ định các giới hạn về chiều dài dây cáp vì khi cáp dài sẽ dẫn đến tình trạng tín hiệu yếu đi mà không thể phục hồi được.
- Nhiễu điện từ (**Electromagnetic interference - EMI**): bao gồm các nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một phương tiện truyền dẫn.
- Nhiễu xuyên kênh (**crosstalk**): hai dây dẫn đặt kề nhau làm nhiễu lẫn nhau.



Hình 4.1 – Mô phỏng trường hợp nhiễu xuyên kênh (**crosstalk**)

I.4. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:

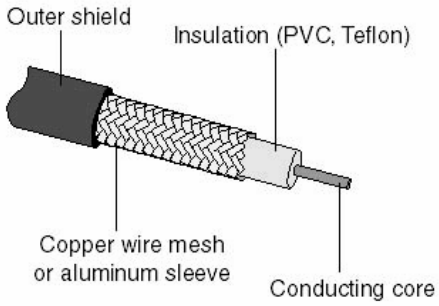
+ Đơn công (**Simplex**): trong kiểu truyền dẫn này, thiết bị phát tín hiệu và thiết bị nhận tín hiệu được phân biệt rõ ràng, thiết bị phát chỉ đảm nhiệm vai trò phát tín hiệu, còn thiết bị thu chỉ đảm nhiệm vai trò nhận tín hiệu. Truyền hình là một ví dụ của kiểu truyền dẫn này.
+ Bán song công (**Half-Duplex**): trong kiểu truyền dẫn này, thiết bị có thể là thiết bị phát, vừa là thiết bị thu. Nhưng tại một thời điểm thì chỉ có thể ở một trạng thái (phát hoặc thu). Bộ đàm là thiết bị hoạt động ở kiểu truyền dẫn này.
+ Song công (**Full-Duplex**): trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

II. CÁC LOẠI CÁP.

II.1. Cáp đồng trục (coaxial).

Là kiểu cáp đầu tiên được dùng trong các **LAN**, cấu tạo của cáp đồng trục gồm:

- Dây dẫn trung tâm: dây đồng hoặc dây đồng bện.
- Một lớp cách điện giữa dây dẫn phía ngoài và dây dẫn phía trong.
- Dây dẫn ngoài: bao quanh dây dẫn trung tâm dưới dạng dây đồng bện hoặc lá. Dây này có tác dụng bảo vệ dây dẫn trung tâm khỏi nhiễu điện từ và được nối đất để thoát nhiễu.
- Ngoài cùng là một lớp vỏ **plastic** bảo vệ cáp.



Hình 4.2 – Chi tiết cáp đồng trục

Ưu điểm của cáp đồng trục: là rẻ tiền, nhẹ, mềm và dễ kéo dây.

Cáp mỏng (**thin cable/thinnet**): có đường kính khoảng 6mm, thuộc họ RG-58, chiều dài đường chạy tối đa là 185 m.

- Cáp RC-58, trở kháng 50 ohm dùng với Ethernet mỏng.
- Cáp RC-59, trở kháng 75 ohm dùng cho truyền hình cáp.
- Cáp RC-62, trở kháng 93 ohm dùng cho ARCnet.

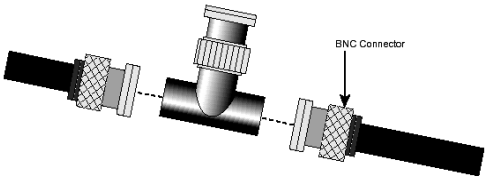
Cáp dày (**thick cable/thicknet**): có đường kính khoảng 13mm thuộc họ RG-58, chiều dài đường chạy tối đa 500m.

Hình 4.3 – So sánh cáp đồng trục: **Thicknet** và **Thinnet.**

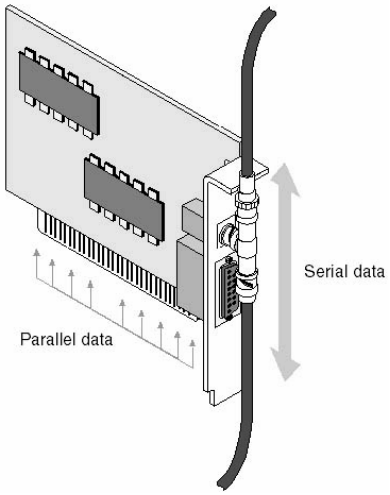
So sánh giữa cáp đồng trục mỏng và đồng trục dày:

- Chi phí: cáp đồng trục thinnet rẻ nhất, cáp đồng trục **thicknet** đắt hơn.
- Tốc độ: mạng Ethernet sử dụng cáp thinnet có tốc độ tối đa 10Mbps và mạng ARCNet có tốc độ tối đa 2.5Mbps.
- **EMI**: có lớp chống nhiễu nên hạn chế được nhiễu.
- Có thể bị nghe trộm tín hiệu trên đường truyền.

Cách lắp đặt dây: muốn nối các đoạn cáp đồng trục mỏng lại với nhau ta dùng đầu nối chữ T và đầu **BNC** như hình vẽ.

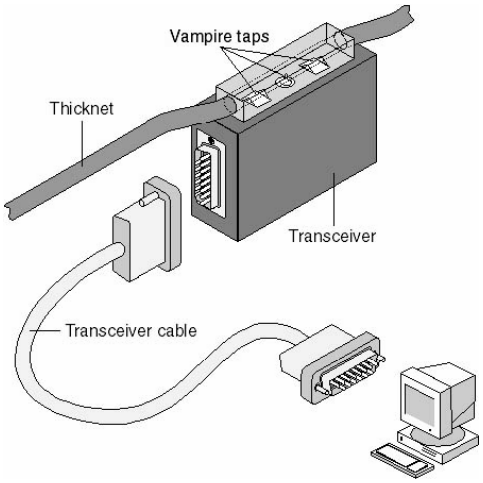


Hình 4.4 – Đầu nối BNC và đầu nối chữ T



Hình 4.5 – Đầu chuyển đổi (gắn vào máy tính)

Muốn đấu nối cáp đồng trục dày ta phải dùng một đầu chuyển đổi **transceiver** và nối kết vào máy tính thông qua cổng **AUI**.



Hình 4.6 – Kết nối cáp **Thicknet** vào máy tính.

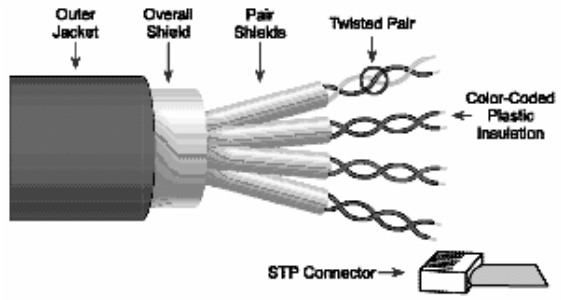
II.2. Cáp xoắn đôi.

Hình 4.7 – Mô tả cáp xoắn đôi

Cáp xoắn đôi gồm nhiều cặp dây đồng xoắn lại với nhau nhằm chống phát xạ nhiễu điện từ. Do giá thành thấp nên cáp xoắn được dùng rất rộng rãi. Có hai loại cáp xoắn đôi được sử dụng rộng rãi trong LAN là: loại có vỏ bọc chống nhiễu và loại không có vỏ bọc chống nhiễu.

Cáp xoắn đôi có vỏ bọc chống nhiễu STP (Shielded Twisted- Pair).

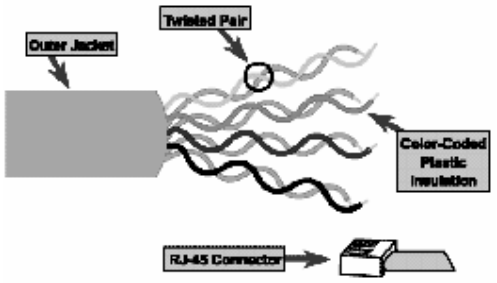
- Gồm nhiều cặp xoắn được phủ bên ngoài một lớp vỏ làm bằng dây đồng bện. Lớp vỏ này có tác dụng chống **EMI** từ ngoài và chống phát xạ nhiễu bên trong. Lớp vỏ bọc chống nhiễu này được nối đất để thoát nhiễu. Cáp xoắn đôi có bọc ít bị tác động bởi nhiễu điện và truyền tín hiệu xa hơn cáp xoắn đôi trần.
- Chi phí: đắt tiền hơn **Thinnet** và **UTP** nhưng lại rẻ tiền hơn **Thicknet** và cáp quang.
- Tốc độ: tốc độ lý thuyết 500Mbps, thực tế khoảng 155Mbps, với đường chạy 100m; tốc độ phổ biến 16Mbps (Token Ring).
- Độ suy dần: tín hiệu yếu dần nếu cáp càng dài, thông thường chiều dài cáp nên ngắn hơn 100m.
- Đầu nối: STP sử dụng đầu nối DIN (DB –9).



Hình 4.8 – Mô tả cáp STP.

Cáp xoắn đôi không có vỏ bọc chống nhiễu UTP (Unshielded Twisted- Pair).

Gồm nhiều cặp xoắn như cáp **STP** nhưng không có lớp vỏ đồng chống nhiễu. Cáp xoắn đôi trần sử dụng chuẩn 10BaseT hoặc 100BaseT. Do giá thành rẻ nên đã nhanh chóng trở thành loại cáp mạng cục bộ được ưu chuộng nhất. Độ dài tối đa của một đoạn cáp là 100 mét. Do không có vỏ bọc chống nhiễu nên cáp **UTP** dễ bị nhiễu khi đặt gần các thiết bị và cáp khác do đó thông thường dùng để đi dây trong nhà. Đầu nối dùng đầu RJ-45.



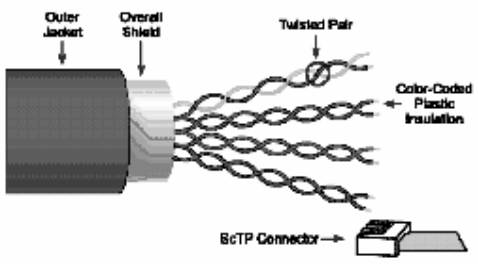
Hình 4.9 – Mô tả cáp UTP

Cáp UTP có năm loại:

- Loại 1: truyền âm thanh, tốc độ < 4Mbps.
- Loại 2: cáp này gồm bốn dây xoắn đôi, tốc độ 4Mbps.
- Loại 3: truyền dữ liệu với tốc độ lên đến 10 Mbps. Cáp này gồm bốn dây xoắn đôi với ba mắt xoắn trên mỗi **foot** (**foot** là đơn vị đo chiều dài, 1 foot = 0.3048 mét).
- Loại 4: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ đạt được 16 Mbps.
- Loại 5: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ 100Mbps.

Cáp xoắn có vỏ bọc ScTP-FTP (Screened Twisted-pair).

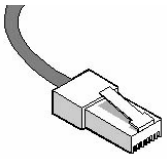
FTP là loại cáp lai tạo giữa cáp **UTP** và **STP**, nó hỗ trợ chiều dài tối đa 100m.



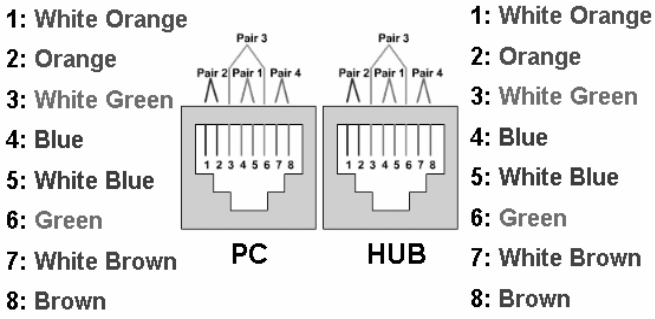
Hình 4.10 – Mô tả cáp FTP

Các kỹ thuật bấm cáp mạng.

- Cáp thẳng (**Straight-through cable**): là cáp dùng để nối PC và các thiết bị mạng như **Hub**, **Switch**, **Router**… Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.

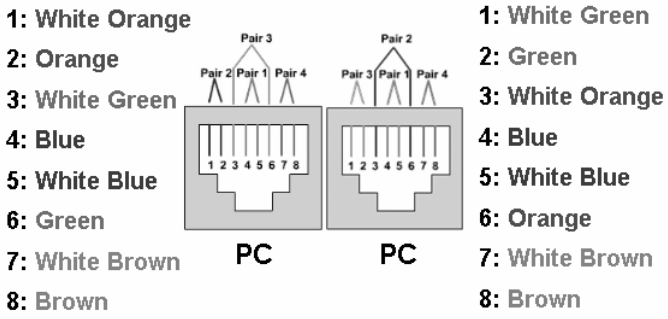


Hình 4.11 – Đầu RJ45.



Hình 4.12 – Cách đấu dây thẳng.

- Cáp chéo (**Crossover cable**): là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như **PC – PC**, **Hub – Hub**, **Switch – Switch**. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu) .

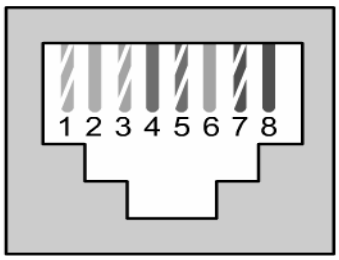


Hình 4.13 – Cách đấu dây chéo.

- Cáp **Console**: dùng để nối PC vào các thiết bị mạng chủ yếu dùng để cấu hình các thiết bị. Thông thường khoảng cách dây **Console** ngắn nên chúng ta không cần chọn cặp dây xoắn, mà chọn theo màu từ 1-8 sao cho dễ nhớ và đầu bên kia ngược lại từ 8-1.

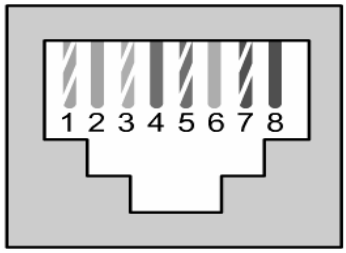
ANSI (Viện tiêu chuẩn quốc gia Hoa kỳ), **TIA** (hiệp hội công nghiệp viễn thông), **EIA** (hiệp hội công nghiệp điện tử) đã đưa ra 2 cách xếp đặt vị trí dây như sau:

- Chuẩn T568-A (còn gọi là Chuẩn A):



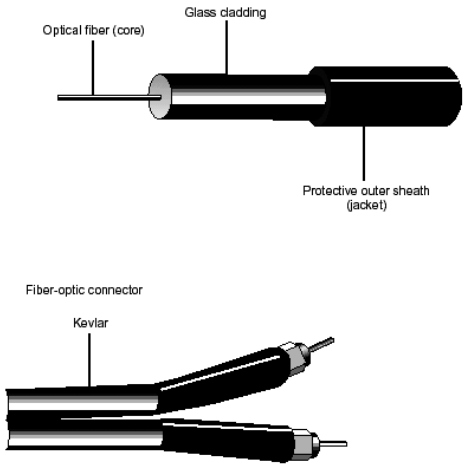
1. Trắng Xanh lá cây (White Green)
2. Xanh lá cây (Green)
3. Trắng Cam (White Orange)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Cam (Orange)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

- Chuẩn T568-B (còn gọi là Chuẩn B):



1. Trắng Cam (White Orange)
2. Cam (Orange)
3. Trắng Xanh lá cây (White Green)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Xanh lá cây (Green)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

II.3. Cáp quang (Fiber-optic cable).



Hình 4.14 – Mô tả cáp quang.

Cáp quang có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng. Sợi quang được tráng một lớp nhằm phản chiếu các tín hiệu. Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông rất cao nên không gặp các sự cố về nhiễu hay bị nghe trộm. Cáp dùng nguồn sáng laser, diode phát xạ ánh sáng. Cáp rất bền và độ suy giảm tín hiệu rất thấp nên đoạn cáp có thể dài đến vài km. Băng thông cho phép đến 2Gbps. Nhưng cáp quang có khuyết điểm là giá thành cao và khó lắp đặt. Các loại cáp quang:

- Loại lõi 8.3 micron, lớp lót 125 micron, chế độ đơn.
- Loại lõi 62.5 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 50 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 100 micron, lớp lót 140 micron, đa chế độ.

Hộp đấu nối cáp quang: do cáp quang không thể bẻ cong nên khi nối cáp quang vào các thiết bị khác chúng ta phải thông qua hộp đấu nối.

Hình 4.15 – Mô tả hộp đấu nối cáp quang.

Đầu nối cáp quang: đầu nối cáp quang rất đa dạng thông thường trên thị trường có các đầu nối như sau: **FT**, **ST**, **FC**…

Hình 4.16 – Một số loại đầu nối cáp quang.

III. ĐƯỜNG TRUYỀN VÔ TUYẾN.

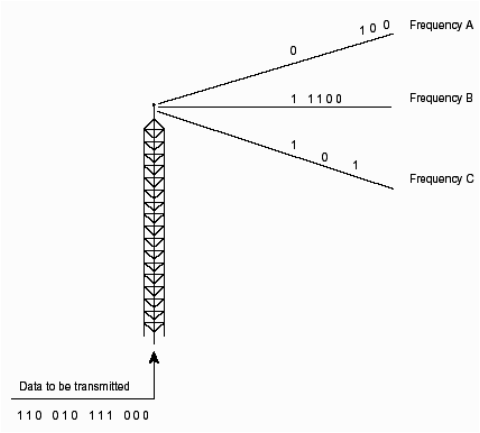
Khi dùng các loại cáp ta gặp một số khó khăn như cơ sở cài đặt cố định, khoảng cách không xa, vì vậy để khắc phục những khuyết điểm trên người ta dùng đường truyền vô tuyến. Đường truyền vô tuyến mang lại những lợi ích sau:

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.
- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.
- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.
- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.
- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng cho phép của cáp đồng và cáp quang.
- Dùng làm kết nối dự phòng cho các kết nối hệ thống cáp.

Tuy nhiên, đường truyền vô tuyến cũng có một số hạn chế:

- Tín hiệu không an toàn.
- Dễ bị nghe lén.
- Khi có vật cản thì tín hiệu suy yếu rất nhanh.
- Băng thông không cao.

III.1. Sóng vô tuyến (radio).

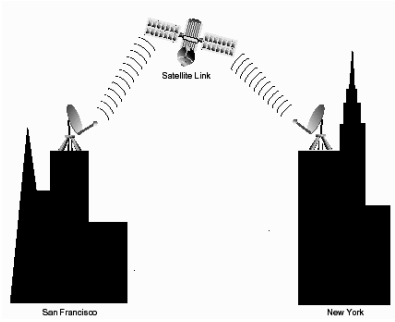


Hình 4.16 – Truyền dữ liệu qua sóng vô tuyến.

Sóng **radio** nằm trong phạm vi từ 10 KHz đến 1 GHz, trong miền này ta có rất nhiều dải tần ví dụ như: sóng ngắn, **VHF** (dùng cho tivi và radio FM), **UHF** (dùng cho tivi). Tại mỗi quốc gia, nhà nước sẽ quản lý cấp phép sử dụng các băng tần để tránh tình trạng các sóng bị nhiễu. Nhưng có một số băng tần được chỉ định là vùng tự do có nghĩa là chúng ta dùng nhưng không cần đăng ký (vùng này thường có dải tần 2,4 Ghz). Tận dụng lợi điểm này các thiết bị Wireless của các hãng như **Cisco**, **Compex** đều dùng ở dải tần này. Tuy nhiên, chúng ta sử dụng tần số không cấp phép sẽ có nguy cơ nhiễu nhiều hơn.

III.2. Sóng viba.

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các nối kết với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps. Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.



Hình 4.17 – Truyền dữ liệu thông qua vệ tinh.

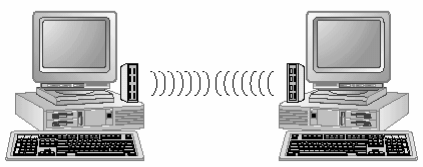
Hình 4.18 – Truyền dữ liệu trực tiếp giữa hai thiết bị.

III.3. Hồng ngoại.

Tất cả mạng vô tuyến hồng ngoại đều hoạt động bằng cách dùng tia hồng ngoại để truyền tải dữ liệu giữa các thiết bị. Phương pháp này có thể truyền tín hiệu ở tốc độ cao do dải thông cao của tia hồng ngoại. Thông thường mạng hồng ngoại có thể truyền với tốc độ từ 1-10 Mbps. Miền tần số từ 100 Ghz đến 1000 GHz. Có bốn loại mạng hồng ngoại:

- Mạng đường ngắm: mạng này chỉ truyền khi máy phát và máy thu có một đường ngắm rõ rệt giữa chúng.
- Mạng hồng ngoại tán xạ: kỹ thuật này phát tia truyền dội tường và sàn nhà rồi mới đến máy thu. Diện tích hiệu dụng bị giới hạn ở khoảng 100 feet (35m) và có tín hiệu chậm do hiện tượng dội tín hiệu.
- Mạng phản xạ: ở loại mạng hồng ngoại này, máy thu-phát quang đặt gần máy tính sẽ truyền tới một vị trí chung, tại đây tia truyền được đổi hướng đến máy tính thích hợp.

- **Broadband optical telepoint**: loại mạng cục bộ vô tuyến hồng ngoại cung cấp các dịch vụ đài rộng. Mạng vô tuyến này có khả năng xử lý các yêu cầu đa phương tiện chất lượng cao, vốn có thể trùng khớp với các yêu cầu đa phương tiện của mạng cáp.



Hình 4.19 – Truyền dữ liệu giữa 2 máy tính thông qua hồng ngoại.

IV. CÁC THIẾT BỊ MẠNG.

IV.1. Card mạng (NIC hay Adapter).

Card mạng là thiết bị nối kết giữa máy tính và cáp mạng. Chúng thường giao tiếp với máy tính qua các khe cắm như: **ISA**, **PCI** hay **USP**… Phần giao tiếp với cáp mạng thông thường theo các chuẩn như: **AUI**, **BNC**, **UTP**… Các chức năng chính của card mạng:

- Chuẩn bị dữ liệu đưa lên mạng: trước khi đưa lên mạng, dữ liệu phải được chuyển từ dạng byte, bit sang tín hiệu điện để có thể truyền trên cáp.
- Gởi dữ liệu đến máy tính khác.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.

Địa chỉ **MAC** (**Media Access Control**): mỗi card mạng có một địa chỉ riêng dùng để phân biệt card mạng này với card mạng khác trên mạng. Địa chỉ này do **IEEE** – Viện Công nghệ Điện và Điện tử – cấp cho các nhà sản xuất card mạng. Từ đó các nhà sản xuất gán cố định địa chỉ này vào chip của mỗi card mạng. Địa chỉ này gồm 6 byte (48 bit), có dạng XXXXXX.XXXXXX, 3 byte đầu là mã số của nhà sản xuất, 3 byte sau là số serial của các card mạng do hãng đó sản xuất. Địa chỉ này được ghi cố định vào **ROM** nên còn gọi là địa chỉ vật lý. Ví dụ địa chỉ vật lý của một card Intel có dạng như sau: 00A0C90C4B3F.

Hình dưới là card mạng RE100TX theo chuẩn Ethernet IEEE 802.3 và IEEE 802.3u. Nó hỗ trợ cả hai băng thông 10Mbps và 100Mbps theo chuẩn 10Base-T và 100Base-TX. Ngoài ra card này còn cung cấp các tính năng như **Wake On LAN**, **Port Trunking**, hỗ trợ cơ chế truyền **full duplex**. Card này cũng hỗ trợ hai cơ chế boot ROM 16 bit (RPL) và 32 bit (PXE).

Hình 4.20 – Card RE100TX.

Hình dưới là card FL1000T 10/100/1000Mbps Gigabit Adapter, nó là card mạng theo chuẩn **Gigabit** dùng đầu nối RJ45 truyền trên môi trường cáp UTP cat 5. Card này cung cấp đường truyền với băng thông lớn và tương thích với card PCI 64 và 32 bit đồng thời nó cũng hỗ trợ cả hai cơ chế truyền **full/half duplex** trên cả ba loại băng thông 10/100/1000 Mbps.

Hình 4.21 – Card FL1000T 10/100/1000Mbps **Gigabit**.

Hình dưới là card mạng không dây WL11A 11Mbps **Wireless PCMCIA LAN Card**, card này giao tiếp với máy theo chuẩn **PCMCIA** nên khi sử dụng cho PC chúng ta phải dùng thêm card chuyển đổi từ PCI sang **PCMCIA**. Card được thiết kế theo chuẩn IEEE802.11b ở dải tần 2.4GHz ISM, dùng cơ chế **CSMA/CA** để xử lý đụng độ, băng thông của card là 11Mbps, có thể mã hóa 64 và 128 bit. Đặc biệt card này hỗ trợ cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**.

Hình 4.22 – Card WL11A.

IV.2. Card mạng dùng cáp điện thoại.

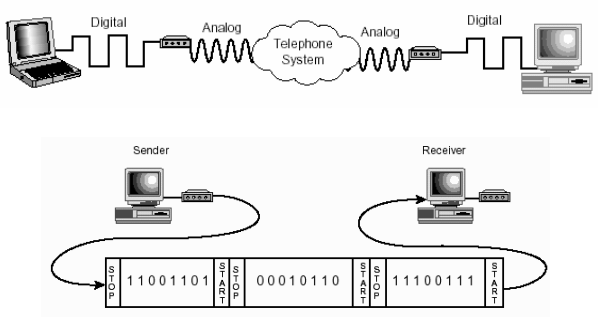
Card HP10 10Mbps **Phoneline Network Adapter** là một card mạng đặc biệt vì nó không dùng cáp đồng trục cũng không dùng cáp UTP mà dùng cáp điện thoại. Một đặc tính quan trọng của card này là truyền số liệu song song với truyền âm thanh trên dây điện thoại. Card này dùng đầu kết nối RJ11 và băng thông 10Mbps, chiều dài cáp có thể dài đến gần 300m.

Hình 4.23 - Card HP10 10Mbps **Phoneline.**

IV.3. Modem.

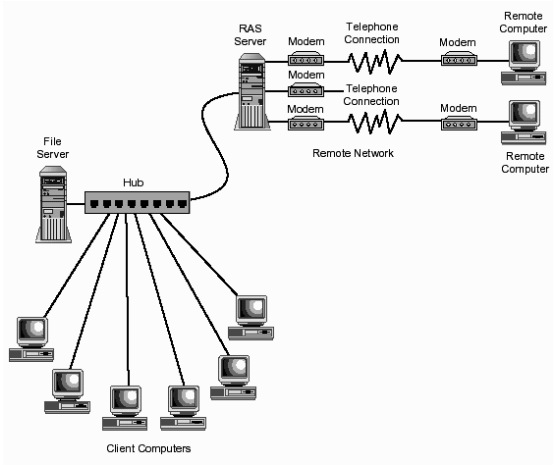
Là thiết bị dùng để nối hai máy tính hay hai thiết bị ở xa thông qua mạng điện thoại. **Modem** thường có hai loại: **internal** (là loại được gắn bên trong máy tính giao tiếp qua khe cắm **ISA** hoặc PCI), **external** (là loại thiết bị đặt bên ngoài **CPU** và giao tiếp với **CPU** thông qua cổng **COM** theo chuẩn RS-232). Cả hai loại trên đều có cổng giao tiếp RJ11 để nối với dây điện thoại.

Chức năng của **Modem** là chuyển đổi tín hiệu số (**digital**) thành tín hiệu tương tự (**analog**) để truyền dữ liệu trên dây điện thoại. Tại đầu nhận, **Modem** chuyển dữ liệu ngược lại từ dạng tín hiệu tương tự sang tín hiệu số để truyền vào máy tính. Thiết bị này giá tương đối thấp nhưng mang lại hiệu quả rất lớn. Nó giúp nối các mạng **LAN** ở xa với nhau thành các mạng **WAN**, giúp người dùng có thể hòa vào mạng nội bộ của công ty một cách dễ dàng dù người đó ở nơi nào.



Hình 4.24 – Mô hình truyền dữ liệu thông qua **Modem**.

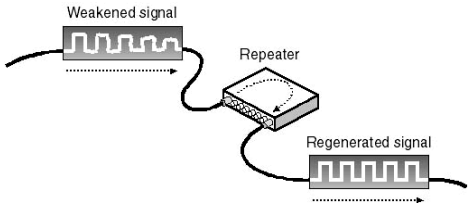
Remote Access Services (**RAS**): là một dịch vụ mềm trên một máy tính hoặc là một dịch vụ trên thiết bị phần cứng. Nó cho phép dùng **Modem** để nối kết hai mạng **LAN** với nhau hoặc một máy tính vào mạng nội bộ.



Hình 4.25 – Sử dụng **RAS** để liên lạc.

IV.4. Repeater.

Là thiết bị dùng để khuếch đại tín hiệu trên các đoạn cáp dài. Khi truyền dữ liệu trên các đoạn cáp dài tín hiệu điện sẽ yếu đi, nếu chúng ta muốn mở rộng kích thước mạng thì chúng ta dùng thiết bị này để khuếch đại tín hiệu và truyền đi tiếp. Nhưng chúng ta chú ý rằng thiết bị này hoạt động ở lớp vật lý trong mô hình **OSI**, nó chỉ hiểu tín hiệu điện nên không lọc được dữ liệu ở bất kỳ dạng nào, và mỗi lần khuếch đại các tín hiệu điện yếu sẽ bị sai do đó nếu cứ tiếp tục dùng nhiều **Repeater** để khuếch đại và mở rộng kích thước mạng thì dữ liệu sẽ ngày càng sai lệch.



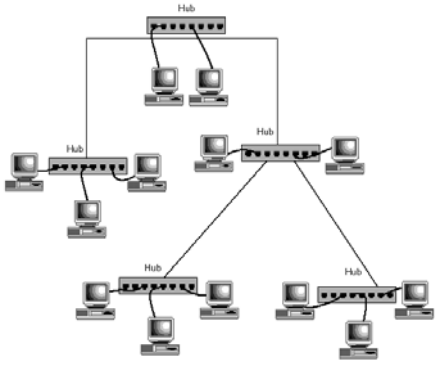
Hình 4.26 – Thiết bị **Repeater**.

IV.5. Hub.

Là thiết bị giống như **Repeater** nhưng nhiều port hơn cho phép nhiều máy tính nối tập trung về thiết bị này. Các chức năng giống như **Repeater** dùng để khuếch đại tín hiệu điện và truyền đến tất cả các port còn lại đồng thời không lọc được dữ liệu. Thông thường **Hub** hoạt động ở lớp 1 (lớp vật lý). Toàn bộ **Hub** (hoặc **Repeater**) được xem là một **Collision Domain**.

Hub gồm có ba loại:

- **Passive Hub**: là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác, không có linh kiện điện tử và nguồn riêng nên không không khuếch đại và xử lý tín hiệu;
- **Active Hub**: là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác với chất lượng cao hơn. Thiết bị này có linh kiện điện tử và nguồn điện riêng nên hoạt động như một repeater có nhiều cổng (**port**);
- **Intelligent Hub**: là một **active hub** có thêm các chức năng vượt trội như cho phép quản lý từ các máy tính, chuyển mạch (**switching**), cho phép tín hiệu điện chuyển đến đúng port cần nhận không chuyển đến các port không liên quan.



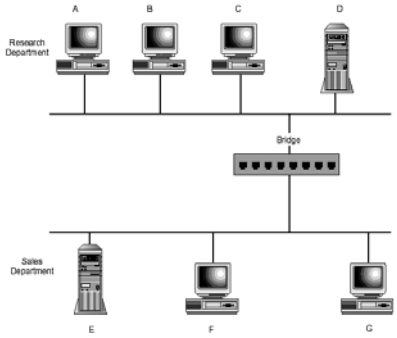
Hình 4.27 – Mô hình mạng sử dụng **Hub**.

IV.6. Bridge (cầu nối).

Là thiết bị cho phép nối kết hai nhánh mạng, có chức năng chuyển có chọn lọc các gói tin đến nhánh mạng chứa máy nhận gói tin. Trong **Bridge** có bảng địa chỉ **MAC**, bảng địa chỉ này sẽ được dùng để quyết định đường đi của gói tin (cách thức truyền đi của một gói tin sẽ được nói rõ hơn ở trong phần trình bày về thiết bị **Switch**). Bảng địa chỉ này có thể được khởi tạo tự động hoặc phải cấu hình bằng tay. **Bridge** hoạt động ở lớp hai (lớp **Data link**) trong mô hình **OSI**.

Ưu điểm của **Bridge** là: cho phép mở rộng cùng một mạng logic với nhiều kiểu cáp khác nhau. Chia mạng thành nhiều phân đoạn khác nhau nhằm giảm lưu lượng trên mạng.

Khuyết điểm: chậm hơn **Repeater** vì phải xử lý các gói tin, chưa tìm được đường đi tối ưu trong trường hợp có nhiều đường đi. Việc xử lý gói tin dựa trên phần mềm.



Hình 4.28 – Mô hình mạng sử dụng **Bridge**.

IV.7. Switch

Là thiết bị giống như bridge nhưng nhiều **port** hơn cho phép ghép nối nhiều đoạn mạng với nhau. **Switch** cũng dựa vào bảng địa chỉ **MAC** để quyết định gói tin nào đi ra **port** nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. **Switch** cũng hoạt động tại lớp hai trong mô hình **OSI**. Việc xử lý gói tin dựa trên phần cứng (**chip**).

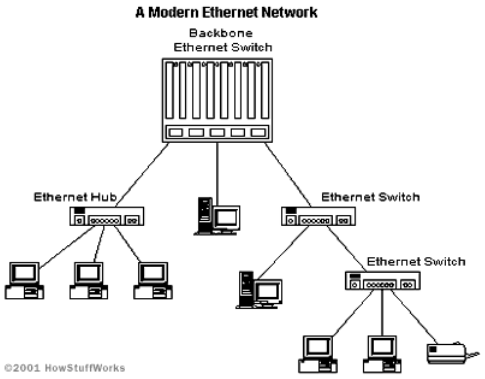
Khi một gói tin đi đến **Switch** (hoặc **Bridge**), **Switch** (hoặc **Bridge**) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng **MAC** chưa, nếu chưa có thì nó sẽ thêm địa chỉ **MAC** này và **port** nguồn (nơi gói tin đi vào **Switch** (hoặc **Bridge**)) vào trong bảng **MAC**.
- Kiểm tra địa chỉ đích của gói tin đã có trong bảng **MAC** chưa:
  - + Nếu chưa có thì nó sẽ gởi gói tin ra tất cả các **port** (ngoại trừ port gói tin đi vào).
  - + Nếu địa chỉ đích đã có trong bảng **MAC**:
    - ③ Nếu port đích trùng với port nguồn thì **Switch** (hoặc **Bridge**) sẽ loại bỏ gói tin.
    - ③ Nếu port đích khác với **port** nguồn thì gói tin sẽ được gởi ra **port** đích tương ứng.

Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ **MAC**.
- **Port** nguồn là **Port** mà gói tin đi vào.
- **Port** đích là **Port** mà gói tin đi ra.

Do cách hoạt động của **Switch** (hoặc **Bridge**) như vậy, nên mỗi **Port** của **Switch** là một **Collision Domain**, và toàn bộ **Switch** được xem là một **Broadcast Domain** (khái niệm **Collision Domain** và **Broadcast Domain** sẽ được giới thiệu trong chương 5, phần "các công nghệ mạng **LAN**").



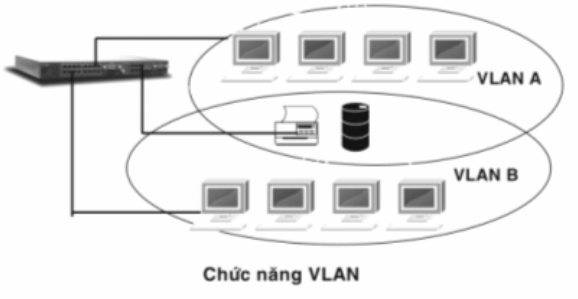
Hình 4.29 – Mô hình mạng sử dụng **Switch**.

Ngoài các tính năng cơ sở, **Switch** còn các tính năng mở rộng như sau:

- Phương pháp chuyển gói tin (**Switching mode**): trong thiết bị của **Cisco** có thể sử dụng một trong ba loại sau:
  - + **Store and Forward**: là tính năng lưu dữ liệu trong bộ đệm trước khi truyền sang các port khác để tránh đụng độ (**collision**), thông thường tốc độ truyền khoảng 148.800 pps. Với kỹ thuật này toàn bộ gói tin phải được nhận đủ trước khi **Switch** truyền frame này đi do đó độ trễ (**latency**) lệ thuộc vào chiều dài của frame.
  - + **Cut Through**: **Switch** sẽ truyền gói tin ngay lập tức một khi nó biết được địa chỉ đích của gói tin. Kỹ thuật này sẽ có độ trễ thấp hơn so với kỹ thuật **Store and Forward** và độ trễ luôn là con số xác định, bất chấp chiều dài của gói tin.
  - + **Fragment Free**: thì **Switch** đọc 64 byte đầu tiên và sau đó bắt đầu truyền dữ liệu.
- **Trunking** (**MAC Base**): ở một số thiết bị **Switch**, tính năng **Trunking** được hiểu là tính năng giúp tăng tốc độ truyền giữa hai **Switch**, nhưng chú ý là hai **Switch** phải cùng loại. Riêng trong thiết bị **Switch** của **Cisco**, Trunking được hiểu là đường truyền dùng để mang thông tin cho các **VLAN**.

Hình 4.30 – Mô tả cách dùng đường **Trunking**.

- **VLAN**: tạo các mạng ảo, nhằm đảm bảo tính bảo mật khi mở rộng mạng bằng cách nối các **Switch** với nhau. Mỗi **VLAN** có thể được xem là một **Broadcast Domain**, nên khi chia các mạng ảo giúp ta sẽ phân vùng miền **broadcast** nhằm cải tiến tốc độ và hiệu quả của hệ thống. Nói cách khác, **VLAN** là một nhóm logic các thiết bị hoặc người sử dụng. Nhóm logic này được chia dựa vào chức năng, ứng dụng, … mà không phụ thuộc vào vị trí địa lý. Chỉ có các thiết bị trong cùng **VLAN** mới liên lạc được với nhau. Nếu muốn các **VLAN** có thể liên lạc được với nhau thì phải sử dụng **Router** để liên kết các **VLAN** lại.



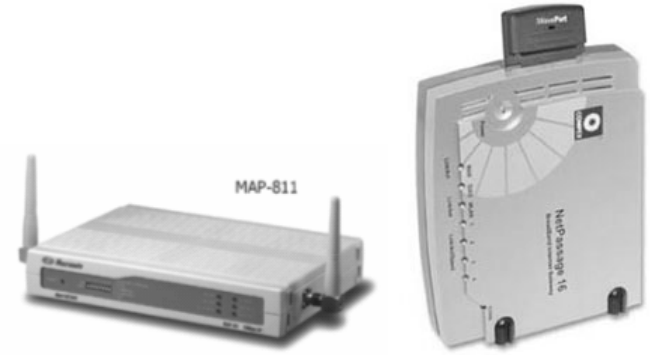
Hình 4.31 – Mô tả cách sử dụng **VLAN**.

- **Spanning Tree**: tạo đường dự phòng, bình thường dữ liệu được truyền trên một cổng mang số thứ tự thấp. Khi mất liên lạc thiết bị tự chuyển sang cổng khác, nhằm đảm bảo mạng hoạt động liên tục. **Spanning Tree** thực chất là hạn chế các đường dư thừa trên mạng.

Hình dưới là **Switch Compex** SRX2216 được thiết kế theo chuẩn IEEE 802.3, IEEE802.3u, **Switch** này thường dùng trong các giải pháp mạng vừa và nhỏ. Thiết bị này hỗ trợ 16 port RJ45 tốc độ 10/100Mbps, 12K **MAC Address**, 2K bộ đệm (**buffer**). Ngoài ra thiết bị này còn có những tính năng như: **Store and Forward**, **Spanning Tree**, **Port Trunking**, **Virtual LAN** giúp chúng ta mở rộng mạng mà không sợ xảy ra đụng độ (**collision**).

Hình 4.31 - **Switch Compex SRX2216**.

IV.8. Wireless Access Point.



Hình 4.32 – Thiết bị Wireless

Wireless Access Point là thiết bị kết nối mạng không dây được thiết kế theo chuẩn IEEE802.11b, cho phép nối **LAN to LAN**, dùng cơ chế **CSMA/CA** để giải quyết tranh chấp, dùng cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**, mã hóa theo 64/128 Bit. Nó còn hỗ trợ tốc độ truyền không dây lên 11Mbps trên băng tần 2,4GHz ISM dùng công nghệ **radio DSSS** (**Direct Sequence Spread Spectrum**)

Hình 4.33 – Mạng sử dụng **Wireless**.

IV.9. Router.

Là thiết bị dùng nối kết các mạng **logic** với nhau, kiểm soát và lọc các gói tin nên hạn chế được lưu lượng trên các mạng **logic** (thông qua cơ chế **Access-list**). Các **Router** dùng bảng định tuyến (**Routing table**) để lưu trữ thông tin về mạng dùng trong trường hợp tìm đường đi tối ưu cho các gói tin. Bảng định tuyến chứa các thông tin về đường đi, thông tin về ước lượng thời gian, khoảng cách… Bảng này có thể cấu hình tĩnh hay tự động. **Router** hiểu được địa chỉ logic **IP** nên thông thường **Router** hoạt động ở lớp mạng (**network**) hoặc cao hơn.

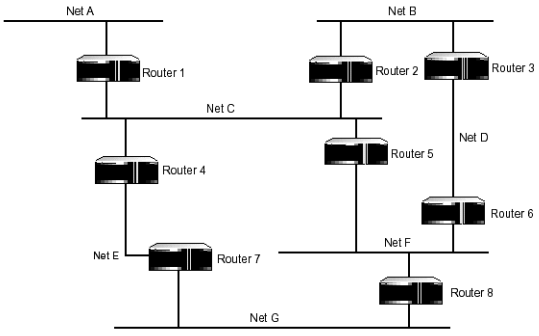
Người ta cũng có thể thực hiện **firewall** ở mức độ đơn giản trên **Router** thông qua tính năng **Access-list** (tạo một danh sách truy cập hợp lệ), thực hiện việc ánh xạ địa chỉ thông qua tính năng **NAT** (chuyển đổi địa chỉ).

Khi một gói tin đến **Router**, **Router** sẽ thực hiện các việc kiểm tra địa chỉ **IP** đích của gói tin:

- Nếu địa chỉ mạng của **IP** đích này có trong bảng định tuyến của **Router**, **Router** sẽ gởi ra port tương ứng.
- Nếu địa chỉ mạng của **IP** đích này không có trong bảng định tuyến, **Router** sẽ kiểm tra xem trong bảng định tuyến của mình có khai báo **Default Gateway** hay không:
    + Nếu có khai báo **Default Gateway** thì gói tin sẽ được **Router** đưa đến **Default Gateway** tương ứng.
    + Nếu không có khai báo **Default Gateway** thì gói tin sẽ bị loại bỏ.

Chú ý: địa chỉ được xét ở đây là địa chỉ **IP**.

Do cách hoạt động của **Router** như đã trình bày, nên mỗi **port** của **Router** là một **Broadcast Domain**.



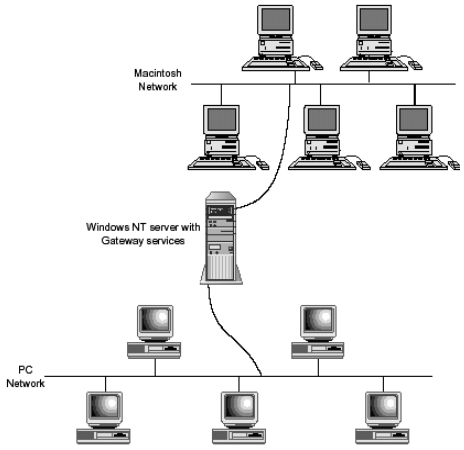
Hình 4.34 – Mô hình mạng sử dụng **Router**.

IV.10. Thiết bị mở rộng.

IV.10.1 Gateway – Proxy:

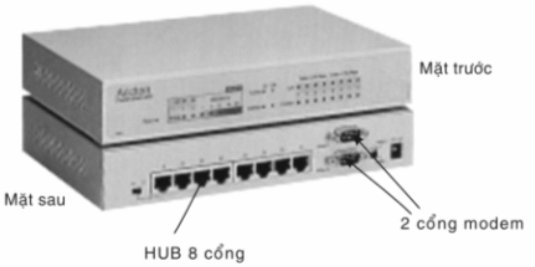
Là thiết bị trung gian dùng để nối kết mạng nội bộ bên trong và mạng bên ngoài. Nó có chức năng kiểm soát tất cả các luồng dữ liệu đi ra và vào mạng nhằm ngăn chặn **hacker** tấn công. **Gateway** cũng hỗ trợ chuyển đổi giữa các giao thức khác nhau, các chuẩn dữ liệu khác nhau (ví dụ **IP/IPX**).

Proxy giống như một **firewall** (bức tường lửa), nâng cao khả năng bảo mật giữa mạng nội bộ bên trong và mạng bên ngoài. **Proxy** cho phép thiết lập các danh sách được phép truy cập vào mạng nội bộ bên trong, cũng như danh sách các ứng dụng mà mạng nội bộ bên trong có thể truy cập ra mạng bên ngoài. Ngoài ra **Proxy** còn là máy đại điện cho các máy trạm bên trong mạng nội bộ truy cập ra Internet, đây là chức năng quan trọng nhất của **Proxy**.



Hình 4.35 – Mô hình mạng sử dụng **Gateway**.

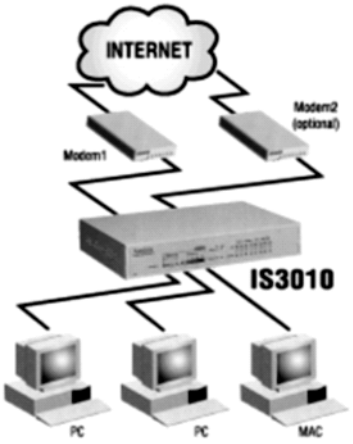
IV.10.2 Thiết bị truy cập Internet.



Hình 4.36 - Thiết bị IS3010

Có nhiều thiết bị dùng để truy cập **Internet**. Hình vẽ trên là một trong những thiết bị vừa cho phép chia sẻ **Internet**, vừa cho phép nâng cao tốc độ đường truyền thông qua việc sử dụng 02 modem cùng một lúc.

Ứng dụng: nhiều máy tính (**LAN**) truy cập **Internet** chung một **account** qua hai **Modem**.



Hình 4.37 – Truy cập **Internet** bằng thiết bị IS3010.

Thiết bị này cấu hình rất đơn giản dùng **Web browser**, **Telnet**, **Console**. Có hai cổng **Modem** cho phép **dial out** hoặc **dial in**, tích hợp sẵn dịch vụ **NAT**, **Default GateWay**, **DHCP** dùng cấp phát **IP** động cho các máy trạm. Hỗ trợ cả hai nghi thức thẩm định quyền truy cập **PAP/CHAP**, hỗ trợ **Filter** (cho hoặc cấm người dùng truy cập **Internet**).

Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về các kiến trúc và công nghệ mạng LAN …	I. Các kiến trúc mạng. II. Các công nghệ mạng LAN.	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

I. CÁC KIẾN TRÚC MẠNG (TOPOLOGY).

I.1. Khái niệm.

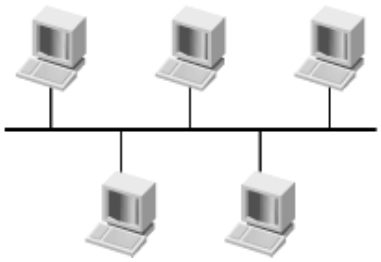
Network topology là sơ đồ dùng biểu diễn các kiểu sắp xếp, bố trí vật lý của máy tính, dây cáp và những thành phần khác trên mạng theo phương diện vật lý.

Có hai kiểu kiến trúc mạng chính là: kiến trúc vật lý (mô tả cách bố trí đường truyền thực sự của mạng), kiến trúc logic (mô tả con đường mà dữ liệu thật sự di chuyển qua các node mạng)

I.2. Các kiểu kiến trúc mạng chính.

Mạng Bus (tuyến)

- Kiến trúc **Bus** là một kiến trúc cho phép nối mạng các máy tính đơn giản và phổ biến nhất. Nó dùng một đoạn cáp nối tất cả máy tính và các thiết bị trong mạng thành một hàng. Khi một máy tính trên mạng gởi dữ liệu dưới dạng tín hiệu điện thì tín hiệu này sẽ được lan truyền trên đoạn cáp đến các máy tính còn lại, tuy nhiên dữ liệu này chỉ được máy tính có địa chỉ so khớp với địa chỉ mã hóa trong dữ liệu chấp nhận. Mỗi lần chỉ có một máy có thể gởi dữ liệu lên mạng vì vậy số lượng máy tính trên bus càng tăng thì hiệu suất thi hành mạng càng chậm.
- Hiện tượng dội tín hiệu: là hiện tượng khi dữ liệu được gởi lên mạng, dữ liệu sẽ đi từ đầu cáp này đến đầu cáp kia. Nếu tín hiệu tiếp tục không ngừng nó sẽ dội tới lui trong dây cáp và ngăn không cho máy tính khác gởi dữ liệu. Để giải quyết tình trạng này người ta dùng một thiết bị terminator (điện trở cuối) đặt ở mỗi đầu cáp để hấp thu các tín hiệu điện tự do.
- *Ưu điểm*: kiến trúc này dùng ít cáp, dễ lắp đặt, giá thành rẻ. Khi mở rộng mạng tương đối đơn giản, nếu khoảng cách xa thì có thể dùng repeater để khuếch đại tín hiệu.
- *Khuyết điểm*: khi đoạn cáp đứt đôi hoặc các đầu nối bị hở ra thì sẽ có hai đầu cáp không nối với terminator nên tín hiệu sẽ dội ngược và làm cho toàn bộ hệ thống mạng sẽ ngưng hoạt động. Những lỗi như thế rất khó phát hiện ra là hỏng chỗ nào nên công tác quản trị rất khó khi mạng lớn (nhiều máy và kích thước lớn).

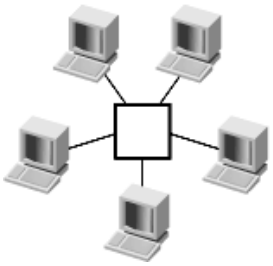


Hình vẽ 5.1 – Kiến trúc mạng **Bus**.

Mạng star (sao)

- Trong kiến trúc này, các máy tính được nối vào một thiết bị đấu nối trung tâm (**Hub** hoặc **Switch**). Tín hiệu được truyền từ máy tính gởi dữ liệu qua hub tín hiệu được khuếch đại và truyền đến tất cả các máy tính khác trên mạng.

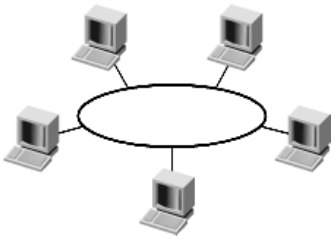
- *Ưu điểm*: kiến trúc star cung cấp tài nguyên và chế độ quản lý tập trung. Khi một đoạn cáp bị hỏng thì chỉ ảnh hưởng đến máy dùng đoạn cáp đó, mạng vẫn hoạt động bình thường. Kiến trúc này cho phép chúng ta có thể mở rộng hoặc thu hẹp mạng một cách dễ dàng.
- *Khuyết điểm*: do mỗi máy tính đều phải nối vào một trung tâm điểm nên kiến trúc này đòi hỏi nhiều cáp và phải tính toán vị trí đặt thiết bị trung tâm. Khi thiết bị trung tâm điểm bị hỏng thì toàn bộ hệ thống mạng cũng ngừng hoạt động.



Hình 5.2 – Kiến trúc mạng **Star**.

Mạng Ring (vòng)

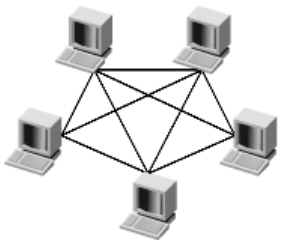
- Trong mạng ring các máy tính và các thiết bị nối với nhau thành một vòng khép kín, không có đầu nào bị hở. Tín hiệu được truyền đi theo một chiều và qua nhiều máy tính. Kiến trúc này dùng phương pháp chuyển thẻ bài (**token passing**) để truyền dữ liệu quanh mạng.
- Phương pháp chuyển thẻ bài là phương pháp dùng thẻ bài chuyển từ máy tính này sang máy tính khác cho đến khi tới máy tính muốn gởi dữ liệu. Máy này sẽ giữ thẻ bài và bắt đầu gởi dữ liệu đi quanh mạng. Dữ liệu chuyển qua từng máy tính cho đến khi tìm được máy tính có địa chỉ khớp với địa chỉ trên dữ liệu. Máy tính đầu nhận sẽ gởi một thông điệp cho máy tính đầu gởi cho biết dữ liệu đã được nhận. Sau khi xác nhận máy tính đầu gởi sẽ tạo thẻ bài mới và thả lên mạng. Vận tốc của thẻ bài xấp xỉ với vận tốc ánh sáng.



Hình 5.3 – Kiến trúc mạng **Ring**.

Mạng Mesh (lưới).

Từng cặp máy tính thiết lập các tuyến kết nối liên điểm do đó số lượng tuyến kết nối nhanh chóng gia tăng khi số lượng máy tính trong mạng tăng lên nên người ta ít dùng cho các mạng lưới lớn.



Hình 5.4 – Kiến trúc mạng **Mesh**.

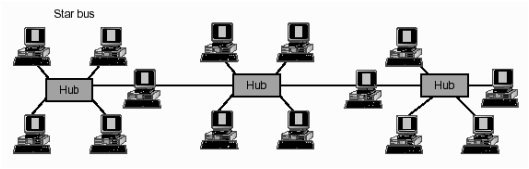
Mạng Cellular (tế bào).

Các mạng tế bào chia vùng địa lý đang được phục vụ thành các tế bào, mỗi tế bào được một trạm trung tâm phục vụ. Các thiết bị sử dụng các tín hiệu radio để truyền thông với trạm trung tâm, và trạm trung tâm sẽ định tuyến các thông điệp đến các thiết bị. Ví dụ điển hình của mạng tế bào là mạng điện thoại di động.

I.3. Các kiến trúc mạng kết hợp.

Mạng star bus.

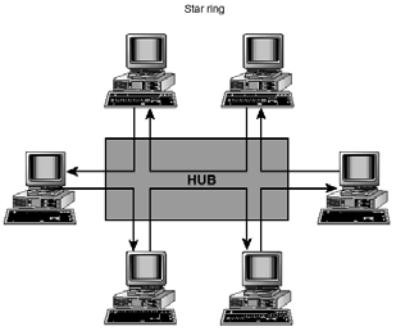
Star bus là mạng kết hợp giữa mạng **star** và mạng **bus**. Trong kiến trúc này một vài mạng có kiến trúc hình **star** được nối với trục cáp chính (**bus**). Nếu một máy tính nào đó bị hỏng thì nó không ảnh hưởng đến phần còn lại của mạng. Nếu một **Hub** bị hỏng thì toàn bộ các máy tính trên **Hub** đó sẽ không thể giao tiếp được.



Hình 5.5 – Kiến trúc mạng **Star-Bus**.

Mạng star ring.

Mạng **Star Ring** tương tự như mạng **Star Bus**. Các **Hub** trong kiến trúc **Star Bus** đều được nối với nhau bằng trục cáp thẳng (**bus**) trong khi **Hub** trong cấu hình **Star Ring** được nối theo dạng hình **Star** với một **Hub** chính.



Hình 5.6 – Kiến trúc mạng **Star-Ring**.

II. CÁC CÔNG NGHỆ MẠNG LAN.

II.1. Khái niệm.

- **Collision Domain**: đây là một vùng có khả năng bị đụng độ do hai hay nhiều máy tính cùng gởi tín hiệu lên môi trường truyền thông.
- **Broadcast Domain**: đây là một vùng mà gói tin phát tán (gói tin **broadcast**) có thể đi qua được. Trong vùng **Broadcast Domain** có thể là vùng bao gồm nhiều **Collision Domain**.

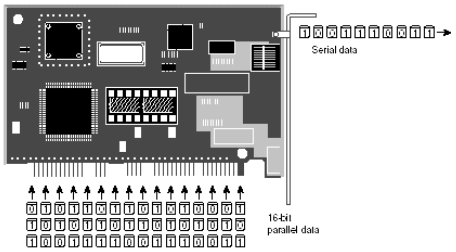
II.2. Ethernet

Đầu tiên, **Ethernet** được phát triển bởi các hãng **Xerox**, **Digital**, **Intel** vào đầu những năm 1970. Phiên bản đầu tiên của **Ethernet** được thiết kế như một hệ thống 2,94 Mbps để nối hơn 100 máy tính vào một sợi cáp dài 1 Km. Sau đó các hãng lớn đã thảo luận và đưa ra chuẩn dành cho **Ethernet** 10 Mbps.

Ethernet chuẩn thường có cấu hình bus, truyền với tốc độ 10Mbps và dựa vào **CSMA/CD** (**Carrier Sense Multiple Access** / **Collision Detection**) để điều chỉnh lưu thông trên đường cáp chính. Tóm lại những đặc điểm cơ bản của **Ethernet** như sau:

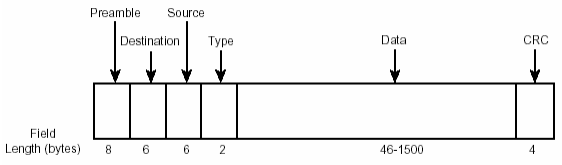
- Cấu hình: **bus** hoặc **star**.
- Phương pháp chia sẻ môi trường truyền: **CSMA/CD**.
- Quy cách kỹ thuật IEEE 802.3
- Vận tốc truyền: 10 – 100 Mbps.
- Cáp: cáp đồng trục mảnh, cáp đồng trục lớn, cáp **UTP**.
- Tên của chuẩn **Ethernet** thể hiện 3 đặc điểm sau:
- Con số đầu tiên thể hiện tốc độ truyền tối đa.
- Từ tiếp theo thể hiện tín hiệu dải tần cơ sở được sử dụng (Base hoặc Broad).
    + **Ethernet** dựa vào tín hiệu **Baseband** sẽ sử dụng toàn bộ băng thông của phương tiện truyền dẫn. Tín hiệu dữ liệu sẽ được truyền trực tiếp trên phương tiện truyền dẫn mà không cần thay đổi kiểu tín hiệu.
    + Trong tín hiệu Br**o**adband (**ethernet** không sử dụng), tín hiệu dữ liệu không bao giờ gởi trực tiếp lên phương tiện truyền dẫn mà phải thực hiện điều chế.
- Các ký tự còn lại thể hiện loại cáp được sử dụng. Ví dụ: chuẩn 10Base2, tốc độ truyền tối đa là 10Mbps, sử dụng tín hiệu **Baseband**, sử dụng cáp **Thinnet**.

Card mạng **Ethernet**: hầu hết các **NIC** cũ đều được cấu hình bằng các **jump** (các chấu cắm chuyển) để ấn định địa chỉ và ngắt. Các **NIC** hiện hành được cấu hình tự động hoặc bằng một chương trình chạy trên máy chứa card mạng, nó cho phép thay đổi các ngắt và địa chỉ bộ nhớ lưu trữ trong một chip bộ nhớ đặc biệt trên **NIC**.



Hình 5.7 – Card mạng **Ethernet**.

Dạng thức khung trong **Ethernet**: **Ethernet** chia dữ liệu thành nhiều khung (**frame**). Khung là một gói thông tin được truyền như một đơn vị duy nhất. Khung trong **Ethernet** có thể dài từ 64 đến 1518 byte, nhưng bản thân khung **Ethernet** đã sử dụng ít nhất 18 byte, nên dữ liệu một khung **Ethernet** có thể dài từ 46 đến 1500 byte. Mỗi khung đều có chứa thông tin điều khiển và tuân theo một cách tổ chức cơ bản. Ví dụ khung **Ethernet** (dùng cho TCP/IP) được truyền qua mạng với các thành phần sau:



Hình 5.8 – Cấu trúc khung **Ethernet**.

Các trường trong **Frame Ethernet**:

- **Preamble**: 8 byte mở đầu.
- **Destination**: 6 byte thể hiện địa chỉ **MAC** đích.
- **Source**: 6 byte thể hiện địa chỉ **MAC** nguồn.
- **Type**: 2 byte thể hiện kiểu giao thức ở tầng trên.
- **Data**: dữ liệu của **Frame**.
- **CRC**: 4 byte dùng để kiểm lỗi của **Frame**.

Các loại **Ethernet** với băng tần cơ sở:

- 10Base2: tốc độ 10, chiều dài cáp nhỏ hơn 200 m, dùng cáp **thinnet** (cáp đồng trục mảnh).
- 10Base5: tốc độ 10, chiều dài cáp nhỏ hơn 500 m, dùng cáp **thicknet** (cáp đồng trục dày).
- 10BaseT: tốc độ 10, dùng cáp xoắn đôi (**Twisted-Pair**).
- 10BaseFL: tốc độ 10, dùng cáp quang (**Fiber optic**).
- 100BaseT: tốc độ 100, dùng cáp xoắn đôi (**Twisted-Pair**).
- 100BaseX: tốc độ 100, dùng cho **multiple media type**.
- 100VG-AnyLAN: tốc độ 100, dùng **voice grade**.

II.2.1 Chuẩn 10Base2

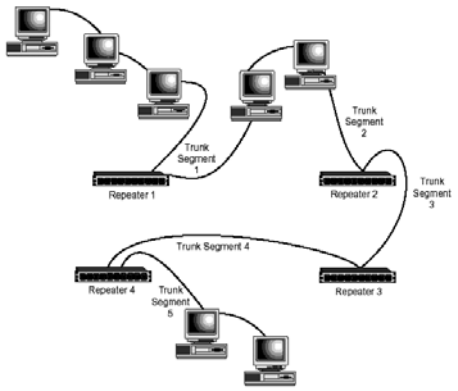
Cấu hình này được xác định theo tiêu chuẩn IEEE 802.3 và bảo đảm tuân thủ các quy tắc sau:

- Khoảng cách tối thiểu giữa hai máy trạm phải cách nhau 0.5m.

- Dùng cáp **Thinnet** (RG-58).

- Tốc độ 10 Mbps.
- Dùng đầu nối chữ T (**T-connector**).
- Không thể vượt quá phân đoạn mạng tối đa là 185m. Toàn bộ hệ thống cáp mạng không thể vượt quá 925m.
- Số nút tối đa trên mỗi phân đoạn mạng là 30.
- **Terminator** (thiết bị đầu cuối) phải có trở kháng 50 ohm và được nối đất.
- Mỗi mạng không thể có trên năm phân đoạn. Các phân đoạn có thể nối tối đa bốn bộ khuếch đại và chỉ có ba trong số năm phân đoạn có thể có nút mạng (tuân thủ quy tắc 5-4-3).

Quy tắc 5-4-3: quy tắc này cho phép kết hợp đến năm đoạn cáp được nối bởi 4 bộ chuyển tiếp, nhưng chỉ có 3 đoạn là nối trạm. Theo hình trên ta thấy đoạn 3, 4 chỉ tồn tại nhằm mục đích làm tăng tổng chiều dài mạng và cho phép máy tính trên đoạn 1, 2, 5 nằm cùng trên một mạng.



Hình 5.9 – Qui tắc 5-4-3.

Ưu điểm chuẩn 10Base2: giá thành rẻ, đơn giản.

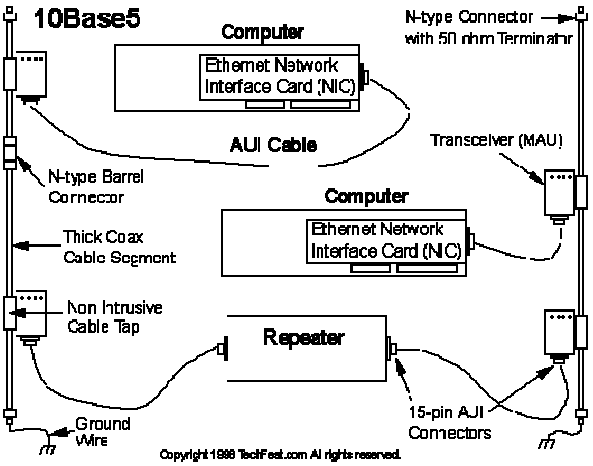
II.2.2 Chuẩn 10Base5

Chuẩn mạng này tuân theo các quy tắc sau:

- Khoảng cách tối thiểu giữa hai nút là 2.5m.
- Dùng cáp **thicknet** (cáp đồng dày).
- Băng tần cơ sở 10Mbps.
- Chiều dài phân đoạn mạng tối đa là 500m.
- Toàn bộ chiều dài mạng không thể vượt quá 2500m.
- Thiết bị đầu cuối (**terminator**) phải được nối đất.
- Cáp thu phát (**tranceiver cable**), nối từ máy tính đến bộ thu phát, có chiều dài tối đa 50m.
- Số nút tối đa cho mỗi phân đoạn mạng là 100 (bao gồm máy tính và tất cả các **repeater**).
- Tuân theo quy tắc 5-4-3.

Ưu điểm: khắc phục được khuyết điểm của mạng 10Base2, hỗ trợ kích thước mạng lớn hơn.

Chú ý: trong các mạng lớn người ta thường kết hợp cáp dày và cáp mảnh. Cáp dày dùng làm cáp chính rất tốt, còn cáp mảnh dùng làm đoạn nhánh.



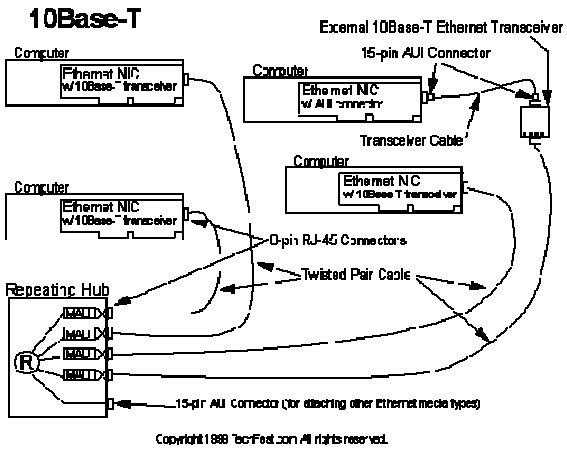
Hình 5.10 - Một ví dụ về chuẩn 10Base5.

II.2.3 Chuẩn 10BaseT.

Chuẩn mạng này tuân theo các quy tắc sau:

- Dùng cáp UTP loại 3, 4, 5 hoặc **STP**, có mức trở kháng là 85-115 ohm, ở 10Mhz.
- Dùng quy cách kỹ thuật 802.3.
- Dùng thiết bị đấu nối trung tâm **Hub**.
- Tốc độ tối đa 10Mbps.
- Dùng đầu nối RJ-45.
- Số nút tối đa là 512 và chúng có thể nối vào 3 phân đoạn bất kỳ với năm phân tuyến tối đa có sẵn.
- Chiều dài tối đa một phân đoạn cáp là 100m.
- Dùng mô hình vật lý **star**.
- Có thể nối các phân đoạn mạng 10BaseT bằng cáp đồng trục hay cáp quang.
- Số lượng máy tính tối đa là 1024.
- Khoảng cách tối thiểu giữa hai máy tính là 2,5m.
- Khoảng cách cáp tối thiểu từ một **Hub** đến một máy tính hoặc một **Hub** khác là 0,5m.

Ưu điểm: do trong mạng 10BaseT dùng thiết bị đấu nối trung tâm nên dữ liệu truyền tin cậy hơn, dễ quản lý. Điều này cũng tạo thuận lợi cho việc định vị và sửa chữa các phân đoạn cáp bị hỏng. Chuẩn này cho phép bạn thiết kế và xây dựng trên từng phân đoạn một trên LAN và có thể tăng dần khi mạng cần phát triển. 10BaseT cũng tương đối rẻ tiền so với các phương án đấu cáp khác.



Hình 5.11 – Một ví dụ về chuẩn 10BaseT.

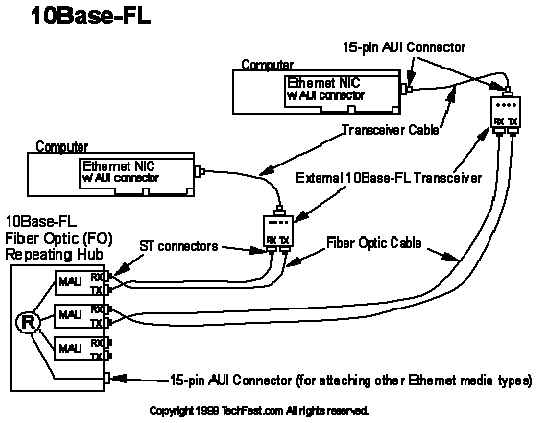
II.2.4 Chuẩn 10BaseFL.

Các đặc điểm của 10BaseFL:

- Tốc độ tối đa 10 Mbps.
- Truyền qua cáp quang.

Ưu điểm:

- Do dùng cáp quang nối các **Repeater** nên khoảng cách tối đa cho một đoạn cáp là 2000m.
- Không sợ bị nhiễu điện từ.
- Số nút tối đa trên một đoạn cáp lớn hơn nhiều so với 10Base2, 10Base5, 10BaseT.



Hình 5.12 – Một ví dụ về chuẩn 10Base-FL.

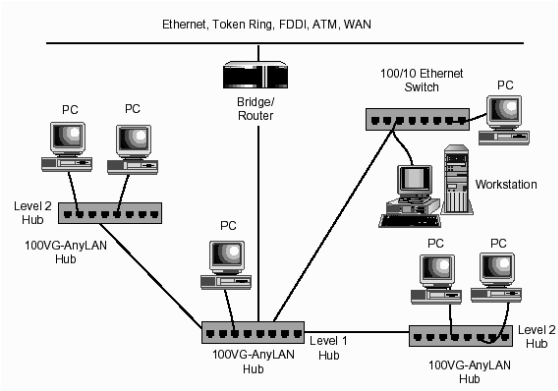
II.2.5 Chuẩn 100VG-AnyLAN.

100VG (Voice Grade) **AnyLan** là công nghệ mạng kết hợp các thành phần của **Ethernet** và **Token Ring**, dùng quy cách kỹ thuật 802.12. Các đặc điểm kỹ thuật:

- Tốc độ truyền dữ liệu tối thiểu là 100Mbps.

- Sử dụng cáp xoắn đôi gồm bốn cặp xoắn (**UTP** loại 3, 4, 5 hoặc **STP**) và cáp quang.

- Khả năng hỗ trợ sàng lọc từng khung có địa chỉ tại **Hub** nhằm tăng cường tính năng bảo mật.
- Chấp nhận cả khung **Ethernet** lẫn gói **Token Ring**.
- Định nghĩa trong IEEE 802.12.
- Mô hình vật lý: **cascaded star**, mọi máy tính được nối với một **Hub**. Có thể mở rộng mạng bằng cách thêm **Hub** con vào **Hub** trung tâm, **Hub** con đóng vai trò như máy tính đối với **Hub** mẹ.
- Chiều dài tối đa của đoạn chạy cáp nối hai **Hub** là 250m.

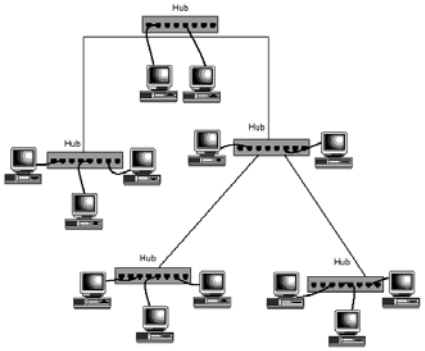


Hình 5.13 – Một ví dụ về chuẩn 100VG-AnyLAN.

II.2.6 Chuẩn 100BaseX.

Tiêu chuẩn 100BaseX **Ethernet** còn gọi là **Fast Ethernet** là sự mở rộng của tiêu chuẩn **Ethernet** có sẵn. Tiêu chuẩn này dùng cáp **UTP Cat5** và phương pháp truy cập **CSMA/CD** trong cấu hình **star bus** với mọi đoạn cáp nối vào một **Hub** tương tự 10BaseT. Tốc độ 100Mbps. Chuẩn 100BaseX có các đặc tả ứng với các loại đường truyền khác nhau:

- 100BaseT4: dùng cáp **UTP** loại 3, 4, 5 có bốn cặp xoắn đôi.
- 100BaseTX: dùng cáp **UTP** loại 5 có hai cặp xoắn đôi hoặc **STP**.
- 100BaseFX: dùng cáp quang có hai dây lõi.



Hình 5.14 – Một ví dụ về chuẩn 100Base-X.

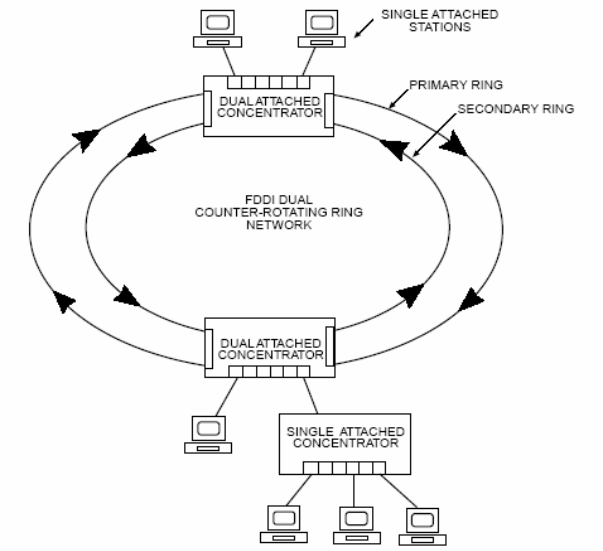
Bảng dưới đây sẽ tóm tắt lại các thông số của một số loại cáp.

Chuẩn	Loại cáp	Chiều dài tối đa	Đầu nối
10Base2	Thinnet	185m	BNC
10Base5	Thicknet	500m	AUI
10Base-T	UTP cat 3-4-5, 2 cặp dây	100m	RJ45
100Base-TX	UTP cat 5, 2 cặp dây	100m	RJ45
100Base-FX	Cáp quang Multimode, lõi 62.5 hoặc 125 micro	400m	MIC, ST, SC
1000Base-CX	STP	25m	RJ45
1000Base-T	UTP cat 5, 4 cặp dây	100m	RJ45
1000Base-SX	Cáp quang Multimode, lõi 62.5 hoặc 50 micro	62.5 micro thì được 275m 50 micro thì được 550m	SC
1000Base-LX	Cáp quang Multimode, lõi 62.5 hoặc 50 micro Cáp quang Singlemode, lõi 9 micro	62.5 micro thì được 440m 50 micro thì được 550m 9 micro thì được 3-10Km	SC

II.3. FDDI.

Một trong những bất lợi chính của các mạng vòng tín bài là sự nhạy cảm của chúng với bất trắc. Vì mỗi máy gắn trên vòng phải chuyển khung cho máy kế nên một hỏng hóc trên máy sẽ làm cho toàn mạng ngưng hoạt động. Phần cứng vòng tín bài thường được thiết kế để tránh những hư hỏng như thế. Tuy nhiên hầu hết các mạng vòng tín bài không thể vượt qua khi sự kết nối bị cắt như khi đường cáp nối hai máy bỗng nhiên bị đứt.

Một số công nghệ mạng vòng đã được thiết kế để khắc phục được hỏng hóc nghiêm trọng. Ví dụ **FDDI** (**Fiber Distributed Data Interconnection**) là công nghệ mạng vòng tín bài có thể truyền dữ liệu ở tốc độ 100 triệu bit/giây, nhanh gấp 8 lần mạng vòng tín bài **IBM**, và nhanh hơn 10 lần mạng **Ethernet**. Để cung ứng tốc độ dữ liệu nhanh như vậy, **FDDI** dùng sợi quang để nối các máy thay cho cáp đồng.

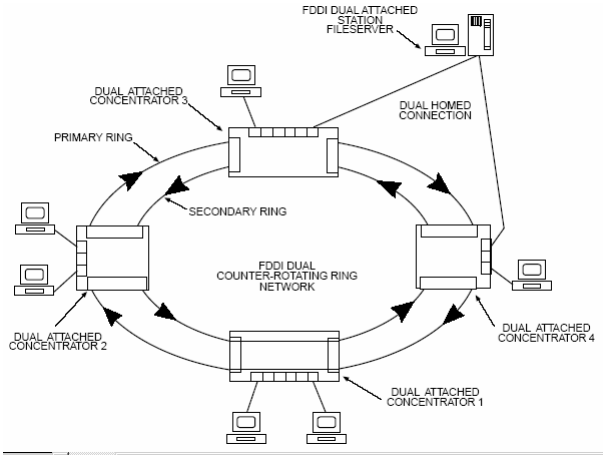


Hình 5.14 - Mạng **FDDI**.

Mạng **FDDI** sử dụng cáp quang có đặc điểm sau:

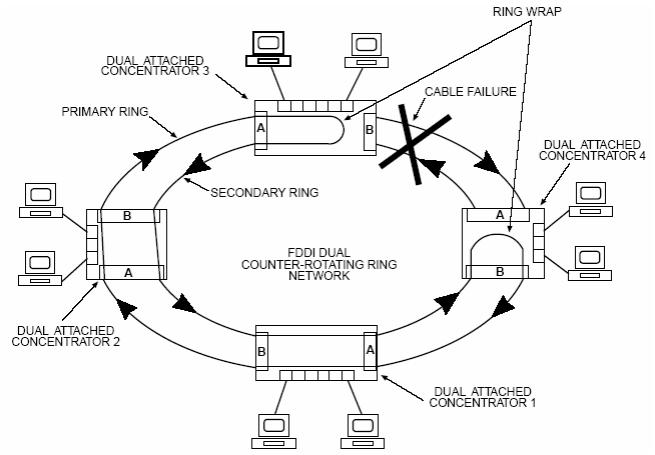
- Chiều dài của cáp: chiều dài tối đa của cáp (2 vòng) là 100Km, nếu cáp (1 vòng) thì chiều dài tối đa là 200Km.
- Số trạm trên mạng: có khả năng hỗ trợ 500 máy trong một mạng.
- Bảo mật: chỉ bị nghe lén khi vòng cáp bị đứt.
- Nhiễu điện từ: không bị nhiễu điện từ.

FDDI dùng tính năng dự phòng để khắc phục sự cố. Một mạng **FDDI** gồm hai vòng - một dùng để gởi dữ liệu khi mọi việc đều ổn, và chỉ sử dụng vòng thứ hai khi vòng một hỏng. Về mặt vật lý, hai đường nối với một cặp máy tính là không hoàn toàn cách biệt. Mỗi sợi quang được bọc trong một vỏ nhựa dẻo và có một vỏ bọc cặp sợi bao bên ngoài tương tự như các đường dây điện trong nhà. Vì vậy có thể lắp đặt hai vòng cùng một lúc.



Hình 5.15 – Sơ đồ hoạt động của mạng **FDDI**.

Điều thú vị là các vòng trong mạng **FDDI** được gọi là xoay ngược (**counter rotating**) vì dữ liệu chạy trong vòng thứ hai ngược lại với hướng dữ liệu vòng thứ nhất. Để hiểu tại sao lại dùng các vòng xoay ngược, hãy xét trường hợp có sự cố nghiêm trọng xảy ra. Thứ nhất vì cặp sợi nối hai trạm thường đi trên cùng đường nên khi đứt một sợi thì thường là đứt luôn sợi kia. Thứ hai, nếu dữ liệu luôn luôn đi theo một hướng trên cả hai sợi, việc ngắt một trạm ra khỏi vòng (ví dụ khi di chuyển máy) sẽ ngắt truyền thông các máy khác. Tuy nhiên, nếu dữ liệu chuyển theo hướng ngược lại ở đường dự trữ, các trạm còn lại có thể cấu hình mạng để sử dụng đường dự phòng.



Hình vẽ 5.16 – Khi cáp giữa hai máy kế tiếp bị đứt.

Phương pháp truy cập mà mạng **FDDI** sử dụng là phương pháp **Token-Ring**. Thẻ **Token** là một **Frame** đặc biệt, chạy xoay vòng trên đường mạng. Khi máy trạm cần truyền dữ liệu, nó sẽ bắt thẻ **Token**, sau khi bắt được thẻ thì nó bắt đầu truyền dữ liệu, sau khi truyền dữ liệu xong thì nó sẽ giải phóng thẻ **Token**. Chỉ có máy trạm nào giữ thẻ **Token** mới được phép truyền dữ liệu lên trên đường mạng.

Tóm tắt

Lý thuyết 6 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về các lớp con LLC, MAC của lớp 2 và các giao thức TCP, UDP, khái niệm port, đặc biệt là các mô hình firewall …	I. Khảo sát chi tiết lớp 2. II. Khảo sát chi tiết lớp 3. III. Khảo sát chi tiết lớp 4. IV. Các mô hình Firewall.	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

I. KHẢO SÁT CHI TIẾT LỚP 2 (DATA LINK).

Lớp 1 liên quan đến môi trường, liên quan các tín hiệu, các luồng bit di chuyển trên môi trường, các thành phần dựa dữ liệu ra môi trường và các cấu hình khác nhau. Nó thực hiện vai trò thiết yếu cho hoạt động truyền tin khả thi giữa các máy tính, nhưng với nỗ lực một mình của nó thì không đủ. Mỗi chức năng có các hạn chế của nó. Lớp 2 hướng tới khắc phục hạn chế này. Ứng với mỗi hạn chế trong lớp 1, lớp 2 có một giải pháp. Ví dụ lớp 1 không thể thông tin với các lớp trên, lớp 2 làm việc này thông qua **LLC** (**Logical Link Control**). Lớp 1 không đặt tên hay định danh cho máy tính thì lớp 2 dùng một lược đồ địa chỉ. Lớp 1 không thể quyết định máy tính nào sẽ truyền dữ liệu nhị phân từ một nhóm cùng muốn truyền tại cùng một thời điểm. Lớp 2 dùng một hệ thống gọi là **MAC** (**Media Access Control**).

I.1. Lớp con LLC.

Lớp con **LCC** tạo ra tính năng linh hoạt trong việc phục vụ cho các giao thức lớp mạng trên nó, trong khi vẫn liên lạc hiệu quả với các kỹ thuật khác nhau bên dưới nó. **LLC** với vai trò là lớp phụ tham gia vào quá trình đóng gói. **LLC** nhận đơn vị dữ liệu giao thức lớp mạng, như là các gói **IP**, và thêm nhiều thông tin điều khiển vào để giúp phân phối gói IP đến đích của nó. Nó thêm hai thành phần địa chỉ của đặc tả 802.2 điểm truy xuất dịch vụ đích **DSAP** (**Destination Service Access Point**) và điểm truy xuất dịch vụ nguồn **SSAP** (**Source Service Access Point**). Nó đóng gói trở lại dạng **IP**, sau đó chuyển xuống lớp phụ **MAC** để tiến hành các kỹ thuật đặc biệt được yêu cầu cho đóng gói tiếp theo. Lớp phụ **LLC** quản lý hoạt động thông tin giữa các thiết bị qua một liên kết đơn trên một mạng. **LLC** được định nghĩa trong đặc tả **IEEE 802.2** và hỗ trợ các dịch vụ kết nối có cả tạo cầu nối và không tạo cầu nối, được dùng bởi các giao thức lớp cao hơn. **IEEE 802.2** định nghĩa ra một số **field** trong các **frame** của lớp liên kết dữ liệu cho phép nhiều giao thức lớp cao hơn chia sẻ một liên kết vật lý đơn.

I.2. Lớp con MAC.

Lớp con **MAC** đề cập đến các giao thức chủ yếu phải theo để truy xuất vào môi trường vật lý. Tóm lại, lớp 2 có 4 khái niệm chính mà cần phải biết:

- Lớp 2 thông tin với các lớp trên thông qua **LLC**.
- Lớp 2 dùng chuẩn địa chỉ hóa ngang bằng (đó là gán các định danh duy nhất-các địa chỉ).
- Lớp 2 dùng kỹ thuật đóng frame để tổ chức hay nhóm dữ liệu.
- Lớp 2 dùng **MAC** để chọn máy tính nào sẽ truyền các dữ liệu nhị phân, từ một nhóm trong đó tất cả các máy tính đều muốn truyền cùng một lúc.

I.3. Quá trình tìm địa chỉ MAC:

Với mạng **TCP/I**P, thì gói tin phải chứa cả địa chỉ **MAC** đích và địa chỉ **IP** đích. Nếu một trong hai địa chỉ này không đúng thì gói tin cũng xem như là không gởi được đến đích. **ARP** là một giao thức dùng để tìm địa chỉ MAC của một thiết bị mạng dựa trên địa chỉ **IP** đã biết.

Một vài thiết bị có lưu trữ bảng chứa địa chỉ **IP** và địa chỉ **MAC** tương ứng với **IP** đó (của các thiết bị trong cùng mạng **LAN** với nó). Bảng này được gọi là bảng **ARP**. Bảng **ARP** này được lưu giữ trong

RAM, và khi thiết bị gởi gói tin lên mạng thì nó sử dụng thông tin trong bảng **ARP** này.

Có 2 cách để thu thập thông tin cho bảng địa chỉ **MAC**.

- Khi có một gói tin được gởi trên đường truyền, thiết bị luôn kiểm tra địa chỉ đích của gói tin (địa chỉ **IP** và địa chỉ **MAC**) có phải là của mình hay không? Sau khi kiểm tra, địa chỉ **IP** và địa chỉ **MAC** đều được lưu vào trong bảng **ARP**.
- Cách thu thập thông tin thứ 2 là thu thập qua gói tin broadcast **ARP request**. Khi máy tính gởi một gói tin **broadcast** dạng **ARP request** thì tất cả các máy khác trên mạng đều phân tích gói tin này.
    + Nếu như địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ thuộc cùng đường mạng với địa chỉ máy gửi.
        ③ Nếu máy đó nhận được gói tin thì máy sẽ trả lời bằng một gói tin **ARP reply** (trong đó có địa chỉ **MAC** và địa chỉ **IP** của máy).
        ③ Nếu địa chỉ đích không tồn tại hoặc thiết bị chưa hoạt động thì sẽ không có gói tin **ARP reply**.
    + Nếu địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ khác đường mạng thì việc tìm địa chỉ **MAC** thường được làm thông qua **Router**, có hai cách để thực hiện:
        ③ Nếu **Router** bật tính năng cho phép thực hiện **Proxy ARP**. Thì khi nhận được gói tin **broadcast ARP request**, **Router** sẽ kiểm tra xem địa chỉ đích có khác đường mạng với địa chỉ nguồn không? Nếu khác địa chỉ nguồn thì **Router** sẽ trả về một **ARP response** để trả lời (trong gói tin này sẽ chứa địa chỉ **MAC** – địa chỉ **MAC** của **interface** nhận gói tin **ARP request**).
        ③ Nếu máy tính gửi có khai báo địa chỉ **Default Gateway** thì máy tính sẽ gởi gói tin đến **Default Gateway** để **Default Gateway** gởi tiếp.

Nếu máy tính nguồn không khai báo **Default Gateway** và tính năng thực hiện **Proxy ARP** không bật thì hai máy tính có địa chỉ đường mạng khác nhau sẽ không thể liên lạc được với nhau.

I.4. Các phương pháp truy cập đường truyền.

I.4.1 Cảm sóng đa truy (CSMA/CD).

Khía cạnh thú vị nhất của **Ethernet** là kỹ thuật đường dùng trong việc phối hợp truyền thông. Mạng **Ethernet** không điều khiển tập trung đến việc các máy luân phiên chia sẻ đường cáp. Lúc đó các máy nối với **Ethernet** sẽ tham gia vào một lược đồ phối hợp phân bổ gọi là Cảm sóng đa truy (**CSMA – Carrier Sence with Multiple Access**). Để xác định cáp có đang dùng không, máy tính có thể kiểm tra sóng mang (**carrier** - dạng tín hiệu mà máy tính truyền trên cáp). Nếu có sóng mang, máy phải chờ cho đến khi bên gởi kết thúc. Về mặt kỹ thuật, kiểm tra một sóng mang được gọi là cảm sóng (**carrier sence**), và ý tưởng sử dụng sự hiện hữu của tín hiệu để quyết định khi nào thì truyền gọi là Cảm sóng đa truy (**CSMA**).

Vì **CSMA** cho phép mỗi máy tính xác định đường cáp chia sẻ có đang được máy khác sử dụng hay không nên nó ngăn cấm một máy cắt ngang việc truyền đang diễn ra. Tuy nhiên, **CSMA** không thể ngăn ngừa tất cả các xung đột có thể xảy ra. Để hiểu lý do tại sao, hãy tưởng tượng chuyện gì xảy ra nếu hai máy tính ở hai đầu cáp đang nghỉ nhận được yêu cầu gởi khung. Cả hai cùng kiểm tín hiệu mang, cùng thấy cáp đang trống và cả hai bắt đầu gởi khung. Các tín hiệu phát từ hai máy sẽ gây nhiễu lẫn nhau. Hai tín hiệu gây nhiễu lẫn nhau gọi là xung đột hay đụng độ (**collision**). Vùng có khả năng xảy ra đụng độ khi truyền gói tin được gọi là **Collision Domain**. Máy đầu tiên trên đường truyền phát hiện được xung đột sẽ phát sinh tín hiệu xung đột cho các máy khác. Tuy xung đột không làm hỏng phần cứng nhưng nó tạo ra một sự truyền thông méo mó và hai khung nhận được sẽ không chính xác. Để xử lý các biến cố như vậy, **Ethernet** yêu cầu mỗi bên gởi tín hiệu giám sát (monitor) trên cáp để bảo đảm không có máy nào khác truyền đồng thời. Khi máy gởi phát hiện đụng độ, nó ngưng truyền ngay lập tức, và tiếp tục bắt đầu lại quá trình chuẩn bị việc truyền tin sau một khoảng thời gian ngẫu nhiên. Việc giám sát cáp như vậy gọi là phát hiện đụng (**CD – collision detect**), và kỹ thuật **Ethernet** đó được gọi là Cảm sóng đa truy với phát hiện đụng (**CSMA/CD**).

I.4.2 Chuyển thẻ bài (Token-passing):

Chúng ta đã biết mạng **LAN** vòng nối các máy thành một vòng tròn kín. Hầu hết các **LAN** dùng đồ hình vòng cũng sử dụng một kỹ thuật truy cập gọi là chuyển thẻ bài (**token-passing**). Khi một máy cần chuyển dữ liệu, nó phải chờ phép trước khi truy cập mạng. Khi giữ được thẻ bài, máy gởi hoàn toàn giữ quyền điều khiển vòng – không có các truyền thông nào khác xảy ra đồng thời. Khi máy gởi truyền frame, các bit chuyển từ máy gởi sang máy kế, và chuyển tiếp sang máy kế và cứ thế cho đến khi các **bit** đi hết vòng và trở về máy gởi.

Tín bài là một khuôn mẫu bit khác với khung dữ liệu thông thường. Thực chất là tín bài trao quyền cho một máy được gởi khung. Như vậy trước khi gởi khung, máy phải chờ tín bài đến. Khi tín bài đến, máy tạm thời loại bỏ tín bài ra khỏi vòng và bắt đầu truyền dữ liệu trên vòng. Tuy có thể có nhiều khung đang chờ gởi đi nhưng máy chỉ gởi một **frame** và truyền lại tín bài. Không như khung dữ liệu dữ liệu đi hết một vòng khi được gởi, tín bài chỉ đi thẳng từ một máy đến máy kế tiếp.

Nếu tất cả các máy trên mạng vòng cần gởi dữ liệu, chuyển tín bài bảo đảm chúng sẽ đến lược và mỗi máy sẽ gởi một frame trước khi chuyển tín bài. Lưu ý là lược đồ này bảo đảm truy cập công bằng: khi tín bài chuyển trên vòng, mỗi máy sẽ có cơ hội sử dụng mạng. Nếu một máy nào đó không gởi dữ liệu khi nhận được tín bài, nó chỉ việc chuyển tín bài mà không trì hoãn. Trong trường hợp đặc biệt không có máy nào truyền dữ liệu, tín bài sẽ quay vòng liên tục, mỗi máy khi nhận được tín bài sẽ chuyển ngay lập tức đến máy kế. Thời gian chuyển tín bài một vòng trong trường hợp này là cực ngắn, vì 2 lý do. Thứ nhất, vì tín bài nhỏ nên có thể chuyển rất nhanh trên đường dây. Thứ hai, sự chuyển tiếp trên mỗi máy được thực hiện bởi phần cứng vòng, điều đó có nghĩa tốc độ không phụ thuộc vào **CPU** của máy.

II. KHẢO SÁT CHI TIẾT LỚP 3 (NETWORK).

Chức năng quan trọng nhất của lớp **Network** là định tuyến (**Routing**), định tuyến là quá trình chuyển thông tin qua mạng từ nơi gởi tới nơi nhận. Định tuyến có hai thành phần là chuyển mạch (**switching**) và chọn đường (**path determination**).

Trong quá trình **switching**, bên gởi (**source or sender**) thêm vào địa chỉ bên gởi, địa chỉ bên nhận, địa chỉ vật lý (**MAC**), địa chỉ của **Router** đầu tiên (hay là địa chỉ **Default-Gateway**) mà packet tới. Khi packet tới **Router**, **Router** sẽ xác định địa chỉ **IP** đích của **packet** (còn gọi là **destination IP address**), nếu như **Router** không nhận ra **IP** đích thì nó sẽ bỏ **packet**, nếu ngược lại thì **Router** sẽ chuyển **packet** tới địa chỉ đích hoặc chuyển packet tới **Router** kế tiếp (**next Router**), khi đó **Router** nó sẽ thay thế **MAC** nguồn, và **MAC** đích bằng **MAC** trên **interface** của nó và **MAC** trên **next hop Router**, khi **packet** chuyển qua mạng lớn (qua nhiều **Router**) thì địa chỉ **IP** nguồn (**source address**) và địa chỉ **IP** đích (**destination address**) không thay đổi nhưng địa chỉ vật lý (địa chỉ **MAC**) bị thay đổi tại mỗi hop.

Thành phần thứ hai của **routing** là **Path-Determination**, **Router** cần có một số cách xác định con đường đi ngắn nhất để chuyển packet tới đích, **Router** cần có nhiều thông tin từ người quản trị (người quản trị phải làm công việc định tuyến) hay từ các **Router** khác để xây dựng bảng **routing** (**Router** tự học định tuyến thông qua các giao thức) mà thông tin này giúp cho nó định tuyến packet đi tới đích.

Trong bảng **routing** địa chỉ mạng đích được ánh xạ tới **interface** (cổng) thích hợp trên **Router**, thông qua **interface** này packet có thể đi tới nó.

Khi có sự thay đổi trên mạng các **Router** trao đổi với nhau bằng các **exchanging message** để cập nhật lại bảng **routing**. Các **exchanging message** bao gồm:

- **Routing update message**.
- **Link-state advertiment** (trạng thái của **sender's link**).

Theo định nghĩa của một số nghi thức **routing** như **RIP**, **IGRP**,… cứ sau một khoảng thời gian (**interal time**) nó sẽ gởi **update message** tới các **Router** khác để cập nhật về sự thay đổi thông tin trên mạng. Khi các **Router** này nhận được thông tin **update**, nó sẽ kiểm tra trong bảng **routing table** của nó với thông tin **update** nếu có sự thay đổi thì nó sẽ xóa **entry** tương ứng và cập nhật thông tin mới vào, ngược lại thì nó sẽ không cập nhật thông tin.

Routing Algorithm là thuật toán định tuyến cho phép chọn **Router**, chọn con đường đi tốt nhất để gởi dữ liệu đến đích. **Routing Algorithm** tùy thuộc vào các yếu tố sau :

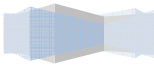
- **Design**.
- **Metrics**.
- **Type**.

Design bao gồm:

- Tính đơn giản (**simplicity**) là thành phần rất quan trọng trong hệ thống giúp giới hạn tài nguyên vật lý (**physical resource**).
- Tính linh hoạt (**plexibility**) để cho phép mạng thích ứng nhanh với sự thay đổi và phát triển của hệ thống, ví dụ như sự thay đổi về băng thông kích thước hàng đợi, độ trễ,…
- Sự hội tụ (**convergence**) tính hội tụ thông tin là mục đích quan trọng của thuật toán **routing**, tính hội tụ nhanh làm cho thông tin trong bảng **routing** được thống nhất một cách nhanh chóng. Ngược lại nó sẽ làm phá vỡ tính thống nhất thông tin định tuyến giữa các **Router**.
- Tính tối ưu (**optimality**): là khả năng mà nghi thức định tuyến lựa chọn đường đi tốt nhất để truyền dữ liệu, để xác định con đường đi tốt nhất **Router** dựa vào metric và **weighting** (trọng lượng) của mỗi **metric**.

Metric được sử dụng trong thuật toán định tuyến để lựa chọn con đường đi tốt nhất, nó bao

gồm:



- **Hop count và path length**.
- **Reliability**.
- **Load**.
- **Delay**.
- **Bandwidth**.
- **Maximum Tranmission Unit** (**MTU**).

Hop count là số lượng host (hay là số lượng **Router**) mà packet phải đi qua từ nguồn tới đích.

Mỗi một đường truyền được gán bởi một giá trị, chỉ có người quản trị mạng mới thay đổi giá trị này, tổng giá trị của các đường truyền đó gọi là **path length**.

Reliability là **metric** cho phép đánh giá mức độ lỗi của một đường truyền.

Load khả năng tải hiện tại trên đường truyền (**busy link**) dựa vào số lượng packet được truyền trong thời gian 1 giây, mức độ xử lý hiện tại của cpu (**CPU Utilization**).

Delay metric thực sự để đo lường một số tác động của một số đại lượng trên đường truyền như băng thông (**bandwidth**), tắc nghẽn đường truyền (**conguestion**), khoảng cách đường truyền (**distance**), khả năng mang thông tin trên đường truyền còn gọi là băng thông của đường truyền được tính băng số bit/giây mà đường truyền đó có thể truyền thông tin, số lượng traffic trên đường truyền quá nhiều sẽ làm giảm băng thông có sẵn cho đường truyền.

MTU là chiều dài tối đa của thông điệp (tính bằng **byte**) mà nó có thể truyền trên đường truyền. MTU của mỗi môi truyền truyền vật lý thì khác nhau. Ví dụ **MTU** cho **ethernet** là 1500.

III. KHẢO SÁT CHI TIẾT LỚP 4 (TRANSPORT)

Các dịch vụ trên lớp **transport** cho phép phân mảnh và tập hợp dữ liệu vào cùng transport-layer data stream, **Transport-layer data stre**am là một kết nối logic giữa bên gởi và bên nhận trên mạng. Lớp **Transport** cung cấp các đặc tính sau :

- **Reliability** (tin cậy) bằng cách đánh số thứ tự của các **segment** (**source secquence**), bên nhận thông báo cho bên gởi biết rằng nó đã nhận được dữ liệu bằng cách thông báo các **ACK** (**acknownledgements**).
- **Flow Control**: là kỹ thuật cho phép điều khiển buffer bên nhận, bên nhận sử dụng kỹ thuật này để ngăn không cho bên gởi gởi dữ liệu quá nhanh làm tràn buffer của bên nhận.
- Hai **protocol** ở lớp **transport layer** là **TCP** và **UDP**,

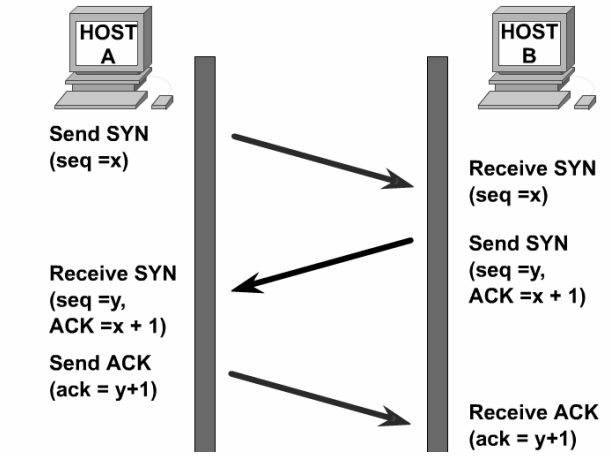
III.1. Giao thức TCP (TCP protocol).

TCP cung cấp kết nối tin cậy giữa hai máy tính, kết nối được thiết lập trước khi dữ liệu bắt đầu truyền. **TCP** còn gọi là nghi thức hướng kết nối, với nghi thức **TCP** thì quá trình hoạt động trải qua ba bước sau:

- Thiết lập kết nối (**connection establishment**).
- Truyền dữ liệu (**data tranfer**).
- Kết thúc kết nối (**connection termination**).

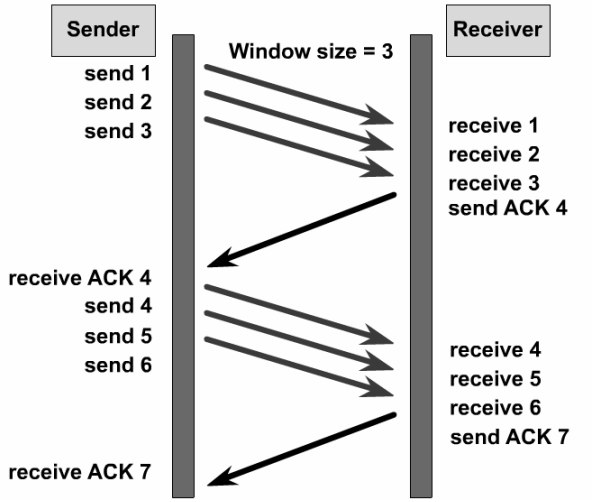
TCP phân chia các thông điệp thành các segment, sau đó nó ráp các segment này lại tại bên nhận, và nó có thể truyền lại những gói dữ liệu nào đã bị mất. Với **TCP** thì dữ liệu đến đích là đúng thứ tự, **TCP** cung cấp **Virtual Circuit** giữa các ứng dụng bên gởi và bên nhận.

Giao thức **TCP** thiết lập một kết nối bằng phương pháp "Bắt tay 3 lần" (**three-way handshake**)



Hình 6.1 – Cách thiết lập kết nối của giao thức **TCP**.

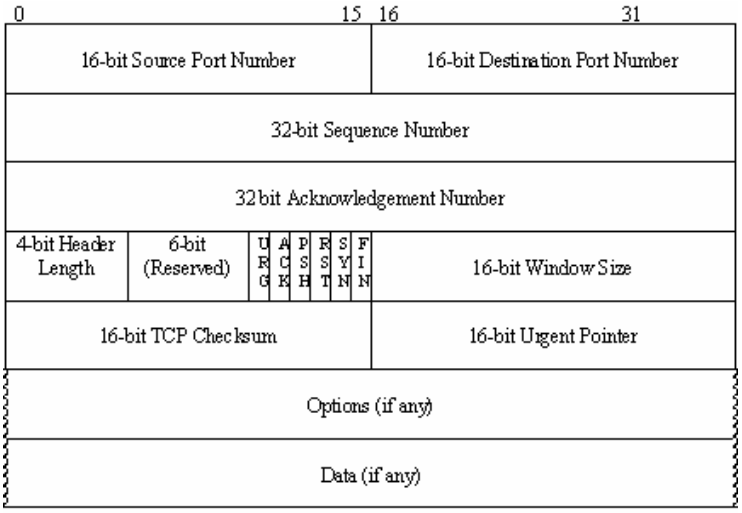
Hình vẽ dưới đây là một ví dụ về cách thức truyền, nhận gói tin bằng giao thức **TCP.**



Hình 6.2 – Minh họa cách truyền, nhận gói tin trong giao thức **TCP**.

Giao thức **TCP** là giao thức có độ tin cậy cao, nhờ vào phương pháp truyền gói tin, như cơ chế điều khiển luồng (**flow control**), các gói tin **ACK**,…

Hình vẽ sau đây thể hiện gói tin của **TCP.**



Hình 6.3 – Cấu trúc gói tin của **TCP**.

Các thành phần trong gói tin:

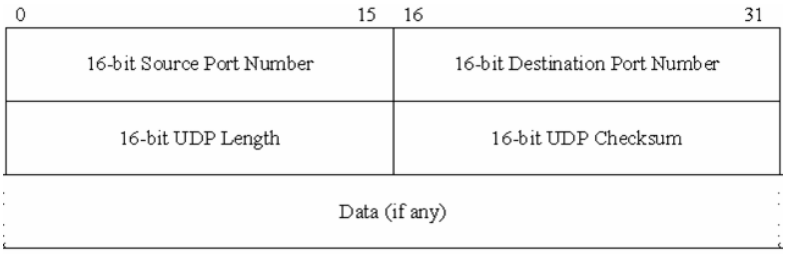
- **Source port**: port nguồn
- **Destination Port**: port đích
- **Sequence number**: số tuần tự (để sắp xếp các gói tin theo đúng trật tự của nó).
- **Acknowledgment number** (**ACK** số): số thứ tự của Packet mà bên nhận đang chờ đợi.
- **Header Length**: chiều dài của gói tin.
- **Reserved**: trả về 0
- **Code bit**: các cờ điều khiển.
- **Windows**: kích thước tối đa mà bên nhận có thể nhận được
- **Checksum**: máy nhận sẽ dùng 16 bit này để kiểm tra dữ liệu trong gói tin có đúng hay không.
- **Data**: dữ liệu trong gói tin (nếu có).

III.2. Giao thức UDP (UDP protocol).

UDP không giống như **TCP**, **UDP** là nghi thức phi kết nối, nghĩa là dữ liệu gởi tới đích là không tin cậy. Bởi vì kết nối không được tạo trước khi dữ liệu truyền, do đó **UDP** nhanh hơn **TCP**.

UDP là nghi thức không tin cậy, nó không đảm bảo dữ liệu đến đích là không bị mất, đúng thứ tự mà nó nhờ các nghi thức ở lớp trên đảm nhận chức năng này. **UDP** có ưu thế hơn **TCP**:

- Nhờ vào việc không phải thiết lập kết nối trước khi thật sự truyền dẫn dữ liệu nên truyền với tốc độ nhanh hơn.
- Bên nhận không cần phải trả về gói tin xác nhận (**ACK**) nên giảm thiểu sự lãng phí băng thông.



Hình 6.4 – Cấu trúc gói tin của **UDP**.

Các thành phần trong gói tin **UDP**:

- **Source Port**: port nguồn.
- **Destination Port**: port đích.
- **UDP Length**: chiều dài của gói tin.
- **UDP Checksum**: dùng để kiểm tra gói tin có bị sai lệch hay không
- **Data**: dữ liệu đi kèm trong gói tin (nếu có).

III.3. Khái niệm Port.

Trong cùng một thời điểm, một máy tính có thể có nhiều chương trình đang chạy. Vậy làm sao để xác định một gói tin sẽ được chương trình nào sử dụng?

Khái niệm **Port** ra đời để giải quyết chuyện đó. Mỗi chương trình ứng dụng mạng đều có một **Port** xác định. Để gởi gói tin đến một chương trình tại máy tính A, ta chỉ cần gởi gói tin đến địa chỉ **IP** của máy A, và **Port** mà chương trình đó đang sử dụng.

TCP hoặc **UDP** dùng **port** hoặc **socket**, nó là con số mà thông qua đó thông tin được truyền lên các lớp cao hơn. Các con số **port** được dùng trong việc lưu vết các cuộc hội thoại khác nhau trên mạng xảy ra trong cùng một thời điểm. P**o**rt là một loại địa chỉ **logic** trên một máy tính, là con số 2 byte. Các **port** có giá trị nhỏ hơn 1024 được dùng làm các **port** chuẩn. Các ứng dụng dùng port riêng có giá trị lớn hơn 1024. Các giá trị **port** được chứa trong phần địa chỉ nguồn và đích của mỗi **segment TCP**.

Một ứng dụng có thể sử dụng port riêng trong miền cho mình để giao dịch trên mạng nhưng chú ý là không được trùng với các **port** chuẩn.

Ví dụ một số port chuẩn mà các phần mềm sử dụng

- **HTTP**: Port number 80
- **FTP**: Port number 21
- **DNS**: Port number 53
- **Telnet**: Port number 23
- **SMTP**: Port number 25
- **TFTP**: Port number 69
- **SNMP**: Port number 161
- **RIP**: Port number 520

IV. CÁC MÔ HÌNH FIREWALL.

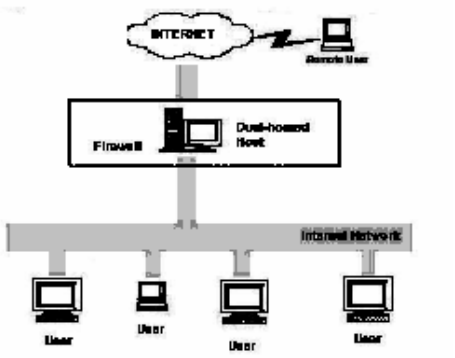
IV.1. Giới thiệu về Firewall.

Firewall hay còn gọi là bức tường lửa được hiểu như là một hệ thống máy tính và thiết bị mạng giúp ta có thể bảo mật và giám sát các truy xuất từ bên trong ra ngoài và ngược lại từ bên ngoài vào trong từ đó ta có thể phòng chống các truy cập bất hợp pháp.

IV.2. Dual homed host.

Firewall kiến trúc kiểu ***Dual-homed host*** được xây dựng dựa trên máy tính **dual-homed host**. Một máy tính được gọi là **dual-homed host** nếu nó có ít nhất hai **network interface**, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là **Router** mềm. Kiến trúc **dual-homed** host rất đơn giản. **Dual-homed host** ở giữa, một bên được kết nối với **Internet** và bên còn lại nối với mạng nội bộ (**LAN**).

Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (**proxy**) chúng hoặc cho phép **users** đăng nhập trực tiếp vào **dual-homed host**. Mọi giao tiếp từ một **host** trong mạng nội bộ và **host** bên ngoài đều bị cấm, **dual-homed host** là nơi giao tiếp duy nhất.



Hình 6.4 – Kiến trúc **Firewall Dual homed host**.

IV.3. Screened Host.

Screened Host có cấu trúc ngược lại với cấu trúc **Dual-homed host**. Kiến trúc này cung cấp các dịch vụ từ một **host** bên trong mạng nội bộ, dùng một **Router** tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp ***Packet Filtering***.

Bastion host được đặt bên trong mạng nội bộ. **Packet Filtering** được cài trên **Router**. Theo cách này, **Bastion host** là hệ thống duy nhất trong mạng nội bộ mà những **host** trên **Internet** có thể kết nối tới. Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong **Bastion host**) mới được cho phép kết nối. Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới **host** này. Vì thế **Bastion host** là **host** cần phải được duy trì ở chế độ bảo mật cao.

Packet filtering cũng cho phép **bastion host** có thể mở kết nối ra bên ngoài. Cấu hình của **packet filtering** trên **screening router** như sau:

- Cho phép tất cả các host bên trong mở kết nối tới **host** bên ngoài thông qua một số dịch vụ cố định.

- Không cho phép tất cả các kết nối từ các **host** bên trong (cấm những **host** này sử dụng dịch **proxy** thông qua **bastion host**).

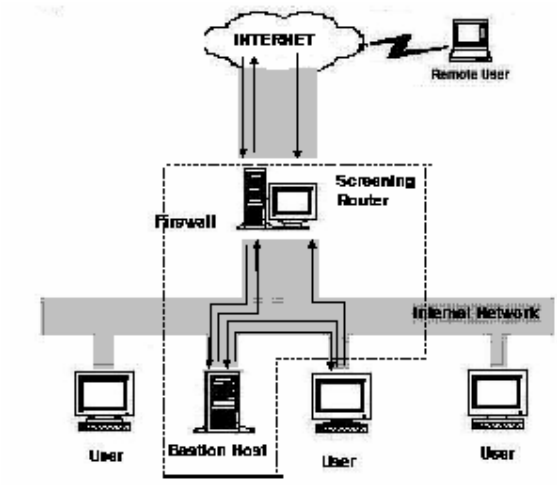
Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau:

- Một số dịch vụ được phép đi vào trực tiếp qua packet filtering.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua **proxy**.

Bởi vì kiến trúc này cho phép các packet đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc **Dual-homed host**, vì thế nó được thiết kế để không một packet nào có thể tới được mạng bên trong. Tuy nhiên trên thực tế thì kiến trúc **dual-homed host** đôi khi cũng có lỗi mà cho phép các packet thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này). Hơn nữa, kiến trúc **dual-homed host** thì dễ dàng bảo vệ **Router** (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các host bên trong mạng.

Xét về toàn diện thì kiến trúc ***Screened host*** cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc ***Dual-homed host***.

So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc ***Screened subnet*** thì kiến trúc **Screened host** có một số bất lợi. Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập ***Bastion Host*** thì không có cách nào để ngăn tách giữa ***Bastion Host*** và các **host** còn lại bên trong mạng nội bộ. **Router** cũng có một số điểm yếu là nếu **Router** bị tổn thương, toàn bộ mạng sẽ bị tấn công. Vì lý do này mà **Sceened *subnet*** trở thành kiến trúc phổ biến nhất.



Hình 6.5 – Kiến trúc **Firewall Screened host**.

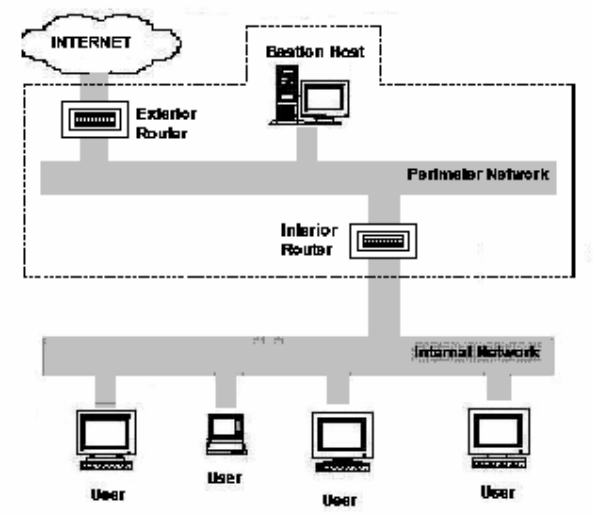
IV.4. Screened Subnet.

Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn *cho **bastion host***, tách **bastion host** khỏi các **host** khác, phần nào tránh lây lan một khi **bastion host** bị tổn thương, người ta đưa ra kiến trúc **firewall** có tên là **Sreened Subnet**.

Kiến trúc **Screened *subnet*** dẫn xuất từ kiến trúc **screened host** bằng cách thêm vào phần an toàn: mạng ngoại vi (**perimeter network**) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách **bastion host** ra khỏi các host thông thường khác. Kiểu **screened subnet** đơn giản bao gồm hai **screened router**:

Router ngoài (**External router** còn gọi là **access router**): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (**bastion host**, **interior router**). Nó cho phép hầu hết những gì outbound từ mạng ngoại vi. Một số qui tắc **packet filtering** đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ **bastion host** và **interior router** vì **bastion host** còn là **host** được cài đặt an toàn ở mức cao. Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai **Router**.

Interior Router (còn gọi là **choke router**): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc **packet filtering** của toàn bộ **firewall**. Các dịch vụ mà **interior router** cho phép giữa **bastion host** và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau. Giới hạn dịch vụ giữa **bastion host** và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi bastion host bị tổn thương và thoả hiệp với bên ngoài. Chẳng hạn nên giới hạn các dịch vụ được phép giữa bastion host và mạng nội bộ như **SMTP** khi có **Email** từ bên ngoài vào, có lẽ chỉ giới hạn kết nối **SMTP** giữa **bastion host** và **Email server** bên trong.



Hình 6.6 – Kiến trúc **Firewall Screened Subnet**.

Tóm tắt

Lý thuyết 6 tiết - Thực hành 20 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kỹ năng sử dụng các công cụ client của các dịch vụ mạng cơ sở như: web, ftp, mail…	I. Dịch vụ Web. II. Dịch vụ FTP. III. Dịch vụ e-mail. IV. Ngôn ngữ HTML.	Dựa vào bài tập môn mạng máy tính.	Dựa vào bài tập môn mạng máy tính.

V. DỊCH VỤ WORLD WIDE WEB.

V.1. Một số khái niệm về Internet.

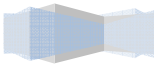
Các thuật ngữ cơ sở.

- **HTTP** (**Hypertext Transfer Protocol**): là giao thức cho phép các máy tính giao tiếp qua **World Wide Web** và kết nối với nhau qua các **hyperlink**.
- **Gopher**: là hệ thống cho phép ta duyệt các tài nguyên trên mạng **Internet**, dịch vụ này ra đời trước **Web** và hoạt động giống như một danh bạ, liệt kê các tập tin sắp xếp theo tầng.
- Dịch vụ trực tuyến (**Online Service**): là những dịch vụ truy cập **Internet** có thu cước phí do các công ty lớn cung cấp như: **AOL** (**America Online**), **CompuServe** hoặc **MSN** (**Microsoft Network**).
- **HTML** (**Hypertext Markup Language**): là ngôn ngữ định dạng dùng để tạo ra các trang Web giúp người dùng có thể đọc và truy cập từ bất kỳ máy nào trên mạng, dùng bất kỳ hệ điều hành nào.
- **WebPage**: là một trang tư liệu Web.
- **WebSite**: là tập hợp các trang Web của một tổ chức, một công ty, một web site có thể có nhiều **Web Server**.
- **Home page**: là trang Web đầu tin của một Web Site hoặc trang Web xuất hiện đầu tin khi khởi động **Web Browser**, đồng thời trang này chứa các liên kết tiêu biểu đến các trang Web còn lại.
- **HyperLink** (**link**): là các mối liên kết giữa các tư liệu. Thông thường, trong một trang Web, các mối liên kết có màu xanh dương và được gạch dưới. Ngoài ra, bất kỳ một hình ảnh, văn bản nào khi di chuyển con trỏ chuột tới chuyển sang hình  đều là các liên kết (**link**).
- **URL** (**Uniform Resource Locator**): là đường dẫn chỉ tới một tập tin trong một máy chủ trên **Internet**. Chuỗi **URL** thường bao gồm: tên giao thức, tên máy chủ và đường dẫn đến tập tin trong máy chủ đó. Ví dụ: http://www.hcmuns.edu.vn/TongQuan/Tongquan.htm có nghĩa là: giao thức sử dụng http:// (**Hypertext Transfer Protocol**), tên máy chủ: **www.hcmuns.edu.vn**, đường dẫn và tên tập tin: /TongQuan/Tongquan.htm.
- Lưu ý: đường dẫn sử dụng dấu "/" thay cho dấu "\".
- **IXP** (**Internet Exchange Provider**): là nhà cung cấp đường truyền và cổng truy cập **Internet**.
- **ISP** (**Internet Service Provider**): là nhà cung cấp dịch vụ Internet cho người dùng trực tiếp qua mạng điện thoại như là cấp quyền truy cập **Internet**, cung cấp các dịch vụ như **Web**, **E-mail**, **Chat**, **Telnet**…
- **ICP** (**Internet Content Provider**): là nhà cung cấp thông tin lên **Internet**, thông tin được cập nhật định kỳ hay thường xuyên và thuộc nhiều lĩnh vực như thể thao, kinh tế giáo dục, chính trị, quân sự …

Các hoạt động chính trên Web.

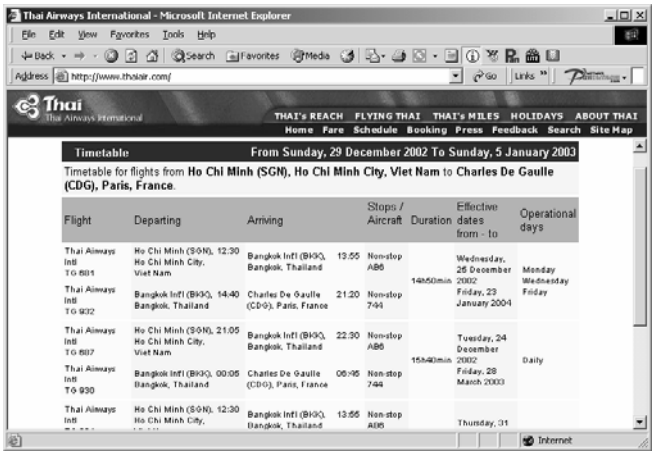
- Duyệt **Web** tìm kiếm thông tin như số điện thoại, địa chỉ nhà, tin tức, tin dự báo thời tiết, bảng giá

chứng khoán, các phần mềm miễn phí…



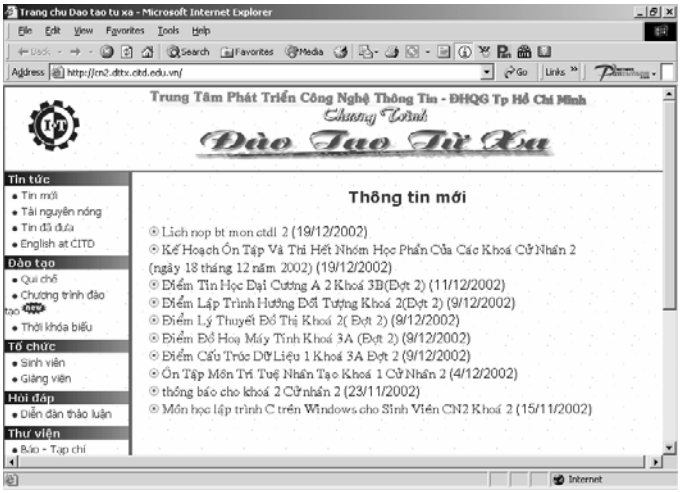
Hình 7.1 – Minh họa một số trang **Web** để tìm kiếm thông tin.

- Giải trí như nghe nhạc,xem phim, chơi game trên mạng.
- Trao đổi **E-mail**.
- Truy xuất và **download** các tập tin.
- Tán ngẫu (chat).
- Sắp xếp các chuyến đi du lịch như đặt vé máy bay, đăng ký phòng khách sạn...



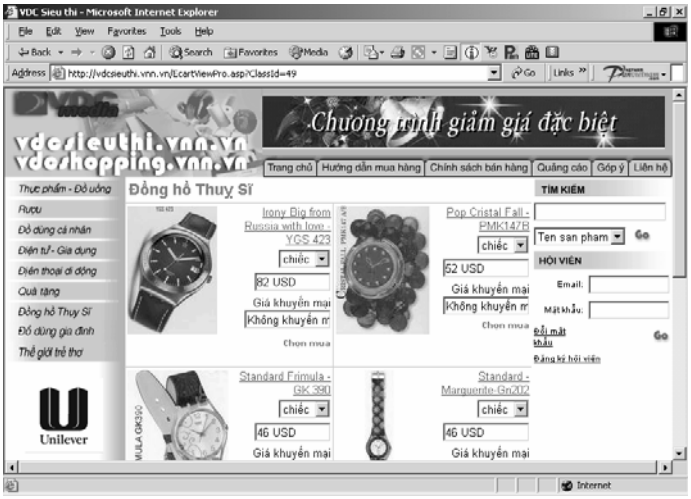
Hình 7.2 – Minh họa một trang **Web** dùng để tìm thông tin các chuyến bay.

- Đào tạo từ xa qua mạng.



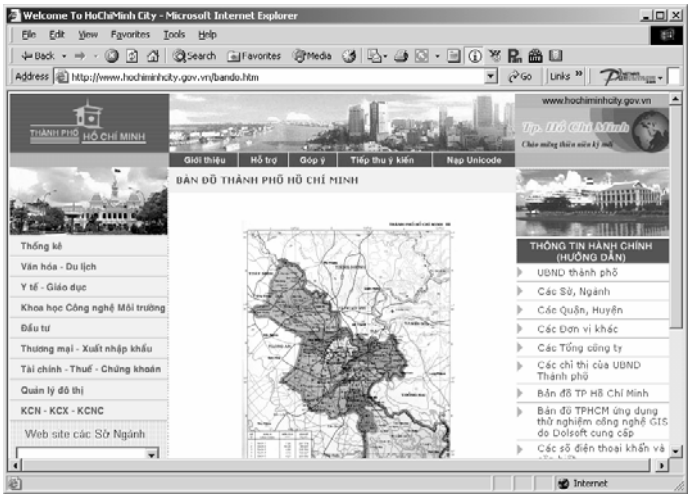
Hình 7.3 – Minh họa một trang **Web** dùng để đào tạo từ xa.

- Hội thảo từ xa.
- Quảng cáo sản phẩm.
- Đặt mua hàng.



Hình 7.4 – Minh họa một số trang **Web** dùng để mua bán qua mạng.

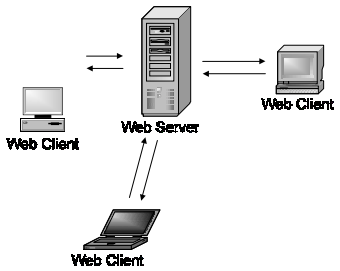
- Thực hiện các giao dịch ngân hàng.
- Hỗ trợ chính phủ điện tử và thương mại điện tử.



Hình 7.5 – Minh họa một trang **Web** của Tp HCM.

V.2. Giới thiệu mô hình hoạt động của Web.

Dịch vụ **World Wide Web** (viết tắt là **www** hoặc **Web**) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản (**hypertext**) và thường được thiết kế bằng ngôn ngữ **HTML** (**Hypertext Markup Language**). Siêu văn bản là các tư liệu có thể là văn bản (**text**), hình ảnh tĩnh (**image**), hình ảnh động (**video**), âm thanh (**audio**)...., được liên kết với nhau qua các mối liên kết (**link**) và được truyền trên mạng dựa trên giao thức **HTTP** (**Hypertext Transfer Protocol**), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng. Mô hình hoạt động:



Hình 7.6 – Mô hình hoạt động của **Web Server**.

Web server: là một ứng dụng được cài đặt trên máy chủ trên mạng với chức năng là tiếp nhận các yêu cầu dạng **HTTP** từ máy trạm và tùy theo yêu cầu này máy chủ sẽ cung cấp cho máy trạm các thông tin web dạng **HTML**.

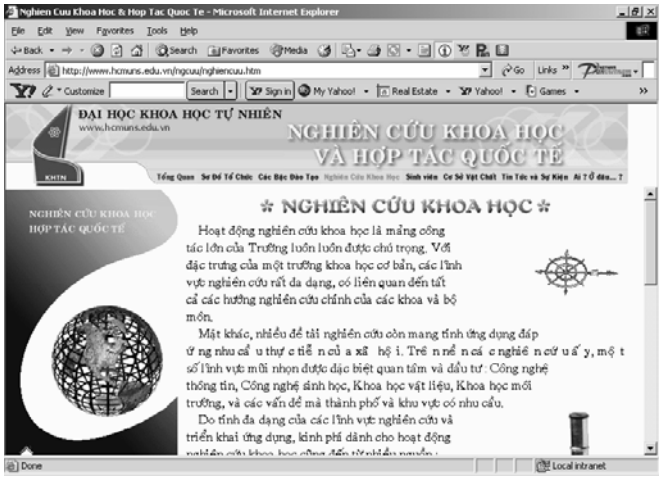
Web Client: là một ứng dụng cài trên máy trạm (máy của người dùng đầu cuối) gọi là **Web Browser** để gởi yêu cầu đến **Web Server** và nhận các thông tin phản hồi rồi hiện lên màn hình giúp người dùng có thể truy xuất được các thông tin trên máy **Server**. Một trong những trình duyệt **Web** (**Web Browser**) phổ biến nhất hiện nay là **Internet Explorer**.

V.3. Khảo sát web browser Internet Explorer.

Chương trình **Internet Explorer** rất quen thuộc với người dùng vì nó đã tích hợp sẵn trong các hệ điều hành của **Microsoft** như **Win9x**, **Win2K**, **WinXP**… Nhưng chú ý là các phiên bản **IE** trên các hệ điều hành **Win9X**, **WinME** là những phiên bản cũ và có nhiều lỗ hổng cần cài phiên bản mới và cài các chương trình sửa lỗi cho các phiên bản đó. (Để sửa lỗi ta nên vào trang **Web Support** của **Microsoft**, rồi **download** các chương trình sửa lỗi cho **IE** và cài lên máy)

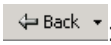
Truy cập vào các Web site.

Trước khi duyệt các **Website** ta phải khởi động chương trình bằng cách click **Start/Programs/Internet Explorer/Internet Explorer**, đối với **Win2K** thì **Start/Programs/Internet Explorer**. Sau khi chương trình đã chạy, ta nhập địa chỉ **Website** mà ta cần truy cập vào ô **Address**. Ví dụ: trong hình dưới đây là địa chỉ: **http://www.hcmuns.edu.vn/ngcuu/nghiencuu.htm**. (1)



Hình 7.7 – Nội dung của trang Web (1)

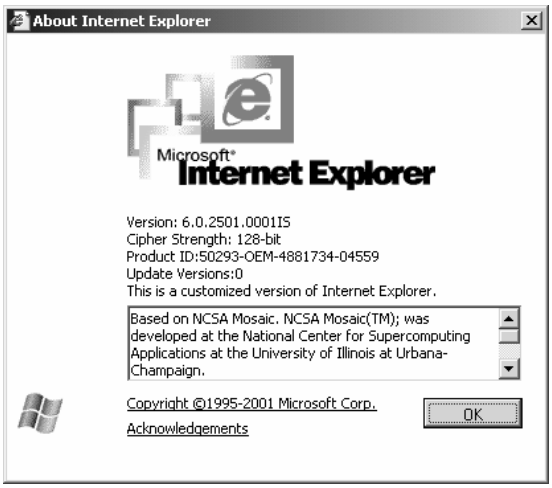
Ngoài ra để duyệt thông tin trên **Website** nhanh ta có thể sử dụng các nút trên thanh công cụ sau:

- Nút quay về trang trước 

: các trang Web đã duyệt qua phần lớn chứa trong thư mục **Temporary Internet Files** (trong **Win98** thì thư mục cache là C**:\Windows\Temporary Internet Files**, trong **Win2K** trở lên là **C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files**), do đó khi cần quay về trang Web trước ta dùng chức năng **Back** để **IE** đọc thông tin trong đĩa cứng không cần lấy từ **Internet** nữa, nhằm tăng tốc độ duyệt **Web**.
- Nút tới trang sau  : cũng tương tự như chức năng **Back**, tính năng **Forward** giúp ta truy cập nhanh trang Web phía sau đã duyệt rồi chứa trong đĩa cứng.
- Nút ngừng tải dữ liệu  : khi ta muốn ngừng truy xuất vào một **Website** hiện tại ta chọn tính năng **Stop**.
- Nút về trang chủ  (**HomePage** hay trang mặc định): giúp ta trở về trang default được quy định trong mục **Option**.
- Nút cập nhật lại thông tin  : khi duyệt các trang Web cũ mà **IE** không chịu lấy thông tin mới trên **Internet** mà cứ lấy thông tin trong đĩa cứng, ta cần chọn chức năng **Refresh** để cập nhật thông tin mới từ **Internet**.

Kiểm tra phiên bản và nâng cấp IE

Trước khi dùng **IE** duyệt **Web** ta cần kiểm tra phiên bản hiện tại để quyết định nâng cấp hoặc cài chương trình sửa lỗi tránh trường hợp duyệt **Web** không an toàn. Xem phiên bản của **IE** Click vào menu **Help** - **About Internet Explorer**, như hình sau là phiên bản 6.0.



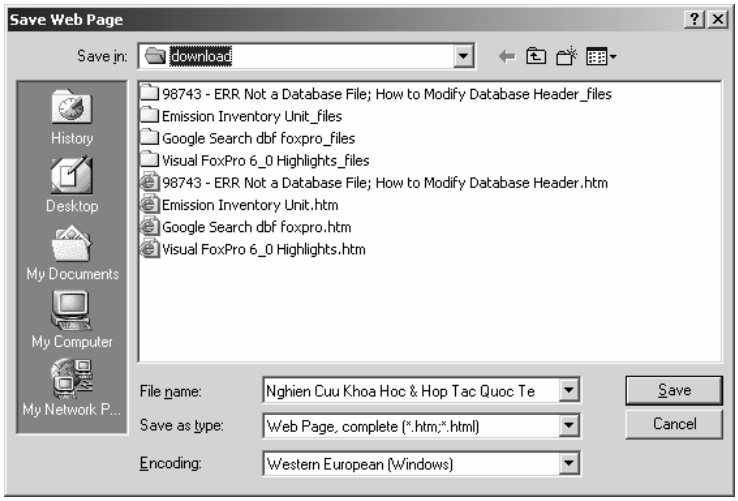
Hình 7.8 – Hộp thoại hiển thị phiên bản **Internet Explorer 6.0**.

Lưu hình và nội dung văn bản từ trang Web.

Như là bạn thấy trên trang Web, có rất nhiều nội dung hay mà bạn cần lưu trữ lại và chia sẻ cho nhiều người cùng biết. Bạn có thể lưu trữ toàn bộ trang web hoặc một phần trang Web như: một đoạn văn bản, hình hoặc những liên kết. Bạn cũng có thể in toàn bộ trang Web ra giấy.

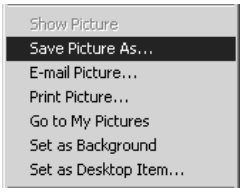
Yêu cầu	Thao tác
Lưu một trang hoặc một hình mà không cần mở nó lên.	Click phải chuột vào kết nối của biểu tượng mà bạn cần muốn lưu và sau đó click **Save Target As**
Copy thông tin từ một trang Web vào một tài liệu.	Chọn thông tin mà bạn muốn sao chép trên trang Web và sau đó vào menu **Edit**, click **Copy**. Bạn chuyển qua tài liệu cần lưu trữ và chọn **Paste**.
Tạo một **shortcut** trên **desktop** cho trang Web hiện tại.	Click phải chuột vào trang hiện tại, và sau đó click **Create Shortcut**
Dùng hình trên trang Web như là hình nền	Click phải chuột vào hình trên trang Web và click vào **Set As Wallpaper** (hoặc **Set As Background**)
Gởi một trang Web trong **E-mail**	Trên menu **File**, chọn **Send**, sau đó click vào **Page by E-mail** hoặc **Link by E-mail**. Một cửa sổ của **mail** mới hiện ra, bạn nhập nội dung vào và gởi **mail**. Chú ý là bạn phải có tài khoản mail và chương trình **E-mail** đã cài đặt trên máy tính của bạn.

Lưu toàn bộ trang Web: vào menu **File** chọn **Save As**, sau đó chọn đường dẫn và nhập tên tập tin cần lưu trữ.



Hình 7.9 – Hộp thoại hiển thị sau khi chọn **Save As**.

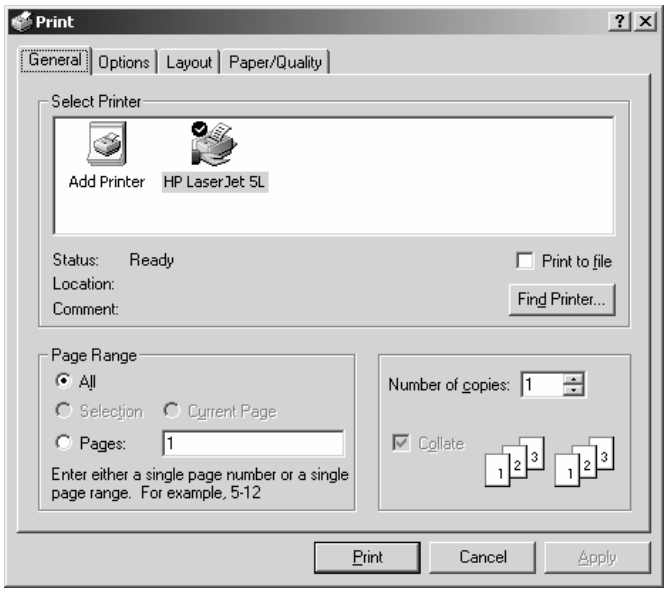
Lưu hình trên trang Web: click phải chuột trên hình cần lưu trữ và chọn chức năng **Save Picture As**, sau đó chọn đường dẫn và tên tập tin cần lưu trữ.



Hình 7.10 – Danh sách các thuộc tính sau khi click chuột phải lên hình ảnh.

In trang Web.

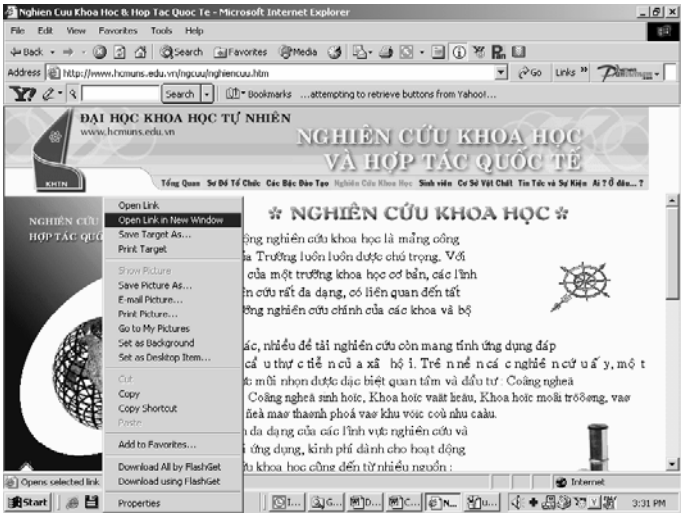
Muốn in trang Web hiện tại, ta vào menu **File**, chọn chức năng **Print** hoặc ấn phím tắt **Ctrl+P**, nhưng bạn chú ý là phải chọn khổ giấy và canh lề cho phù hợp.



Hình 7.11 – Hộp thoại hiển thị sau khi chọn lựa **Print** (hoặc **Ctrl-P**).

Liên kết đến các trang Web khác.

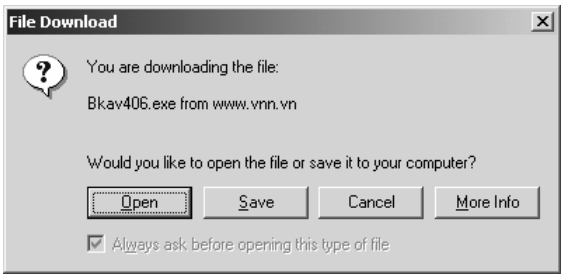
Bạn có thể click chuột vào các liên kết để truy cập vào các trang Web khác, nhưng khi đó nội dung trang web mới sẽ chồng lên trang cũ, nếu bạn muốn nội dung trang Web mới hiển thị trong một cửa sổ khác thì bạn click phải chuột vào liên kết và chọn **Open Link in New Windows**



Hình 7.12 – Hộp thoại hiển thị khi click chuột phải vào Link “Nghiên cứu”.

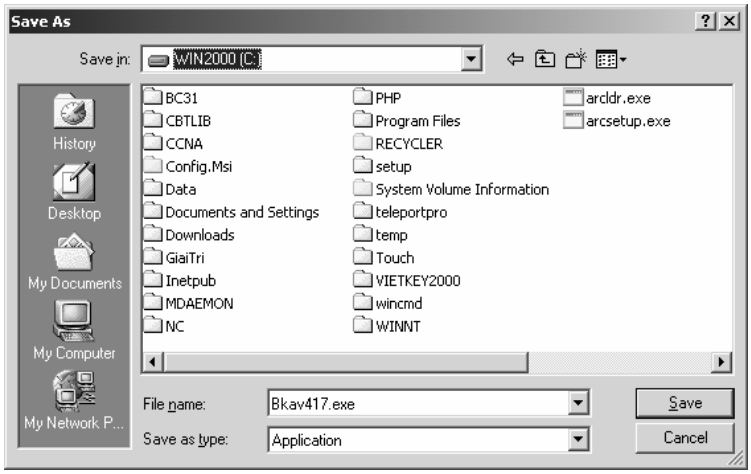
Download.

Download file là quá trình tải một file từ **Internet** về máy trạm, bạn click vào liên kết, **IE** xuất hiện hộp thoại **download**, bạn chọn **Save**, hộp thoại **Save As** xuất hiện, bạn chọn đường dẫn và nhập tên tập tin cần lưu trữ. Click vào nút **Save**.



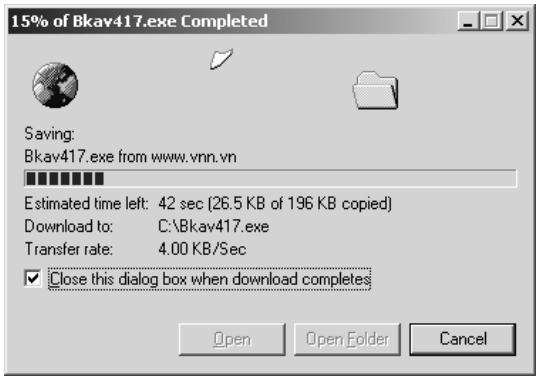
Hình 7.13 – Hộp thoại hiển thị sau khi chọn **Download**.

Chỉ ra đường dẫn và nhập vào tên tập tin, Click nút **Save.**



Hình 7.14 – Hộp thoại hiển thị sau khi chọn **Save**.

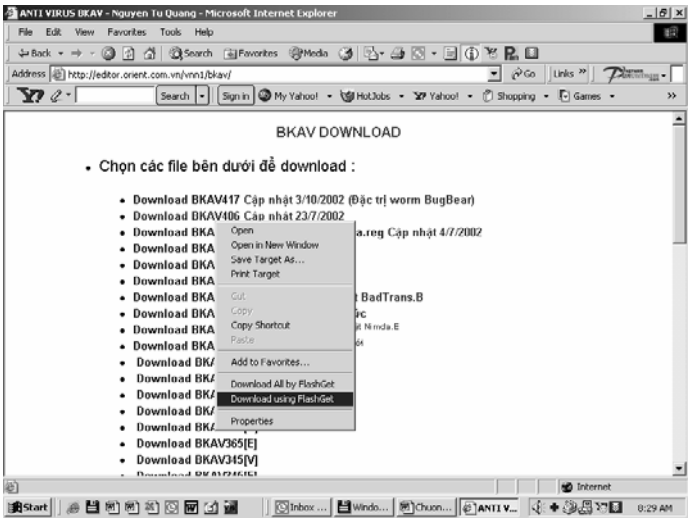
Hình dưới là hiển thị trạng thái **download** như thời gian dự đoán sẽ hoàn thành, số **byte** đã **download**, số **byte** cần **download**, tên tập tin, tốc độ truyền.



Hình 7.15 – Hộp thoại hiển thị quá trình download của tập tin Bkav417.exe

Một lưu ý quan trọng là khi đang **download** đường mạng bị nghẽn hoặc đứt kết nối thì xem như phần đã **download** không còn được sử dụng nữa. Khi **download** những tập tin có kích thước lớn thì làm theo cách này là không khả thi vì kết nối mạng rất dễ đứt trong khi thời gian **download** rất lâu. Muốn vậy ta phải dùng phần mềm **download** chuyên nghiệp có tính năng **download** tiếp tục (**resume**) khi kết nối mạng đứt và cho phép cắt tập tin thành nhiều phần nhỏ giúp **download** nhanh hơn ví dụ như: **FlashGet**, **NetAnt**…

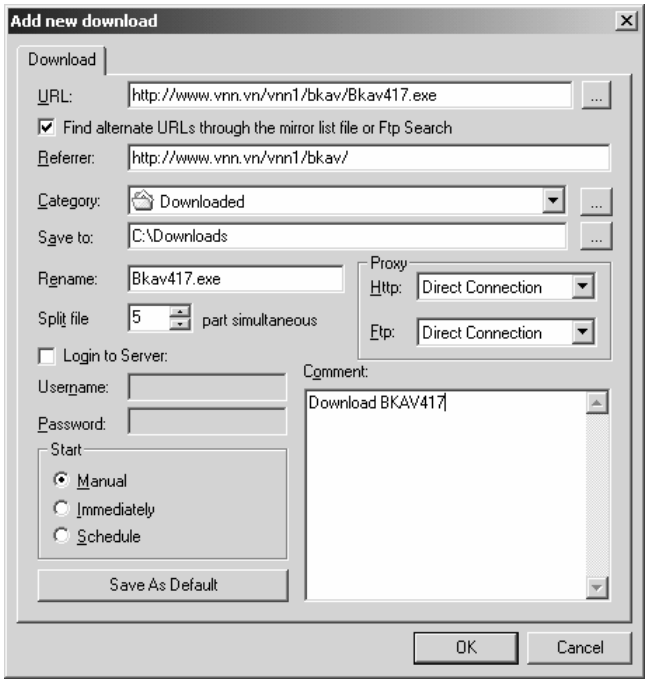
Ví dụ sau ta dùng **FlashGet** để **download** một chương trình diệt **Virus**, chú ý trước khi bạn dùng theo hướng dẫn bạn phải cài đặt chương trình **FlashGet** trước trên máy của bạn.



Hình 7.16 – Hộp thoại hiển thị khi click chuột phải vào **Bkav406**.

Bạn click phải chuột vào **link** và chọn chức năng **Download using FlashGet**, hộp thoại **Add New Download** xuất hiện và bạn nhập một số thông tin phù hợp như **proxy**, số phần chia tập tin, sau đó chọn **OK**.

Trong mục **Split File** ta nhập giá trị số phần tập tin bị cắt ra, mục **Proxy** là cổng ra ngoài **Internet** của máy bạn.



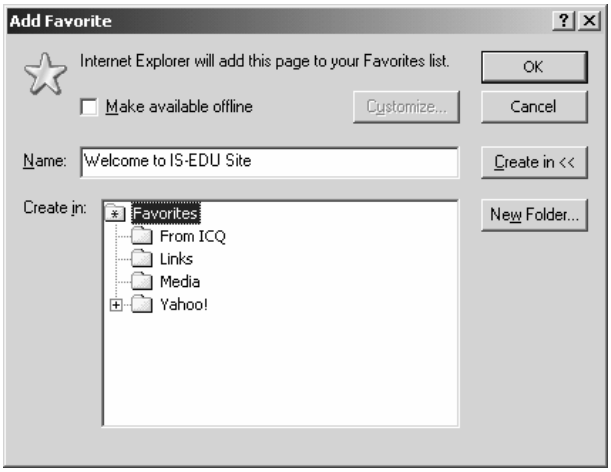
Hình 7.17 – Hộp thoại hiển thị sau khi chọn **Download using FlashGet**.

Trong ví dụ này file **Bkav405**.exe được phân ra thành 5 tập tin và trên màn hình hiển thị tiến độ **download** của mỗi phần.

Hình 7.18 – Hộp thoại hiển thị tiến trình download tập tin Bkav405.exe

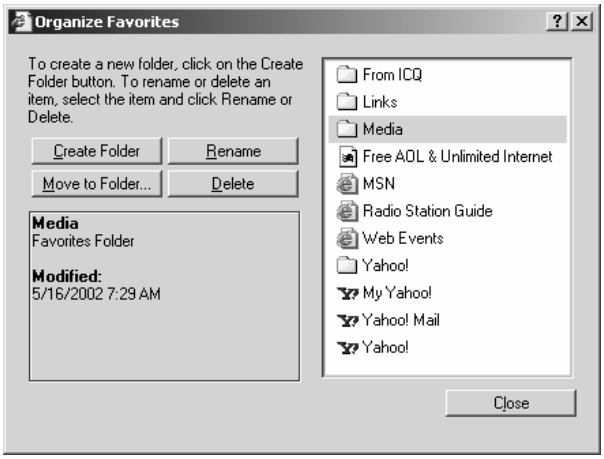
Tổ chức lưu trữ địa chỉ các trang Web thường truy cập.

Khi duyệt Web, ta muốn lưu lại địa chỉ một số trang Web hay và tổ chức theo trật tự dễ nhớ, dễ tìm kiếm. Muốn lưu địa chỉ trang Web hiện hành bạn vào menu **Favorites** chọn **Add to Favorites**, hộp thoại **Add Favorites** xuất hiện, bạn chọn vị trí lưu và nhập tên của trang Web, sau đó chọn **OK**. Nếu bạn muốn tạo thêm thư mục riêng thì chọn **New Folder.**



Hình 7.19 – Hộp thoại hiển thị sau khi chọn **Add Favorites**.

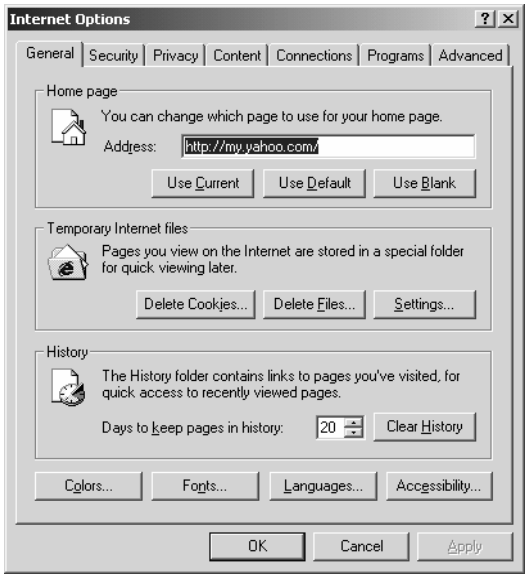
Bạn muốn tìm địa chỉ các trang Web đã lưu hay sắp xếp các địa chỉ của các trang này theo tổ chức nhất định bạn vào menu **Favorites** và chọn chức năng **Organize Favorites**. Hộp thoại **Organize Favorites** xuất hiện, bạn Click vào **Create Folder** để tạo mục mới, thay đổi tên thư mục click vào **Rename**, di chuyển thư mục chọn **Move to Folder**, xóa chọn **Delete**. Bạn muốn xem nội dung mục nào thì **Double Click** vào mục đó. Muốn di chuyển trang Web hoặc một thư mục con vào một thư mục khác thì bạn click và kéo thả vào thư mục đó.



Hình 7.20 – Hộp thoại **Organize Favorites**.

Cấu hình Internet Option.

Phần lớn các cấu hình quan trọng của **IE** đều tập trung trong hộp thoại **Internet Options**. Muốn mở hộp thoại này bạn vào menu **Tools** chọn **Internet Option**.



Hình 7.21 – Hộp thoại **Internet Options**.

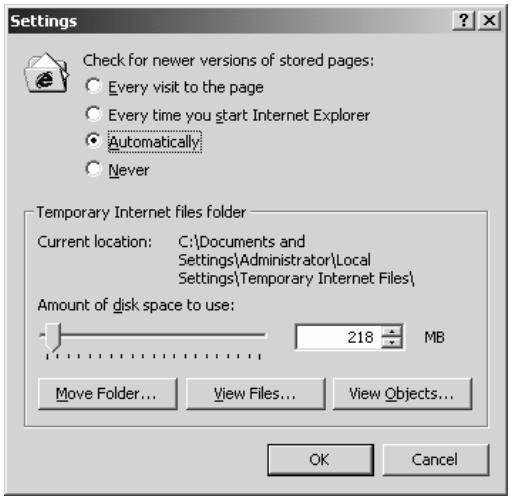
Trong phần **HomePage**, chỉ ra địa chỉ trang Web làm **HomePage** trong ô **Address**. Ngoài ra, còn có thể sử dụng các nút lệnh như : sử dụng trang Web hiện hành làm **HomePage** click vào **Use Current**, sử dụng http://www.adminviet.net/ làm **HomePage** click vào **Use Default**, không sử dụng **HomePage** click vào **Use Blank**.

Khi truy cập thông tin Web, để tiết kiệm thời gian cho các lần truy cập sau, các **Web Browser** thường lưu trữ tạm các thông tin đã truy cập trên đĩa. Vùng lưu trữ tạm này gọi là **Cache**. Như vậy, khi truy cập một trang Web, trước tiên **Web Browser** sẽ kiểm tra trang Web cần truy cập đã có trong **cache** hay chưa, nếu có nó sẽ hiển thị thông tin trong **cache** thay vì phải truy cập vào **Web Server** để lấy thông tin. Tuy nhiên, thông tin lưu trữ trong **cache** có thể bị lạc hậu so với thông tin thực tế do đó các **Web Browser** phải có cơ chế kiểm tra. Trong **Internet Explorer**, có bốn cơ chế:

- **Every visit to the page**: kiểm tra thông tin trong **cache** so với thông tin thực tế mỗi lần truy cập vào một trang Web.
- **Every time you start Internet Explorer**: kiểm tra thông tin trong **cache** so với thông tin thực tế mỗi lần khởi động **Internet Explorer**.
- **Automatically**: tự động hệ thống **IE** sẽ kiểm tra.
- **Never**: không cần kiểm tra, luôn lấy thông tin trong **Cache**.

Cấu hình **Temporary Internet Files**:

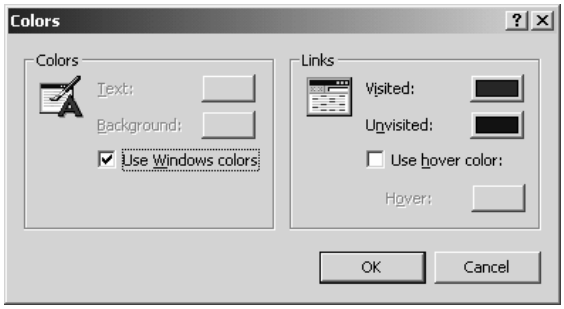
- Click vào **Delete Cookies** để xoá các thông tin mà **IE** lưu trữ trong **Cookies**.
- Click vào **Delete Files** để xoá các file được lưu trữ trong vùng lưu trữ tạm (**cache**)
- Click vào **Setting** để cấu hình các thông số cho vùng lưu trữ tạm. Bạn chọn cách thức kiểm tra của **IE** và thay đổi kích thước của vùng lưu trữ tạm.



Hình 7.22 – Hộp thoại **Settings**.

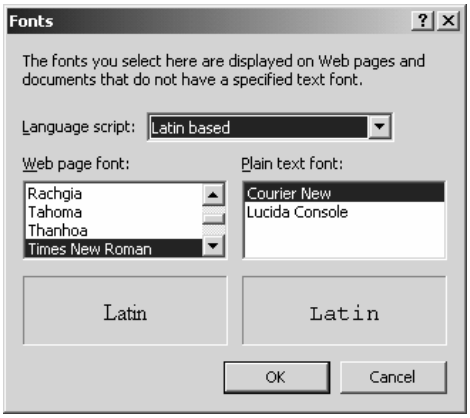
Cấu hình **History**: trong mục **Days to keep pages in history** cho phép ta quy định số ngày mà **IE** nhớ các địa chỉ trang Web mà ta đã duyệt qua. Muốn xóa tất cả các địa chỉ này ta click và nút **Clear History**.

Click vào nút **Colors** để thay đổi màu của các thành phần sau như : màu của văn bản bình thường (các văn bản không phải link), màu nền, màu của các **Link** chưa duyệt qua, màu của các **Link** đã duyệt qua. Ngoài ra, để các link đổi màu khi di chuyển con trỏ chuột tới thì chọn **Use Hover color**, sau đó chỉ định màu cho **Hover**.



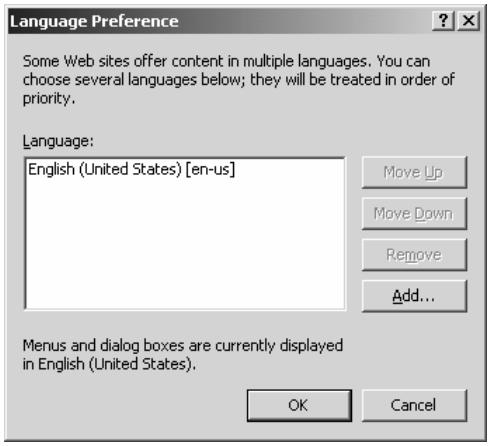
Hình 7.23 – Hộp thoại **Colors**.

Click vào nút **Font** để thay đổi cấu hình của **Font**.



Hình 7.24 – Hộp thoại **Fonts**.

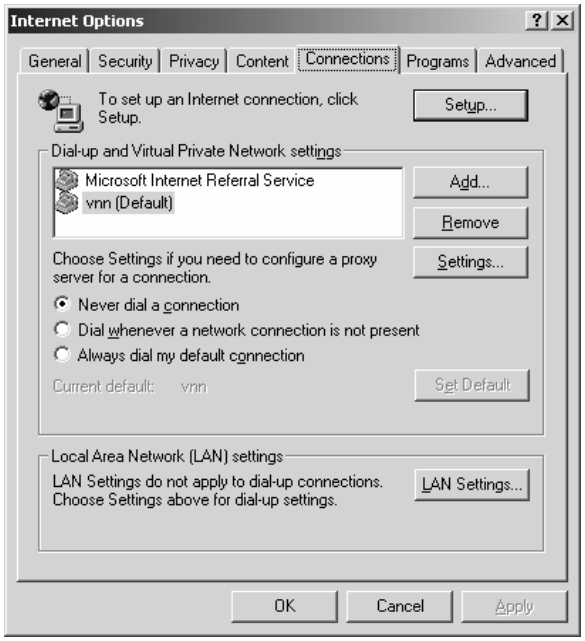
Click vào nút **Language** để chọn ngôn ngữ hiển thị nếu Website đó hỗ trợ đa ngôn ngữ.



Hình 7.25 – Hộp thoại **Language**.

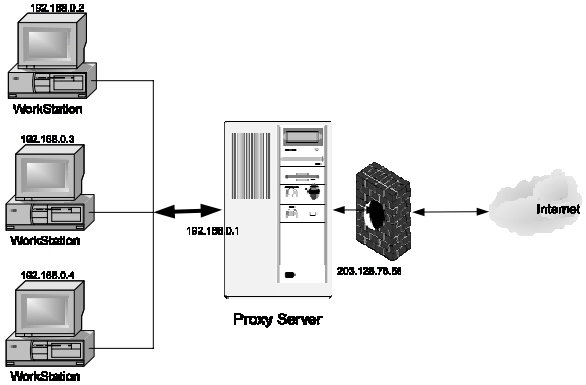
Cấu hình kết nối Internet.

Muốn truy cập được **Internet**, bạn phải tạo các kết nối **Internet**, hai kết nối thông dụng là **Dial-up** và **LAN**. Trong **Tab Connections** bạn có thể chọn các kết nối **Dial-up** có sẵn hay tạo kết nối khác. Nếu bạn chọn hình thức kết nối **Internet** qua mạng **LAN** thì bạn click vào nút **LAN Settings**.



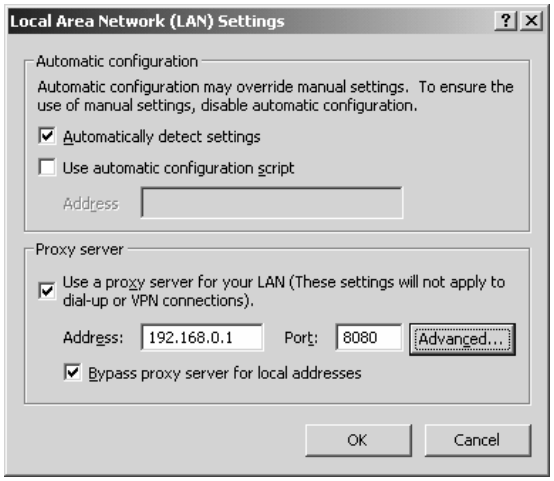
Hình 7.26 – Hộp thoại **Internet Options – Tab Connections**.

Thông thường các máy trạm truy cập **Internet** qua mạng **LAN** thì các máy trạm này không trực tiếp lên **Internet** để lấy thông tin mà gởi yêu cầu đến một máy làm đại diện (**proxy**). Máy đại diện này được kết trực tiếp lên **Internet**, do đó máy này sẽ lấy thông tin giúp các máy trạm và gởi trả các thông tin về cho các máy trạm. Máy trạm nhận thông tin và hiển thị nội dung lên màn hình giúp cho người dùng cảm giác như mình được trực tiếp sử dụng các dịch vụ **Internet** nhưng thực tế thì không. Như vậy, các máy trạm muốn truy cập **Internet** thì phải khai báo địa chỉ máy **Proxy**.



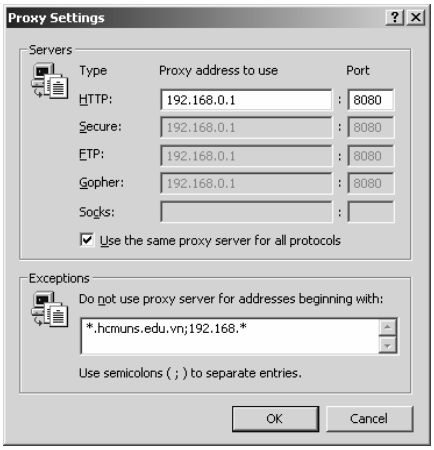
Hình 7.27 – Mô tả mô hình hoạt động của **Proxy**.

Trong hộp thoại **LAN Setting**, bạn nhập địa chỉ **IP** của **Proxy** và giá trị **port** mà **proxy** cho phép các máy trạm đi qua.



Hình 7.28 – Hộp thoại **LAN Settings**.

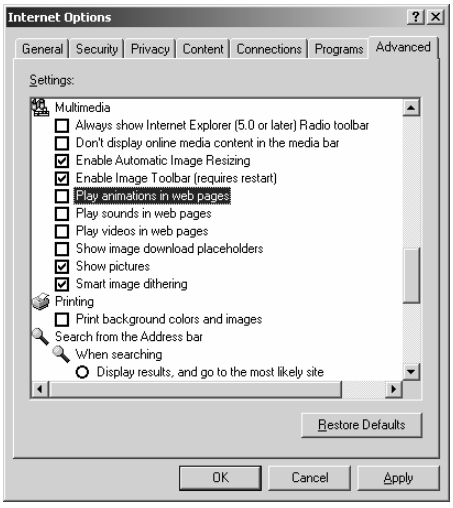
Ngoài ra có một số địa chỉ mà ta muốn truy cập trực tiếp mà không cần qua **Proxy**, thì ta nhập vào ô **Exceptions**.



Hình 7.29 – Hộp thoại **Proxy Settings**.

Duyệt web không trình diễn hình và nhạc

Đôi lúc ta cần tìm nhanh một tài liệu nào đó trên mạng mà chỉ cần text không cần hình ảnh thì ta nên tắt chế độ trình diễn hình và nhạc trên **IE** vì khi tắt các chế độ này đi thì trang web sẽ được duyệt nhanh hơn. Ta vào menu **Tools/Internet Option** chọn **Tab Advanced**, trong mục **Multimedia** bỏ các đánh dấu vào các mục: **play animations**, **play sounds**, **play videos**.



Hình 7.30 – Hộp thoại **Internet Options – Tab Advance**.

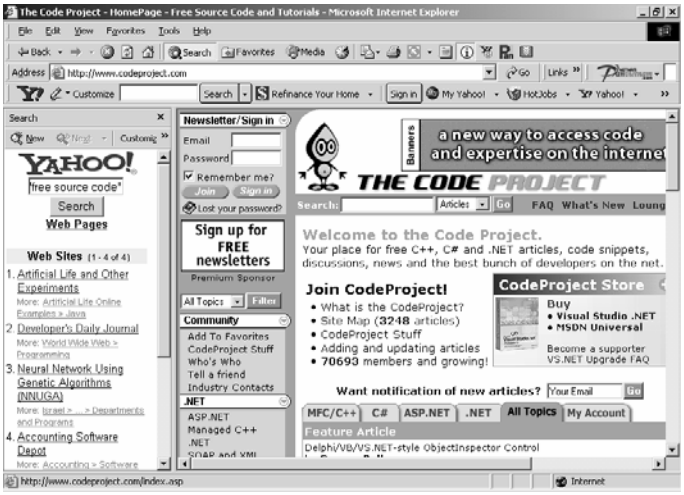
V.4. Search Engine và tìm kiếm thông tin trên Web.

Giới thiệu về Search Engine.

Search Engine thông thường là một hệ thống mạng lớn chạy song song và có thể xử lý phân tán chạy trên nhiều máy tính. Hệ thống này được chia thành ba tầng chính, gồm tầng thu thập thông tin, nhận dạng và chuyển đổi thông tin thành dạng text, lập cơ sở dữ liệu cho các thông tin dạng text. Mỗi tầng được chia thành nhiều đơn vị độc lập hoạt động theo kiểu chia sẻ tính toán hoặc dự trữ (redundant), từ đó tính tin cậy và hiệu năng của hệ thống rất cao. Đơn vị khai thác dữ liệu được tích hợp cùng với phần lập chỉ mục cơ sở dữ liệu, cho phép khai thác qua các client sử dụng giao thức **TCP/IP** trên bất kỳ hệ thống nào (**Windows**, **Unix**…). Việc chia hệ thống thành các khối chức năng phối hợp với nhau thông qua bộ điều phối, hệ thống có thể phân tán để xử lý trên nhiều máy tính nhỏ hay tập trung toàn bộ trên hệ thống máy lớn. Vì vậy, lượng dữ liệu mà hệ thống có thể phục vụ, về mặt nguyên tắc cho phép đến hàng trăm triệu tài liệu.

Tìm kiếm thông tin trên Web

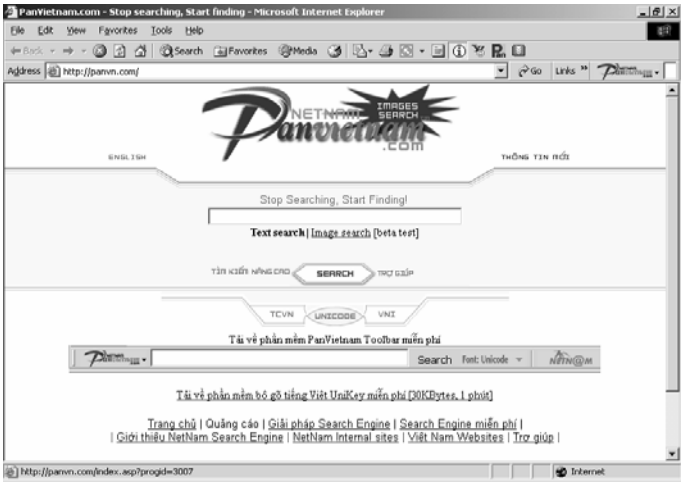
Công cụ tìm kiếm trên **IE**, bạn muốn tìm kiếm trong **IE** bạn click vào nút **Search** trên thanh trạng thái, bên trái của cửa sổ **IE** xuất hiện hộp thoại tìm kiếm, bạn nhập chuỗi cần tìm kiếm. Ví dụ như hình sau ta tìm kiếm các trang Web cung cấp miễn phí các **source code** hỗ trợ học tập.



Hình 7.31 – Kết quả sau khi **Search** bằng từ khóa "**free source code**".

Công cụ tìm kiếm ***Panvietnam***, **Panvietnam** sử dụng hầu hết các công nghệ mới nhất trong tìm kiếm thông tin tương tự như **Google** nhưng nó còn tích hợp thêm các công nghệ đặc thù dành cho **Việt Nam** như:

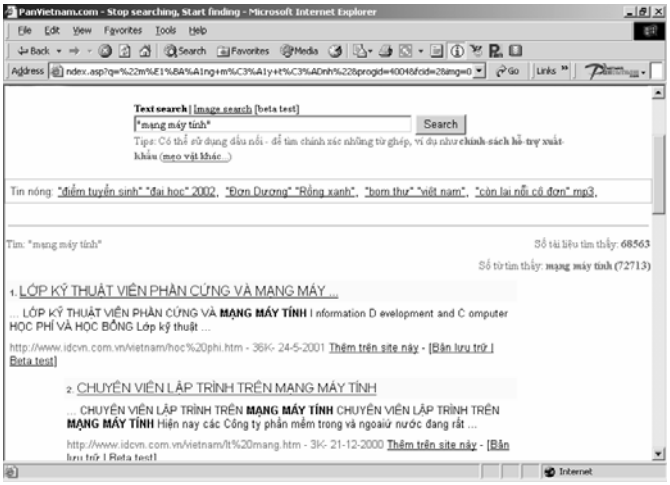
- Hỗ trợ tiếng việt với cả ba bộ mã chính như : **Unicode**, **TCVN**, **VNI**. Suy đoán bộ mã tiếng việt thông minh.
- Xử lý song song.
- Cơ chế trả lời kết quả thông minh.
- Hỗ trợ mọi hệ thống sử dụng chuẩn giao tiếp **TCP** (**Windows**, **Unix**, **Macitosh**).
- Không giới hạn số lượng tài liệu tìm kiếm.
- Tốc độ cập nhật thông tin mới nhanh.
- Hỗ trợ trên 200 định dạng tài liệu phổ biến nhất.



Hình 7.32 – Trang Web **Panvietnam**.

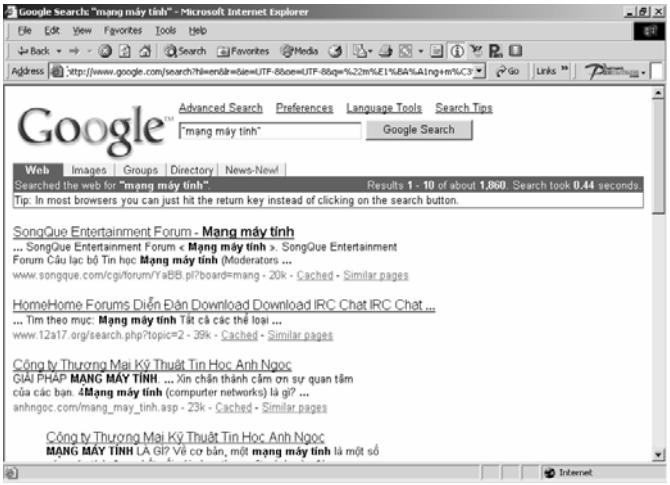
Bạn nhập vào chuỗi cần tìm kiếm mạng máy tính thì kết quả trả về như hình sau. Mỗi kết quả tìm được là một đường link đến một Website chứa thông tin mà ta cần tìm. Muốn xem chi tiết nội dung thì ta

click chuột vào đường **link** này.



Hình 7.33 – Kết quả search từ khóa “mạng máy tính” trên **PanVietnam**.

Công cụ tìm kiếm ***Google***, **Google** là một công cụ tìm kiếm thông tin toàn cầu trên **Internet** mạnh nhất hiện nay. Tiện ích này giúp ta có thể tìm kiếm thông tin với rất nhiều ngôn ngữ khác nhau. Trong hình sau ta cũng tìm kiếm các trang Web chứa thông tin mạng máy tính.

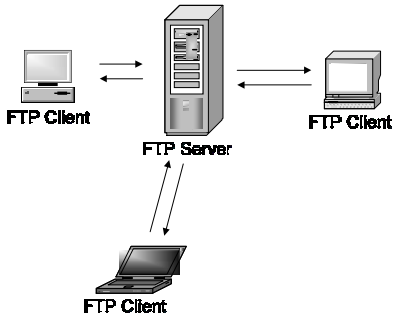


Hình 7.34 – Kết quả **search** từ khóa “mạng máy tính” trên **Google**.

VI. DỊCH VỤ FTP.

VI.1. Mô hình hoạt động của FTP.

FTP (**File Transfer Protocol**) là một dịch vụ cho phép ta truyền tải file giữa hai máy tính ở xa dùng giao thức **TCP/IP**. **FTP** cũng là một ứng dụng theo mô hình **client-server**, nghĩa là máy làm **FTP Server** sẽ quản lý các kết nối và cung cấp dịch vụ tập tin cho các máy trạm. Nói tóm lại **FTP Server** thường là một máy tính phục vụ cho việc quảng bá các tập tin cho người dùng hoặc là một nơi cho phép người dùng chia sẻ tập tin với những người dùng khác trên **Internet**. Máy trạm muốn kết nối vào **FTP Server** thì phải được **Server** cấp cho một **account** có đầy đủ các thông tin như: địa chỉ máy **Server** (tên hoặc địa chỉ **IP**), **username** và **password**. Phần lớn các **FTP Server** cho phép các máy trạm kết nối vào mình thông qua **account anonymous** (**account anonymous** thường được truy cập với **password** rỗng). Các máy trạm có thể sử dụng các lệnh **ftp** đã tích hợp sẵn trong hệ điều hành hoặc phần mềm chuyên dụng khác để tương tác với máy **FTP Server**.



Hình 7.35 – Mô hình hoạt động của **FTP Server**.

VI.2. Tập hợp các lệnh FTP.

Lệnh	Chức năng
!	Chạy chương trình **command dos** trên máy tính cục bộ.
?	Hiển thị giúp đỡ của các lệnh **Ftp**, lệnh này giống với lệnh **Help**.
Append	Chèn nội dung của một tập tin trên máy tính cục bộ vào cuối của một tập tin trên máy tính ở xa (máy **FTP Server**), dùng định dạng tập tin hiện tại.
Ascii	Đặt loại định dạng truyền file là **ASCII**, giá trị này là mặc định khi khởi tạo kết nối **FTP**.

Bell	Bật trạng thái chuông là **on/off**. Nếu là **on** thì sau mỗi lần lệnh truyền file hoàn thành thì máy phát ra tiếng chuông. Mặc định trạng thái này là **off**.
Binary	Đặt loại định dạng truyền file là **binary**.
Bye	Tắt kết nối với máy tính ở xa và thoát khỏi chương trình **FTP**.
Cd	Thay đổi thư mục hiện thành trên máy ở xa(**Server**).
Close	Ngừng phiên giao dịch với máy tính ở xa và trở về dòng lệnh của chương trình **ftp**.
Debug	Bật trạng thái **Debugg on/off**. Nếu là **on** thì mỗi lệnh gởi đến máy tính ở xa thì chương trình sẽ in ra các thông báo. Mặc định là trạng thái là **off**.
Delete	Xoá tập tin trên máy tính ở xa.
Dir	Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại.
Disconnect	Tắt kết nối với máy tính ở xa và trở về dòng lệnh **FTP**.
Get	Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại.
Help	Hiển thị giúp đỡ của các lệnh **Ftp**.
Lcd	Thay đổi thư mục hiện trên máy tính cục bộ. Mặc định là thư mục đang làm việc trên máy tính cục bộ.
Ls	Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại.
Mdelete	Xóa nhiều tập tin cùng trên một máy tính ở xa.

Mget	Chép nhiều tập tin từ máy tính ở xa về máy tính cục bộ dùng định dạng truyền file hiện tại.
mkdir	Tạo thư mục trên máy tính ở xa.
Mput	Chép nhiều tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại.
open	Mở một kết nối đến máy **FTP Server**.
Put	Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại.
Pwd	Hiển thị thư mục hiện hành trên máy tính ở xa.
Quit	Tắt kết nối với máy tính ở xa và thoát khỏi chương trình **FTP**.
Recv	Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. Tương tự như lệnh Get.
Rename	Đổi tên tập tin, thư mục trên máy tính ở xa.
Rmdir	Xóa một thư mục ở xa.
Send	Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. Tương tự như Put.
Status	Hiển thị các trạng thái lựa chọn của kết nối FTP.
type	Đặt hoặc hiển thị định dạng truyền file.
user	Định người dùng khi kết nối đến máy tính ở xa.

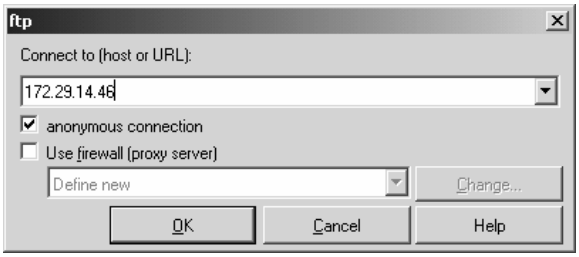
VI.3. Dùng FTP trong Windows Commander.

Giới thiệu.

Windows Commander là chương trình quản lý tập tin và thư mục được sử dụng rộng rãi nhất hiện nay. Đồng thời **Windows Commander** cũng đã tích hợp chương trình **FTP Client**. Với chương trình trạm này, bạn có thể truy cập đến 10 **FTP Server** cùng lúc trên **Internet** hoặc trên **Intranet**. Chương trình **FTP client** này không chỉ cho phép **upload** và **download file** mà còn hỗ trợ truyền files trực tiếp từ máy tính ở xa đến một máy tính khác. Bạn có thể thao tác trên **FTP Client** giống như các tính năng của **Windows Commander**. Ví dụ như: sao chép (F5), đổi tên (SHIFT+F6), xóa (F8), tạo thư mục (F7).

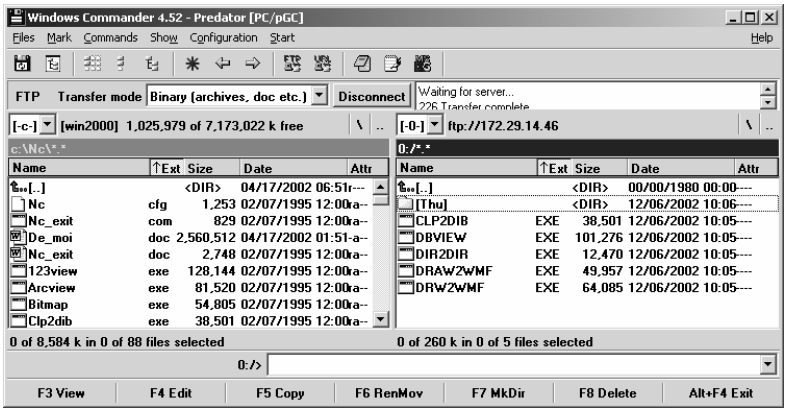
Tạo kết nối mới:

Bạn vào menu **Commands** chọn **FTP New Connection**. Hộp thoại **FTP** xuất hiện, trong mục **Connection to** bạn nhập vào địa chỉ của máy **FTP Server** mà bạn cần kết nối, chọn **OK**.



Hình 7.36 – Hộp thoại sau khi chọn **FTP New Connection**.

Sau đó chương trình yêu cầu bạn nhập **User** và **Password** vào. Nếu đúng chương trình sẽ kết nối vào **Server** và lúc đó trên màn hình có hai cửa sổ. Cửa sổ bên trái hiển thị các tập tin trên máy cục bộ, cửa sổ bên phải hiển thị các tập tin trên máy tính ở xa (máy **Server**).



Hình 7.37 – Giao diện chương trình **Windows Commander**.

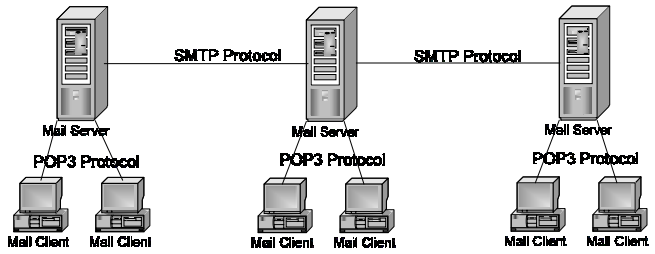
Sau khi đã kết nối bạn có thể thực hiện các thao tác tập tin giữa máy tính cục bộ và máy tính ở xa thông qua hai cửa sổ trên. Khi muốn hủy kết nối bạn click chuột vào nút **Disconnect**, chương trình sẽ trở về trạng thái bình thường.

VII. E-MAIL.

VII.1. Mô hình hoạt động.

E-mail (**electronic mail**) là thư điện tử, là một hình thức trao đổi thư từ nhưng thông qua mạng **Internet**. Dịch vụ này được sử dụng rất phổ biến và không đòi hỏi hai máy tính gởi và nhận thư phải kết nối **online** trên mạng..

Tại mỗi **Mail Server** thông thường gồm hai dịch vụ: **POP3** (**Post Office Protocol 3**) làm nhiệm vụ giao tiếp mail giữa **Mail Client** và **Mail Server**, **SMTP** (**Simple E-mail Transfer Protocol**) làm nhiệm vụ giao tiếp **mail** giữa các máy **Mail Server**.



Hình 7.38 – Mô hình hoạt động của **Mail Server**.

Để sử dụng **E-mail**, người dùng cần có một **account mail** do nhà cung cấp dịch vụ **Internet** (**ISP**) cấp bao gồm các thông tin sau: địa chỉ **mail** (ví dụ: **nvteo@hcm.vnn.vn**), **username**, **password** và địa chỉ của **Mail Server** mà mình đăng ký. Sau đó chọn một chương trình **Mail Client** (**Outlook Express**, **Eudora**, **Netscape**...) và cấu hình các thông số trên vào chương trình đó. Từ đó bạn có thể sử dụng chương trình này để soạn thảo và gởi nhận mail một cách dễ dàng.

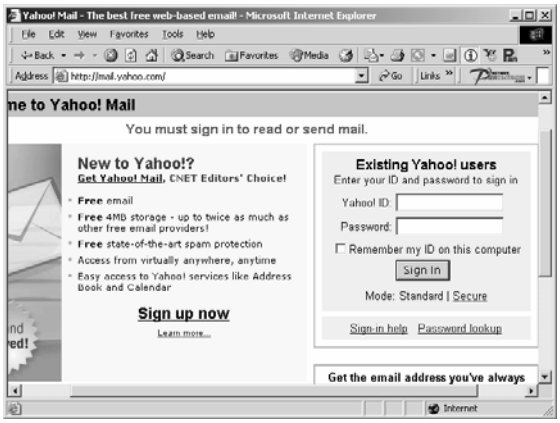
VII.2. Các loại mail.

Thông thường có hai loại mail thông dụng là WebMail và **POP Mail**. **Webmail** là loại mail mà hình thức giao dịch mail giữa **Client** và **Server** dựa trên giao thức **Web** (**http**), thông thường **Webmail** là miễn phí. Còn **POP Mail** là loại mail mà các **Mail Client** tương tác với **MAIL SERVER** bằng giao thức **POP3**. Mail loại này tiện lợi và an toàn hơn nên thông thường là phải đăng ký thuê bao với nhà cung cấp dịch vụ.

VII.3. Sử dụng WebMail.

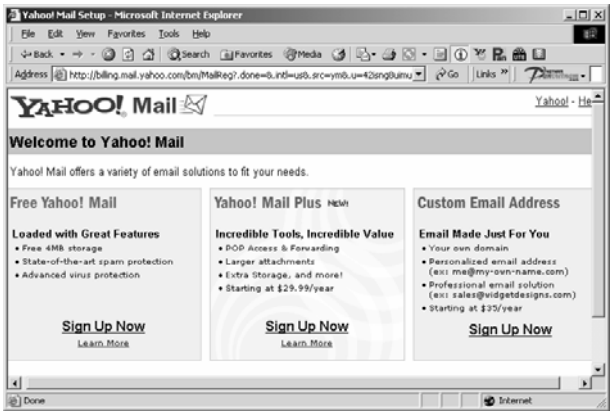
Bạn muốn có một địa chỉ mail **Internet** để giao dịch với bạn bè trên thế giới, bạn có thể đến nhà cung cấp dịch vụ **Internet** để đăng ký hoặc tự tạo cho mình một địa chỉ mail miễn phí trên các **Website** nổi tiếng như **Yahoo**, **Hotmail**, **Fpt**, **Vnn**... Trong ví dụ này sẽ hướng dẫn bạn tạo một địa chỉ mail miễn phí trên **Yahoo**.

Đầu tiên bạn vào **Website** của **Yahoo** và bạn click vào **Sign up now**.



Hình 7.39 – Trang Web Mail của **Yahoo**.

Yahoo sẽ hiện ra ba dịch vụ mail cung cấp cho khách hàng và bạn chọn dịch vụ đầu tiên vì đây là dịch vụ miễn phí. Hai dịch vụ sau đều phải thuê bao. Bạn click vào **Sign up now** trong phần **Free Yahoo Mail**.

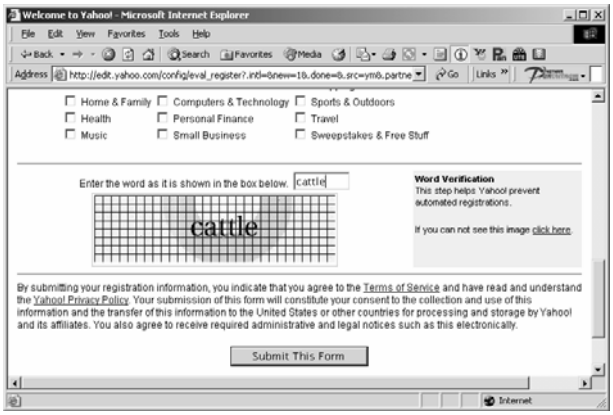


Hình 7.40 – Giao diện sau khi chọn **Sign up now**.

Yahoo sẽ hiện bảng thông tin cá nhân và bạn nhập vào các thông tin này như: địa chỉ mail mà bạn đề xuất, password, ngày tháng năm sinh, tên, mã vùng.

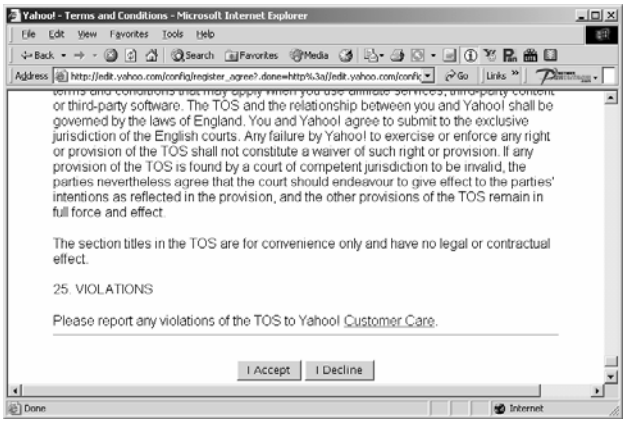
Hình 7.41 – Giao diện để tạo một địa chỉ mail **Yahoo** mới.

Để tránh các **hacker** tạo tự động địa chỉ mail, **Yahoo** xây dựng tính năng **Word Verification**. Do đó bạn phải quan sát chữ trên hình và nhập chữ đó vào **textbox** của mục **Word Verification**. Sau đó click vào **Submit This Form** để cập nhật các thông tin vừa nhập lên **Yahoo Server**.



Hình 7.42 – Giao diện để tạo một địa chỉ mail **Yahoo** mới (tt).

Nếu thông tin nào không phù hợp thì **Yahoo** sẽ tô màu đỏ, lúc đó bạn xem hướng dẫn của **Yahoo** và điều chỉnh cho phù hợp. Sau khi đăng ký thành công **Yahoo** sẽ thông báo với bạn các thông tin về **Yahoo**, bạn click vào **I Accept** để hoàn thành quá trình đăng ký.



Hình 7.43 – Giao diện gởi các thông tin tạo một địa chỉ mail mới.

Nếu quá trình đăng ký thành công thì **Yahoo** sẽ thông báo như màn hình sau. Từ đây bạn có thể sử dụng địa chỉ mail **hocvienmang02@yahoo.com** để giao dịch với mọi người trên thế giới.

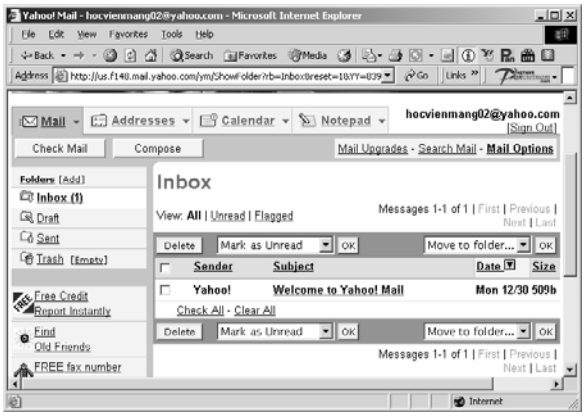
Hình 7.44 – Giao diện sau khi tạo thành công một địa chỉ mail **Yahoo** mới.

Bạn đã có một **account mail** trên **Yahoo**, mỗi lần bạn muốn gởi nhận mail thì bạn vào trang Web **http://mail.yahoo.com**, sau đó bạn nhập **ID mail** và **password** vào chọn **Sign in**

Hình 7.45 – Giao diện để bắt đầu đăng nhập vào **Mail Yahoo**.

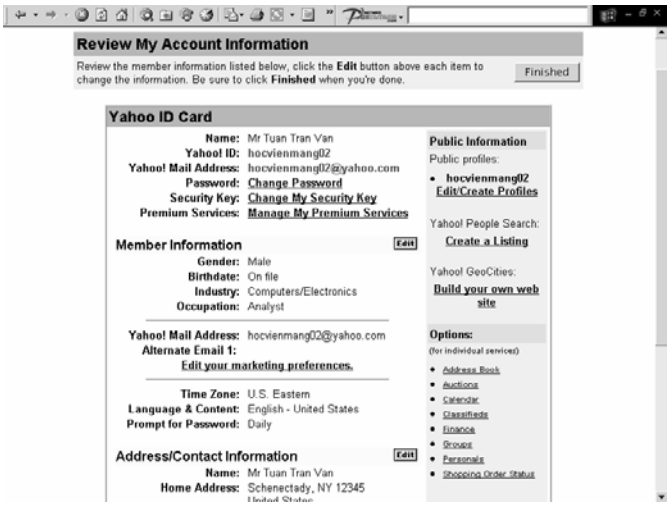
Yahoo cung cấp cho bạn một giao diện tương tác mail rất tiện lợi. Muốn xem các mail mới nhận được bạn click vào **Inbox**, lúc đó cửa sổ bên phải sẽ hiện toàn bộ các mail mà bạn nhận được. Bạn click vào chủ đề của mail để đọc nội dung chi tiết của mail. Bạn click vào các mục còn lại như: **Draft** chứa các mail soạn chưa hoàn thành, **Sent** chứa các mail đã gởi đi, **Trash** chứa các mail đã xóa giúp bạn có thể

phục hồi các mail bị xóa nhầm.



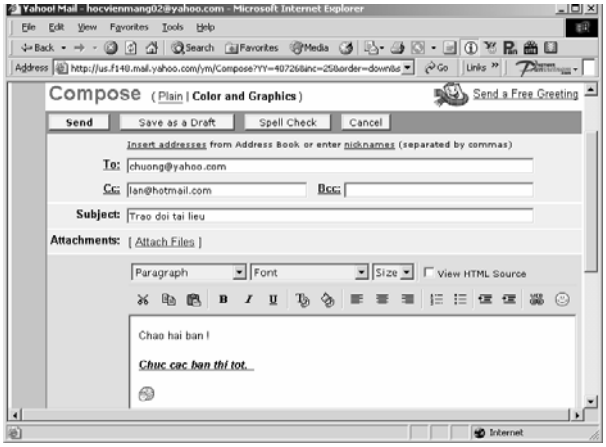
Hình 7.46 – Giao diện sau khi đăng nhập vào **Mail Yahoo**.

Muốn thay đổi các thông tin cá nhân hoặc thay đổi **password** bạn click vào **Mail Option**, sau đó bạn thay đổi những thông tin cần thiết.



Hình 7.47 – Giao diện sau khi chọn lựa **Mail Option**.

Bạn muốn gởi mail thì click vào **Compose**, màn hình soạn thảo mail xuất hiện. Trong mục **To** bạn nhập địa chỉ mail mà bạn cần gởi đến. Mục **Cc** và **Bcc** bạn nhập vào địa chỉ mail của những người cùng nhận mail này. Mục **Subject** bạn nhập chủ đề của mail, **Attachments** cho phép bạn gởi mail có file đính kèm. Các nút khác trên thanh công cụ giúp bạn soạn thảo mail, các tính năng này giống như các tính năng của các nút trên thanh công cụ của **Word**. Sau khi soạn thảo xong bạn click vào **Send** để gởi mail đi.



Hình 7.48 – Giao diện sau khi chọn lựa **Compose** (để tạo một mail mới).

VII.4. Sử dụng Outlook Express.

Giới thiệu:

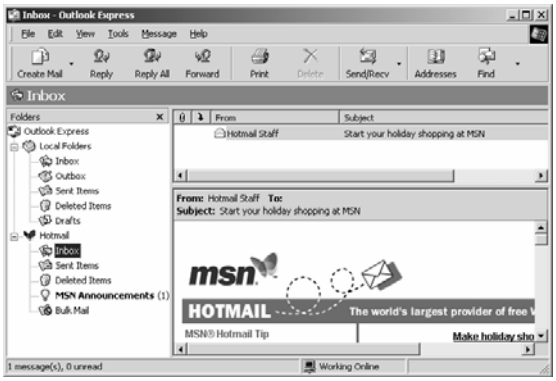
Với một kết nối **Internet** và chương trình **Outlook Express**, bạn có thể trao đổi thư điện tử (**E-mail**) với tất cả mọi người trên **Internet** và gia nhập vào bất kỳ một nhóm tin (**newsgroup**) nào.

Chương trình **Internet Connection Wizard** giúp bạn kết nối với một hoặc nhiều **Mail** hoặc **News Server**. Khi bạn cấu hình thì bạn cần những thông tin từ nhà cung cấp dịch vụ **Internet** (**ISP**) hoặc người quản trị mạng nội bộ (**LAN administrator**) như:

- Cấu hình tài khoản mail, bạn cần tên tài khoản của bạn (**account name**) và mật khẩu (**password**). Đồng thời bạn phải có tên (**mail.hcm.vnn.vn**) hoặc địa chỉ (**203.168.10.200**) của **Incoming** và **Outcoming Mail Server**.
- Đọc tin, bạn cần tên của **News Server** mà bạn muốn kết nối. Nếu có yêu cầu bạn phải có tên tài khoản và mật khẩu.

Một chương trình **Mail Client** cơ bản thông thường có các folder sau:

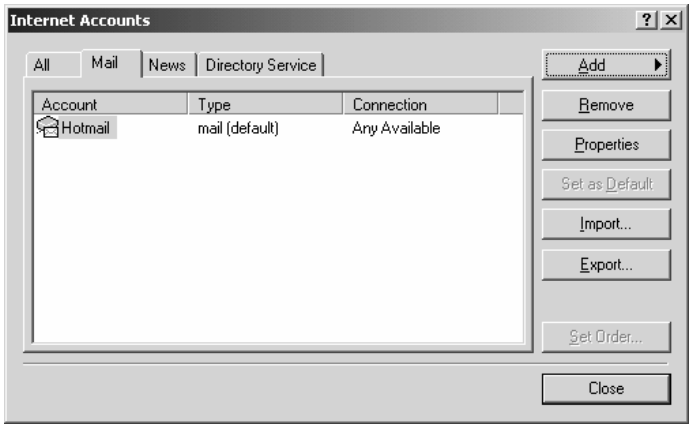
- **Inbox**: chứa các thư đã nhận
- **Outbox**: chứa các thư chuẩn bị gởi đi
- **Send** Items: chứa các thư đã gởi đi
- **Deleted Items**: chứa các thư đã xóa, giúp ta có thể phục hồi khi xoá nhập một thư nào đó.
- **Drafts**: chứa các mail đang soạn dở dang.



Hình 7.49 – Giao diện của **Outlook Express**.

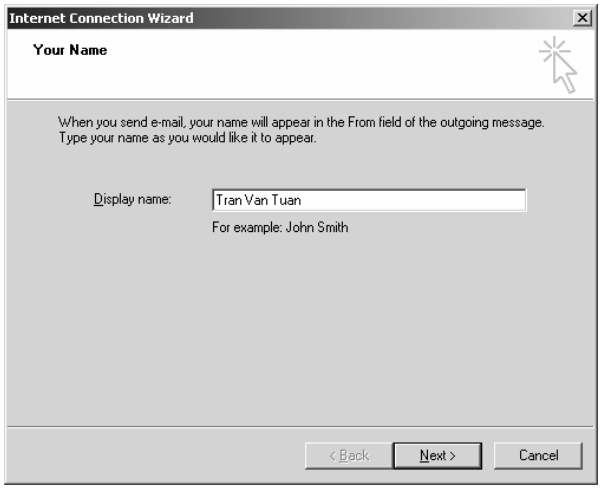
Các cấu hình cơ bản.

Thêm tài khoản mail: muốn cấu hình mail bạn phải biết loại **Mail Server** bạn dùng (**POP3**, **IMAP**, **HTTP**), tài khoản, mật khẩu, tên của **incoming mail server** loại P**O**P3 và **IMAP**, tên của **outcoming mail server**. Sau khi có đủ các thông tin bạn vào menu **Tools**, click vào **Account**, hội thoại **Internet Account** xuất hiện, click vào nút **Add**, chọn **mail**.



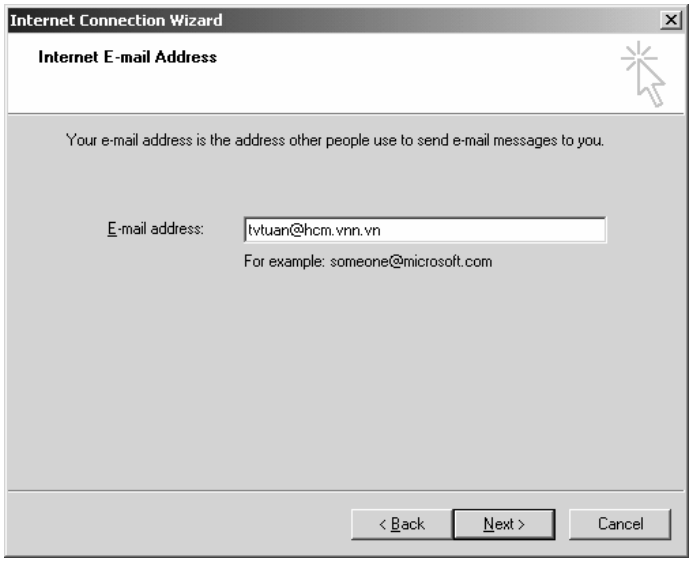
Hình 7.50 – Hộp thoại **Internet Accounts**.

Sau khi hộp thoại **Internet Connection Wizard** xuất hiện, trong mục **Display name** bạn nhập tên của bạn vào, chọn **Next.**



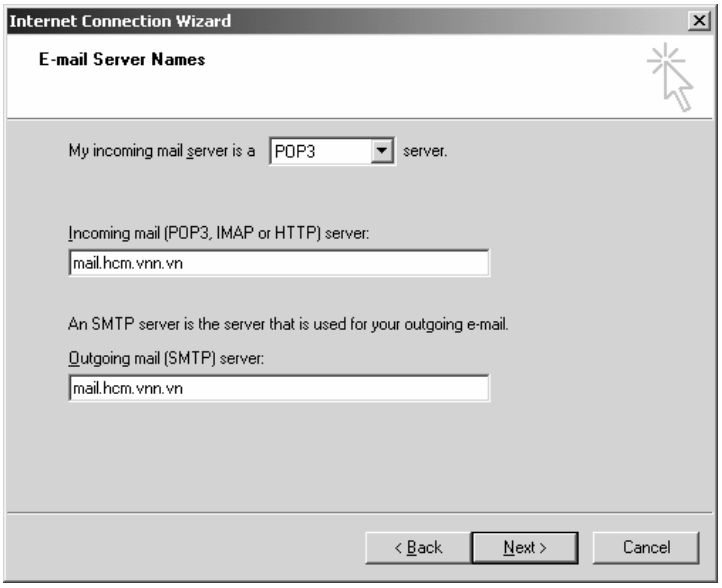
Hình 7.51 – Giao diện hộp thoại **Internet Connection Wizard**.

Trong hộp thoại **Internet E-Mail Address**, trong mục **E-mail address** bạn nhập vào địa chỉ mail của bạn vào.



Hình 7.52 – Hộp thoại **Internet Connection Wizard** (tt).

Trong hộp thoại **E-mail Server Name** bạn nhập vào tên hoặc địa chỉ của **Server Incoming** và **Outcoming**. Đồng thời bạn chú ý là hiện tại mình đang dùng **protocol pop3** để tương tác với **Server Mail** (bạn có thể sử dụng các protocol khác như **imap**, **http** nhưng với điều kiện là **Server Mail** phải hỗ trợ), sau đó chọn **Next**.

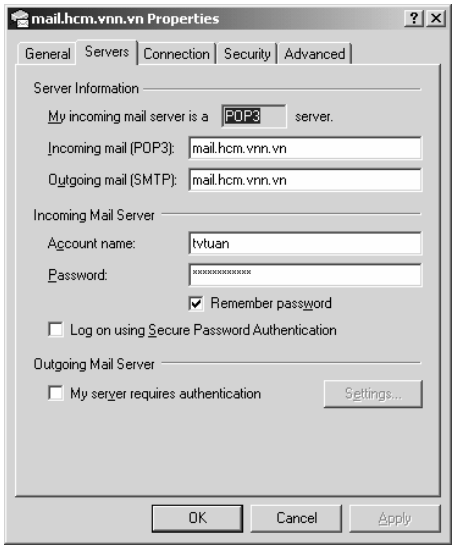


Hình 7.53 – Hộp thoại **Internet Connection Wizard** (tt).

Trong hộp thoại **Internet Mail Logon**, trong mục **account name** bạn nhập vào tài khoản của bạn, mục **password** bạn nhập vào mật khẩu của bạn. Nếu bạn đánh dấu vào **Remember password** thì **password** sẽ được nhớ, lần sau bạn check mail thì **outlook** không yêu cầu bạn nhập **password** nữa.

Hình 7.54 – Hộp thoại **Internet Connection Wizard** (tt).

Chọn **Finish** để hoàn thành. Bạn muốn kiểm tra lại các thông tin mình vừa cấu hình bạn chọn **Account** trong **Tab Mail** và click vào nút **Properties.**



Hình 7.55 – Hộp thoại **Mail Properties**.

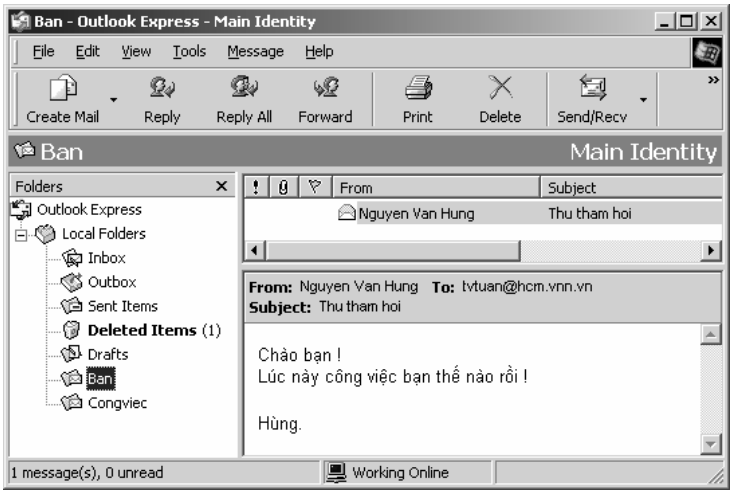
Nhận và đọc thư: sau khi click vào nút **Send/Recv** trên thanh công cụ, **Outlook** sẽ gởi các mail trong **Outbox** ra ngoài và nhận các mail mới đưa vào **Inbox**. Muốn đọc nội dung các mail mới này, ta click chuột vào **Inbox**, lúc đó bên phải sẽ xuất hiện thông tin chi tiết của các mail này và bên dưới là nội dung của mail. Bạn xem hình phía trên.

Xem tập tin gởi kèm: trong màn hình **Preview**, click chuột vào biểu tượng chiếc kẹp giấy, sau đó chọn tập tin gởi kèm rồi chọn **Open** để mở tập tin hoặc chọn **Save to disk** để lưu tập tin vào đĩa.

Trả lời thư: chọn thư cần trả lời và click vào nút **Reply** trên thanh công cụ, sau đó nhập nội dung trả lời và click vào **Send** để gởi đi.

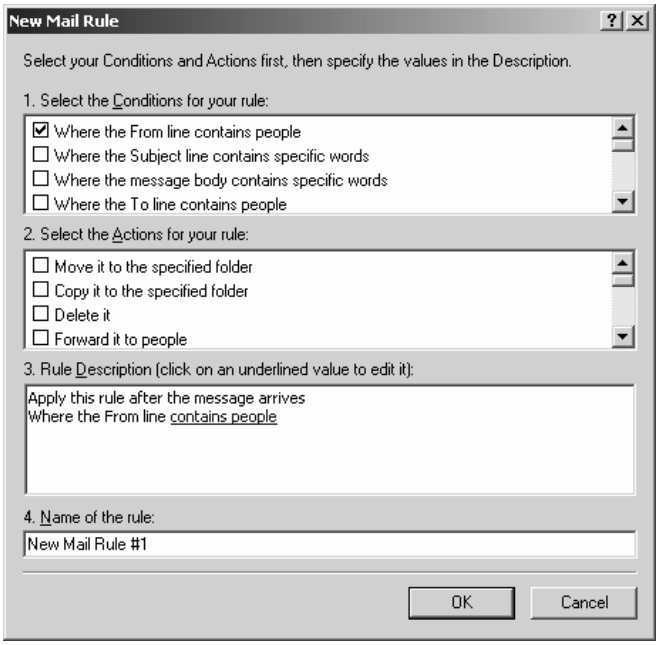
Chuyển tiếp thư: đôi lúc ta muốn chuyển toàn bộ nội dung một mail mà ta nhận được đến một người khác thì ta click phải chuột trên mail đó và chọn chức năng **Forward**, sau đó nhập địa chỉ cần gởi đến. Nếu có nhiều địa chỉ thì các địa chỉ này cách nhau bởi dấu chấm hoặc chấm phẩy.

Tổ chức và sắp xếp thư: để tiện lợi cho việc tìm kiếm và xử lý mail ta nên sắp xếp các mail theo một tổ chức thư mục nhất định. Trước tiên ta cần tạo thêm các thư mục mở rộng bằng cách click phải chuột vào **Local Folders**, chọn **New Folders** và nhập tên thư mục cần tạo. Trong ví dụ sau ta tạo folder **Ban** để chứa các mail của bạn bè, folder **Congviec** để chứa các mail công việc. Sau đó ta vào **Inbox** chọn mail cần di chuyển rồi click phải chuột trên mail đó, chọn **Move to Folder**.



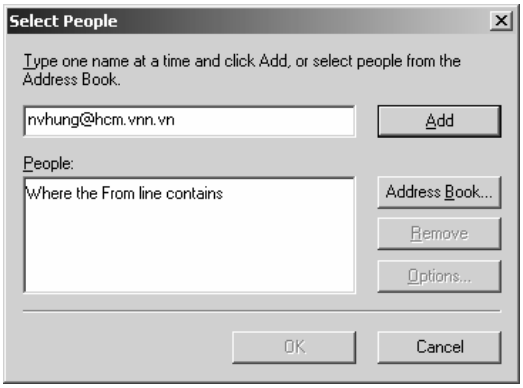
Hình 7.56 – Mail của "Nguyen Van Hung" đã được gởi vào thư mục "Ban".

Quản lý thư bằng các quy tắc (**Rules**): khi bạn giao dịch mail với nhiều người mà bạn sắp xếp các mail bằng tay thì mất rất nhiều thời gian. **Outlook** cung cấp cho ta công cụ **Message Rules** giúp ta có thể quản lý tự động các mail một cách dễ dàng. Một quy tắc (**Rule**) gồm hai phần: phần điều kiện (**Conditions**) chứa một hoặc nhiều điều kiện về mail, phần hành động (**Actions**) chứa một hoặc nhiều hành động ứng với các diều kiện trên. Ví dụ ta muốn khi nhận bất kỳ mail nào của anh Nguyen Van Hung thì tự động chuyển vào Folder **Ban**. Ta làm các bước như sau: vào menu **Tools**/**Message Rules/Mail**… Hộp thoại **New Mail Rules** xuất hiện, trong mục điều kiện (**Select the conditions for your rule**) bạn check vào **Where the from line contains people** thì phía dưới mục **Rules Decription** chứa hàng chữ màu xanh **contains people**.



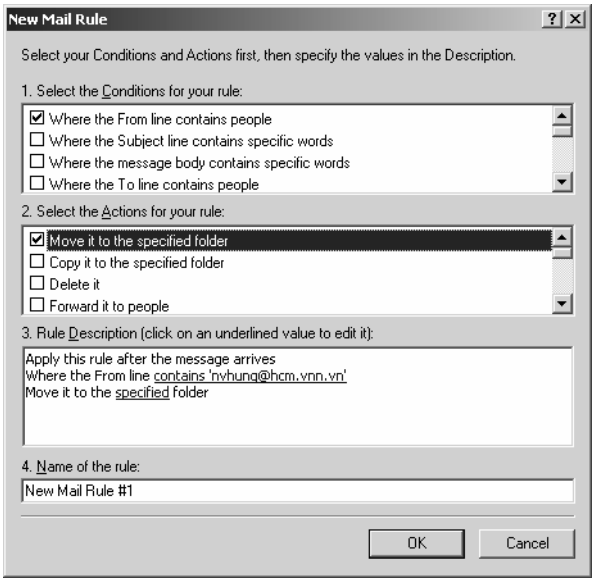
Hình 7.57 – Hộp thoại **New Mail Rule**.

Bạn click vào hàng chữ màu xanh **contains people**, hộp thoại **Select People** xuất hiện. Bạn nhập vào địa chỉ mai của anh Nguyễn Văn Hùng: **nvhung@hcm.vnn.vn**, chọn Add, chọn OK.



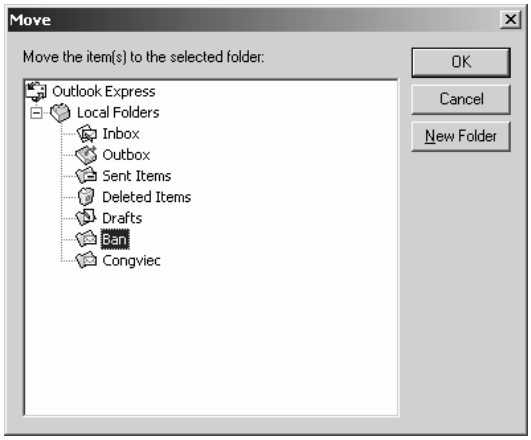
Hình 7.58 - Hộp thoại sau khi chọn **Contains people**.

Bước kế tiếp là bạn chọn hành động cho điều kiện này, trong mục **Select the Actions for your rule** bạn check vào **Move it to the specified folder**.



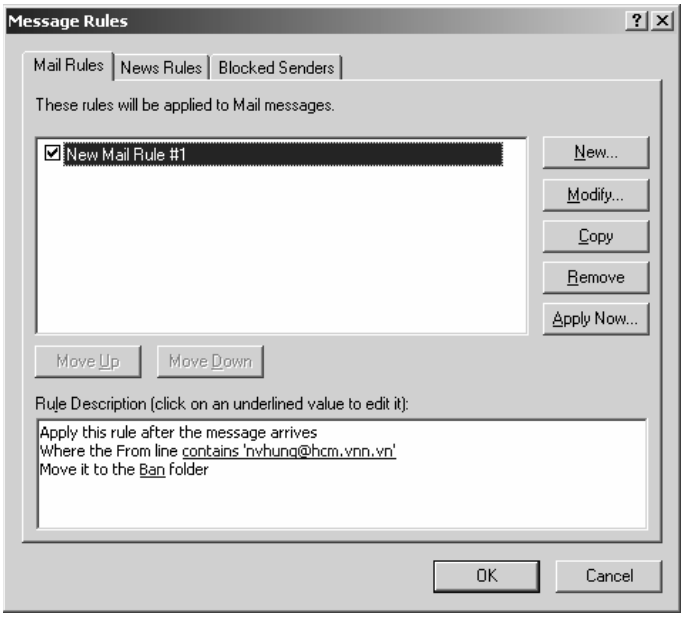
Hình 7.59 – Hộp thoại **New Mail Rule** (tt).

Trong mục **Rule Description**, click vào hàng chữ màu xanh **specified** để chỉ ra thư mục mail sẽ di chuyển đến.



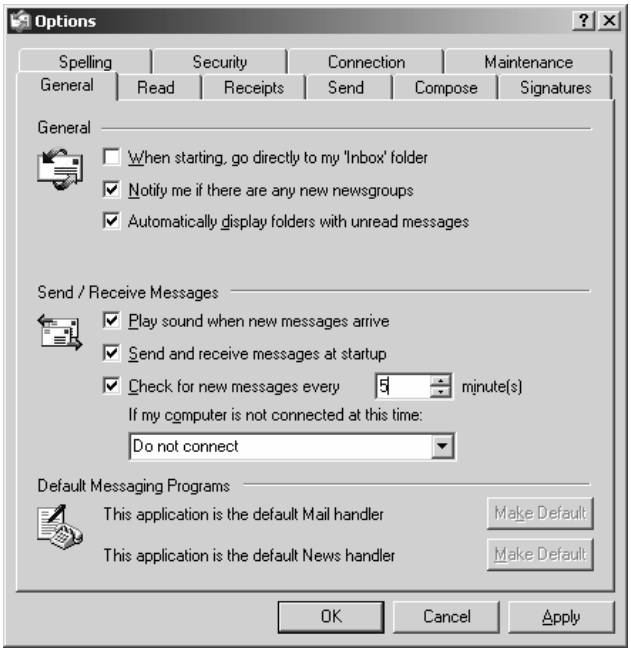
Hình 7.60 – Hộp thoại sau khi chọn **Specified Folder**.

Sau khi hoàn thành bạn sẽ có một quy tắc như sau:



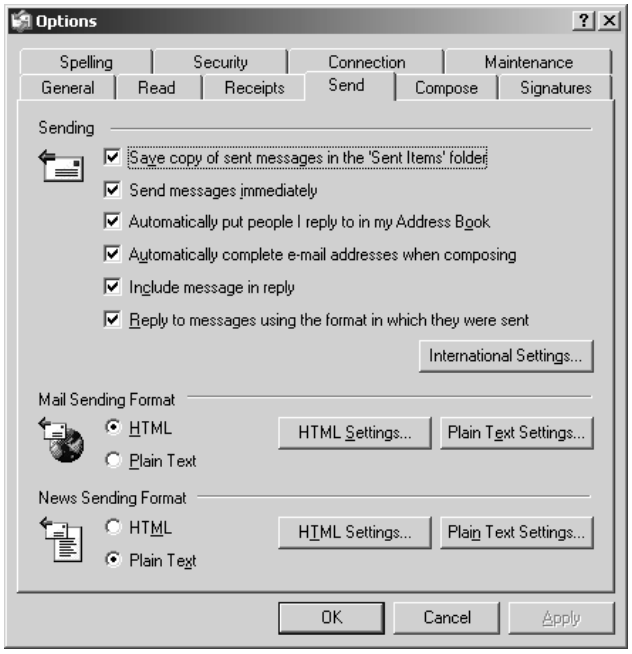
Hình 7.61 – Hộp thoại **Message Rules**.

Xác định thời gian check mail tự động: bạn vào menu **Tools/Option**, hộp thoại **Option** xuất hiện, trong **Tab General**, mục **Send/Receive Messages** bạn check vào **Check for new message every XX minute**, đồng thời bạn nhập vào thời gian check mail tự động.



Hình 7.62 – Hộp thoại **Options**.

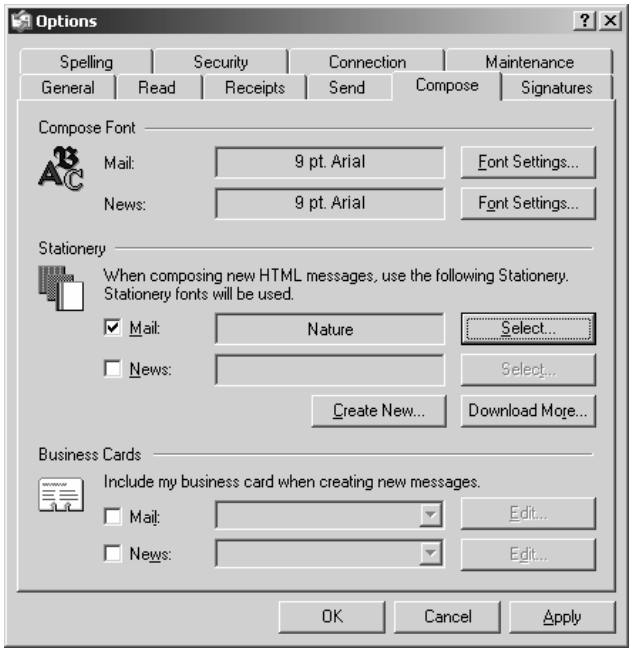
Mail có hai định dạng cơ bản là: **HTML** và **Plain Text**. Dạng **HTML** cho phép ta soạn thảo mail như một trang Web có thể chèn hình ảnh, âm thanh vào mail, làm cho mail có thể sống động hơn. Dạng **Plain Text** chỉ cho phép ta soạn thảo mail như một tài liệu văn bản trong suốt. Muốn chọn định dạng mail bạn vào **Tab Send** trong hộp thoại **Option**, mục **Mail Sending Format** bạn chọn định dạng mà bạn muốn.



Hình 7.63 – Hộp thoại **Options** – **Tab Send**.

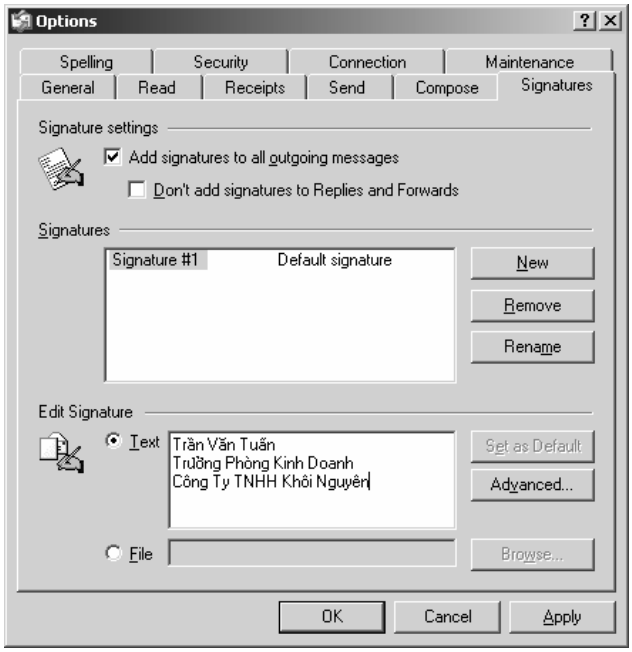
Sử dụng **Stationary**: **Stationary** là một khuôn mẫu mail được thiết kế sẵn giúp bạn có thể soạn thảo

mail nhanh và trình bày đẹp. Bạn vào **tab Compose** trong hộp thoại **Option**, mục **Stationery**, check vào mail và bạn click vào **Select** để chọn khuôn mẫu vừa ý.



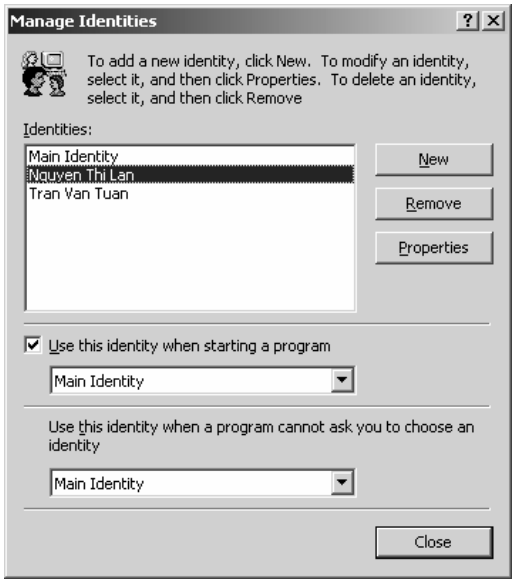
Hình 7.64 – Hộp thoại **Options** – **Tab Compose**.

Chèn đối tượng **Signatures**: **Signature** là những thông tin cá nhân được gởi tự động kèm theo thư. Thông thường các thông tin này là tên công ty, số điện thoại, fax… Bạn muốn chèn các thông tin này bạn vào **Tab Signatures** trong hộp thoại **Option**. Click và **New** để tạo **Signature** mới, trong mục **Text** nhập vào các thông tin cần thiết.



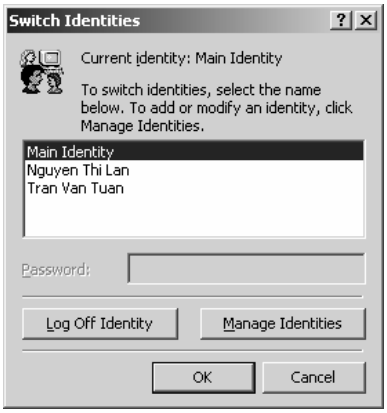
Hình 7.65 – Hộp thoại **Options** – **Tab Signatures**.

Quản lý nhiều người dùng trong **Outlook**: đôi lúc nhiều người dùng chung một chương trình **Outlook** để gởi nhận mail và họ muốn mail của họ được bảo mật có nghĩa là mail của riêng người nào thì người đó mới được đọc. Lúc đó ta sử dụng tính năng Identity của **Outlook**, trước hết ta tạo ra **Identity** cho từng người bằng cách vào menu **File/Identities/Manager Identities**, sau đó click vào New và nhập tên của các thành viên. Nếu muốn bảo mật tuyệt đối thì check vào mục sử dụng **password**.



Hình 7.66 – Hộp thoại **Manage Identities**.

Ta chuyển vào **Identity** bằng cách vào menu **File/Switch Indentity** và chọn người cần chuyển vào, sau đó bạn cấu hình từ đầu cho riêng bạn xem như là bạn sở hữu riêng một chương trình **Outlook Express**. Chú ý là sau khi sử dụng xong bạn phải chọn chức năng **Log off** để thoát khỏi **Identity** của mình tránh tình trạng người khác đọc được mail của mình.



Hình 7.67 – Hộp thoại **Switch Identities**.

VIII. XÂY DỰNG TRANG WEB.

VIII.1. Giới thiệu ngôn ngữ HTML.

Ngôn ngữ **HTML** (**HyperText Markup Language**) là một ngôn ngữ mô tả, bao gồm tập hợp các thẻ (tag) dùng để mô tả các trang Web. Mỗi thẻ thông thường là một cặp chỉ vị trí bắt đầu thẻ và vị trí kết thúc thẻ.

VIII.2. Các thẻ (Tag) trong HTML.

- <HTML></HTML> :thẻ nhận dạng tài liệu, đặt ở vị trí bắt đầu và kết thúc tập tin.
- <TITLE></TITLE>: chỉ ra nội dung tiêu đề của trang Web, nội dung này sẽ được hiển thị trên thanh tiêu đề của chương trình **Browser**. Thẻ này chỉ đặt trong phần **Header**.
- <HEAD></HEAD>: chỉ ra phần header của trang Web, thẻ này có thể bỏ qua.
- <BODY></BODY>: thẻ này chỉ ra phần nội dung của trang Web.
- <H?></H?>: định dạng văn bản theo **heading**, giá trị này từ 1 đến 6, giá trị càng nhỏ chữ càng lớn.
- <H? ALIGN=LEFT | CENTER | RIGHT></H?> : định dạng canh lề cho văn bản.
- <EM></EM>: hiển thị văn bản ở dạng nghiêng theo **logical type**.
- <STRONG></STRONG>: hiển thị văn bản ở dạng in đậm theo **logical type.**
- <BIG></BIG> : chọn kích thước **font** lớn.
- <SMALL></SMALL>: chọn kích thước **font** nhỏ.
- <B></B> :hiển thị văn bản ở dạng in đậm theo **physical type**.
- <I></I>: hiển thị văn bản ở dạng nghiêng theo **physical type**.
- <U></U>: hiển thị văn bản ở dạng gạch dưới theo **physical type**.
- <STRIKE></STRIKE>: hiển thị văn bản ở dạng **strikeout** theo **logical type**.
- <S></S>: hiển thị văn bản ở dạng **strikeout** theo **physical type**.
- :hiển thị văn bản ở dạng **Subscript** theo **logical type**.
- : hiển thị văn bản ở dạng **superscript** theo **logical type**.
- <CENTER></CENTER>: định dạng canh giữa cho văn bản và hình.
- <BLINK></BLINK>: hiển thị văn bản dạng nhấp nháy.
- <FONT SIZE=?></FONT>: chọn kích thước **font** có giá trị từ 1 đến 7.
- <BASEFONT SIZE=?> : chỉ định kích thước font dạng văn bản, có giá trị từ 1-7. Mặc định là 3.
- <FONT COLOR="#$$$$$$"></FONT> : chỉ định màu của văn bản, giá trị dưới dạng **hexa**.
- <FONT FACE="***"></FONT>: chọn **font** cho văn bản
- <MULTICOL COLS=?></MULTICOL>: tạo văn bản có nhiều cột.
- <A HREF="URL"></A> : tạo một link đến một đối tượng **URL**.
- <A HREF="URL#***"></A>: tạo một link đến một đối tượng **URL** được chỉ định.
- <A HREF="URL" TARGET="*** | _blank | _self | _parent|_top"></A>: tạo một link đến một đối tượng URL chỉ định cửa sổ hiển thị.
- <IMG SRC="URL">: hiển thị ảnh.

- <IMG SRC="URL" ALIGN=TOP | BOTTOM | MIDDLE | LEFT | RIGHT>: canh lề trái phải của ảnh

- <IMG SRC="URL" ALIGN=TEXTTOP | ABSMIDDLE | BASELINE | ABSBOTTOM >: canh phía trên và phía dưới của ảnh.
- <HR> : Tạo hàng ngang
- <HR ALIGN=LEFT | RIGHT | CENTER > : canh lề
- <HR SIZE=?>: độ dày tính theo **pixel**.
- <HR WIDTH=?>: độ rộng tính theo **pixel**.
- <UL><LI></UL>: tạo danh sách không sắp xếp, đặt <LI> trước mỗi đối tượng của danh sách.
- <BODY BACKGROUND="URL">: tạo nền của trang Web.
- <BODY BGCOLOR="#$$$$$$">: đặt màu nền cho trang Web, giá trị này hệ hexa theo thứ tự red/green/blue.
- <BODY TEXT="#$$$$$$"> : màu chữ.
- <BODY LINK="#$$$$$$">: màu link.
- <BODY VLINK="#$$$$$$">: màu các trang link đã duyệt qua.
- <BODY ALINK="#$$$$$$"> : màu link đang được chọn.
- <FORM ACTION="URL" METHOD=GET | POST></FORM> : định nghĩa một **form** và phương thức hoạt động của **form**.
- <INPUT TYPE="TEXT | PASSWORD | CHECKBOX | RADIO | IMAGE | HIDDEN | SUBMIT | RESET "> : đưa các đối tượng vào **form**.
- <INPUT NAME="***"> : tên của trường trong **form**.
- <INPUT VALUE="***"> :giá trị của trường trong **form**.
- <INPUT SIZE=?> : kích thước của **field** tính bằng **characters**.
- <SELECT></SELECT>: tạo list lựa chọn.
- <SELECT NAME="***"></SELECT> : tên của **list**.
- <TEXTAREA ROWS=? COLS=?></TEXTAREA>: tạo một hộp nhập liệu.
- <TABLE></TABLE> : định nghĩa một bảng.
- <TABLE BORDER=?></TABLE>: kích thước **border**.
- <TABLE WIDTH=?>: độ rộng của bảng tính theo **pixel**.
- <TR></TR> : tạo dòng của bảng.
- <TR ALIGN=LEFT | RIGHT | CENTER | MIDDLE | BOTTOM VALIGN=TOP | BOTTOM | MIDDLE>: canh lề trong dòng của bảng.
- <TD></TD> : tạo ô trong bảng
- <TD ALIGN=LEFT | RIGHT | CENTER | MIDDLE | BOTTOM VALIGN=TOP | BOTTOM | MIDDLE> : canh lề trong ô củabảng.
- <TD BGCOLOR="#$$$$$$"> : định màu trong ô của bảng.
- <FRAMESET> </FRAMESET>: khai báo **frame**.
- <FRAMESET ROWS=,,,></FRAMESET>: độ rộng của hàng tính theo **pixel** hoặc %.
- <FRAMESET COLS=,,,></FRAMESET>: độ rộng của cột tính theo **pixel** hoặc %.
- <FRAMESET BORDER=?>: độ rộng của **border**.
- <FRAMESET BORDERCOLOR="#$$$$$$"> : màu của **border.**

- <FRAME SRC="URL">: hiển thị nội dung của tài liệu trong **Frame**.

- <FRAME SCROLLING="YES | NO | AUTO">: đặt thuộc tính **Scrollbar** cho **frame**.

VIII.3. Các ví dụ về HTML.

Cấu trúc cơ bản của một trang html gồm hai phần chính: phần **header** (nằm giữa tag **<head>** và tag **</head>**) chứa thông tin chung về trang Web, phần nội dung chính của trang Web (đặt giữa hai tag **<body>** và **</body>** chứa nội dung sẽ được hiển thị trên trang web.

```
<HTML>
<HEAD>
<TITLE></TITLE>
</HEAD>
<BODY>
Noi dung trang Web
</BODY>
</HTML>
```

Đặt màu nền cho trang Web:

```
<BODY BGCOLOR="#FF0000">
Noi dung trang Web
</BODY>
```

Đặt **picture** làm nền:

```
<BODY BACKGROUND="swirlies.gif">
Noi dung trang Web
</BODY>
```

Đặt chế độ nghiêng, đậm, gạch dưới:

```
<BODY BGCOLOR="#FFFFFF">
<U>Noi dung </U> <I>trang </I> <B>Web</B>
</BODY>
```

Chọn **font** :

```
<font color="#00FF00" face=".VnArial" size="7">font chu</font>
```

Các thuộc tính của **text**:

```
<BODY BGCOLOR="#FFFFFF">
Noi dung <U><I><B><FONT COLOR="#FF0000" FACE="ARIAL"
SIZE="7">trang Web</FONT></B></I></U>
</BODY>
```

Xuống dòng:

```
<BODY BGCOLOR="#FFFFFF">
   Hey!<BR>
   What's<BR>
   going<BR>
```

***on
***

here??

</BODY>

Canh **text**:

```
<BODY BGCOLOR="#FFFFFF">
<CENTER>Something really cool</CENTER>
 </BODY>
```

Chèn hình vào trang Web:

```
<BODY BGCOLOR="#FFFFFF">
<IMG SRC="copper.gif" WIDTH=82 HEIGHT=68>
</BODY>
```

Cấp thư mục: SRC="../../copper.gif"

Liên kết:

```
<BODY BGCOLOR="#FFFFFF">
Go to <A HREF="http://home.netscape.com/">Netscape!</A>
</BODY>
```

hoặc :

```
Click <A HREF="lesson04.html">here</A> to be magically
```

Gởi mail:

```
<BODY BGCOLOR="#FFFFFF">
Send me <A HREF="mailto:forrest@bubbagump.com">Mail!</A>
</BODY>
```

Liên kết bằng hình:

```
<BODY BGCOLOR="#FFFFFF">
Go to <A HREF="http://home.netscape.com/"> <IMG SRC="copper.gif"
WIDTH=82 HEIGHT=68 BORDER=0></A>
</BODY>
```

Danh sách trang trí kiểu (‘.’)

```
<BODY BGCOLOR="#FFFFFF">
What I want for Christmas
<UL>
<LI>a big red truck
<LI>a real fast speedboat
<LI>a drum set
<LI>a BB gun
<LI>a Melanie Griffith
</UL>
</BODY>
```

Danh sách trang trí kiểu số:(1,2,3..)

```
<BODY BGCOLOR="#FFFFFF">
 What I want for Christmas
<OL>
<LI>a big red truck
<LI>a real fast speedboat
 <LI>a drum set
<LI>a BB gun
<LI>a Melanie Griffith
</OL>
</BODY>
```

Đường kẻ ngang:

```
<HR WIDTH=20%>
hoặc:
<HR >
<HR WIDTH=60% SIZE=1>
<HR WIDTH=60% SIZE=3 NOSHADE>
```

Frame

Frame chia theo cột:

```
<FRAMESET COLS="50%,50%">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
</FRAMESET>
```

Frame chia theo dòng:

```
<FRAMESET ROWS="10%,20%,30%,15%,25%">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
<FRAME SRC="kim.html">
<FRAME SRC="tina.html">
<FRAME SRC="shannon.html">
</FRAMESET>
```

Frame chia tự động:

```
<FRAMESET COLS="50,*">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
</FRAMESET>
```

Frame chia frame:

```
<FRAMESET COLS="50,*,2*">
<FRAMESET ROWS="50,*,*">
```

< *FRAME SRC="lisa.html">*

<FRAME SRC="lisa.html">
<FRAME SRC="lisa.html">
</FRAMESET>
<FRAME SRC="terri.html">
<FRAMESET ROWS="50%,50%">
<FRAME SRC="kim.html">
<FRAME SRC="tina.html">
</FRAMESET>
</FRAMESET>

Độ rộng của **line**, màu **line** của **frame**:

<FRAMESET COLS="154,*" BORDER=20 BORDERCOLOR="#FFOOOO">
<FRAMESET ROWS="170,*" FRAMEBORDER=NO >
<FRAME SRC="world.gif" WIDTH=146 HEIGHT=162 SCROLLING=NO
MARGINWIDTH=1 MARGINHEIGHT=1>
<FRAME SRC="lisa.html">
</FRAMESET>
<FRAME SRC="terri.html">
</FRAMESET>

Form

Gởi mail:

<FORM METHOD=POST ACTION="mailto:xxx@xxx.xxx"
ENCTYPE="application/x-www-form-urlencoded">
</FORM>

Các đối tượng trong **form**:

<INPUT TYPE=TEXT NAME="ADDRESS" VALUE="44 Cherry St" SIZE=30>
<INPUT TYPE=PASSWORD NAME="USER PASSWORD">

Radio button:

<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Ed" CHECKED> Ed Holleran
<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Rick"> Rick Weinberg
<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Tom"> Tom Studd<P>

Check Box:

<INPUT TYPE=CHECKBOX NAME="ED" VALUE="YES" CHECKED> Ed Holleran
<INPUT TYPE=CHECKBOX NAME="Rick" VALUE="YES"> Rick Weinberg

ComboBox:

<SELECT NAME="BEST FRIEND">
<OPTION VALUE="Ed">Ed
<OPTION VALUE="Rick">Rick
<OPTION VALUE="Tom" SELECTED>Tom

< ***OPTION VALUE="Guido">Guido***

```
</SELECT>
```

List Box:

```
<SELECT NAME="BEST FRIEND" SIZE=4>
<OPTION VALUE="Ed">Ed
<OPTION VALUE="Rick">Rick
<OPTION VALUE="Tom" SELECTED>Tom
<OPTION VALUE="Guido">Guido
<OPTION VALUE="Horace">Horace
<OPTION VALUE="Reggie">Reggie
<OPTION VALUE="Myron">Myron
</SELECT>
```

Text Area:

```
<TEXTAREA NAME="COMMENTS" ROWS=6 COLS=50>
</TEXTAREA>
```

Nút **Submit, Reset**:

```
<INPUT TYPE=SUBMIT>
<INPUT TYPE=RESET>
```

Table

Chia dòng, cột:

```
<table border="1" width="100%">
<tr>
<td width="50%"> </td>
<td width="50%"> </td>
</tr>
<tr>
<td width="50%"> </td>
<td width="50%"> </td>
</tr>
</table>
```

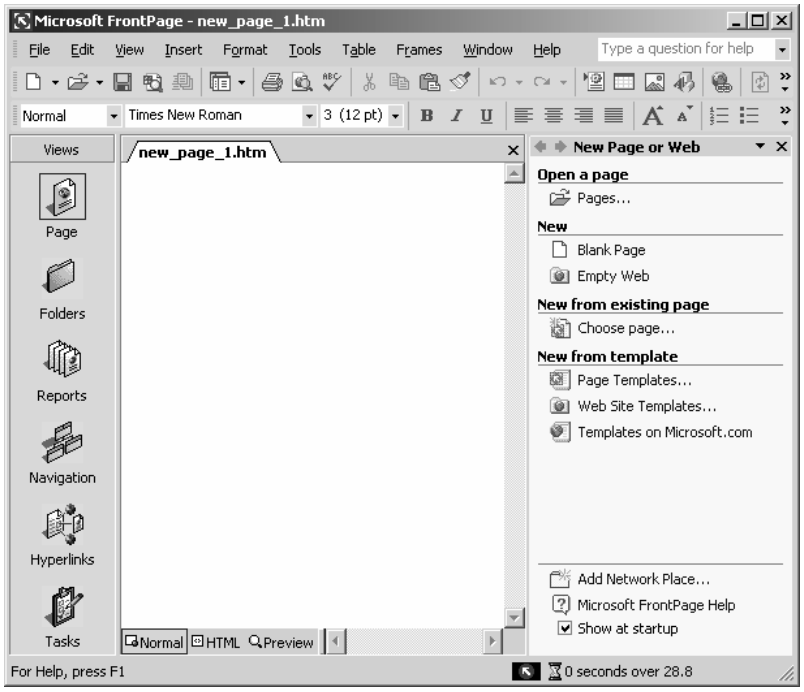
VIII.4. Giới thiệu công cụ tạo web FrontPage.

Giới thiệu về FrontPage.

FrontPage là chương trình giúp ta soạn thảo nhanh các trang Web là không cần thuộc các **tag html**. Đồng thời công cụ này cũng giúp ta kiểm tra các liên kết của các trang Web và duyệt trước nội dung các trang web giống như khi duyệt bằng trình duyệt Web.

FrontPage là một trong các chương trình ứng dụng trong bộ **Office** của **Microsoft**, nên cách sử dụng của chương trình này cũng tương tự như **Word** hay **Excel**, do đó người dùng rất dễ làm quen.

Khởi động chương trình **FrontPage**: chọn **Start/Programs/Microsoft FrontPage**



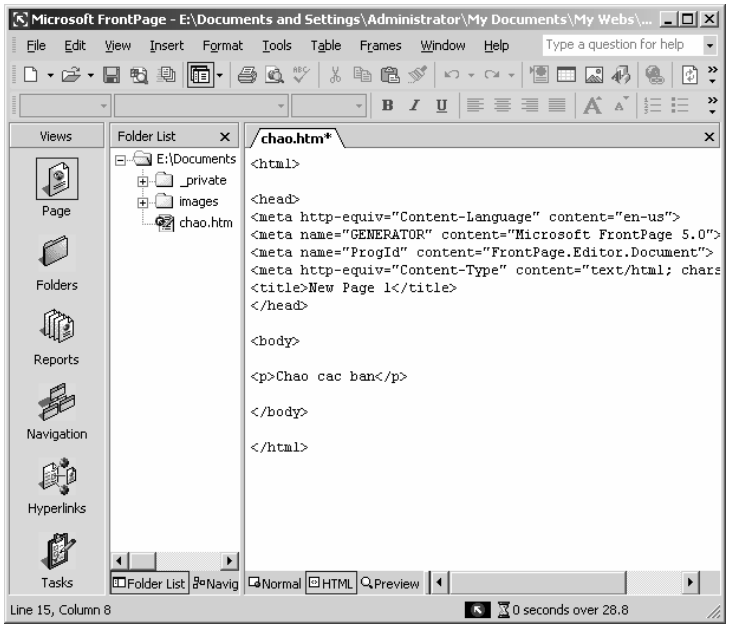
Hình 7.68 – Giao diện chương trình **FrontPage**.

Tạo một trang Web mới: trong **FrontPage** vào menu **File/New/Page** or **Web** hoặc click chuột vào icon "**New**" trên thanh công cụ. Sau đó vào menu **File** chọn **Save** và nhập tên trang Web cần lưu trữ. Thông thường phần mở rộng của tập tin Web là **htm** hoặc **html**. Trong cửa sổ làm việc của **ProntPage** có ba chế độ hiển thị là "**Normal**", "**HTML**", "**Preview**".

Normal là chế độ soạn thảo Web.

HTML là chế độ hiển thị nội dung **source html** của trang Web.

Preview là chế độ duyệt Web giống như trình duyệt web dùng để kiểm tra trước khi đưa trang Web lên mạng.



Hình 7.69 – Giao diện khi chọn chế độ xem là HTML.

Thanh công cụ định dạng văn bản với các tính năng thông dụng sau:

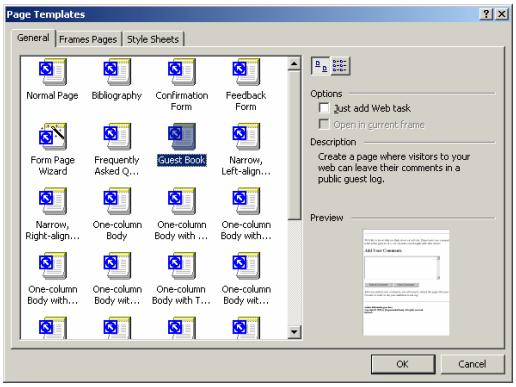
Hình 7.70 – Thanh công cụ định dạng văn bản.

- Chọn kiểu văn bản
- Chọn loại font thích hợp
- Chọn kích thước chữ
- Định dạng in đậm, in nghiêng, gạch dưới
- Canh lề trái, phải, giữa, đều hai bên lề
- Tăng giảm kích thước chữ
- Định dạng danh sách sắp xếp dạng number, bullet
- Định dạng Tab sang trái hay sang phải
- Chọn đường viền khung
- Chọn màu văn bản, màu nền

Tạo trang Web mới theo các mẫu định sẵn: ta chọn "**Page Templates**" để tạo các trang Web theo các mẫu định sẵn.

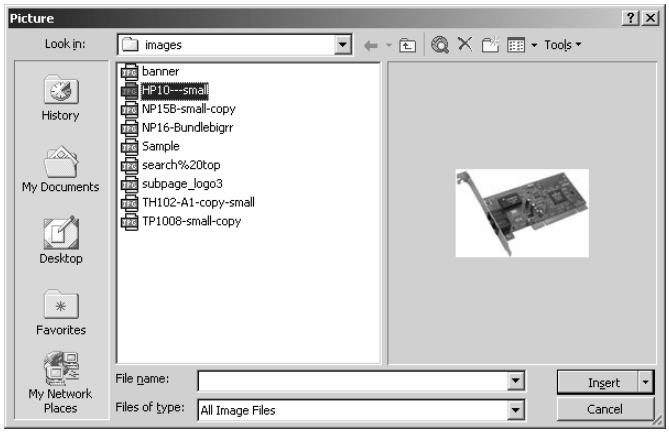
Hình 7.71 – Các cách tạo một trang mới.

Sao đó ta chọn mẫu phù hợp như hình sau và chọn OK.



Hình 7.72 – Các **Page Templates** định sẵn.

Chèn hình ảnh: ta chọn vị trí chèn ảnh bằng cách đặt con trỏ tại vị trí này, sau đó vào menu **Insert/Picture/From File**… Hộp thoại **Picture** xuất hiện, ta chọn tên tập tin ảnh cần chèn.



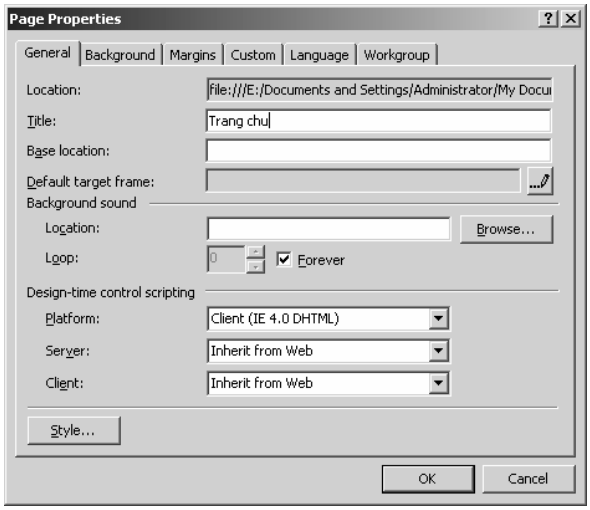
Hình 7.73 – Hộp thoại **Picture**.

Kết quả được hiển thị trên trang Web như sau:

- **Đây là card mạng:**

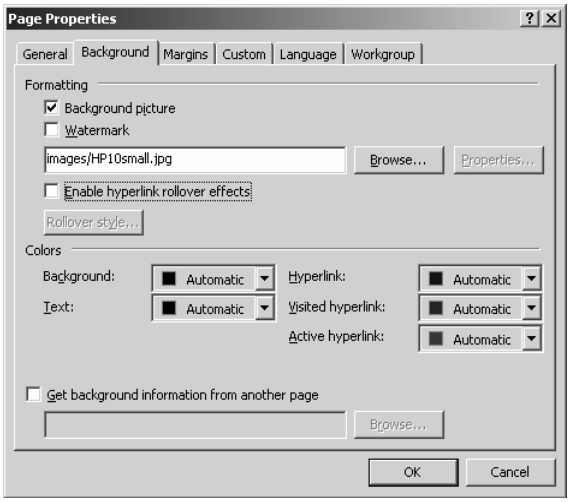
Hình 7.74 – Kết quả hiển thị của trang Web.

Đặt tiêu đề và chương trình điều khiển script cho trang web: chọn chức năng **file/properties** và nhập nội dung tiêu đề vào ô "**Title**" và chọn OK.



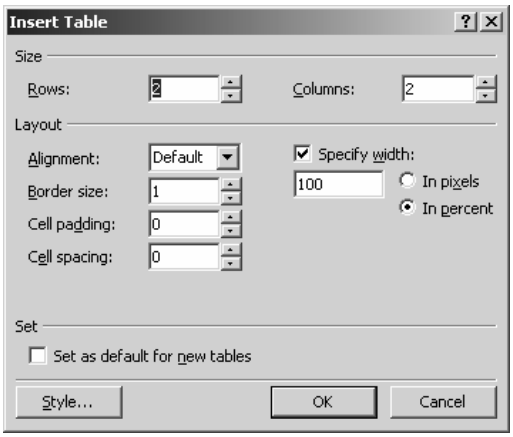
Hình 7.75 – Hộp thoại **Page Properties**.

Định nền cho trang Web: ta có thể chọn màu hoặc một hình ảnh bất kỳ để làm nền cho trang Web bằng cách chọn menu **Format/Background**… Nếu chọn hình làm nền thì check vào "**Background Image**" và click chuột vào nút "**Browse**" để chỉ ra tập tin ảnh cần làm nền, sau đó chọn **OK**.



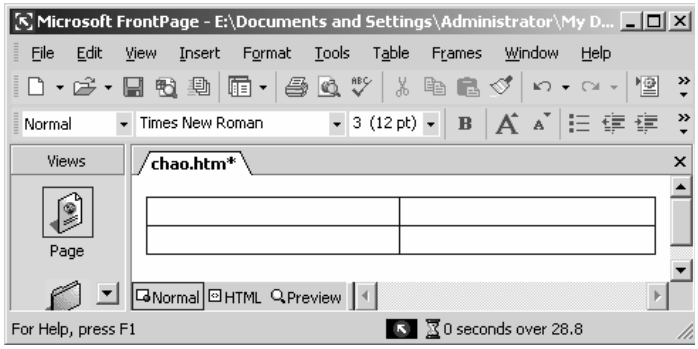
Hình 7.75 – Hộp thoại **Page Properties** – **Tab Background**.

Tạo bảng (**Table**): công cụ chính để bố trí các đối tượng trên trang Web là bảng. Bảng giúp ta có thể chia nhỏ trang Web thành nhiều ô (**cell**). Tại mỗi ô ta có thể trình bày dạng văn bản hoặc hình ảnh. Muốn tạo một bảng mới trước tiên ta đặt con trỏ tại vị trí cần chèn bảng, sau đó chọn menu **Table/Insert/Table**… Trong hộp thoại "**Insert Table**" ta nhập số dòng cần tạo vào mục "**Rows**" và số cột vào mục "**Columns**". Các thông số trình bày khác như: **Alignment** (canh lề bảng), **Border size** (kích thước của đường viền), **Cell padding** (độ cao của ô), **Cell spacing** (khoảng cách giữa hai ô)…



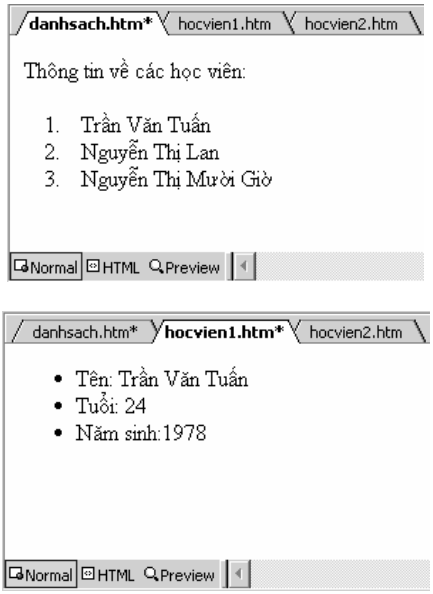
Hình 7.76 – Hộp thoại **Insert Table**.

Trên trang Web sẽ xuất hiện một bảng như sau:



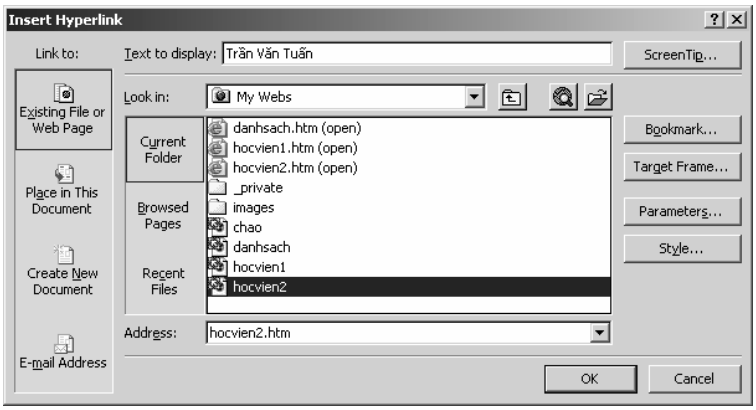
Hình 7.77 – Kết quả sau khi **Insert table**.

Tạo liên kết (**hyperlink**): liên kết giúp ta kết nối các trang Web đơn thành một **Website**. Muốn tạo các liên kết trước hết ta phải có các trang Web đã thiết kế hoàn chỉnh và chú ý đến vị trí (đường dẫn) của trang Web này. Ví dụ ta có ba trang Web: danhsach.htm (chứa tin danh sách các học viên), hocvien1.htm (chứa thông tin chi tiết của học viên 1), hocvien2.htm (chứa thông tin chi tiết của học viên 2).



Hình 7.78 – Nội dung của các trang Web (danhsach.htm và hocvien1.htm).

Bây giờ, ta muốn tạo liên kết giữa trang danhsach.htm đến các trang hocvien.htm nhằm giúp người duyệt web muốn xem thông tin của học viên nào thì click vào tên của học viên đó. Tạo liên kết cho một đoạn văn bản ta phải tô đen đoạn văn bản, sau đó click phải chuột chọn "Hyperlink…" hoặc tạo liên kết cho một hình ta cũng làm tương tự chọn hình ảnh cần tạo liên kết và click phải chuột chọn "**Hyperlink**…". Hộp thoại "**Insert Hyperlink**" xuất hiện, ta chọn tên tập tin trang Web cần liên kết đến và chọn **OK**.

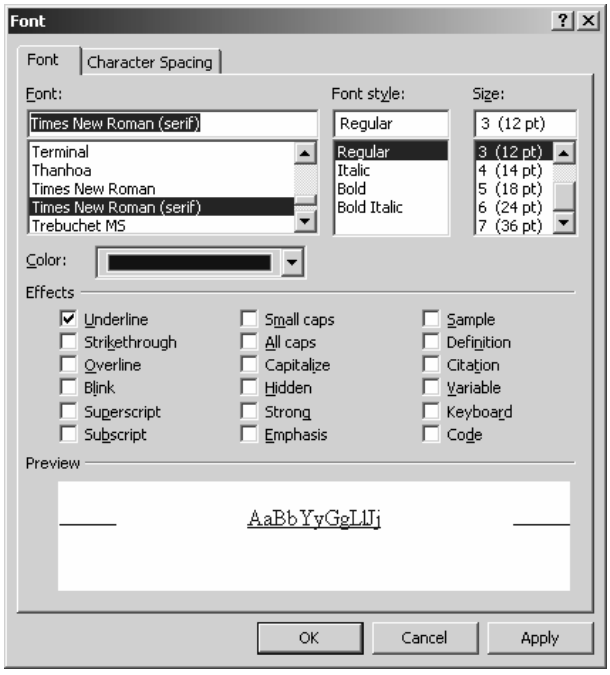


Hình 7.79 – Hộp thoại **Insert Hyperlink**.

Bạn kiểm tra lại các mối liên kết bằng cách mở trang danhsach.htm và chuyển qua chế độ hiển thị **Preview**, sau đó rê chuột đến tên của các học viên thì thấy con chuột có biểu tượng hình bàn tay, khi click vào thì nội dung trang Web hocvien.htm sẽ được hiển thị.

Hình 7.80 – Kết quả sau khi **insert hyperlink**.

Các lựa chọn trong hộp thoại **Font**: chọn menu **Format/Font**, hộp thoại **Font** xuất hiện

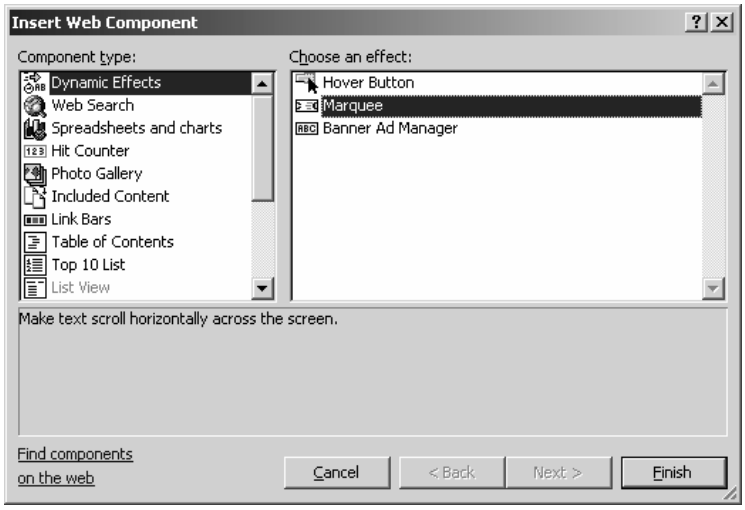


Hình 7.81 – Hộp thoại **Font**.

Các hiệu ứng thông dụng là:

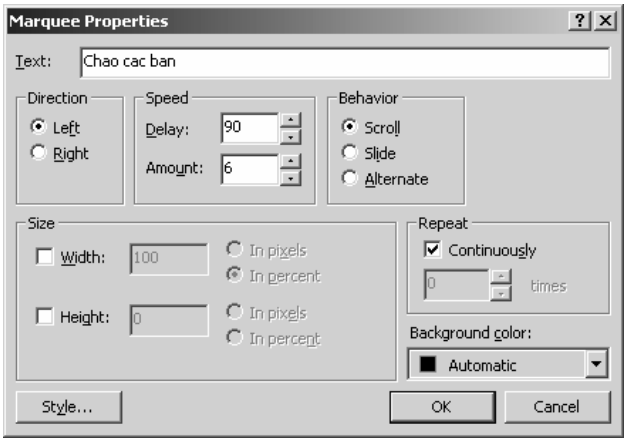
- **Underline**: gạch dưới
- **Strikethrough**: gạch ngang
- **Overline**: gạch trên
- **Blink**: nhấp nháy
- **SuperScript**: dạng lũy thừa trên
- **SubScript**: dạng số dưới

Tạo dòng chữ chạy **Marquee**: đặt con trỏ đến vị trí cần chèn, chọn menu **Insert/Web Component/Marquee**… Hộp thoại "**Insert Web Component**" xuất hiện, trong danh sách "**Component type**" chọn "**Dynamic Effect**", mục "**Effect**" chọn **Marquee**, sau đó chọn **Finish**.



Hình 7.82 – Hộp thoại **Insert Web Component**.

Hộp thoại "**Marquee Properties**" xuất hiện, ta nhập nội dung cần hiển thị vào mục **Text** và chọn **OK**.



Hình 7.83 – Hộp thoại **Marquee Properties**.

IX. GIỚI THIỆU VỀ JAVA SCRIPT VÀ VB SCRIPT.

IX.1. Giới thiệu về ngôn ngữ script.

Ngôn ngữ **Script** là một ngôn ngữ lập trình nhằm bổ sung tính năng động của trang Web (**Dynamic HTML**). Ngôn ngữ này giúp giảm xử lý cho **Server** thay vì dùng **CGI script** tại **Server** thì ta dùng **Java script** tại **Client**.

Các ngôn ngữ **script** thông dụng như: **javascript** (**NetScape**), **jscript** (**Microsoft**), **VBScript** (**Microsoft**).

VBScript có lợi thế trong môi trường **Windows**, dùng cho các **ActiveX control** và rất giống **VB**. **VBScript** cũng là ngôn ngữ dùng cho **Server**, nó phối hợp với những đối tượng **Server** để tạo ra những trang Web động từ **Server** (ví dụ như **ASP**).

IX.2. Tổng quan Java Script.

Khi cần thiết kế một trang Web động như máy tính tay (***Calculators***), hiển thị giờ (**D*isplay time***), hiển thị trạng thái thông tin phản hồi(***Feedback***), giải trí trên web (**Entertainment**) thì ta dùng các ngôn ngữ **script** này… **Java Script** không phải là java.

Cú pháp:

Gần giống như các ngôn ngữ lập trình khác như **Pascal, C++, Java**...

Khai báo và dùng biến

- var x = 7
- var y,z = "19"
- var lk = "lucky"
- 5 + x // giá trị là 12
- lk + z // giá trị là "lucky19"
- lk + x // giá trị là "lucky7"
- x + z // giá trị là 26
- **Java script** tự động chuyển kiểu cho phù hợp và tự gán giá trị ban đầu là 0 khi ta khai báo biến.

Các loại dữ liệu trong Java Script

- Số như -5, 0 hoặc 3.3333
- Chuỗi như "Click Here" hoặc "JavaScript"
- Giá trị logic như: `true` hoặc `false`
- **JavaScript element** xem như là một hàm hoặc một đối tượng
- Giá trị `null`

Các hằng

- Hệ thập phân 123, -3434
- Hệ 8(octal): 017
- Hệ 16(hexadecimal): 0x12EF5
- Kiểu dữ liệu số trong **java script** dùng 32 bit

Chuỗi

- Khởi tạo, phép toán trên chuỗi
- \t tab
- \n return
- \b backspace

Đổi kiểu

- stringthing + numberthing= string
- numberthing + stringthing= number

Các phép toán: +, -, *, /, %, ++, --, = =, !=, <, <=, >, >=, …

```
x = 4 + y;
y = 5.5 - z;
z = 10 / w;
w = 1.4e5 * v;
  n = -m;
 y = ++x;
 z = x++;
if (x = 3) { }
(x < 17) && buttonPressed && (z == "Meta")
(x < 17) || buttonPressed || (z == "Meta")
(x < 25) && beaupage()
(x - 3.0) < epsilon || (3.0 - x) < epsilon
```

Chú thích

```
/* …… */
//…….
Trong htnl <!--  …… -->
```

Cấu trúc điều khiển

```
if (điều kiện) { câu lệnh}
if (điều kiện) { câu lệnh} else {câu lệnh}
Cấu trúc While:
                        while (điều kiện) { câu lệnh}
```

IX.3. Sự kiện trong html và java script.

Các tác động thông thường lên trang web là:

- Chọn một liên kết.
- Di chuyển đến trang trước hoặc trang sau trong các trang đã duyệt.
- Mở một trang Web mới dùng chức năng "**New Window**".
- Thoát khỏi trình duyệt web.

Các sự kiện thường gặp đối với các đối tượng là:

- Di chuyển chuột
- Thay đổi trạng thái.

Chèn đoạn mã **java script** trong **html**:

```
<SCRIPT LANGUAGE="LangName" [SRC="URL"]>
<SCRIPT LANGUAGE="JavaScript" SRC="jscode/click.js"> </SCRIPT>
```

Ẩn nội dung **source** đi:

```
<SCRIPT LANGUAGE="JavaScript">
<!--
```

```
function dontclickme()     {
```

```
    alert("Ban da click chuot");
    return(false);
}
<!-- end script -->
</SCRIPT>
```

Một trang Web hoàn chỉnh dùng **code Jaca Script**: ví dụ tạo một nút "Chao", khi click vào nút này xuất hiện thông báo "Chao cac ban"

```
<HTML>
<HEAD>
<TITLE>Chao ban</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function dontclickme() {
    alert("Chao cac ban");
}
<!-- end script -->
</SCRIPT>
</HEAD>
<BODY>
<FORM>
<INPUT TYPE="button" NAME="chao" VALUE="Chao!" onClick="dontclickme()">
</FORM>
</BODY>
</HTML>
```

Ta có thể viết lệnh **Java script** trực tiếp vào sự kiện:

```
<HTML>
<HEAD>
<TITLE>Chao ban</TITLE>
</HEAD>
<BODY>
<FORM>
<INPUT TYPE="button" NAME="chao" VALUE="Chao!"
 onClick="alert('Chao cac ban');">
</FORM>
</BODY>
</HTML>
```


Bắt sự kiện của **List**: ví dụ kiểm tra sự thay đổi giá trị **listbox** dùng hàm onChange()

```
<HTML><HEAD>
<TITLE>Su kien List</TITLE>
```

```
<SCRIPT LANGUAGE="JavaScript">
```

```
<!--
function Thongbao(str) {
    alert(str);
}
<!-- end script -->
</SCRIPT>
</HEAD>
<BODY>
<SELECT NAME="Ten" onChange="Thongbao('Co su thay doi')">
<OPTION SELECTED>Lan</OPTION>
<OPTION>Cuc</OPTION>
<OPTION>Hong</OPTION>
</SELECT>
</BODY>
</HTML>
```

Bắt sự kiện của **document** (dùng khi cần gọi hàm lúc trang Web vừa mở hoặc khi đóng trang Web):

```
<BODY onLoad="loadfunc()" onUnload="unloadfunc()">
```

IX.4. VB Script và OLE Controls.

Khai báo biến

Dùng từ khóa **Dim** để khai báo biến:

```
<SCRIPT LANGUAGE="VBS">
<!--
Dim MyVariable
-->
</SCRIPT>
```

Mảng

```
<SCRIPT LANGUAGE="VBS">
<!- -Một mảng 3 D
    Dim theArray(99, 49, 9)
-->
</SCRIPT>
```

Cấu trúc điều khiển trong VBScript

Cấu trúc IF...THEN...ELSE

```
<SCRIPT LANGUAGE="VBS">
        <!--
         If (điều kiện) Then
```

Mã lệnh

```
            Else
                Mã lệnh
            End If
        -->
        </SCRIPT>
```

Cấu trúc DO...WHILE

```
<SCRIPT LANGUAGE="VBS">
        <!--
            Do While (Điều kiện)
Mã lệnh
            Loop
        -->
    </SCRIPT>
```

Hàm trong VB Script

Cách tạo hàm:

```
<SCRIPT LANGUAGE="VBS">
        <!--
      Sub TenHam()
            Mã lệnh
        End Sub
        Function TenHam(biến)
            Mã lệnh
        End Function
        -->
        </SCRIPT>
```

VB Script trong HTML

Ví dụ Hello:

```
<HTML>
<HEAD><TITLE>Trang Web Thu Nghiem</TITLE>
<SCRIPT LANGUAGE="VBS">
<!--
Sub Button1_OnClick
    MsgBox "Chao ban!"
End Sub     -->
</SCRIPT>
</HEAD>
<BODY>
```

```
<H3>Trang Web Thu Nghiem VB Script</H3><HR>
```

```
<FORM><INPUT NAME="Button1" TYPE="BUTTON" VALUE="Ban Click vao day"> </FORM>
        </BODY>
        </HTML>
```

Cách viết khác của ví dụ trên:

```
<SCRIPT LANGUAGE="VBS" EVENT="OnClick" FOR="Button1">
<!-- the message
    MsgBox "HELLO THERE!"
-->
</SCRIPT>
```

Tóm tắt

Lý thuyết 4 tiết - Thực hành 3 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về họ hệ điều hành Windows Server 2003, cách thức cài đặt Server bằng tay và cài đặt tự động …	I. Tổng quan về họ hệ điều hành Windows Server 2003. II. Cài đặt Windows Server 2003. III. Tự động hóa quá trình cài đặt.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. TỔNG QUAN VỀ HỌ HỆ ĐIỀU HÀNH WINDOWS SERVER 2003

Như chúng ta đã biết họ hệ điều hành **Windows 2000 Server** có 3 phiên bản chính là: **Windows 2000 Server**, **Windows 2000 Advanced Server**, **Windows 2000 Datacenter Server**. Với mỗi phiên bản **Microsoft** bổ sung các tính năng mở rộng cho từng loại dịch vụ. Đến khi họ **Server 2003** ra đời thì **Mircosoft** cũng dựa trên tính năng của từng phiên bản để phân loại do đó có rất nhiều phiên bản của họ **Server 2003** được tung ra thị trường. Nhưng 4 phiên bản được sử dụng rộng rãi nhất là: **Windows Server 2003 Standard Edition**, **Enterprise Edition**, **Datacenter Edition**, **Web Edition**.

So với các phiên bản 2000 thì họ hệ điều hành **Server** phiên bản 2003 có những đặc tính mới sau:

- Khả năng kết chùm các **Server** để san sẻ tải (**Network Load Balancing Clusters**) và cài đặt nóng RAM (**hot swap**).
- **Windows Server 2003** hỗ trợ hệ điều hành **WinXP** tốt hơn như: hiểu được chính sách nhóm (**group policy**) được thiết lập trong **WinXP**, có bộ công cụ quản trị mạng đầy đủ các tính năng chạy trên **WinXP.**
- Tính năng cơ bản của **Mail Server** được tính hợp sẵn: đối với các công ty nhỏ không đủ chi phí để mua **Exchange** để xây dựng **Mail Server** thì có thể sử dụng dịch vụ **POP3** và **SMTP** đã tích hợp sẵn vào **Windows Server 2003** để làm một hệ thống mail đơn giản phục vụ cho công ty.
- Cung cấp miễn phí hệ cơ sở dữ liệu thu gọn **MSDE (Mircosoft Database Engine)** được cắt xén từ **SQL Server 2000**.Tuy **MSDE** không có công cụ quản trị nhưng nó cũng giúp ích cho các công ty nhỏ triển khai được các ứng dụng liên quan đến cơ sở dữ liệu mà không phải tốn chi phí nhiều để mua bản **SQL Server**.
- **NAT Traversal** hỗ trợ **IPSec** đó là một cải tiến mới trên môi trường 2003 này, nó cho phép các máy bên trong mạng nội bộ thực hiện các kết nối **peer-to-peer** đến các máy bên ngoài **Internet**, đặt biệt là các thông tin được truyền giữa các máy này có thể được mã hóa hoàn toàn.
- Bổ sung thêm tính năng **NetBIOS over TCP/IP** cho dịch vụ **RRAS (Routing and Remote Access)**. Tính năng này cho phép bạn duyệt các máy tính trong mạng ở xa thông qua công cụ **Network Neighborhood**.
- Phiên bản **Active Directory 1.1** ra đời cho phép chúng ta ủy quyền giữa các gốc rừng với nhau đồng thời việc backup dữ liệu của **Active Directory** cũng dễ dàng hơn.
- Hỗ trợ tốt hơn công tác quản trị từ xa do **Windows 2003** cải tiến **RDP (Remote Desktop Protocol)** có thể truyền trên đường truyền 40Kbps. **Web Admin** cũng ra đời giúp người dùng quản trị Server từ xa thông qua một dịch vụ Web một cách trực quan và dễ dàng.
- Hỗ trợ môi trường quản trị **Server** thông qua dòng lệnh phong phú hơn
- Các **Cluster NTFS** có kích thước bất kỳ khác **với Windows 2000 Server** chỉ hỗ trợ 4KB.
- Cho phép tạo nhiều gốc **DFS (Distributed File System)** trên cùng một Server.

Bảng so sánh các đặc tính của Windows Server 2003:

II. CHUẨN BỊ CÀI ĐẶT WINDOWS SERVER 2003.

Hoạch định và chuẩn bị đầy đủ là yếu tố quan trọng quyết định quá trình cài đặt có trơn tru hay không. Trước khi cài đặt, bạn phải biết được những gì cần có để có thể cài đặt thành công và bạn đã có được tất cả những thông tin cần thiết để cung cấp cho quá trình cài đặt. Để lên kế hoạch cho việc nâng cấp hoặc cài mới các **Server** bạn nên tham khảo các hướng dẫn từ **Microsoft Windows Server 2003 Deployment Kit** . Các thông tin cần biết trước khi nâng cấp hoặc cài mới hệ điều hành:

- Phần cứng đáp ứng được yêu cầu của **Windows Server 2003**.
- Làm sao để biết được phần cứng của hệ thống có được **Windows Server 2003** hỗ trợ hay không.
- Điểm khác biệt giữa cách cài đặt mới và cách nâng cấp (**upgrade**).
- Những lựa chọn cài đặt nào thích hợp với hệ thống của bạn, chẳng hạn như chiến lược chia

partition đĩa, và bạn sẽ sử dụng hệ thống tập tin nào…

II.1. Yêu cầu phần cứng

	x86, 2GB cho máy	dòng x86 32bit, 64CPU		x86, 733MHz cho máy	x86, 512GB cho máy			

II.2. Tương thích phần cứng

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server của bạn là kiểm tra xem phần cứng của máy tính hiện tại có tương thích với sản phẩm hệ điều hành trong họ **Windows Server 2003**. Bạn có thể làm việc này bằng cách chạy chương trình kiểm tra tương thích có sẵn trong đĩa CD hoặc từ trang Web **Catalog**. Nếu chạy chương trình kiểm tra từ đĩa CD, tại dấu nhắc lệnh bạn nhập: ***\i386\winnt32 /checkupgradeonly***.

II.3. Cài đặt mới hoặc nâng cấp

Trong một số trường hợp hệ thống **Server** chúng ta đang hoạt động tốt, các ứng dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu chúng ta phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2003**. Chúng ta cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dùng và dữ liệu hay cài đặt mới hệ điều hành rồi sau cấu hình và cài đặt ứng dụng lại. Đây là vấn đề cần xem xét và lựa chọn cho hợp lý.

Các điểm cần xem xét khi nâng cấp:

- Với nâng cấp (**upgrade**) thì việc cấu hình **Server** đơn giản, các thông tin của bạn được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)…
- Với nâng cấp bạn không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì bạn cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp bạn cần xem hệ điều hành hiện tại có nằm trong danh sách các hệ điều hành hỗ trợ nâng cấp thành **Windows Server 2003** không ?
- Trong một số trường hợp đặc biệt như bạn cần nâng cấp một máy tính đang làm chức năng **Domain Controller** hoặc nâng cấp một máy tính đang có các phần mềm quan trọng thì bạn nên tham khảo thêm thông tin hướng dẫn của **Microsoft** chứa trong thư mục **\Docs** trên đĩa CD **Windows Server 2003 Enterprise**.

Các hệ điều hành cho phép nâng cấp thành **Windows Server 2003 Enterprise Edition**:

- **Windows NT Server 4.0** với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Terminal Server Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Enterprise Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows 2000 Server.**
- **Windows 2000 Advanced Server.**
- **Windows Server 2003, Standard Edition.**

II.4. Phân chia ổ đĩa.

Đây là việc phân chia ổ đĩa vật lý thành các **partition logic**. Khi chia **partition**, bạn phải quan tâm các yếu tố sau:

- **Lượng không gian cần cấp phát:** bạn phải biết được không gian chiếm dụng bởi hệ điều hành, các chương trình ứng dụng, các dữ liệu đã có và sắp phát sinh.
- **Partition system và boot:** khi cài đặt **Windows 2003 Server** sẽ được lưu ở hai vị trí là **partition system** và **partition boot**. **Partition system** là nơi chứa các tập tin giúp cho việc khởi động **Windows 2003 Server**. Các tập tin này không chiếm nhiều không gian đĩa. Theo mặc định, **partition active** của máy tính sẽ được chọn làm **partition system**, vốn thường là ổ đĩa C:. **Partition boot** là nơi chứa các tập tin của hệ điều hành. Theo mặc định các tập tin này lưu trong thư mục **WINDOWS**. Tuy nhiên bạn có thể chỉ định thư mục khác trong quá trình cài đặt. **Microsoft** đề nghị **partition** này nhỏ nhất là 1,5 GB.
- Cấu hình đĩa đặc biệt: **Windows 2003 Server** hỗ trợ nhiều cấu hình đĩa khác nhau. Các lựa chọn có thể là **volume simple**, **spanned**, **striped**, **mirrored** hoặc là **RAID-5**.

- **Tiện ích phân chia partition:** nếu bạn định chia **partition** trước khi cài đặt, bạn có thể sử dụng nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu bạn chỉ cần tạo một **partition** để cài đặt **Windows 2003 Server**, sau đó sử dụng công cụ **Disk Management** để tạo thêm các **partition** khác.

II.5. Chọn hệ thống tập tin.

Bạn có thể chọn sử dụng một trong ba loại hệ thống tập tin sau:

- ***FAT16*** (**file allocation table**)***:*** là hệ thống được sử dụng phổ biến trên các hệ điều hành **DOS** và **Windows 3.x**. Có nhược điểm là **partition** bị giới hạn ở kích thước 2GB và không có các tính năng bảo mật như **NTFS.**
- ***FAT32:*** được đưa ra năm 1996 theo bản **Windows 95 OEM Service Release 2 (OSR2)**. Có nhiều ưu điểm hơn **FAT16** như: hỗ trợ **partition** lớn đến 2TB; có các tính năng dung lỗi và sử dụng không gian đĩa cứng hiệu quả hơn do giảm kích thước **cluster**. Tuy nhiên **FAT32** lại có nhược điểm là không cung cấp các tính năng bảo mật như **NTFS**.
- ***NTFS:*** là hệ thống tập tin được sử dụng trên các hệ điều hành **Windows NT, Windows 2000**, **Windows 2003**. **Windows 2000, Windows 2003** sử dụng **NTFS** phiên bản 5. Có các đặc điểm sau: chỉ định khả năng an toàn cho từng tập tin, thư mục; nén dữ liệu, tăng không gian lưu trữ; có thể chỉ định hạn ngạch sử dụng đĩa cho từng người dùng; có thể mã hoá các tập tin, nâng cao khả năng bảo mật.

II.6. Chọn chế độ sử dụng giấy phép.

Bạn chọn một trong hai chế độ giấy phép sau đây:

- **Per server licensing**: là lựa chọn tốt nhất trong trường hợp mạng chỉ có một Server và phục cho một số lượng Client nhất định. Khi chọn chế độ giấy phép này, chúng ta phải xác định số lượng giấy phép tại thời điểm cài đặt hệ điều hành. Số lượng giấy phép tùy thuộc vào số kết nối đồng thời của các Client đến Server. Tuy nhiên, trong quá trình sử dụng chúng ta có thể thay đổi số lượng kết nối đồng thời cho phù hợp với tình hình hiện tại của mạng.
- **Per Seat licensing**: là lựa chọn tốt nhất trong trường hợp mạng có nhiều Server. Trong chế độ giấy phép này thì mỗi Client chỉ cần một giấy phép duy nhất để truy xuất đến tất cả các Server và không giới hạn số lượng kết nối đồng thời đến Server.

II.7. Chọn phương án kết nối mạng.

II.7.1 Các giao thức kết nối mạng.

Windows 2003 mặc định chỉ cài một giao thức **TCP/IP**, còn những giao thức còn lại như **IPX**, **AppleTalk** là những tùy chọn có thể cài đặt sau nếu cần thiết. Riêng giao thức **NetBEUI**, **Windows 2003** không đưa vào trong các tùy chọn cài đặt mà chỉ cung cấp kèm theo đĩa **CD-ROM** cài đặt **Windows 2003** và được lưu trong thư mục **\VALUEADD\MSFT\NET\NETBEUI**.

II.7.2 Thành viên trong Workgroup hoặc Domain.

Nếu máy tính của bạn nằm trong một mạng nhỏ, phân tán hoặc các máy tính không được nối mạng với nhau, bạn có thể chọn cho máy tính làm thành viên của **workgroup**, đơn giản bạn chỉ cần cho biết tên

workgroup là xong.

Nếu hệ thống mạng của bạn làm việc theo cơ chế quản lý tập trung, trên mạng đã có một vài máy **Windows 2000 Server** hoặc **Windows 2003 Server** sử dụng **Active Directory** thì bạn có thể chọn cho máy tính tham gia **domain** này. Trong trường hợp này, bạn phải cho biết tên chính xác của **domain** cùng với tài khoản (gồm có **username** và **password**) của một người dùng có quyền bổ sung thêm máy tính vào **domain**. Ví dụ như tài khoản của người quản trị mạng (**Administrator**).

Các thiết lập về ngôn ngữ và các giá trị cục bộ.

Windows 2000 Server hỗ trợ rất nhiều ngôn ngữ, bạn có thể chọn ngôn ngữ của mình nếu được hỗ trợ. Các giá trị **local** gồm có hệ thống số, đơn vị tiền tệ, cách hiển thị thời gian, ngày tháng.

III. CÀI ĐẶT WINDOWS SERVER 2003.

III.1. Giai đoạn Preinstallation.

Sau khi kiểm tra và chắc chắn rằng máy của mình đã hội đủ các điều kiện để cài đặt **Windows 2003 Server**, bạn phải chọn một trong các cách sau đây để bắt đầu quá trình cài đặt.

III.1.1 Cài đặt từ hệ điều hành khác.

Nếu máy tính của bạn đã có một hệ điều hành và bạn muốn nâng cấp lên **Windows 2003 Server** hoặc là bạn muốn khởi động kép, đầu tiên bạn cho máy tính khởi động bằng hệ điều hành có sẵn này, sau đó tiến hành quá trình cài đặt **Windows 2003 Server**.

Tuỳ theo hệ điều hành đang sử dụng là gì, bạn có thể sử dụng hai lệnh sau trong thư mục **I386**:

- **WINNT32.EXE** nếu là Windows 9x hoặc Windows NT.
- **WINNT.EXE** nếu là hệ điều hành khác.

III.1.2 Cài đặt trực tiếp từ đĩa CD Windows 2003.

Nếu máy tính của bạn hỗ trợ tính năng khởi động từ đĩa CD, bạn chỉ cần đặt đĩa CD vào ổ đĩa và khởi động lại máy tính. Lưu ý là bạn phải cấu hình **CMOS Setup**, chỉ định thiết bị khởi động đầu tiên là ổ đĩa **CDROM**. Khi máy tính khởi động lên thì quá trình cài đặt tự động thi hành, sau đó làm theo những hướng dẫn trên màn hình để cài đặt **Windows 2003**.

III.1.3 Cài đặt Windows 2003 Server từ mạng.

Để có thể cài đặt theo kiểu này, bạn phải có một Server phân phối tập tin, chứa bộ nguồn cài đặt **Windows 2003 Server** và đã chia sẻ thư mục này. Sau đó tiến hành theo các bước sau:

- Khởi động máy tính định cài đặt.
- Kết nối vào máy Server và truy cập vào thư mục chia sẻ chứa bộ nguồn cài đặt.
- Thi hành lệnh **WINNT.EXE** hoặc **WINNT32.EXE** tuỳ theo hệ điều hành đang sử dụng trên máy.
- Thực hiện theo hướng dẫn của chương trình cài đặt.

III.2. Giai đoạn Text-Based Setup.

Trong qúa trình cài đặt nên chú ý đến các thông tin hướng dẫn ở thanh trạng thái.

Giai đoạn **Text-based setup** diễn ra một số bước như sau:

(1) Cấu hình **BIOS** của máy tính để có thể khởi động từ ổ đĩa **CD-ROM.**

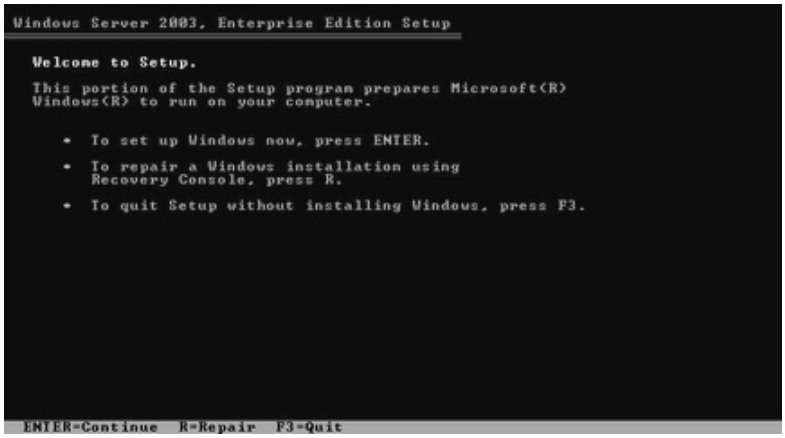
(2) Đưa đĩa cài đặt **Windows 2003 Server** vào ổ đĩa **CD-ROM** và khởi động lại máy.

(3) Khi máy khởi động từ đĩa **CD-ROM** sẽ xuất hiện một thông báo "**Press any key to continue…**" yêu cầu nhấn một phím bất kỳ để bắt đầu quá trình cài đặt.

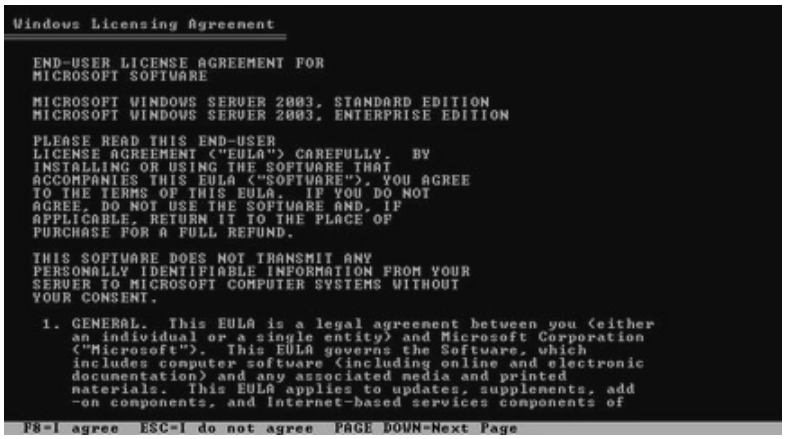
(4) Nếu máy có ổ đĩa **SCSI** thì phải nhấn phím F6 để chỉ Driver của ổ đĩa đó.

(5) Trình cài đặt tiến hành chép các tập tin và **driver** cần thiết cho quá trình cài đặt.

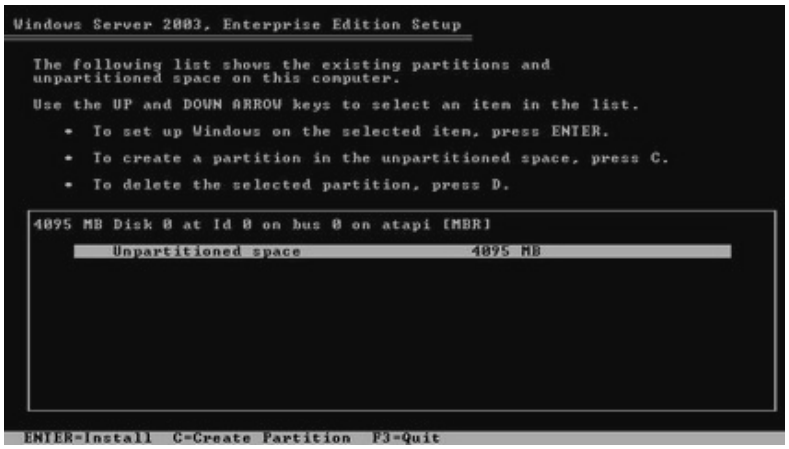
(6) Nhấn **Enter** để bắt đầu cài đặt.



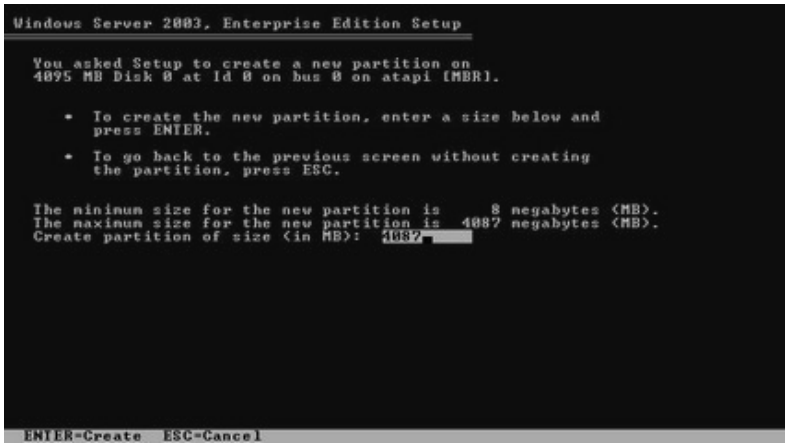
(7) Nhấn phím **F8** để chấp nhận thỏa thuận bản quyền và tiếp tục quá trình cài đặt. Nếu nhấn **ESC**, thì chương trình cài đặt kết.



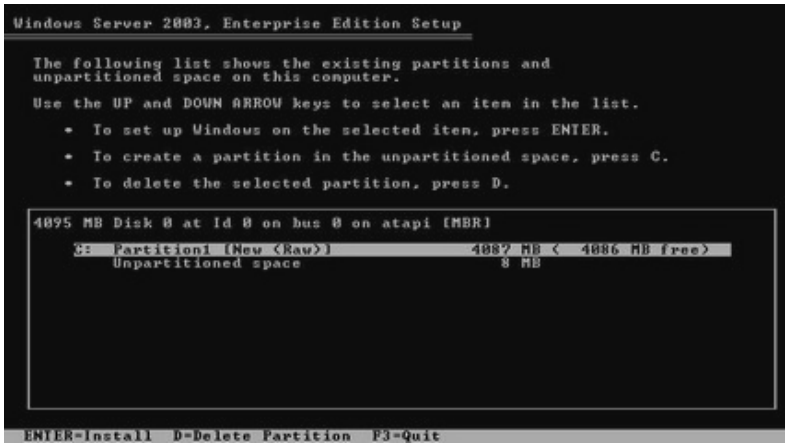
(8) Chọn một vùng trống trên ổ đĩa và nhấn phím **C** để tạo một **Partition** mới chứa hệ điều hành.



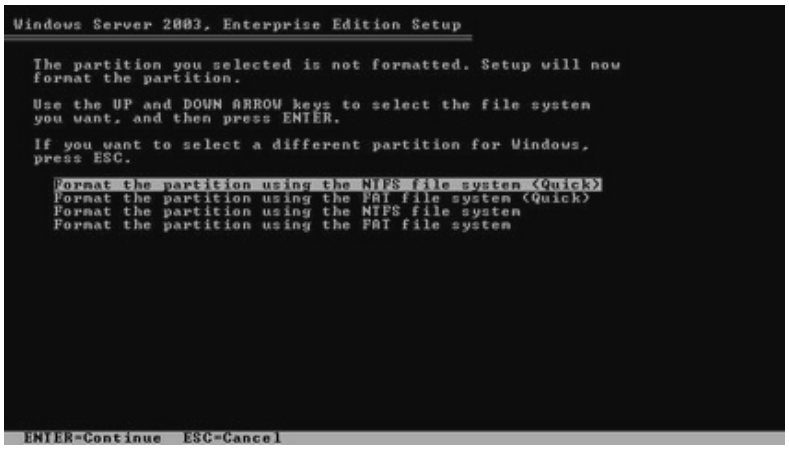
(9) Nhập vào kích thước của **Partition** mới và nhấn **Enter**.



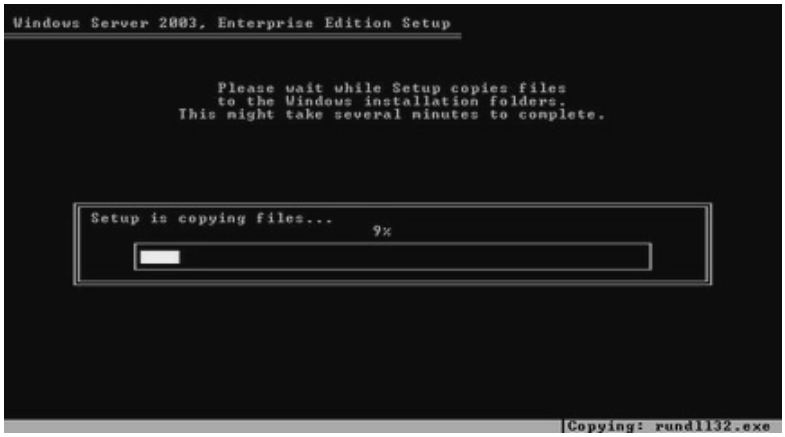
(10) Chọn **Partition** vừa tạo và nhấn **Enter** để tiếp tục.



(11) Chọn kiểu hệ thống tập tin (**FAT** hay **NTFS**) để định dạng cho **partition**. Nhấn **Enter** để tiếp tục.



(12) Trình cài đặt sẽ chép các tập tin của hệ điều hành vào **partition** đã chọn.

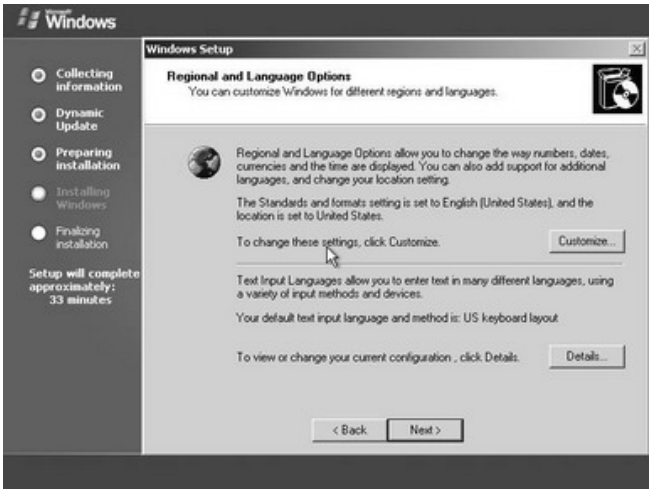


(13) Khởi động lại hệ thống để bắt đầu giai đoạn **Graphical Based**. Trong khi khởi động, không nhấn bất kỳ phím nào khi hệ thống yêu cầu "**Press any key to continue…**"

III.3. Giai đoạn Graphical-Based Setup.

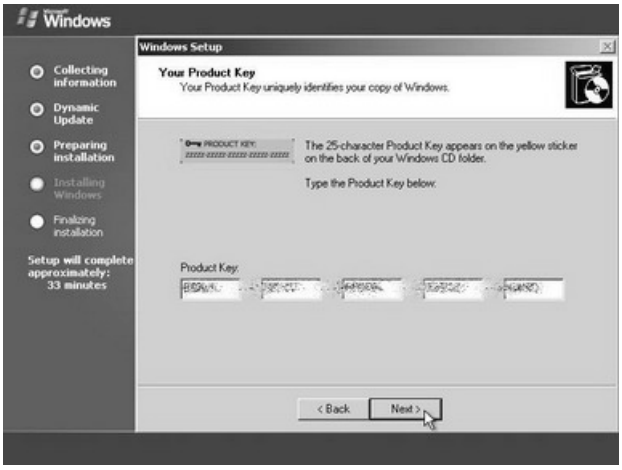
(1) Bắt đầu giai đoạn **Graphical**, trình cài đặt sẽ cài **driver** cho các thiết bị mà nó tìm thấy trong hệ thống.

(2) Tại hộp thoại **Regional and Language Options**, cho phép chọn các tùy chọn liên quan đến ngôn ngữ, số đếm, đơn vị tiền tệ, định dạng ngày tháng năm,….Sau khi đã thay đổi các tùy chọn phù hợp, nhấn **Next** để tiếp tục.

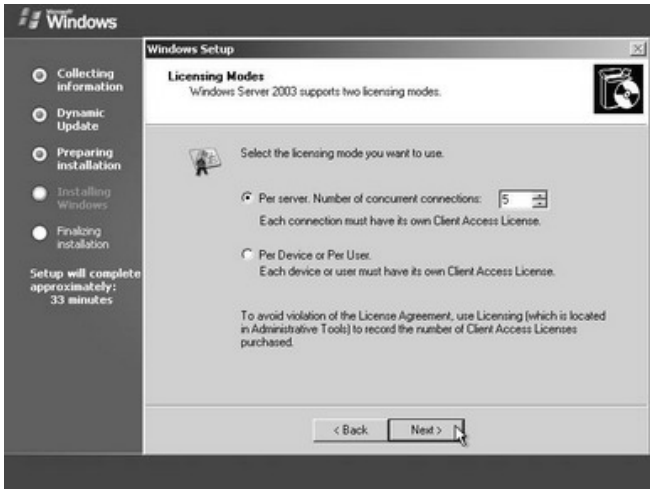


(3) Tại hộp thoại **Personalize Your Software**, điền tên người sử dụng và tên tổ chức. Nhấn **Next**.

(4) Tại hộp thoại **Your Product Key**, điền vào 25 số **CD-Key** vào 5 ô trống bên dưới. Nhấn **Next**.



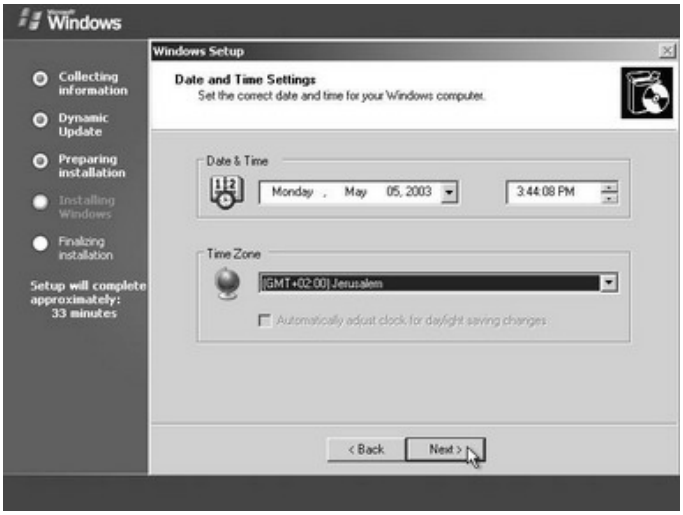
(5) Tại hộp thoại **Licensing Mode**, chọn chế độ bản quyền là **Per Server** hoặc **Per Seat** tùy thuộc vào tình hình thực tế của mỗi hệ thống mạng.



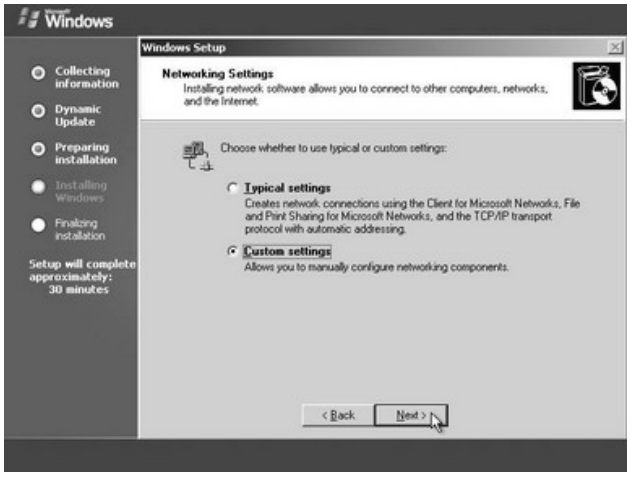
(6) Tại hộp thoại **Computer Name and Administrator Password**, điền vào tên của **Server** và **Password** của người quản trị (**Administrator**).

(7) Tại hộp thoại **Date and Time Settings**, thay đổi ngày, tháng, và múi giờ (**Time zone**) cho thích

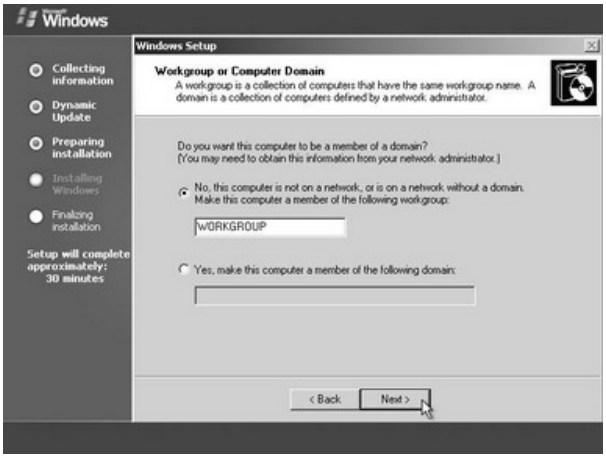
hợp.



(8) Tại hộp thoại **Networking Settings**, chọn **Custom settings** để thay đổi các thông số giao thức **TCP/IP**. Các thông số này có thể thay đổi lại sau khi quá trình cài đặt hoàn tất.



(9) Tại hộp thoại **Workgroup or Computer Domain**, tùy chọn gia nhập **Server** vào một **Workgroup** hay một **Domain** có sẵn. Nếu muốn gia nhập vào **Domain** thì đánh vào tên **Domain** vào ô bên dưới.



(10) Sau khi chép đầy đủ các tập tin, quá trình cài đặt kết thúc.

IV. TỰ ĐỘNG HÓA QUÁ TRÌNH CÀI ĐẶT.

Nếu bạn dự định cài đặt hệ điều hành **Windows 2003 Server** trên nhiều máy tính, bạn có thể đến từng máy và tự tay thực hiện quá trình cài đặt như đã hướng dẫn trong chương trước. Tuy nhiên, chắc chắn công việc này sẽ vô cùng nhàm chán và không hiệu quả. Lúc này việc tự động hoá quá trình cài đặt sẽ giúp công việc của bạn trở nên đơn giản, hiệu quả và ít tốn kém hơn.

Có nhiều phương pháp hỗ trợ việc cài đặt tự động. Chẳng hạn, bạn có thể sử dụng phương pháp dùng ảnh đĩa (**disk image**) hoặc phương pháp cài đặt không cần theo dõi (**unattended installation**) thông qua một kịch bản (**script**) hay tập tin trả lời.

IV.1. Giới thiệu kịch bản cài đặt.

Kịch bản cài đặt là một tập tin văn bản có nội dung trả lời trước tất cả các câu hỏi mà trình cài đặt hỏi như: tên máy, **CD-Key**,….Để trình cài đặt có thể đọc hiểu các nội dung trong kịch bản thì nó phải được tạo ra theo một cấu trúc được quy định trước. Để tạo ra được các kịch bản cài đặt, có thể dùng bất kỳ chương trình soạn thảo văn bản nào, chẳng hạn như **Notepad**. Tuy nhiên, kịch bản là một tập tin có cấu trúc nên trong quá trình soạn thảo có thể xảy ra các sai sót dẫn đến quá trình tự động hóa cài đặt không diễn ra theo ý muốn. Do đó, **Microsoft** đã tạo ra một tiện ích có tên là **Setup Manager** (**setupmgr.exe**) để giúp cho việc tạo ra kịch bản cài đặt được dễ dàng hơn. Sau khi có được kịch bản, có thể sử dụng **Notepad** để thêm, sửa lại một số thông tin để sử dụng kịch bản vào quá trình cài đặt tự động hiệu quả hơn.

IV.2. Tự động hóa dùng tham biến dòng lệnh.

Khi tiến hành cài đặt **Windows 2003 Server**, ngoài cách khởi động và cài trực tiếp từ đĩa **CD-ROM**, còn có thể dùng một trong hai lệnh sau: **winnt.exe** dùng với các máy đang chạy hệ điều hành DOS, **windows 3.x** hoặc **Windows for workgroup**; **winnt32.exe** khi máy đang chạy hệ điều hành **Windows 9x**, **Windows NT** hoặc mới hơn. Hai lệnh trên được đặt trong thư mục **I386** của đĩa cài đặt.

Sau đây là cú pháp cài đặt từ 2 lệnh trên:

winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]]

[/udf:id [,UDB_file]]

Ý nghĩa các tham số:

/s

Chỉ rỏ vị trí đặt của bộ nguồn cài đặt (thư mục I386). Đường dẫn phải là dạng đầy đủ, ví dụ: e:\i386 hoặc **\\server\i386**. Giá trị mặc định là thư mục hiện hành.

/t

Hướng chương trình cài đặt đặt thư mục tạm vào một ổ đĩa và cài **Windows** vào ổ đĩa đó. Nếu không chỉ định, trình cài đặt sẽ tự xác định.

/u

Cài đặt không cần theo dõi với một tập tin trả lời tự động (kịch bản). Nếu sử dụng /u thì phải sử dụng /s.

/udf

Chỉ định tên của **Server** và tập tin cơ sở dữ liệu chứa tên, các thông tin đặc trưng cho mỗi máy (unattend.udf).

winnt32 [**/checkupgradeonly**] [**/s:***sourcepath*] [**/tempdrive:***drive_letter***:**] [**/unattend**[*num*]**:**[*answer_file*]]

[**/udf:***id* [,*UDB_file*]]

Ý nghĩa của các tham số:

/checkupgradeonly

Kiểm tra xem máy có tương thích để nâng cấp và cài đặt **Windows 2003 Server** hay không?

/tempdrive

Tương tự như tham số /t

/unattend

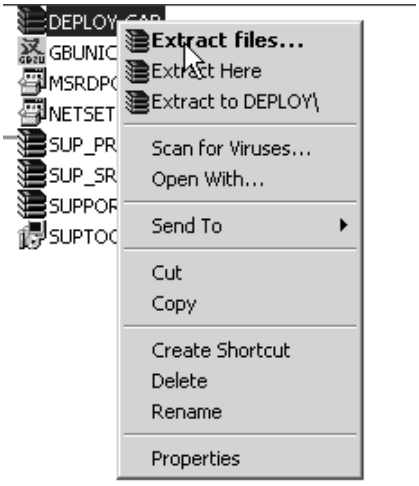
Tương tư như tham số /u

IV.3. Sử dụng Setup Manager để tạo ra tập tin trả lời.

Setup Manager là một tiện ích giúp cho việc tạo các tập tin trả lời sử dụng trong cài đặt không cần theo dõi. Theo mặc định, **Setup Manager** không được cài đặt, mà được đặt trong tập tin **Deploy.Cab**. Chỉ có thể chạy tiện ích **Setup Manager** trên các hệ điều hành **Windows 2000, Windows XP, Windows 2003**.

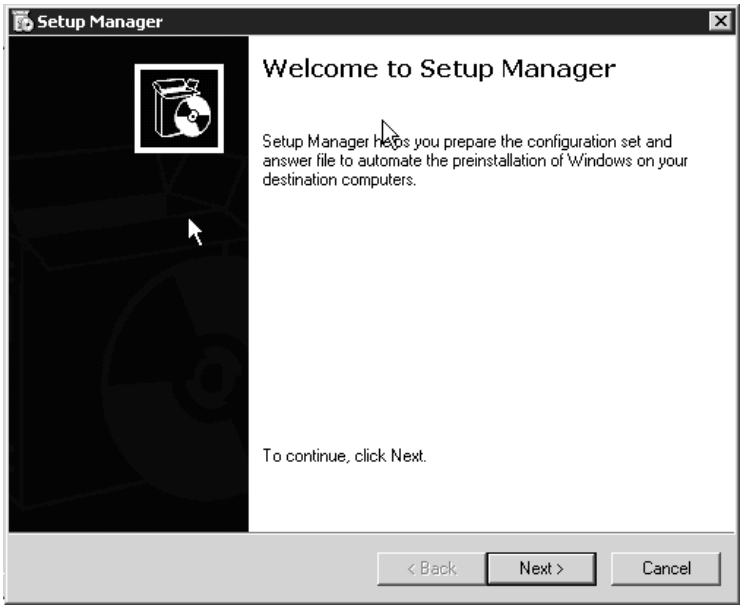
Tạo tập tin trả lời tự động bằng **Setup Manager**:

(1) Giải nén tập tin **Deploy.cab** được lưu trong thư mục **Support\Tools** trên đĩa cài đặt **Windows 2003**.

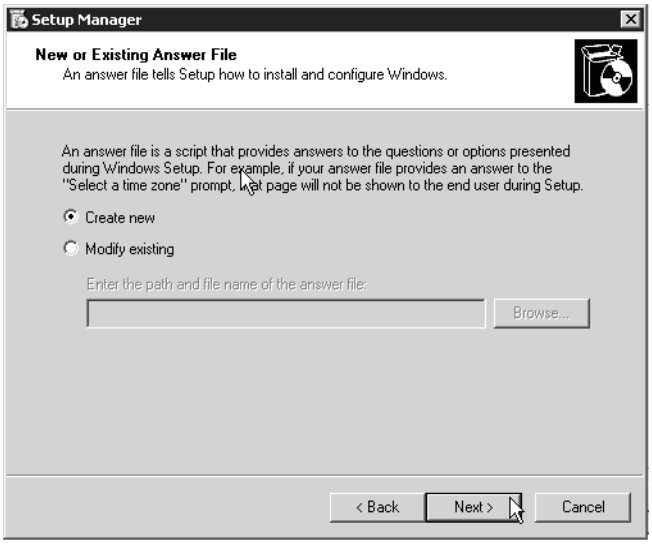


(2) Thi hành tập tin **Setupmgr.exe**

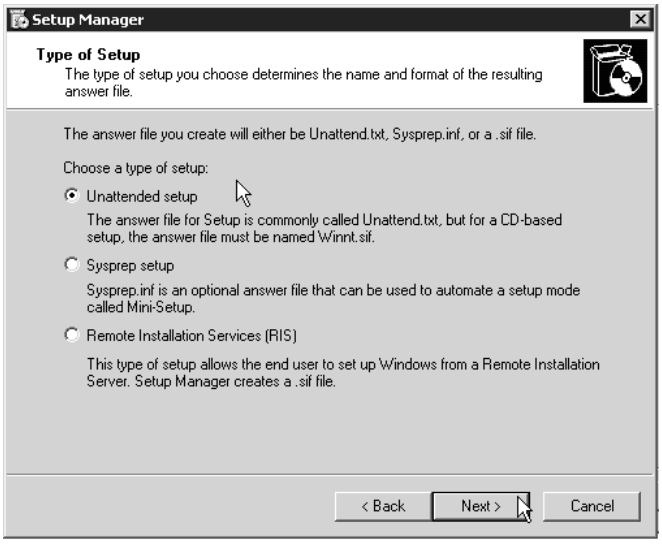
(3) Hộp thoại **Setup Manager** xuất hiện, nhấn **Next** để tiếp tục.



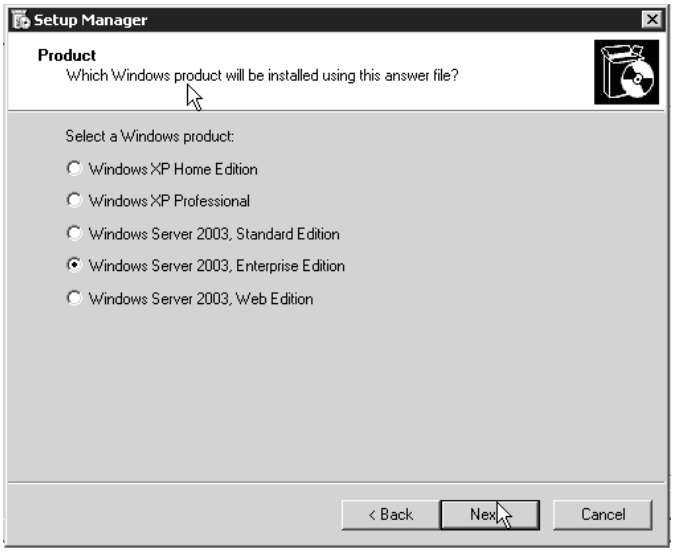
(4) Xuất hiện hộp thoại **New or Existing Answer File**. Hộp thoại này cho phép bạn chỉ định tạo ra một tập tin trả lời mới, một tập tin trả lời phản ánh cấu hình của máy tính hiện hành hoặc là chỉnh sửa một tập tin sẵn có. Bạn chọn **Create new** và nhấn **Next**.



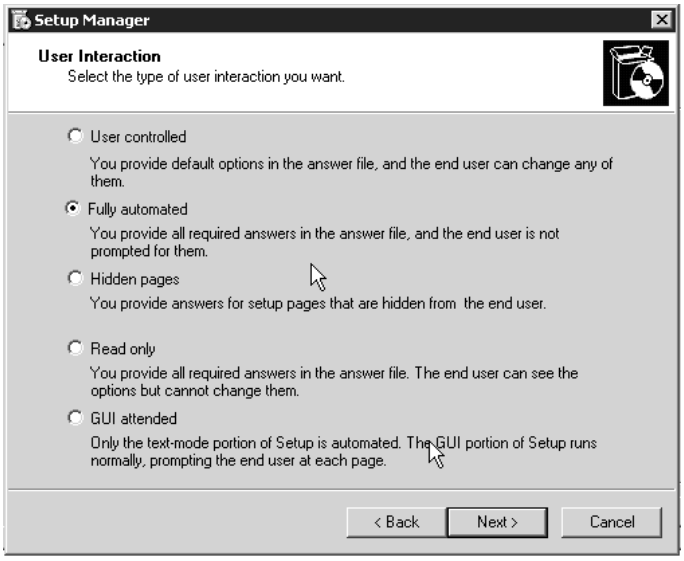
(5) Tiếp theo là hộp thoại **Type of Setup**. Chọn **Unattended Setup** và chọn **Next**.



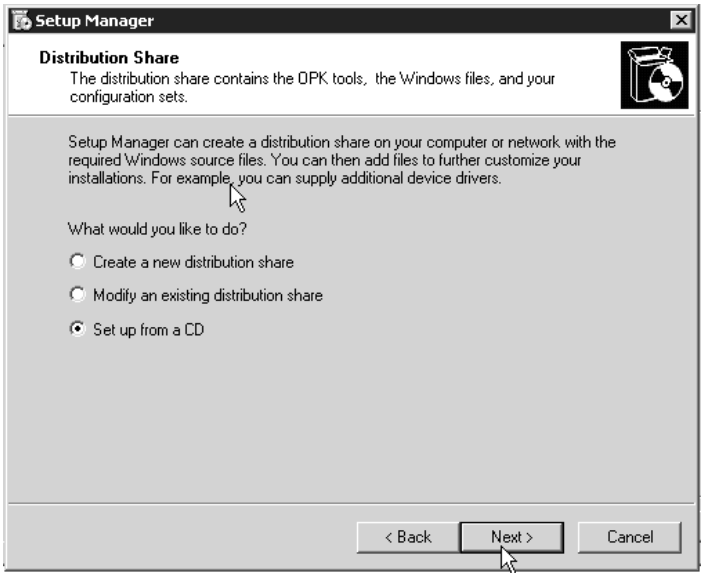
(6) Trong hộp thoại **Product**, chọn hệ điều hành cài đặt sử dụng tập tin trả lời tự động. Chọn **Windows Server 2003, Enterprise Edition**, nhấn **Next**.



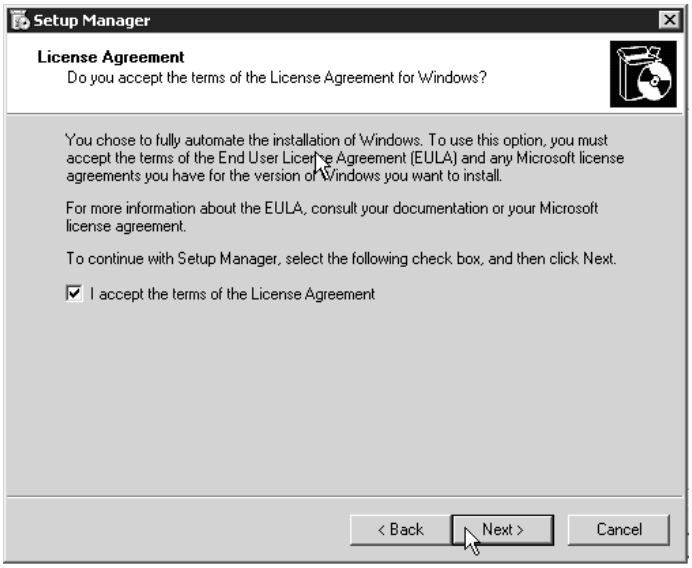
(7) Tại hộp thoại **User Interaction**, chọn mức độ tương tác với trình cài đặt của người sử dụng. Chọn **Fully Automated**, nhấn **Next**.



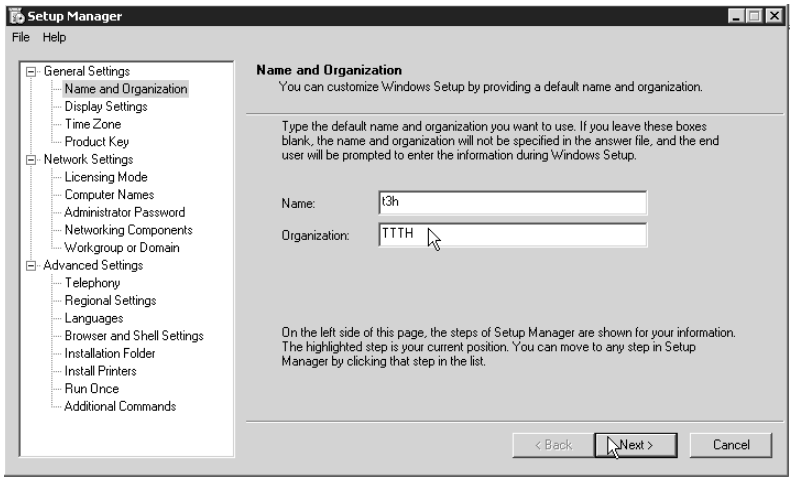
(8) Xuất hiện hộp thoại **Distribution Share**, chọn **Setup from a CD**, nhấn **Next**.



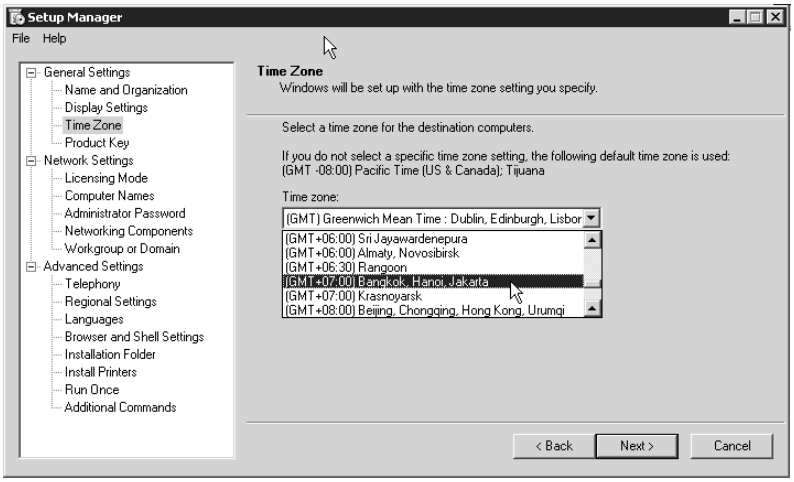
(9) Tại hộp thoại **License Agreement**, đánh dấu vào **I accept the terms of …**, nhấn **Next**.



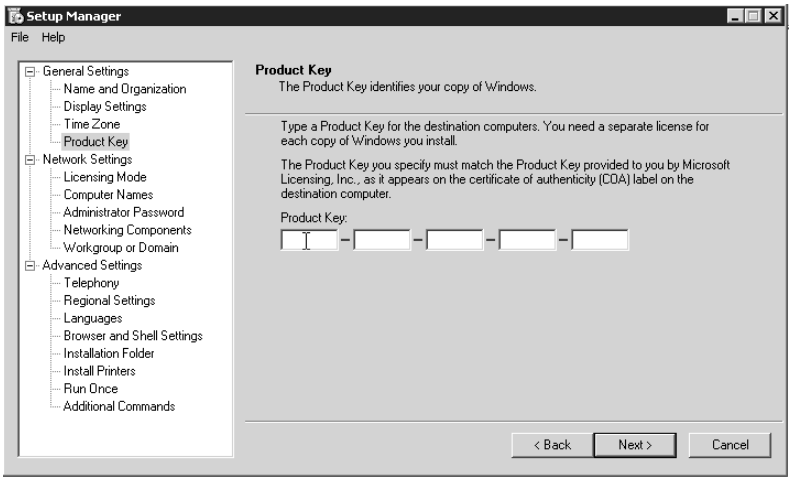
(10) Tại cửa sổ **Setup Manager**, chọn mục **Name and Organization**. Điền tên và tổ chức sử dụng hệ điều hành. Nhấn **Next**.



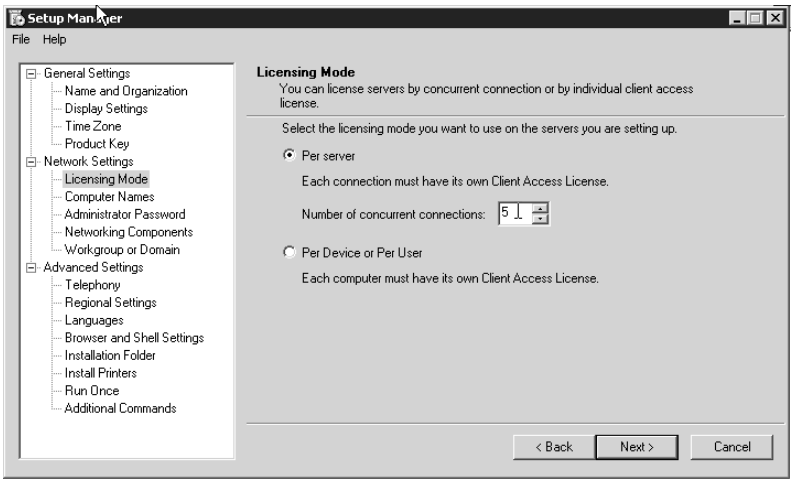
(11) Chọn mục **Time Zone** chọn múi giờ (**GMT+7:00) Bangkok, Hanoi, Jarkata**. Nhấn **Next**.



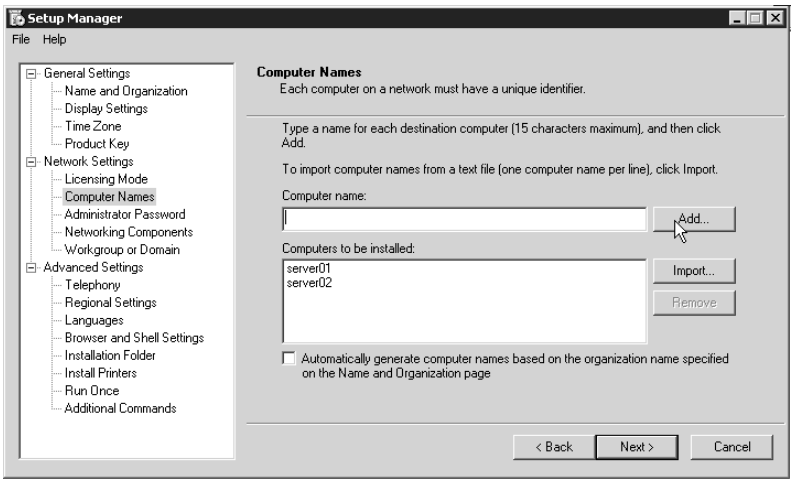
(12) Tại mục **Product Key**, điền **CD-Key** vào trong 5 ô trống. Nhấn **Next**.



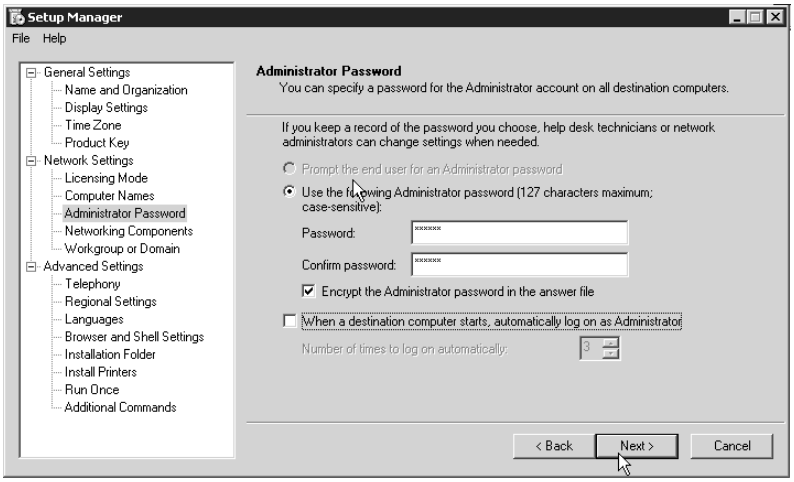
(13) Tại mục **Licensing Mode**, chọn loại bản quyền thích hợp. Nhấn **Next**.



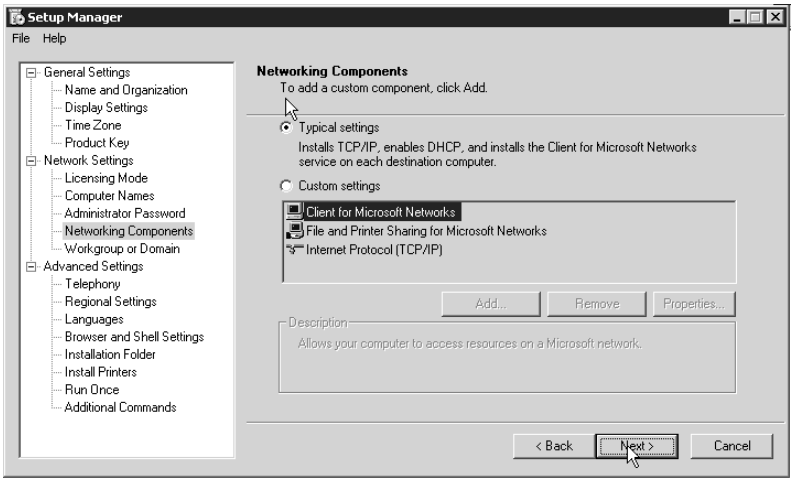
(14) Tại mục **Computer Names**, điền tên của các máy dự định cài đặt. Nhấn **Next**.



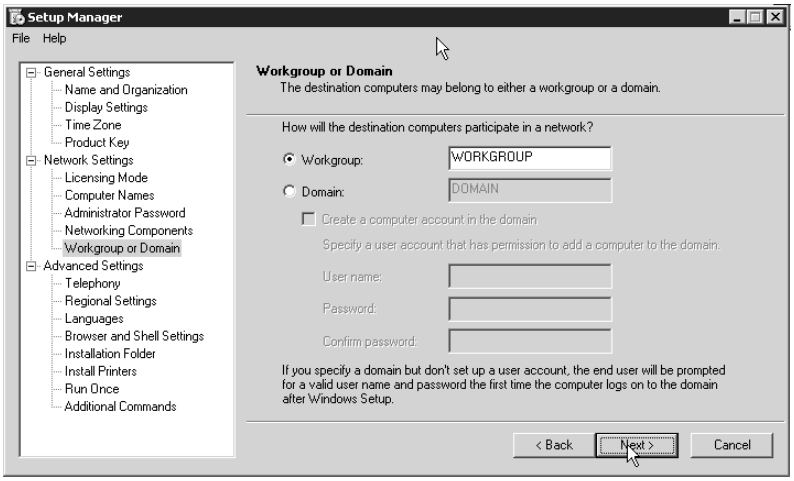
(15) Tại mục **Administrator Password**, nhập vào **password** của người quản trị. Nếu muốn mã hóa **password** thì đánh dấu chọn vào mục "**Encrypt the Administrator password…**". Nhấn **Next**.



(16) Tại mục **Network Component**, cấu hình các thông số cho giao thức **TCP/IP** và cài thêm các giao thức. Nhấn **Next**.



(17) Tại mục **Workgroup or Domain**, gia nhập máy vào **Workgroup** hoặc **Domain** có sẵn. Nhấn **Next**.



(18) Cuối cùng, trong thư mục đã chỉ định, **Setup Manager** sẽ tạo ra ba tập tin. Nếu bạn không thay đổi tên thì các tập tin là:

Unattend.txt: đây là tập tin trả lời, chứa tất cả các câu trả lời mà **Setup Manager** thu thập được.

Unattend.udb: đây là tập tin cơ sở dữ liệu chứa tên các máy tính sẽ được cài đặt. Tập tin này chỉ được tạo ra khi bạn chỉ định danh sách các tập tin và được sử dụng khi bạn thực hiện cài đặt không cần theo dõi.

Unattend.bat: chứa dòng lệnh với các tham số được thiết lập sẵn. Tập tin này cũng thiết lập các biến môi trường chỉ định vị trí các tập tin liên quan.

IV.4. Sử dụng tập tin trả lời

Có nhiều cách để sử dụng các tập tin được tạo ra trong bước trên. Bạn có thể thực hiện theo một trong hai cách dưới đây:

IV.4.1 Sử dụng đĩa CD Windows 2003 Server có thể khởi động được

Sửa tập tin **Unattend.txt** thành **WINNT.SIF** và lưu lên đĩa mềm.

Đưa đĩa CD **Windows 2000 Server** và đĩa mềm trên vào ổ đĩa, khởi động lại máy tính, đảm bảo ổ đĩa CD là thiết bị khởi động đầu tiên. Chương trình cài đặt trên đĩa CD sẽ tự động tìm đọc tập tin **WINNT.SIF** trên đĩa mềm và tiến hành cài đặt không cần theo dõi.

IV.4.2 Sử dụng một bộ nguồn cài đặt Windows 2003 Server

Chép các tập tin đã tạo trong bước trên vào thư mục **I386** của nguồn cài đặt **Windows 2003 Server**.

Chuyển vào thư mục **I386**.

Tuỳ theo hệ điều hành đang sử dụng mà sử dụng lệnh **WINNT.EXE** hoặc **WINNT32.EXE** theo cú pháp sau:

```
WINNT /s:e:\i386 /u:unattend.txt
```

hoặc

```
WINNT32 /s:e:\i386 /unattend:unattend.txt
```

Nếu chương trình **Setup Manager** tạo ra tập tin **Unatend.UDB** do bạn đã nhập vào danh sách tên các máy tính, và giả định bạn định đặt tên máy tính này là **server01** thì cú pháp lệnh sẽ như sau:

```
WINNT /s:e:\i386 /u:unattend.txt /udf:server01,unattend.udf
```

Tóm tắt

Lý thuyết 4 tiết - Thực hành 8 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về hệ thống Active Directory trên Windows Server 2003, cách tổ chức, nâng cấp để tạo thành Domain Controller …	I. Các mô hình mạng trong môi trường Microsoft. II. Active Directory. III. Cài đặt và cấu hình Active Directory.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. CÁC MÔ HÌNH MẠNG TRONG MÔI TRƯỜNG MICROSOFT.

I.1. Mô hình Workgroup.

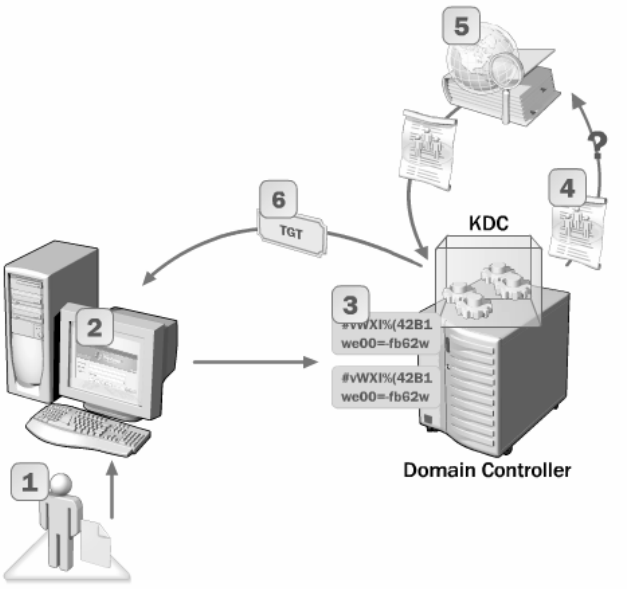
Mô hình mạng **workgroup** còn gọi là mô hình mạng **peer-to-peer**, là mô hình mà trong đó các máy tính có vai trò như nhau được nối kết với nhau. Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ, các máy tự quản lý tài nguyên cục bộ của mình. Trong hệ thống mạng không có máy tính chuyên cung cấp dịch vụ và quản lý hệ thống mạng. Mô hình này chỉ phù hợp với các mạng nhỏ, dưới mười máy tính và yêu cầu bảo mật không cao.

Đồng thời trong mô hình mạng này các máy tính sử dụng hệ điều hành hỗ trợ đa người dùng lưu trữ thông tin người dùng trong một tập tin **SAM (Security Accounts Manager)** ngay chính trên máy tính cục bộ. Thông tin này bao gồm: **username** (tên đăng nhập), **fullname**, **password**, **description**… Tất nhiên tập tin **SAM** này được mã hóa nhằm tránh người dùng khác ăn cấp mật khẩu để tấn công vào máy tính. Do thông tin người dùng được lưu trữ cục bộ trên các máy trạm nên việc chứng thực người dùng đăng nhập máy tính cũng do các máy tính này tự chứng thực.

I.2. Mô hình Domain.

Khác với mô hình **Workgroup**, mô hình **Domain** hoạt động theo cơ chế **client-server**, trong hệ thống mạng phải có ít nhất một máy tính làm chức năng điều khiển vùng (**Domain Controller**), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng. Việc chứng thực người dùng và quản lý tài nguyên mạng được tập trung lại tại các **Server** trong miền. Mô hình này được áp dụng cho các công ty vừa và lớn.

Trong mô hình **Domain** của **Windows Server 2003** thì các thông tin người dùng được tập trung lại do dịch vụ **Active Directory** quản lý và được lưu trữ trên máy tính điều khiển vùng (**domain controller**) với tên tập tin là **NTDS.DIT**. Tập tin cơ sở dữ liệu này được xây dựng theo công nghệ tương tự như phần mềm **Access** của **Microsoft** nên nó có thể lưu trữ hàng triệu người dùng, cải tiến hơn so với công nghệ cũ chỉ lưu trữ được khoảng 5 nghìn tài khoản người dùng. Do các thông tin người dùng được lưu trữ tập trung nên việc chứng thực người dùng đăng nhập vào mạng cũng tập trung và do máy điều khiển vùng chứng thực.



Hình 2.1: các bước chứng thực khi người dùng đăng nhập.

II. ACTIVE DIRECTORY.

II.1. Giới thiệu Active Directory.

Có thể so sánh **Active Directory** với **LANManager** trên **Windows NT 4.0**. Về căn bản, **Active Directory** là một cơ sở dữ liệu của các tài nguyên trên mạng (còn gọi là đối tượng) cũng như các thông tin liên quan đến các đối tượng đó. Tuy vậy, **Active Directory** không phải là một khái niệm mới bởi **Novell** đã sử dụng dịch vụ thư mục (**directory service**) trong nhiều năm rồi.

Mặc dù **Windows NT 4.0** là một hệ điều hành mạng khá tốt, nhưng hệ điều hành này lại không thích hợp trong các hệ thống mạng tầm cỡ xí nghiệp. Đối với các hệ thống mạng nhỏ, công cụ **Network Neighborhood** khá tiện dụng, nhưng khi dùng trong hệ thống mạng lớn, việc duyệt và tìm kiếm trên mạng sẽ là một ác mộng (và càng tệ hơn nếu bạn không biết chính xác tên của máy in hoặc **Server** đó là gì). Hơn nữa, để có thể quản lý được hệ thống mạng lớn như vậy, bạn thường phải phân chia thành nhiều domain và thiết lập các mối quan hệ uỷ quyền thích hợp. **Active Directory** giải quyết được các vấn đề như vậy và cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp. Lúc này, dịch vụ thư mục trong mỗi **domain** có thể lưu trữ hơn mười triệu đối tượng, đủ để phục vụ mười triệu người dùng trong mỗi **domain**.

II.2. Chức năng của Active Directory.

- Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.
- Cung cấp một **Server** đóng vai trò chứng thực (**authentication server**) hoặc **Server** quản lý đăng nhập (**logon Server**), **Server** này còn gọi là **domain controller** (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (**index**) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng.

- Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (**rights**) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền **backup** dữ liệu hay **shutdown Server** từ xa…
- Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (**subdomain**) hay các đơn vị tổ chức **OU** (**Organizational Unit**). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

II.3. Directory Services.

II.3.1 Giới thiệu Directory Services.

Directory Services (dịch vụ danh bạ) là hệ thống thông tin chứa trong **NTDS.DIT** và các chương trình quản lý, khai thác tập tin này. Dịch vụ danh bạ là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống **Active Directory**. Một hệ thống với những tính năng vượt trội của **Microsoft**.

II.3.2 Các thành phần trong Directory Services.

Đầu tiên, bạn phải biết được những thành phần cấu tạo nên dịch vụ danh bạ là gì? Bạn có thể so sánh dịch vụ danh bạ với một quyển sổ lưu số điện thoại. Cả hai đều chứa danh sách của nhiều đối tượng khác nhau cũng như các thông tin và thuộc tính liên quan đến các đối tượng đó.

a. **Object** (đối tượng).

Trong hệ thống cơ sở dữ liệu, đối tượng bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, … Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.

b. **Attribute** (thuộc tính).

Một thuộc tính mô tả một đối tượng. Ví dụ, mật khẩu và tên là thuộc tính của đối tượng người dùng mạng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Lấy ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ **IP**.

c. **Schema** (cấu trúc tổ chức).

Một **schema** định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó. Ví dụ, cho rằng tất cả các đối tượng máy in đều được định nghĩa bằng các thuộc tính tên, loại **PDL** và tốc độ. Danh sách các đối tượng này hình thành nên **schema** cho lớp đối tượng "máy in". **Schema** có đặc tính là tuỳ biến được, nghĩa là các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được. Nói tóm lại **Schema** có thể xem là một danh bạ của cái danh bạ **Active Directory**.

d. **Container** (vật chứa).

Vật chứa tương tự với khái niệm thư mục trong **Windows**. Một thư mục có thể chứa các tập tin và các thư mục khác. Trong **Active Directory**, một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:

- **Domain**: khái niệm này được trình bày chi tiết ở phần sau.
- **Site**: một **site** là một vị trí. **Site** được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ, công ty XYZ có tổng hành dinh đặt ở **San Fransisco**, một chi nhánh đặt ở **Denver** và một văn

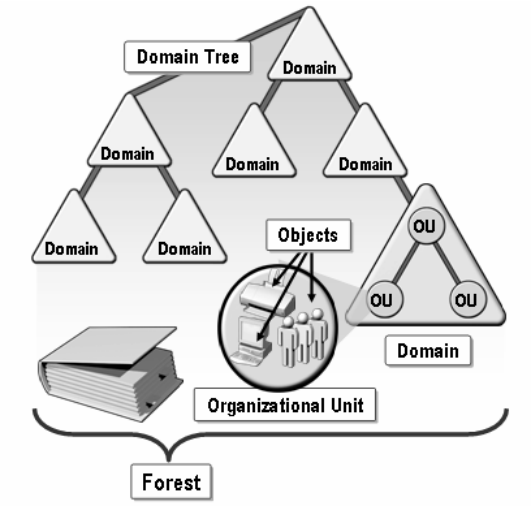
phòng đại diện đặt ở **Portland** kết nối về tổng hành dinh bằng **Dialup Networking**. Như vậy hệ thống mạng này có ba **site**.

- **OU (Organizational Unit):** là một loại vật chứa mà bạn có thể đưa vào đó người dùng, nhóm, máy tính và những **OU** khác. Một **OU** không thể chứa các đối tượng nằm trong domain khác. Nhờ việc một **OU** có thể chứa các **OU** khác, bạn có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain. Bạn nên sử dụng **OU** để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

e. Global Catalog.

- Dịch vụ **Global Catalog** dùng để xác định vị trí của một đối tượng mà người dùng được cấp quyền truy cập. Việc tìm kiếm được thực hiện xa hơn những gì đã có trong **Windows NT** và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.
- Giả sử bạn phải in một tài liệu dày 50 trang thành 1000 bản, chắc chắn bạn sẽ không dùng một máy in **HP Laserjet 4L**. Bạn sẽ phải tìm một máy in chuyên dụng, in với tốc độ 100ppm và có khả năng đóng tài liệu thành quyển. Nhờ **Global Catalog**, bạn tìm kiếm trên mạng một máy in với các thuộc tính như vậy và tìm thấy được một máy **Xerox Docutech 6135**. Bạn có thể cài đặt **driver** cho máy in đó và gửi **print job** đến máy in. Nhưng nếu bạn ở **Portland** và máy in thì ở **Seattle** thì sao? **Global Catalog** sẽ cung cấp thông tin này và bạn có thể gửi **email** cho chủ nhân của máy in, nhờ họ in giùm.
- Một ví dụ khác, giả sử bạn nhận được một thư thoại từ một người tên **Betty Doe** ở bộ phận kế toán. Đoạn thư thoại của cô ta bị cắt xén và bạn không thể biết được số điện thoại của cô ta. Bạn có thể dùng **Global Catalog** để tìm thông tin về cô ta nhờ tên, và nhờ đó bạn có được số điện thoại của cô ta.
- Khi một đối tượng được tạo mới trong **Active Directory**, đối tượng được gán một con số phân biệt gọi là **GUID** (**Global Unique Identifier**). **GUID** của một đối tượng luôn luôn cố định cho dù bạn có di chuyển đối tượng đi đến khu vực khác.

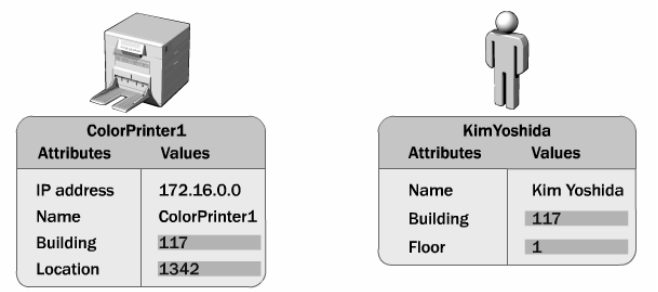
II.4. Kiến trúc của Active Directory.



Hình 2.2: kiến trúc của **Active Directory**.

II.4.1 Objects.

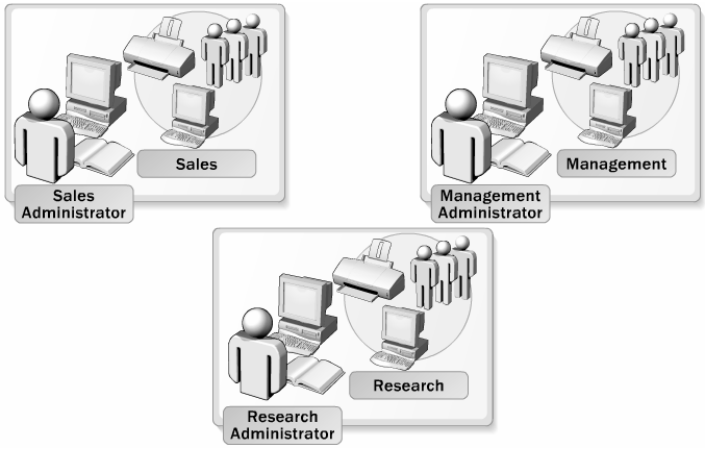
Trước khi tìm hiểu khái niệm **Object**, chúng ta phải tìm hiểu trước hai khái niệm **Object classes và Attributes**. **Object classes** là một bản thiết kế mẫu hay một khuôn mẫu cho các loại đối tượng mà bạn có thể tạo ra trong **Active Directory**. Có ba loại **object classes** thông dụng là: **User, Computer, Printer**. Khái niệm thứ hai là **Attributes**, nó được định nghĩa là tập các giá trị phù hợp và được kết hợp với một đối tượng cụ thể. Như vậy **Object** là một đối tượng duy nhất được định nghĩa bởi các giá trị được gán cho các thuộc tính của object **classes**. Ví dụ hình sau minh họa hai đối tượng là: máy in **ColorPrinter1** và người dùng **KimYoshida**.



II.4.2 Organizational Units.

Organizational Unit hay **OU** là đơn vị nhỏ nhất trong hệ thống **AD**, nó được xem là một vật chứa các đối tượng (**Object**) được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. **OU** cũng được thiết lập dựa trên **subnet IP** và được định nghĩa là "một hoặc nhiều **subnet** kết nối tốt với nhau". Việc sử dụng **OU** có hai công dụng chính sau:

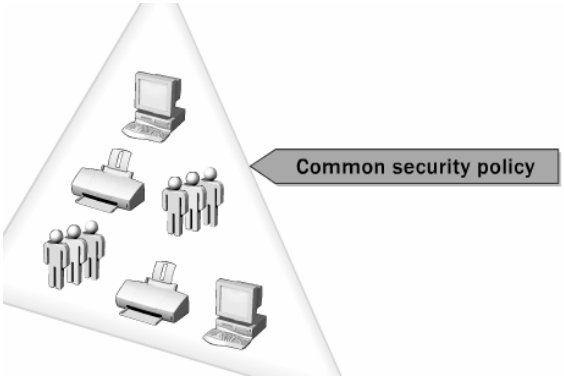
- Trao quyền kiểm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một phụ tá quản trị viên nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.
- Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong OU thông qua việc sử dụng các đối tượng chính sách nhóm (**GPO**), các chính sách nhóm này chúng ta sẽ tìm hiểu ở các chương sau.



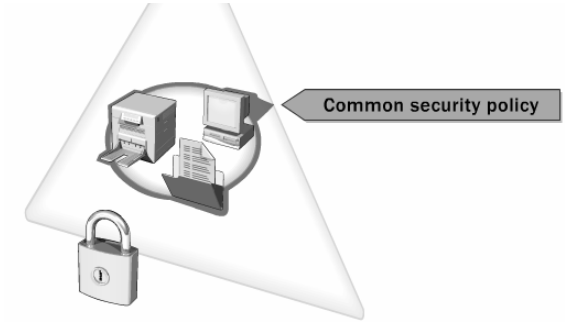
II.4.3 Domain.

Domain là đơn vị chức năng nòng cốt của cấu trúc **logic Active Directory**. Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các **Server** dễ dàng hơn. **Domain** đáp ứng ba chức năng chính sau:

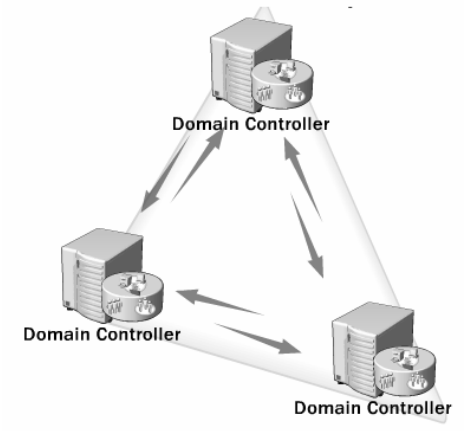
- Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối tượng, là một tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có chung một cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các **domain** khác.



- Giúp chúng ta quản lý bảo mật các các tài nguyên chia sẻ.

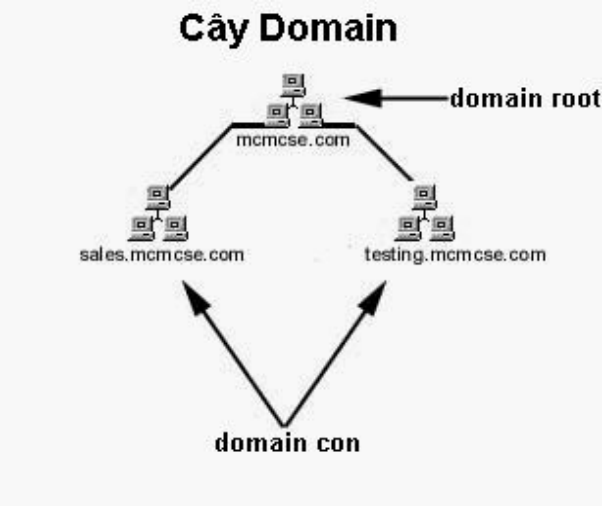


- Cung cấp các **Server** dự phòng làm chức năng điều khiển vùng (**domain controller**), đồng thời đảm bảo các thông tin trên các **Server** này được được đồng bộ với nhau.



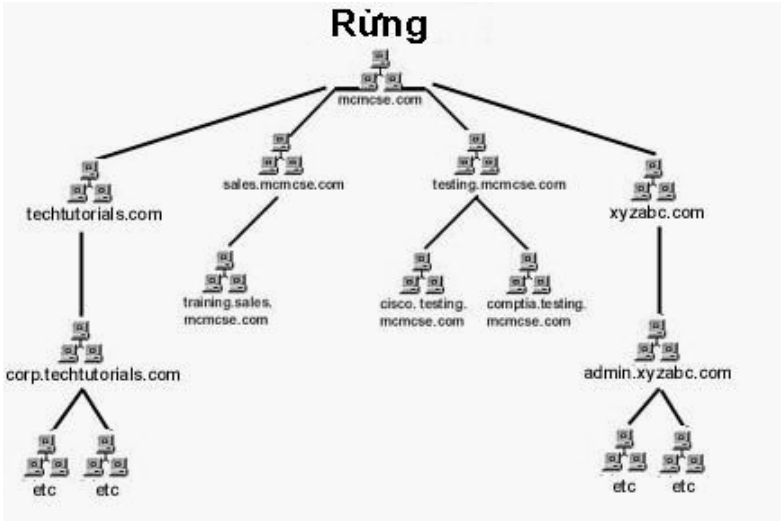
II.4.4 Domain Tree.

Domain Tree là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain** con (**child domain**). Tên của các **domain** con phải khác biệt nhau. Khi một **domain root** và ít nhất một **domain** con được tạo ra thì hình thành một cây **domain**. Khái niệm này bạn sẽ thường nghe thấy khi làm việc với một dịch vụ thư mục. Bạn có thể thấy cấu trúc sẽ có hình dáng của một cây khi có nhiều nhánh xuất hiện.



II.4.5 Forest.

Forest (rừng) được xây dựng trên một hoặc nhiều **Domain Tree**, nói cách khác **Forest** là tập hợp các **Domain Tree** có thiết lập quan hệ và ủy quyền cho nhau. Ví dụ giả sử một công ty nào đó, chẳng hạn như **Microsoft**, thu mua một công ty khác. Thông thường, mỗi công ty đều có một hệ thống **Domain Tree** riêng và để tiện quản lý, các cây này sẽ được hợp nhất với nhau bằng một khái niệm là rừng.



Trong ví dụ trên, công ty mcmcse.com thu mua được techtutorials.com và xyzabc.com và hình thành rừng từ gốc mcmcse.com.

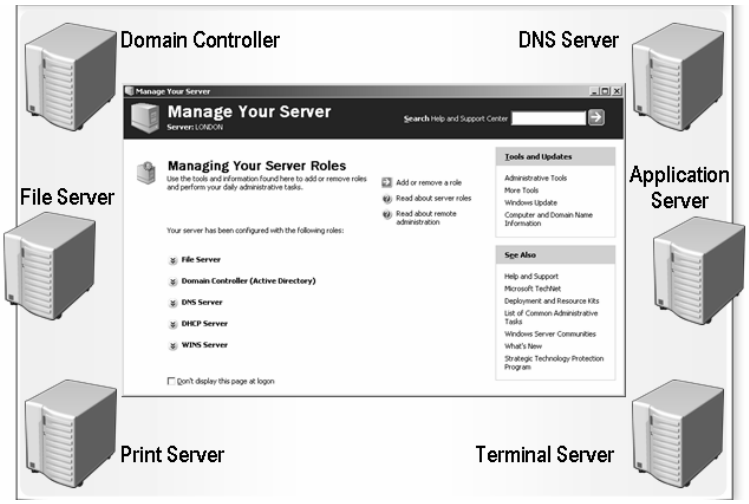
III. CÀI ĐẶT VÀ CẤU HÌNH ACTIVE DIRECTORY.

III.1. Nâng cấp Server thành Domain Controller.

III.1.1 Giới thiệu.

Một khái niệm không thay đổi từ **Windows NT 4.0** là **domain**. Một **domain** vẫn còn là trung tâm của mạng **Windows 2000** và **Windows 2003**, tuy nhiên lại được thiết lập khác đi. Các máy điều khiển vùng (**domain controller – DC**) không còn phân biệt là **PDC (Primary Domain Controller)** hoặc là **BDC (Backup Domain Controller)**. Bây giờ, đơn giản chỉ còn là **DC**. Theo mặc định, tất cả các máy **Windows Server 2003** khi mới cài đặt đều là **Server** độc lập (**standalone server**). Chương trình **DCPROMO** chính là **Active Directory Installation Wizard** và được dùng để nâng cấp một máy không phải là **DC** (**Server Stand-alone**) thành một máy **DC** và ngược lại giáng cấp một máy **DC** thành một **Server** bình thường. Chú ý đối với **Windows Server 2003** thì bạn có thể đổi tên máy tính khi đã nâng cấp thành **DC**.

Trước khi nâng cấp **Server** thành **Domain Controller**, bạn cần khai báo đầy đủ các thông số **TCP/IP**, đặc biệt là phải khai báo **DNS Server** có địa chỉ chính là địa chỉ IP của **Server** cần nâng cấp. Nếu bạn có khả năng cấu hình dịch vụ **DNS** thì bạn nên cài đặt dịch vụ này trước khi nâng cấp **Server**, còn ngược lại thì bạn chọn cài đặt **DNS** tự động trong quá trình nâng cấp. Có hai cách để bạn chạy chương trình **Active Directory Installation Wizard**: bạn dùng tiện ích **Manage Your Server** trong **Administrative Tools** hoặc nhấp chuột vào **Start** ◴ **Run**, gõ lệnh **DCPROMO**.

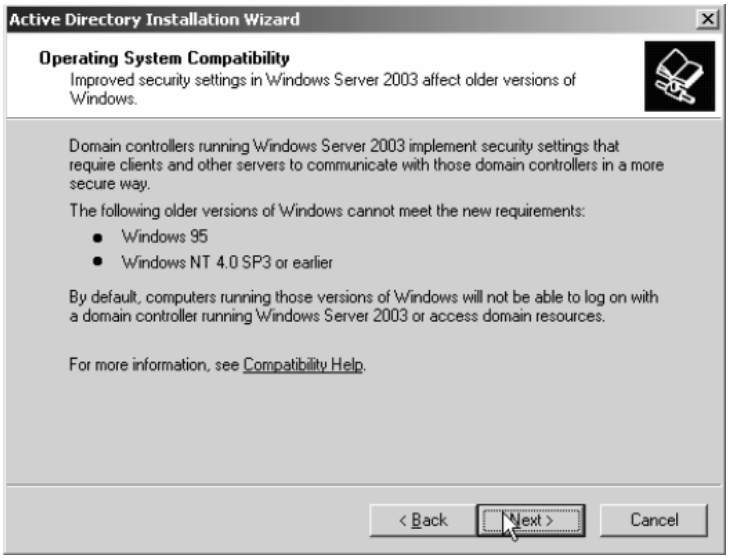


III.1.2 Các bước cài đặt.

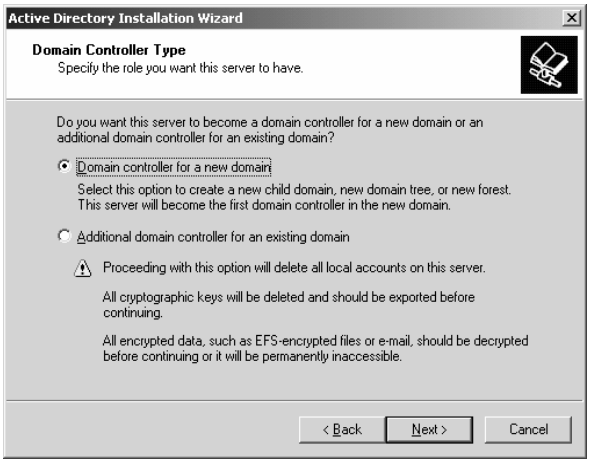
Chọn menu **Start** ◴ **Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**.

Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** để tiếp tục.

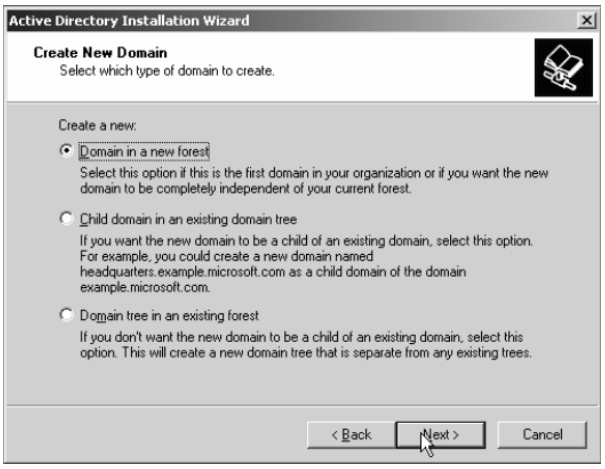
Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục.



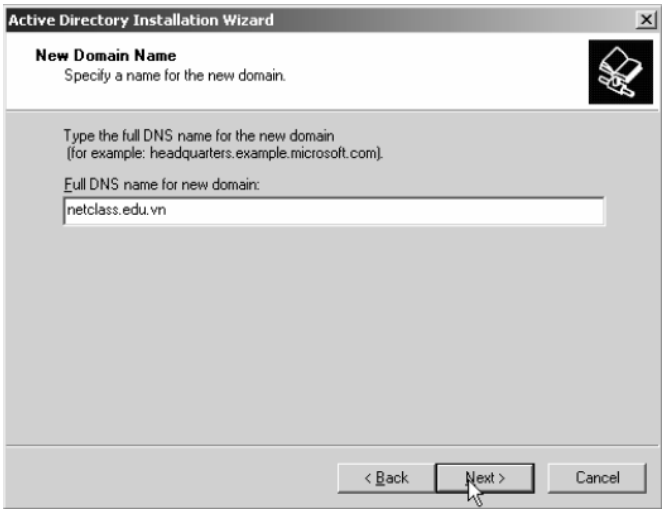
Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain cotroller for an existing domain**.)



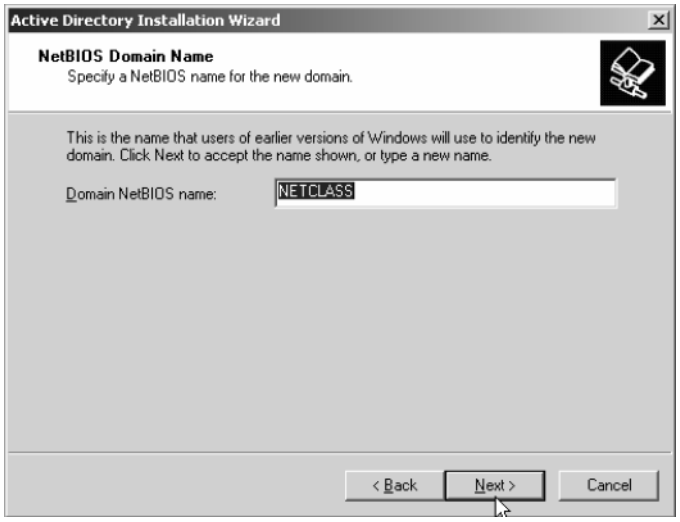
Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo **domain** đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một **domain** con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn.



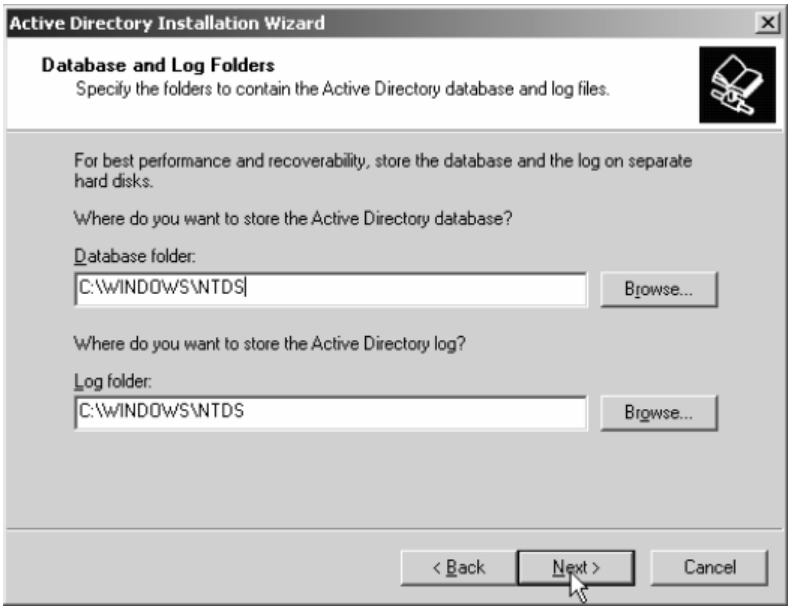
Hộp thoại **New Domain Name** yêu cầu bạn tên **DNS** đầy đủ của **domain** mà bạn cần xây dựng.



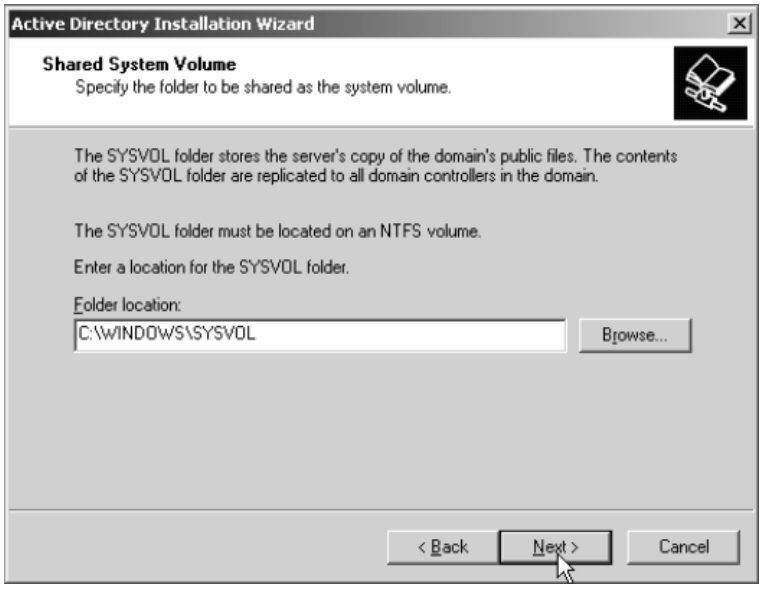
Hộp thoại **NetBIOS Domain Name**, yêu cầu bạn cho biết tên **domain** theo chuẩn **NetBIOS** để tương thích với các máy **Windows NT**. Theo mặc định, tên **Domain NetBIOS** giống phần đầu của tên **Full DNS**, bạn có thể đổi sang tên khác hoặc chấp nhận giá trị mặc định. Chọn **Next** để tiếp tục.



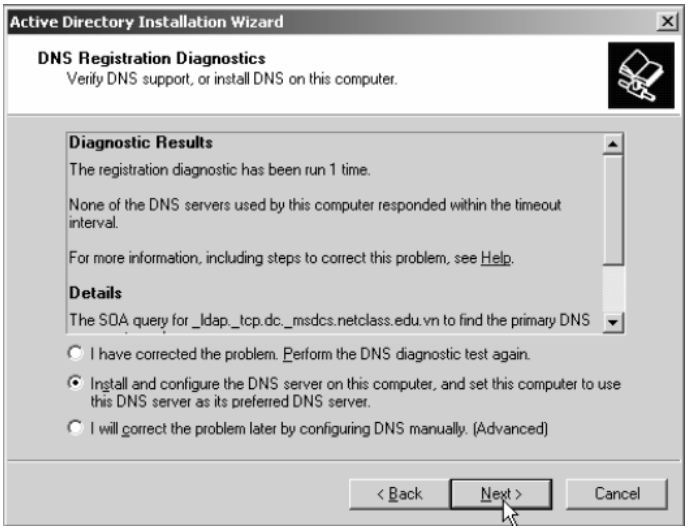
Hộp thoại **Database and Log Locations** cho phép bạn chỉ định vị trí lưu trữ **database Active Directory** và các tập tin **log**. Bạn có thể chỉ định vị trí khác hoặc chấp nhận giá trị mặc định. Tuy nhiên theo khuyến cáo của các nhà quản trị mạng thì chúng ta nên đặt tập tin chứa thông tin giao dịch (**transaction log**) ở một đĩa cứng vật lý khác với đĩa cứng chứa cơ sở dữ liệu của **Active Directory** nhằm tăng hiệu năng của hệ thống. Bạn chọn **Next** để tiếp tục.



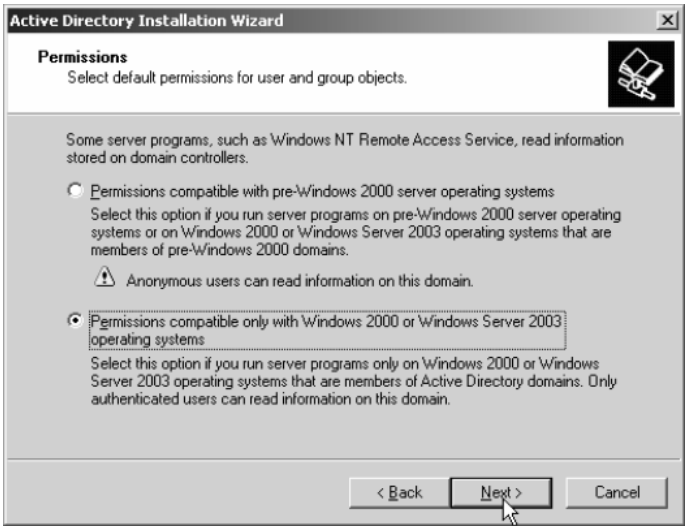
Hộp thoại **Shared System Volume** cho phép bạn chỉ định ví trí của thư mục **SYSVOL**. Thư mục này phải nằm trên một **NTFS5 Volume**. Tất cả dữ liệu đặt trong thư mục **Sysvol** này sẽ được tự động sao chép sang các **Domain Controller** khác trong miền. Bạn có thể chấp nhận giá trị mặc định hoặc chỉ định ví trí khác, sau đó chọn **Next** tiếp tục. (Nếu **partition** không sử dụng định dạng **NTFS5**, bạn sẽ thấy một thông báo lỗi yêu cầu phải đổi hệ thống tập tin).



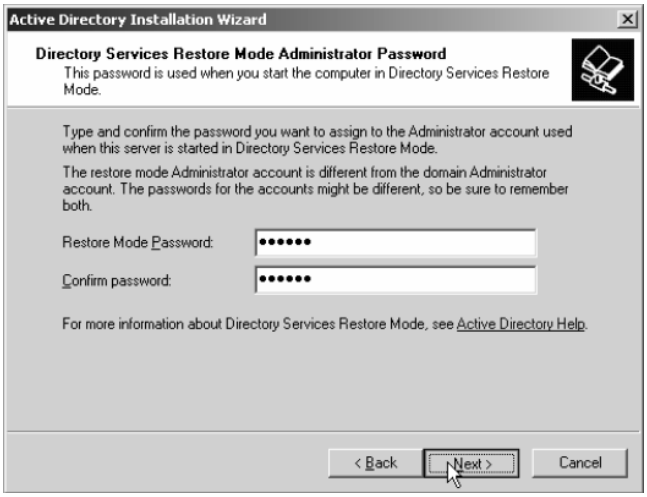
DNS là dịch vụ phân giải tên kết hợp với **Active Directory** để phân giải tên các máy tính trong miền. Do đó để hệ thống **Active Directory** hoạt động được thì trong miền phải có ít nhất một **DNS Server** phân giải miền mà chúng ta cần thiết lập. Theo đúng lý thuyết thì chúng ta phải cài đặt và cấu hình dịch vụ **DNS** hoàn chỉnh trước khi nâng cấp **Server**, nhưng do hiện tại các bạn chưa học về dịch vụ này nên chúng ta chấp nhận cho hệ thống tự động cài đặt dịch vụ này. Chúng ta sẽ tìm hiểu chi tiết dịch vụ **DNS** ở giáo trình "Dịch Vụ Mạng". Trong hộp thoại xuất hiện bạn chọn lựa chọn thứ hai để hệ thống tự động cài đặt và cấu hình dịch vụ **DNS**.



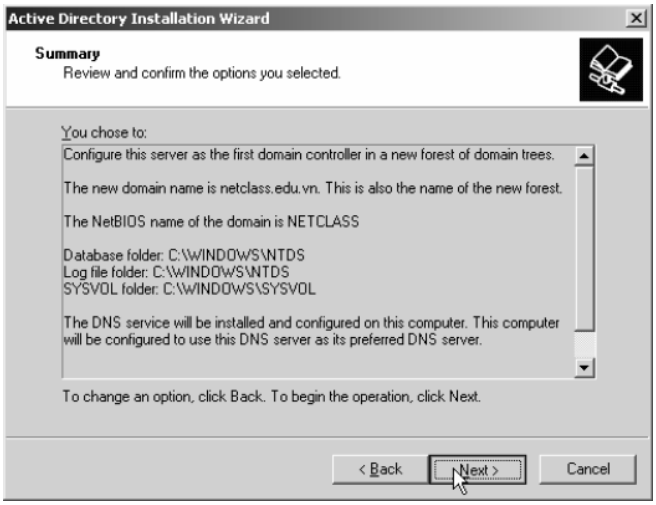
Trong hộp thoại **Permissions**, bạn chọn giá trị **Permission Compatible with pre-Windows 2000 servers** khi hệ thống có các **Server** phiên bản trước **Windows 2000**, hoặc chọn **Permissions compatible only with Windows 2000 servers** or **Windows Server 2003** khi hệ thống của bạn chỉ toàn các **Server Windows 2000** và **Windows Server 2003**.



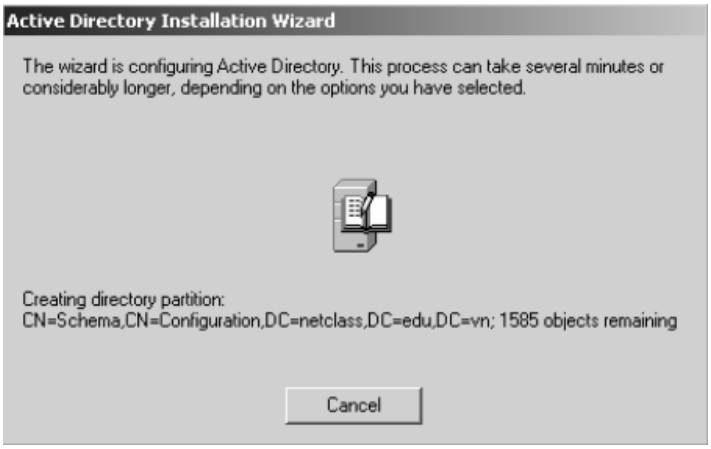
Trong hộp thoại **Directory Services Restore Mode Administrator Password**, bạn sẽ chỉ định mật khẩu dùng trong trường hợp **Server** phải khởi động vào chế độ **Directory Services Restore Mode**. Nhấn chọn **Next** để tiếp tục.



Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.



Hộp thoại **Configuring Active Directory** cho bạn biết quá trình cài đặt đang thực hiện những gì. Quá trình này sẽ chiếm nhiều thời gian. Chương trình cài đặt cũng yêu cầu bạn cung cấp nguồn cài đặt **Windows Server 2003** để tiến hành sao chép các tập tin nếu tìm không thấy.



Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.

Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình thăng cấp kết thúc.

III.2. Gia nhập máy trạm vào Domain.

III.2.1 Giới thiệu.

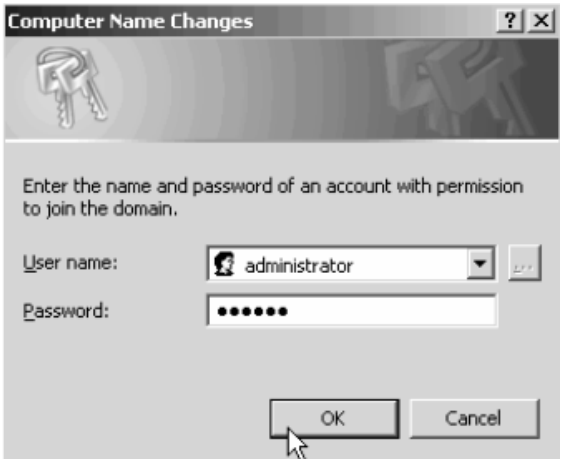
Một máy trạm gia nhập vào một **domain** thực sự là việc tạo ra một mối quan hệ tin cậy (**trust relationship**) giữa máy trạm đó với các máy **Domain Controller** trong vùng. Sau khi đã thiết lập quan hệ tin cậy thì việc chứng thực người dùng **logon** vào mạng trên máy trạm này sẽ do các máy điều khiển vùng đảm nhiệm. Nhưng chú ý việc gia nhập một máy trạm vào miền phải có sự đồng ý của người quản trị mạng cấp miền và quản trị viên cục bộ trên máy trạm đó. Nói cách khác khi bạn muốn gia nhập một máy trạm vào miền, bạn phải đăng nhập cục bộ vào máy trạm với vai trò là **administrator**, sau đó gia nhập vào miền, hệ thống sẽ yêu cầu bạn xác thực bằng một tài khoản người dùng cấp miền có quyền **Add Workstation to Domain** (bạn có thể dùng trực tiếp tài khoản **administrator** cấp miền).

III.2.2 Các bước cài đặt.

Đăng nhập cục bộ vào máy trạm với vai trò người quản trị (có thể dùng trực tiếp tài khoản **administrator**).

Nhấp phải chuột trên biểu tượng My Computer, chọn **Properties**, hộp thoại **System Properties** xuất hiện, trong **Tab Computer Name**, bạn nhấp chuột vào nút **Change**. Hộp thoại nhập liệu xuất hiện bạn nhập tên miền của mạng cần gia nhập vào mục **Member of Domain**.

Máy trạm dựa trên tên miền mà bạn đã khai báo để tìm đến **Domain Controller** gần nhất và xin gia nhập vào mạng, **Server** sẽ yêu cầu bạn xác thực với một tài khoản người dùng cấp miền có quyền quản trị.



Sau khi xác thực chính xác và hệ thống chấp nhận máy trạm này gia nhập vào miền thì hệ thống xuất hiện thông báo thành công và yêu cầu bạn **reboot** máy lại để đăng nhập vào mạng.

Đến đây, bạn thấy hộp thoại **Log on to Windows** mà bạn dùng mỗi ngày có vài điều khác, đó là xuất hiện thêm mục **Log on to**, và cho phép bạn chọn một trong hai phần là: **NETCLASS**, **This Computer**. Bạn chọn mục **NETCLASS** khi bạn muốn đăng nhập vào miền, nhớ rằng lúc này bạn phải dùng tài khoản người dùng cấp miền. Bạn chọn mục **This Computer** khi bạn muốn **logon** cục bộ vào máy trạm nào và nhớ dùng tài khoản cục bộ của máy.

III.3. Xây dựng các Domain Controller đồng hành.

III.3.1 Giới thiệu.

Domain Controller là máy tính điều khiển mọi hoạt động của mạng nếu máy này có sự cố thì toàn bộ hệ thống mạng bị tê liệt. Do tính năng quan trọng này nên trong một hệ thống mạng thông thường chúng ta phải xây dựng ít nhất hai máy tính **Domain Controller**. Như đã trình bày ở trên thì **Windows Server 2003** không còn phân biệt máy **Primary Domain Controller** và **Backup Domain Controller** nữa, mà nó xem hai máy này có vai trò ngang nhau, cùng nhau tham gia chứng thực người dùng. Như chúng ta đã biết, công việc chứng thực đăng nhập thường được thực hiện vào đầu giờ mỗi buổi làm việc, nếu mạng của bạn chỉ có một máy điều khiển dùng và 10.000 nhân viên thì chuyện gì sẽ xẩy ra vào mỗi buổi sáng? Để giải quyết trường hợp trên, **Microsoft** cho phép các máy điều khiển vùng trong mạng cùng nhau hoạt động đông thời, chia sẻ công việc của nhau, khi có một máy bị sự cố thì các máy còn lại đảm nhiệm luôn công việc máy này. Do đó trong tài liệu này chúng tôi gọi các máy này là các máy điều khiển vùng đồng hành. Nhưng khi khảo sát sâu về **Active Directory** thì máy điều khiển vùng được tạo đầu tiên vẫn có vai trò đặc biệt hơn đó là **FSMO (flexible single master of operations)**.

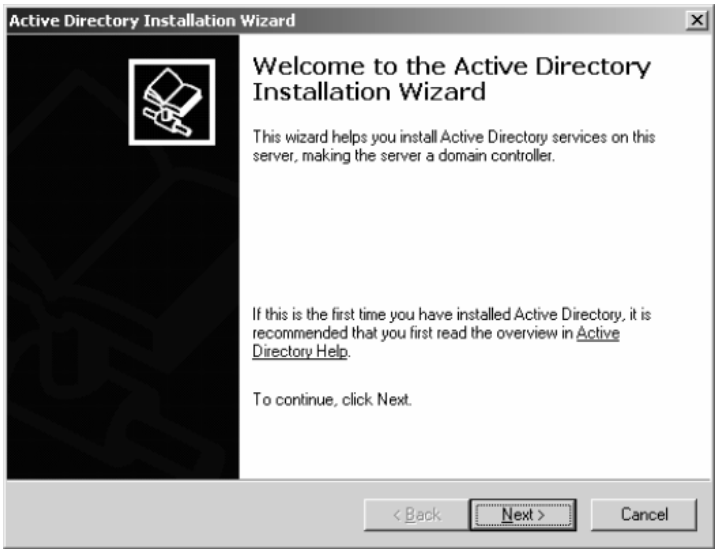
Chú ý để đảm bảo các máy điều khiển vùng này hoạt động chính xác thì chúng phải liên lạc và trao đổi thông tin với nhau khi có các thay đổi về thông tin người dùng như: tạo mới tài khoản, đổi mật khẩu, xóa tài khoản. Việc trao đổi thông tin này gọi là **Active Directory Replication**. Đặc biệt các server **Active Directory** cho phép nén dữ liệu trước khi gởi đến các server khác, tỉ lệ nén đến **10:1**, đo đó chúng có thể truyền trên các đường truyền **WAN** chậm chạp.

Trong hệ thống mạng máy tính của chúng ta nếu tất cả các máy điều khiển vùng đều là **Windows Server 2003** thì chúng ta nên chuyển miền trong mạng này sang cấp độ hoạt động **Windows Server 2003** (**Windows Server 2003 functional level**) để khai thác hết các tính năng mới của **Active Directory**.

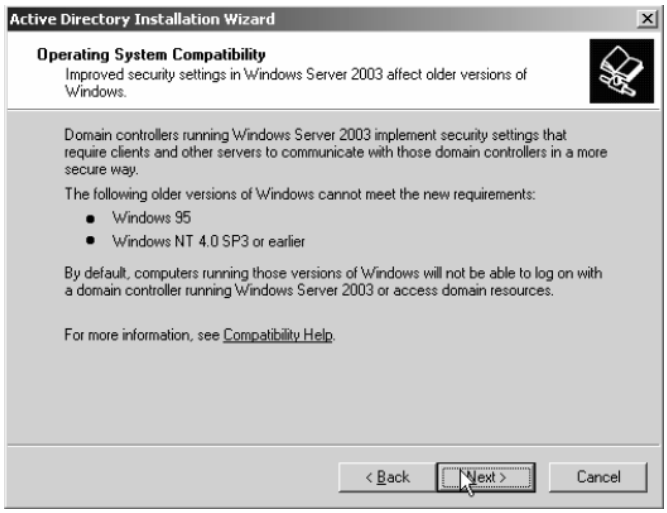
III.3.2 Các bước cài đặt.

Chọn menu **Start** 🕘 **Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**.

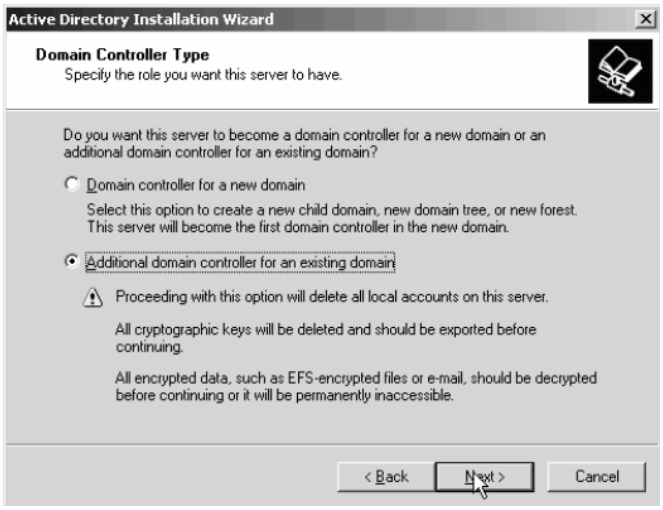
Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** để tiếp tục.



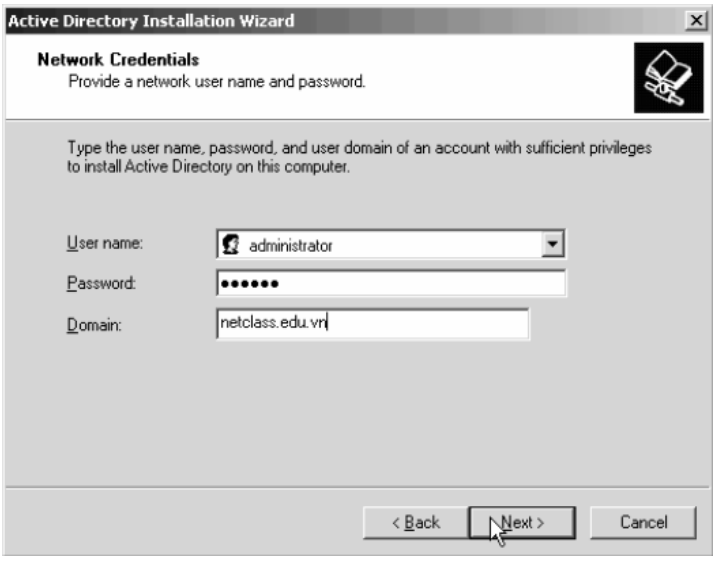
Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục.



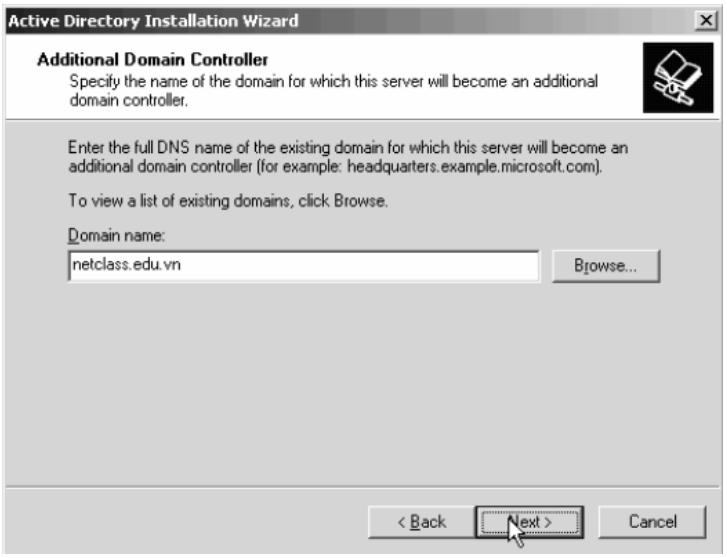
Trong hộp thoại **Domain Controller Type**, chọn mục **Additional domain cotroller for an existing domain** và nhấn chọn **Next**, vì chúng ta muốn bổ sung thêm máy điều khiển vùng vào một **domain** có sẵn.



Tiếp theo hệ thống yêu cầu bạn xác thực bạn phải người quản trị cấp miền thì mới có quyền tạo các **Domain Controller**. Bạn nhập tài khoản người dùng có quyền quản trị vào hộp thoại này.

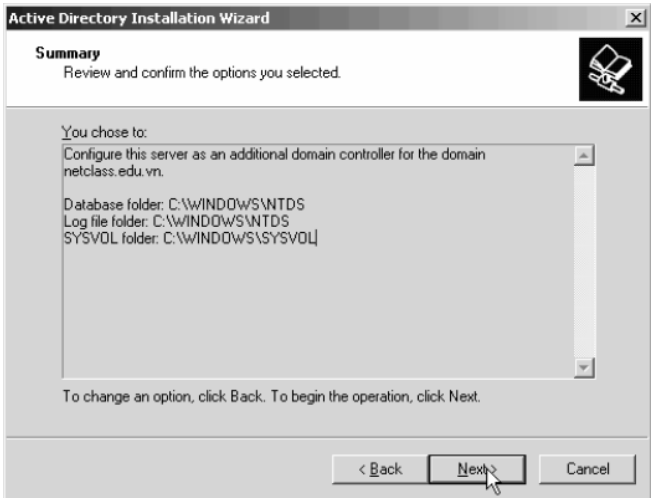


Chương trình yêu cầu bạn nhập **Full DNS Name** của miền mà bạn cần tạo thêm **Domain Controller**.



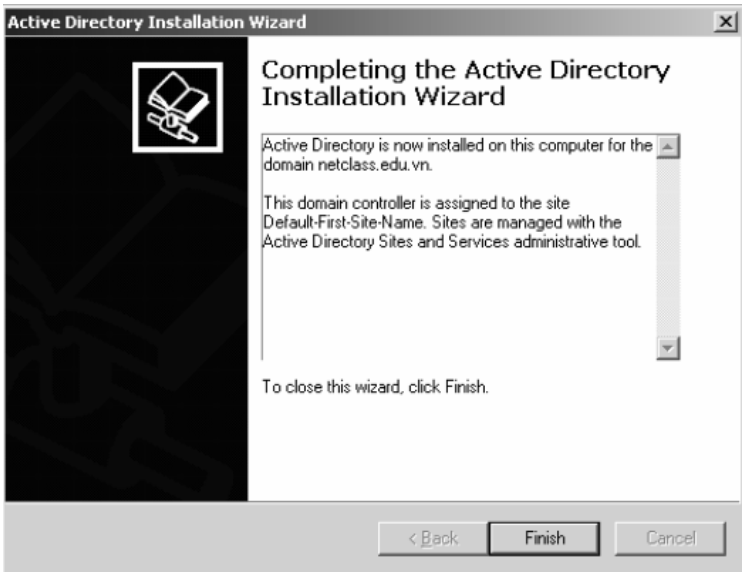
Tương tự như quá trình nâng cấp **Server** thành **Domain Controller** đã trình bày ở trên, các bước tiếp theo chúng ta chỉ định thư mục chứa cơ sở dữ liệu của **Active Directory**, **Transaction Log** và thư mục **Sysvol**.

Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.



Đến đây hệ thống sẽ xây dựng một **Domain Controller** mới và đồng bộ dữ liệu **Active Directory** giữa hai **Domain Controller** này.

Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.



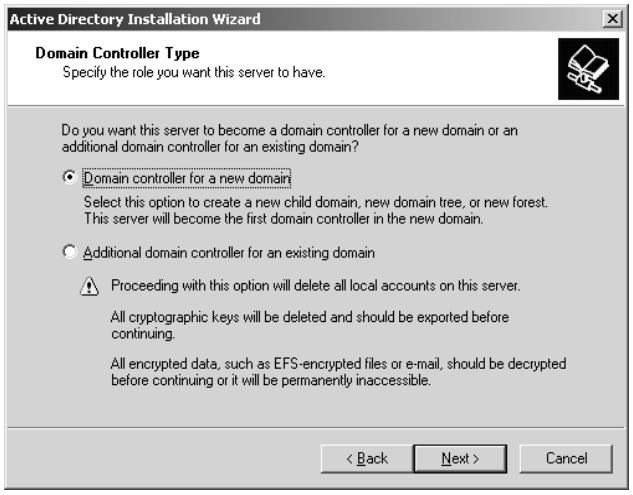
Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình xây dựng thêm một **Domain Controller** đồng hành đã hoàn tất.

III.4. Xây dựng Subdomain.

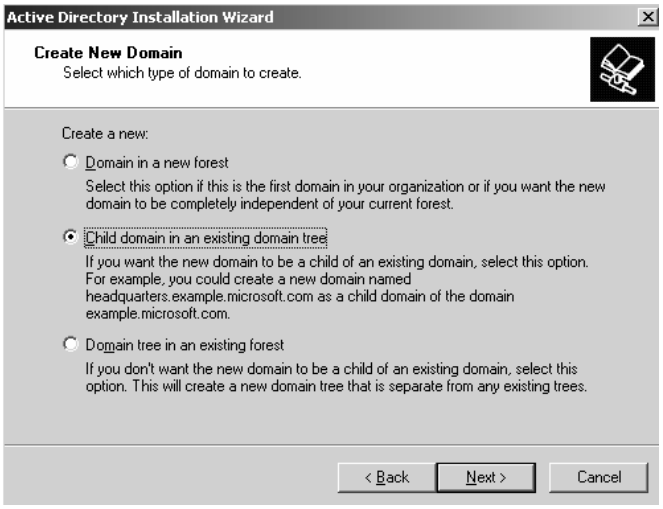
Sau khi bạn đã xây dựng **Domain Controller** đầu tiên quản lý miền, lúc ấy **Domain Controller** này là một gốc của rừng hoặc **Domain Tree** đầu tiên, từ đây bạn có thể tạo thêm các **subdomain** cho hệ thống. Để tạo thêm một **Domain Controller** cho một **subdomain** bạn làm các bước sau:

Tại **member server**, bạn cũng chạy chương trình **Active Directory Installation Wizard**, các bước đầu bạn cũng chọn tương tự như phần nâng cấp phía trên.

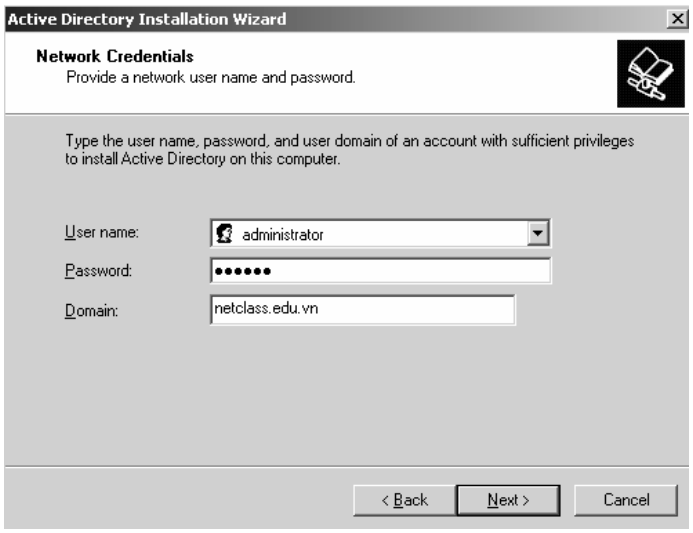
Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain cotroller for an existing domain**.)



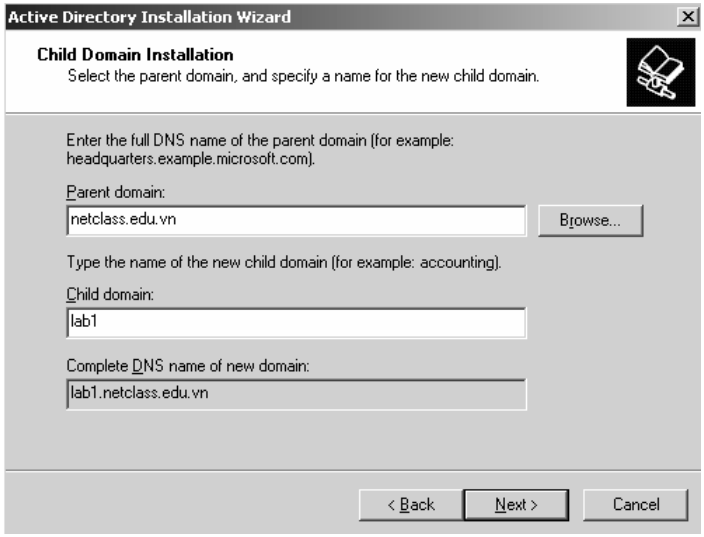
Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo domain đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một domain con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn. Trong trường hợp này bạn cần tạo một **Domain Controller** cho một **Child domain,** nên bạn đánh dấu vào mục lựa chọn thứ hai.



Để tạo một **child domain** trong một **domain tree** có sẵn, hệ thống yêu cầu bạn phải xác nhận bạn là người quản trị cấp **domain tree**. Trong hộp thoại này bạn nhập tài khoản và mật khẩu của người quản trị cấp rừng và tên của **domain tree** hiện tại.

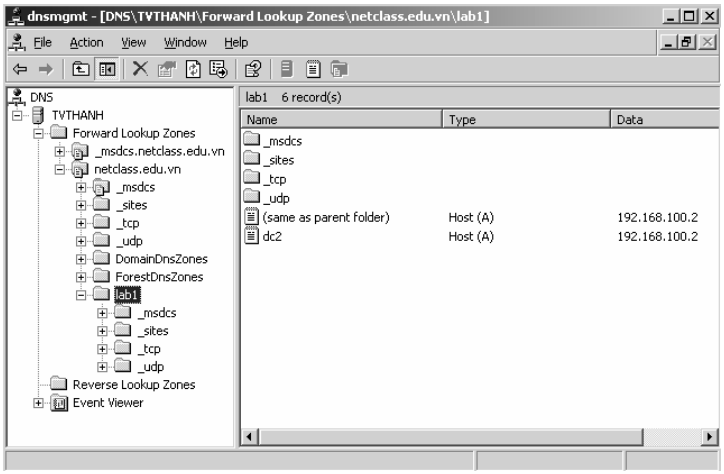


Tiếp theo bạn nhập tên của **domain tree** hiện đang có và tên của **child domain** cần tạo.



Các quá trình tiếp theo tương tự như quá trình tạo **Domain Controller** của phần trên.

Cuối cùng bạn có thể kiểm tra cây **DNS** của hệ thống trên **Server** quản lý gốc rừng có tạo thêm một **child domain** không, đồng thời bạn có thể cấu hình thêm chi dịch vụ **DNS** nhằm phục vụ tốt hơn cho hệ thống.

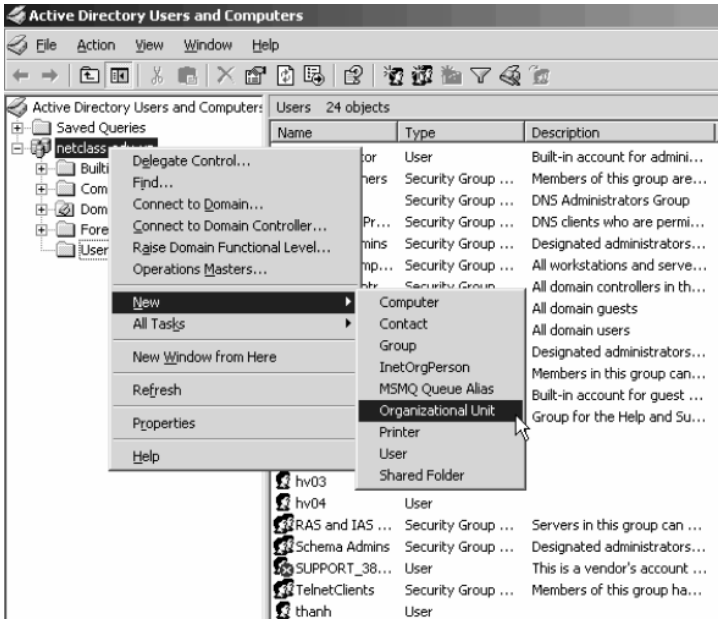


III.5. Xây dựng Organizational Unit.

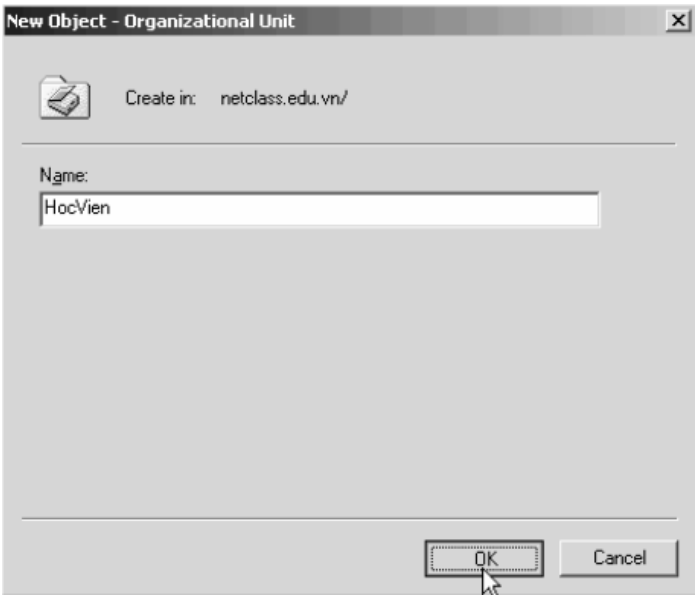
Như đã trình bày ở phần lý thuyết thì **OU** là một nhóm tài khoản người dùng, máy tính và tài nguyên mạng được tạo ra nhằm mục đích dễ dàng quản lý hơn và ủy quyền cho các quản trị viên địa phương giải quyết các công việc đơn giản. Đặc biệt hơn là thông qua **OU** chúng ta có thể áp đặt các giới hạn phần mềm và giới hạn phần cứng thông qua các **Group Policy**. Muốn xây dựng một **OU** bạn làm theo các bước sau:

Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ Active **Directory User and Computer**, để mở chương trình **Active Directory User and Computer**.

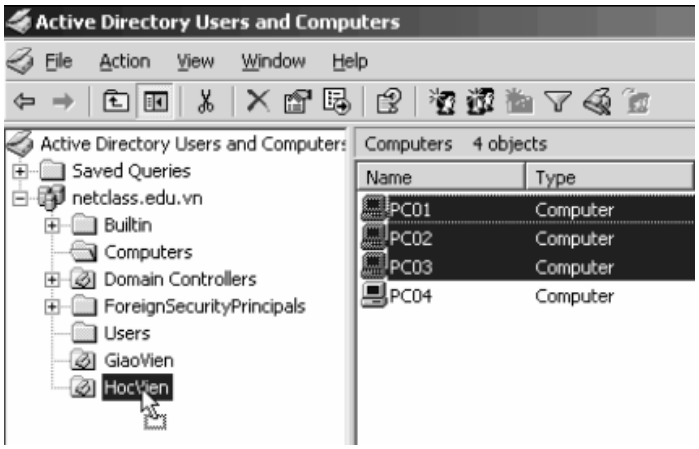
Chương trình mở ra, bạn nhấp phải chuột trên tên miền và chọn **New-Organizational Unit**.



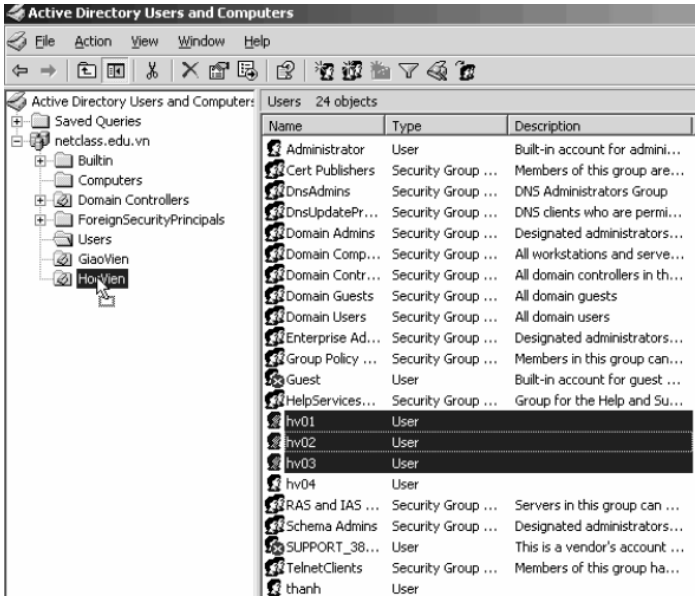
Hộp thoại xuất hiện, yêu cầu chúng ta nhập tên **OU** cần tạo, trong ví dụ này **OU** cần tạo có tên là **HocVien**.



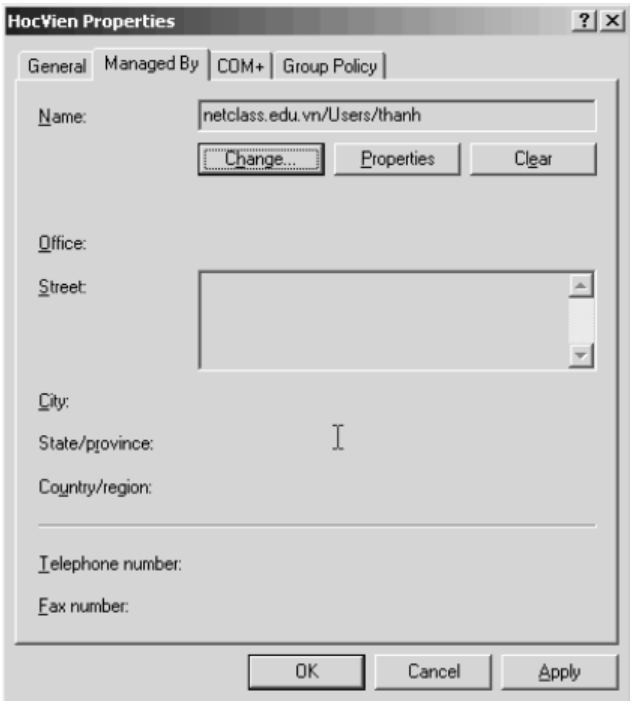
Đưa các máy trạm đã gia nhập nhập mạng cần quản lý vào **OU** vừa tạo.



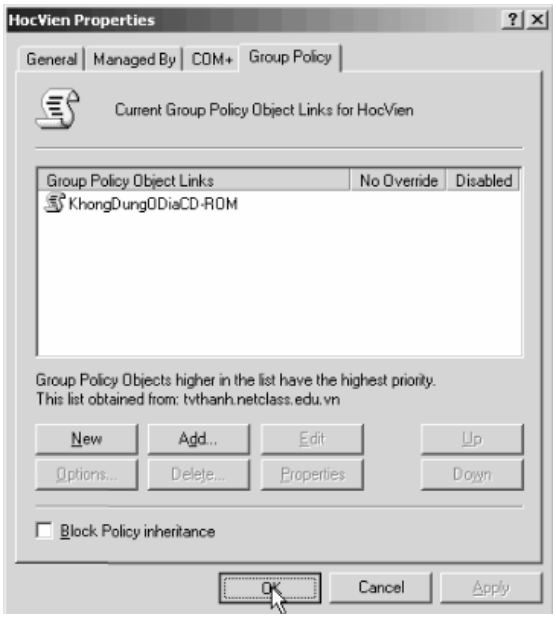
Tiếp theo bạn đưa các tài khoản người dùng cần quản lý vào **OU** vừa tạo.



Sau khi đã đưa các máy tính và tài khoản người dùng vào **OU**, bước tiếp theo là bạn chỉ ra người nào hoặc nhóm nào sẽ quản lý **OU** này. Bạn nhấp phải chuột vào **OU** vừa tạo, chọn **Properties**, hộp thoại xuất hiện, trong **Tab Managed By**, bạn nhấp chuột vào nút **Change** để chọn người dùng quản lý **OU** này, trong ví dụ này chúng ta chọn tài khoản Thanh quản lý **OU**.

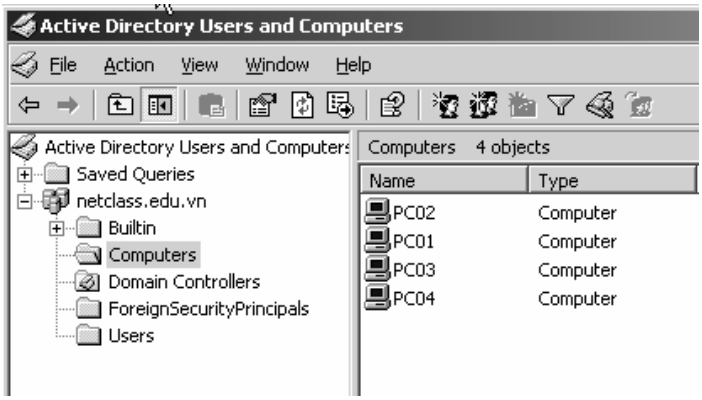


Bước cuối cùng này rất quan trọng, chúng ta sẽ tìm hiểu chi tiết ở chương **Group Policy**, đó là thiết lập các **Group Policy** áp dụng cho **OU** này. Bạn vào **Tab Group Policy**, nhấp chuột vào nút **New** để tạo mới một **GPO**, sau đó nhấp chuột vào nút **Edit** để hiệu chỉnh chính sách. Trong ví dụ này chúng ta tạo một chính sách cấm không cho phép dùng ổ đĩa **CD-ROM** áp dụng cho tất cả các người dùng trong **OU**.



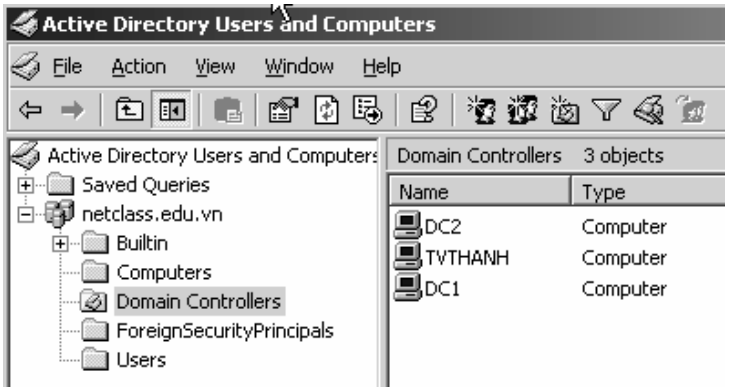
III.6. Công cụ quản trị các đối tượng trong Active Directory.

Một trong bốn công cụ quản trị hệ thống **Active Directory** thì công cụ **Active Directory User and Computer** là công cụ quan trọng nhất và chúng ta sẽ gặp lại nhiều trong trong giáo trình này, từng bước ta sẽ khảo sát hết các tính năng trong công cụ này. Công cụ này có chức năng tạo và quản lý các đối tượng cơ bản của hệ thống **Active Directory**.



Theo hình trên chúng ta thấy trong miền netclass.edu.vn có các mục sau:

- **Builtin**: chứa các nhóm người dùng đã được tạo và định nghĩa quyền sẵn.
- **Computers**: chứa các máy trạm mặc định đang là thành viên của miền. Bạn cũng có thể dùng tính năng này để kiểm tra một máy trạm gia nhập vào miền có thành công không.
- **Domain Controllers**: chứa các điều khiển vùng (**Domain Controller**) hiện đang hoạt động trong miền. Bạn cũng có thể dùng tính năng này để kiểm tra việc tạo thêm **Domain Controller** đồng hành có thành công không.
- **ForeignSecurityPrincipals**: là một vật chứa mặc định dành cho các đối tượng bên ngoài miền đang xem xét, từ các miền đã thiết lập quan hệ tin cậy (**trusted domain**).
- **Users**: chứa các tài khoản người dùng mặc định trên miền.



Tóm tắt

Lý thuyết 4 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về tài khoản người dùng, nhóm, các thuộc tính của tài khoản người dùng, các nhóm tạo sẵn …	I. Định nghĩa tài khoản người dùng và tài khoản nhóm. II. Chứng thực và kiểm soát truy cập. III. Các tài khoản tạo sẵn. IV. Quản lý tài khoản người dùng và nhóm cục bộ. V. Quản lý tài khoản người dùng và nhóm trên Active Directory.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

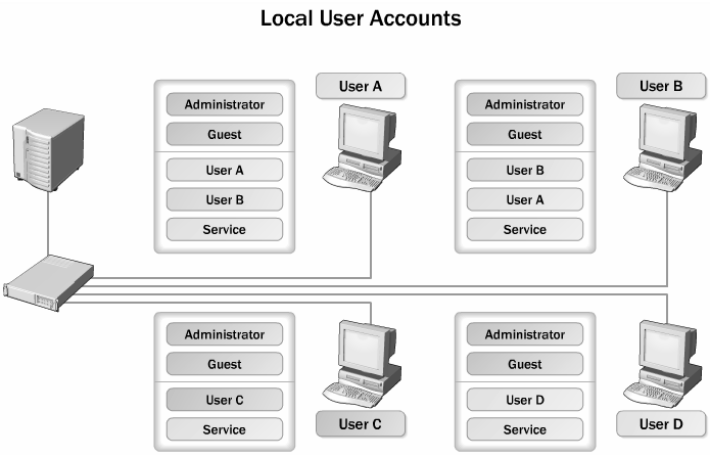
I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM.

I.1. Tài khoản người dùng.

Tài khoản người dùng (**user account**) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng **username**. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

I.1.1 Tài khoản người dùng cục bộ.

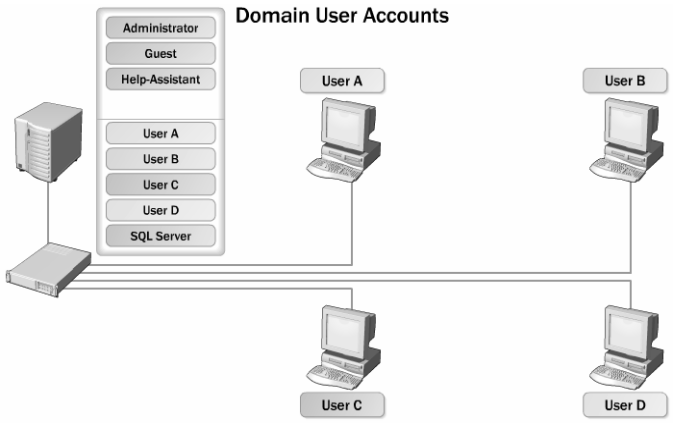
Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép **logon**, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy **domain controller** hoặc máy tính chứa tài nguyên chia sẻ. Bạn tạo tài khoản người dùng cục bộ với công cụ **Local Users and Group** trong **Computer Management (COMPMGMT.MSC)**. Các tài khoản cục bộ tạo ra trên máy **stand-alone server**, **member server** hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu **SAM** (**Security Accounts Manager**). Tập tin **SAM** này được đặt trong thư mục **\Windows\system32\config**.



Hình 3.1: lưu trữ thông tin tài khoản người dùng cục bộ

I.1.2 Tài khoản người dùng miền.

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



Hình 3.2: lưu trữ thông tin tài khoản người dùng miền.

I.1.3 Yêu cầu về tài khoản người dùng.

- Mỗi **username** phải từ 1 đến 20 ký tự (trên **Windows Server 2003** thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành **Windows NT 4.0** về trước thì mặc định chỉ hiểu 20 ký tự).
- Mỗi **username** là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.
- **Username** không chứa các ký tự sau: " / \ [ ] : ; | = , + * ? < >
- Trong một **username** có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

I.2. Tài khoản nhóm.

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**).

I.2.1 Nhóm bảo mật.

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (**rights**) và quyền truy cập (**permission**). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các **SID**. Có ba loại nhóm bảo mật chính là: **local**, **global** và **universal**. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: **local, domain local, global và universal**.

Local group (nhóm cục bộ) là loại nhóm có trên các **máy stand-alone Server, member server, Win2K Pro hay WinXP**. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.

Domain local group (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là **local group** nhưng nằm trên máy **Domain Controller**. Các máy **Domain Controller** có một cơ sở dữ liệu **Active Directory** chung và được sao chép đồng bộ với nhau do đó một **local group** trên một **Domain Controller** này thì cũng sẽ có mặt trên các **Domain Controller** anh em của nó, như vậy **local group** này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục **Built-in** của **Active Directory** là các **domain local**.

Global group (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong **Active Directory** và được tạo trên các **Domain Controller**. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm **global** có thể đặt vào trong một nhóm **local** của các server thành viên trong miền. Chú ý khi tạo nhiều nhóm **global** thì có thể làm tăng tải trọng công việc của **Global Catalog**.

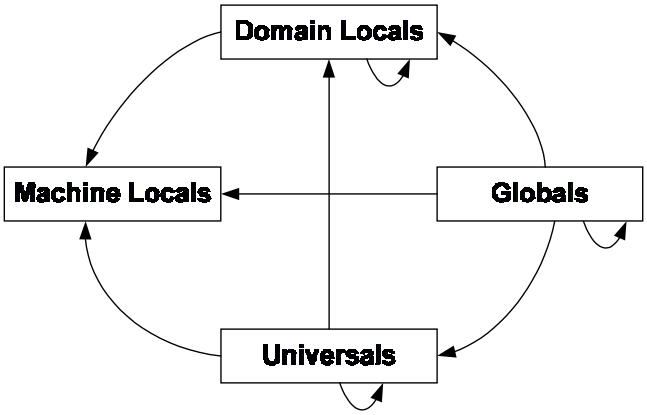
Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như **global group** nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm **global group** và **local group** vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của bạn phải hoạt động ở chế độ **Windows 2000 native functional level** hoặc **Windows Server 2003 functional level** có nghĩa là tất cả các máy **Domain Controller** trong mạng đều phải là **Windows Server 2003** hoặc **Windows 2000 Server**.

I.2.2 Nhóm phân phối.

Nhóm phân phối là một loại nhóm phi bảo mật, không có **SID** và không xuất hiện trong các **ACL (Access Control List)**. Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phố thư (**e-mail**) hoặc các tin nhắn (**message**). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm **MS Exchange**.

I.2.3 Qui tắc gia nhập nhóm.

- Tất cả các nhóm **Domain local**, **Global**, **Universal** đều có thể đặt vào trong nhóm **Machine Local**.
- Tất cả các nhóm **Domain local**, **Global**, **Universal** đều có thể đặt vào trong chính loại nhóm của mình.
- Nhóm **Global** và **Universal** có thể đặt vào trong nhóm **Domain local**.
- Nhóm **Global** có thể đặt vào trong nhóm **Universal**.



Hình 3.3: khả năng gia nhập của các loại nhóm.

II. CHỨNG THỰC VÀ KIỂM SOÁT TRUY CẬP.

II.1. Các giao thức chứng thực.

Chứng thực trong **Windows Server 2003** là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng. Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng. Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ. Với tài khoản miền, thông tin đăng nhập được chứng thực trên **Active Directory** và người dùng có quyền truy cập các tài nguyên trên mạng. Như vậy với tài khoản người dùng miền ta có thể chứng thực trên bất kỳ máy tính nào trong miền. **Windows 2003** hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là:

- **Kerberos V5**: là giao thức chuẩn **Internet** dùng để chứng thực người dùng và hệ thống.
- **NT LAN Manager** (**NTLM**): là giao thức chứng thực chính của **Windows NT**.
- **Secure Socket Layer/Transport Layer Security** (**SSL/TLS**): là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ **Web** an toàn.

II.2. Số nhận diện bảo mật SID.

Tuy hệ thống **Windows Server 2003** dựa vào tài khoản người dùng (**user account**) để mô tả các quyền hệ thống (**rights**) và quyền truy cập (**permission**) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật **SID (Security Identifier)**. **SID** là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này. **SID** bao gồm phần **SID** vùng cộng thêm với một **RID** của người dùng không trùng lặp. **SID** có dạng chuẩn "**S-1-5-21-D1-D2-D3-RID**", khi đó tất cả các **SID** trong miền đều có cùng giá trị **D1, D2, D3**, nhưng giá trị **RID** là khác nhau. Hai mục đích chính của việc hệ thống sử dụng **SID** là:

- Dễ dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.
- Khi xóa một tài khoản thì **SID** của tài khoản đó không còn giá trị nữa, nếu chúng ta có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi

tạo tài khoản mới thì giá trị **SID** của tài khoản này là một giá trị mới.

II.3. Kiểm soát hoạt động truy cập của đối tượng.

Active Directory là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật **ACE**. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng **Active Directory** trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập **ACE** (**Access Control Entry**). Một **ACL (Access Control List)** chứa nhiều **ACE**, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. **ACL** có đặc tính kế thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

III. CÁC TÀI KHOẢN TẠO SẴN.

III.1. Tài khoản người dùng tạo sẵn.

Tài khoản người dùng tạo sẵn (**Built-in**) là những tài khoản người dùng mà khi ta cài đặt **Windows Server 2003** thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằng trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

Tên tài khoản	Mô tả

Administrator	**Administrator** là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt **Windows Server 2003**. Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in…
Guest	Tài khoản **Guest** cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập **Internet** hoặc in ấn.
ILS_Anonymous_ User	Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt.
IUSR_computer-name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**.
IWAM_computer-name	Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**.
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**)
TSInternetUser	Là tài khoản đặc biệt được dùng cho **Terminal Services**.

III.2. Tài khoản nhóm Domain Local tạo sẵn.

Nhưng chúng ta đã thấy trong công cụ **Active Directory User** and **Computers**, **container Users** chứa nhóm **universal**, nhóm **domain** local và nhóm **global** là do hệ thống đã mặc định quy định trước. Nhưng một số nhóm **domain** local đặc biệt được đặt trong **container Built-in**, các nhóm này không được di chuyển sang các **OU** khác, đồng thời nó cũng được gán một số quyền cố định trước nhằm phục vụ cho công tác quản trị. Bạn cũng chú ý rằng là không có quyền xóa các nhóm đặc biệt này.

Tên nhóm	Mô tả

Administrators	Nhóm này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm **Domain Admins** và **Enterprise Admins** là thành viên mặc định của nhóm **Administrators**.
Account Operators	Thành viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong **container Built-in** và **OU**.
Domain Controllers	Nhóm này chỉ có trên các **Domain Controller** và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các **Domain Controller** nhưng không có quyền quản trị các chính sách bảo mật.
Backup Operators	Thành viên của nhóm này có quyền lưu trữ dự phòng (**Backup**) và phục hồi (**Retore**) hệ thống tập tin. Trong trường hợp hệ thống tập tin là **NTFS** và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ **Backup**. Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
Guests	Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vãng lai không phải là thành viên của mạng. Mặc định các tài khoản **Guest** bị khóa
Print Operator	Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Server Operators	Thành viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ…
Users	Mặc định mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế.
Replicator	Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong **Directory Services**, nhóm này không có thành viên mặc định.
Incoming Forest Trust Builders	Thành viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặc định.
Network Configuration Operators	Thành viên nhóm này có quyền sửa đổi các thông số **TCP/IP** trên các máy **Domain Controller** trong miền.

Pre-Windows 2000 Compatible Access	Nhóm này có quyền truy cập đến tất cả các tài khoản người dùng và tài khoản nhóm trong miền, nhằm hỗ trợ cho các hệ thống **WinNT** cũ.
Remote Desktop User	Thành viên nhóm này có thể đăng nhập từ xa vào các **Domain Controller** trong miền, nhóm này không có thành viên mặc định.
Performace Log Users	Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy **Domain Controller**, nhóm này cũng không có thành viên mặc định.
Performace Monitor Users	Thành viên nhóm này có khả năng giám sát từ xa các máy **Domain Controller**.

Ngoài ra còn một số nhóm khác như **DHCP Users, DHCP Administrators, DNS Administrators**… các nhóm này phục vụ chủ yếu cho các dịch vụ, chúng ta sẽ tìm hiểu cụ thể trong từng dịch vụ ở giáo trình "Dịch Vụ Mạng". Chú ý theo mặc định hai nhóm **Domain Computers** và **Domain Controllers** được dành riêng cho tài khoản máy tính, nhưng bạn vẫn có thể đưa tài khoản người dùng vào hai nhóm này.

III.3. Tài khoản nhóm Global tạo sẵn.

Tên nhóm	Mô tả
Domain Admins	Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các **member server** và các máy trạm (**Win2K Pro, WinXP**) đã đưa nhóm **Domain Admins** là thành viên của nhóm cục bộ **Administrators** trên các máy này.
Domain Users	Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ **Users** trên các máy **server** thành viên và máy trạm.
Group Policy Creator Owners	Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản **administrator** miền là thành viên của nhóm này.
Enterprise Admins	Đây là một nhóm **universal**, thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm **administrators** trên các **Domain Controller** trong rừng.
Schema Admins	Nhóm **universal** này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (**schema**) của **Active Directory**.

III.4. Các nhóm tạo sẵn đặc biệt.

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server 2003** còn có một số nhóm tạo sẵn đặt biệt, chúng không xuất hiện trên cửa sổ của công cụ **Active Directory User** and **Computer**, mà chúng chỉ xuất hiện trên các **ACL** của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

- **Interactive**: đại diện cho những người dùng đang sử dụng máy tại chỗ.
- **Network**: đại diện cho tất cả những người dùng đang nối kết mạng đến một máy tính khác.
- **Everyone**: đại diện cho tất cả mọi người dùng.
- **System**: đại diện cho hệ điều hành.
- **Creator owner**: đại diện cho những người tạo ra, những người sở hữa một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (**print job**)…
- **Authenticated users**: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm **everyone**.
- **Anonymous logon**: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ **FTP**.
- **Service**: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.
- **Dialup**: đại diện cho những người đang truy cập hệ thống thông qua **Dial-up Networking**.

IV. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM CỤC BỘ.

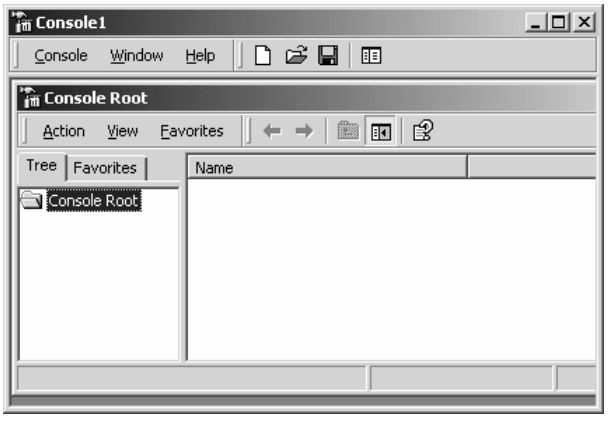
IV.1. Công cụ quản lý tài khoản người dùng cục bộ.

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai phương thức truy cập đến công cụ **Local Users and Groups**:

- Dùng như một **MMC** (**Microsoft Management Console**) snap-in.
- Dùng thông qua công cụ **Computer Management.**

Các bước dùng để chèn **Local Users and Groups snap-in** vào trong **MMC**:

Chọn **Start** ⏲ **Run**, nhập vào hộp thoại **MMC** và ấn phím **Enter** để mở cửa sổ **MMC**.



Chọn **Console** ⏲ **Add/Remove Snap-in** để mở hộp thoại **Add/Remove Snap-in**.

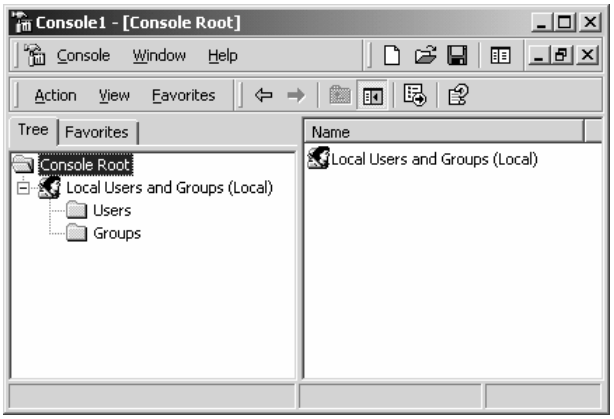
Nhấp chuột vào nút **Add** để mở hộp thoại **Add Standalone Snap-in**.

Chọn **Local Users and Groups** và nhấp chuột vào nút **Add**.

Hộp thoại **Choose Target Machine** xuất hiện, ta chọn **Local Computer** và nhấp chuột vào nút **Finish** để trở lại hộp thoại **Add Standalone Snap-in**.

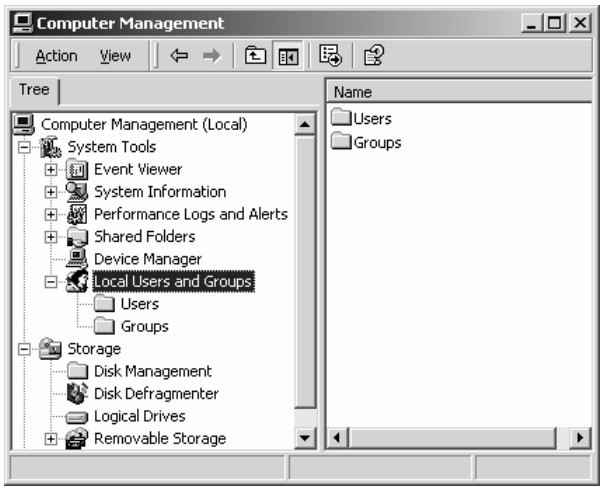
Nhấp chuột vào nút **Close** để trở lại hộp thoại **Add/Remove Snap-in**.

Nhấp chuột vào nút **OK**, ta sẽ nhìn thấy **Local Users and Groups snap-in** đã chèn vào **MMC** như hình sau.



Lưu **Console** bằng cách chọn **Console** 🕘 **Save**, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu **console** ngay trên **Desktop**.

Nếu máy tính của bạn không có cấu hình **MMC** thì cách nhanh nhất để truy cập công cụ **Local Users and Groups** thông qua công cụ **Computer Management**. Nhấp phải chuột vào **My Computer** và chọn **Manage** từ **pop-up menu** và mở cửa sổ **Computer Management**. Trong mục **System Tools**, ta sẽ nhìn thấy mục **Local Users and Groups**

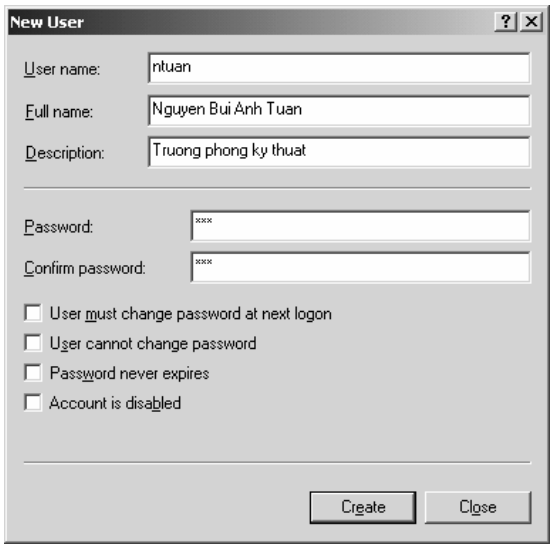


Cách khác để truy cập đến công cụ **Local Users and Groups** là vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Computer Management**.

IV.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ.

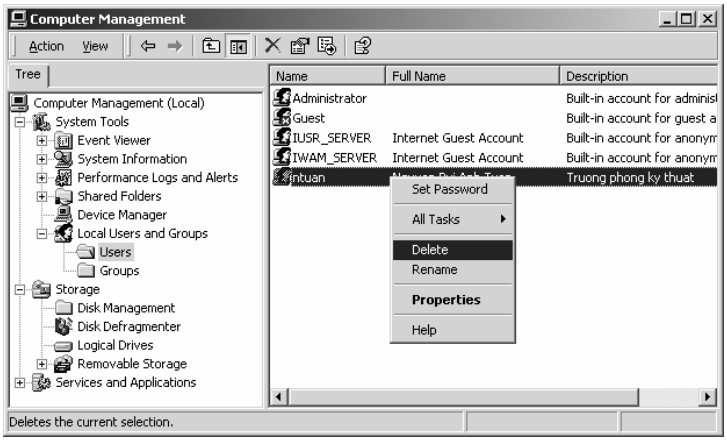
IV.2.1 Tạo tài khoản mới.

Trong công cụ **Local Users and Groups**, ta nhấp phải chuột vào **Users** và chọn **New User**, hộp thoại **New User** hiển thị bạn nhập các thông tin cần thiết vào, nhưng quan trọng nhất và bắt buộc phải có là mục **Username**.

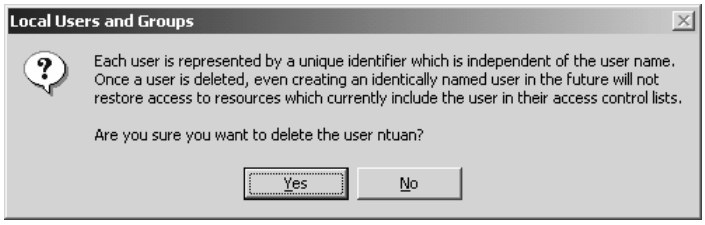


IV.2.2 Xóa tài khoản.

Bạn nên xóa tài khoản người dùng, nếu bạn chắc rằng tài khoản này không bao giờ cần dùng lại nữa. Muốn xóa tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần xóa, nhấp phải chuột và chọn **Delete** hoặc vào thực đơn **Action** ⏲ **Delete**.

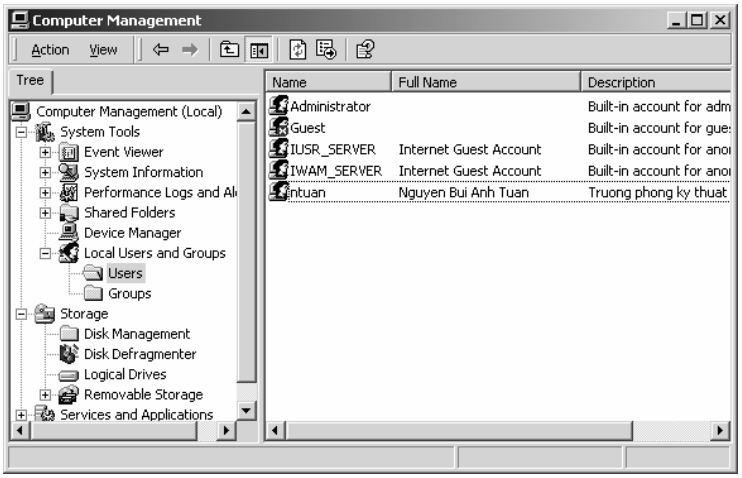


Chú ý: khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

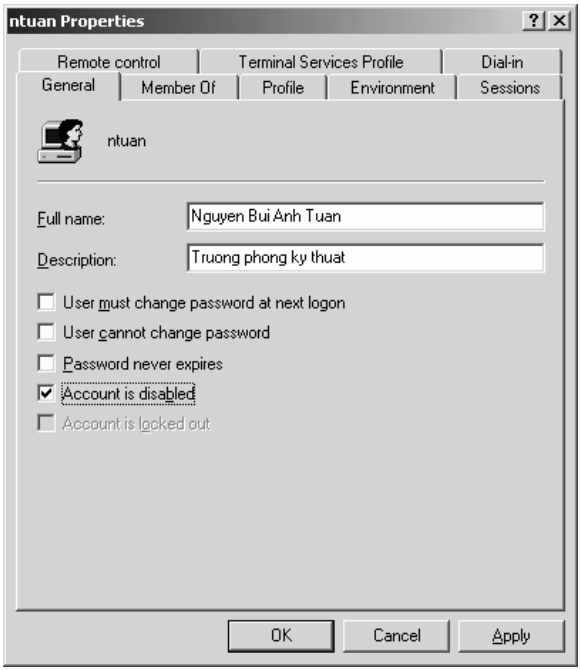


IV.2.3 Khóa tài khoản.

Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu bạn xóa tài khoản này đi thì không thể phục hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.



Trong **Tab General**, đánh dấu vào mục **Account is disabled**.



IV.2.4 Đổi tên tài khoản.

Bạn có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời bạn cũng có thể điều chỉnh các thông tin của tài khoản người dùng thông qua chức năng này. Chức năng này có ưu điểm là khi bạn thay đổi tên người dùng nhưng **SID** của tài khoản vẫn không thay đổi. Muốn thay đổi tên tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.

IV.2.5 Thay đổi mật khẩu.

Muốn đổi mật mã của người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn **Reset password**.

V. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM TRÊN ACTIVE DIRECTORY.

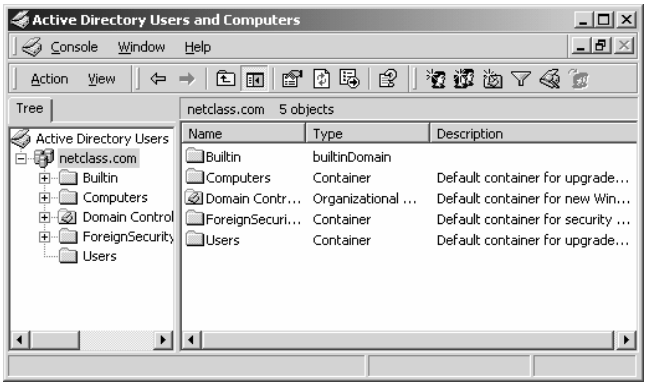
V.1. Tạo mới tài khoản người dùng.

Bạn có thể dùng công cụ **Active Directory User and Computers** trong **Administrative Tools** ngay trên máy **Domain Controller** để tạo các tài khoản người dùng miền. Công cụ này cho phép bạn quản lý tài khoản người dùng từ xa thậm chí trên các máy trạm không phải dùng hệ điều hành **Server** như **WinXP, Win2K Pro**. Muốn thế trên các máy trạm này phải cài thêm bộ công cụ **Admin Pack**. Bộ công cụ này nằm trên **Server** trong thư mục **\Windows\system32\ADMINPAK.MSI**. Tạo một tài khoản người dùng trên **Active Directory**, ta làm các bước sau:

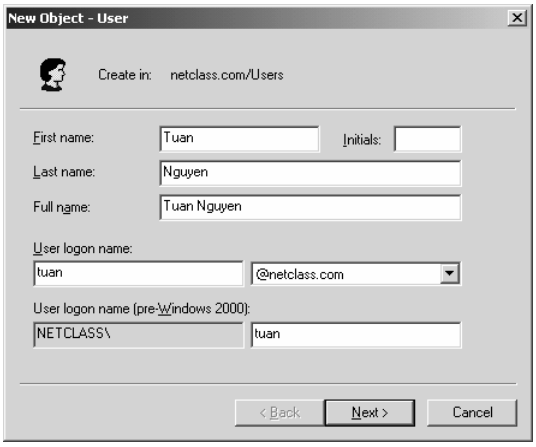
Chọn **Start** ◴ **Programs** ◴ **Administrative Tools** ◴ **Active Directory Users and Computers**.

Cửa sổ **Active Directory Users and Computers** xuất hiện, bạn nhấp phải chuột vào mục **Users**, chọn

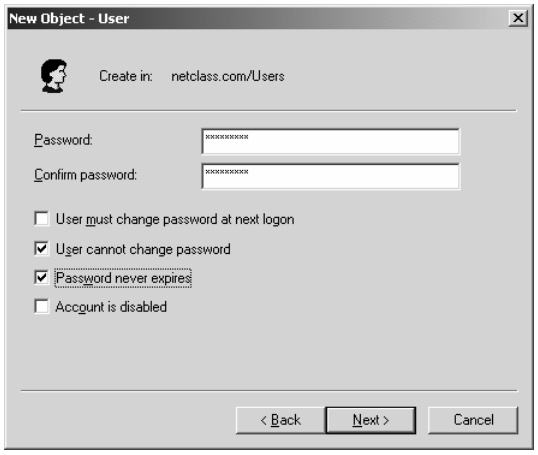
New ⏲ **User**.



Hộp thoại **New Object-User** xuất hiện như hình sau, bạn nhập tên mô tả người dùng, tên tài khoản logon vào mạng. Giá trị **Full Name** sẽ tự động phát sinh khi bạn nhập giá trị **First Name** và **Last Name**, nhưng bạn vẫn có thể thay đổi được. Chú ý: giá trị quan trọng nhất và bắt buộc phải có là **logon name** (**username**). Chuỗi này là duy nhất cho một tài khoản người dùng theo như định nghĩa trên phần lý thuyết. Trong môi trường **Windows 2000** và **2003**, Microsoft đưa thêm một khái niệm hậu tố **UPN** (**Universal Principal Name**), trong ví dụ này là **"@netclass.edu.vn"**. Hậu tố **UPN** này gắn vào sau chuỗi **username** dùng để tạo thành một tên **username** đầy đủ dùng để chứng thực ở cấp rừng hoặc chứng thực ở một miền khác có quan hệ tin cậy với miền của người dùng đó, trong ví dụ này thì tên **username** đầy đủ là "**tuan@netclass.edu.vn**". Ngoài ra trong hộp thoại này cũng cho phép chúng ta đặt tên **username** của tài khoản người dùng phục vụ cho hệ thống cũ (**pre-Windows 2000**). Sau khi việc nhập các thông tin hoàn thành bạn nhấp chuột vào nút **Next** để tiếp tục.



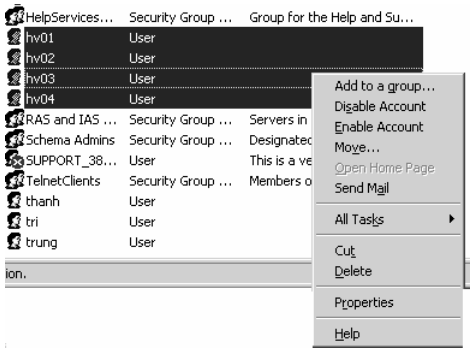
Hộp thoại thứ hai xuất hiện, cho phép bạn nhập vào mật khẩu (**password**) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản. Các lựa chọn này chúng ta sẽ tìm hiểu chi tiết ở phần tiếp theo.



Hộp thoại cuối cùng xuất hiện và nó hiển thị các thông tin đã cấu hình cho người dùng. Nếu tất cả các thông tin đã chính xác thì bạn nhấp chuột vào nút **Finish** để hoàn thành, còn nếu cần chỉnh sửa lại thì nhấp chuột vào nút **Back** để trở về các hộp thoại trước.

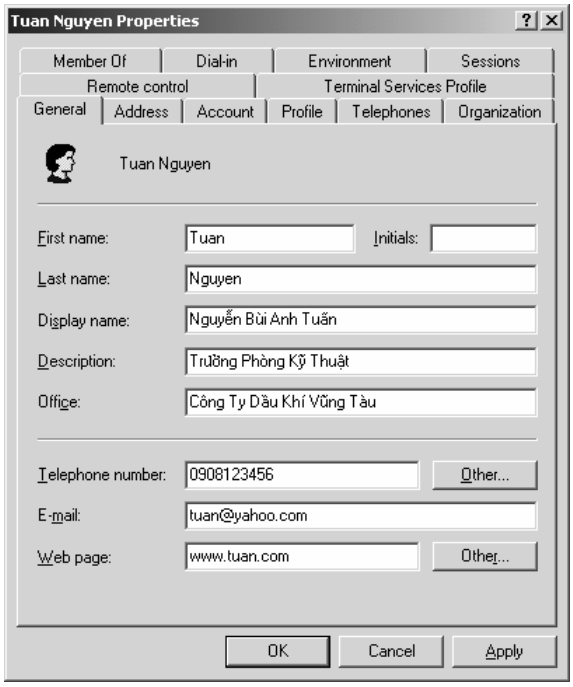
V.2. Các thuộc tính của tài khoản người dùng

Muốn quản lý các thuộc tính của các tài khoản người ta dùng công cụ **Active Directory Users and Computers** (bằng cách chọn **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Active Directory Users and Computers**), sau đó chọn thư mục **Users** và nhấp đôi chuột vào tài khoản người dùng cần khảo sát. Hộp thoại **Properties** xuất hiện, trong hộp thoại này chứa 12 **Tab** chính, ta sẽ lần lượt khảo sát các **Tab** này. Ngoài ra bạn có thể gom nhóm (dùng hai phím **Shift, Ctrl**) và hiệu chỉnh thông tin của nhiều tài khoản người dùng cùng một lúc.

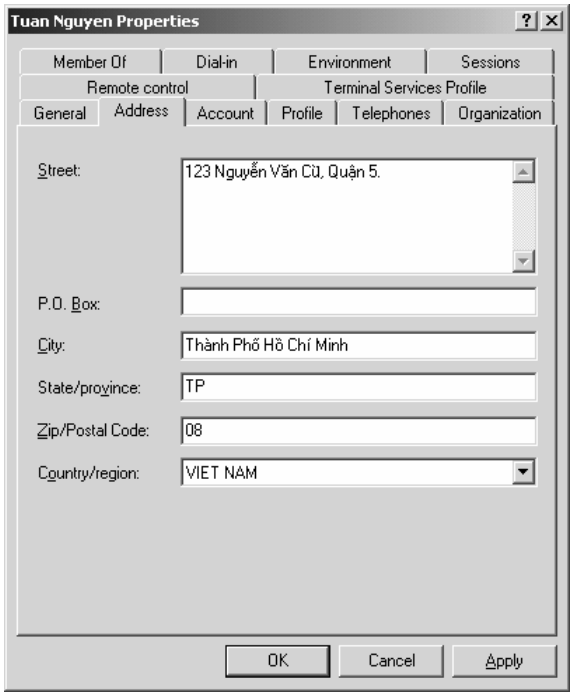


V.2.1 Các thông tin mở rộng của người dùng

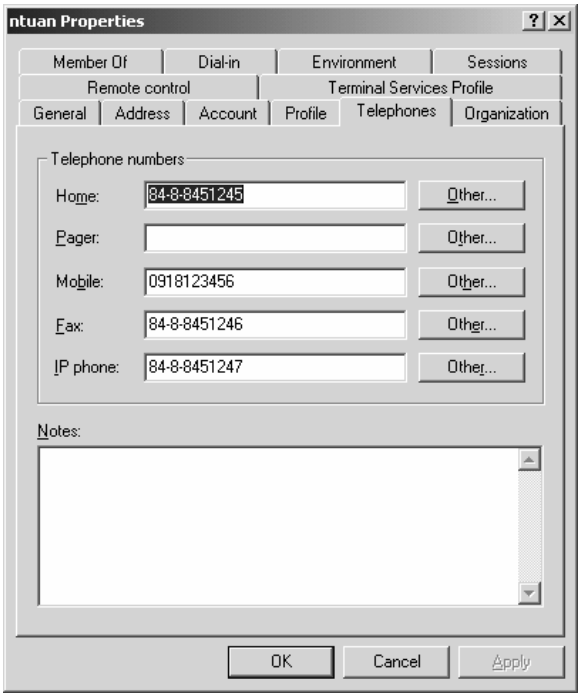
Tab **General** chứa các thông tin chung của người dùng trên mạng mà bạn đã nhập trong lúc tạo người dùng mới. Đồng thời bạn có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và trang địa chỉ trang Web cá nhân…



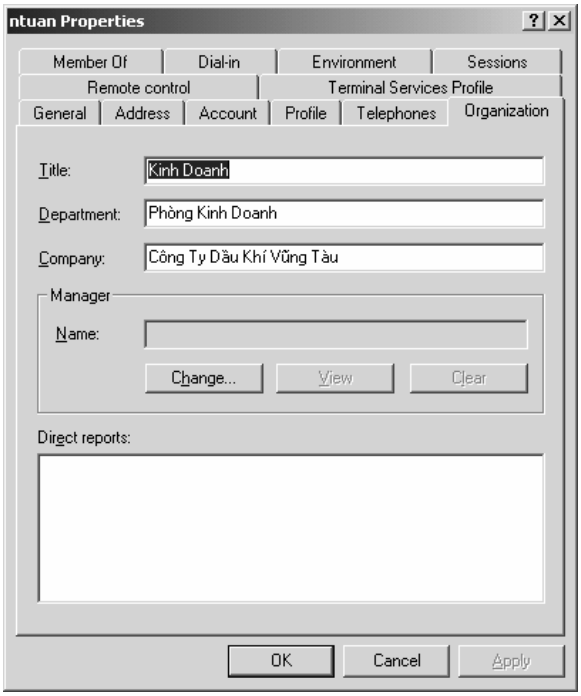
Tab **Address** cho phép bạn có thể khai báo chi tiết các thông tin liên quan đến địa chỉ của tài khoản người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia…



Tab **Telephones** cho phép bạn khai báo chi tiết các số điện thoại của tài khoản người dùng.

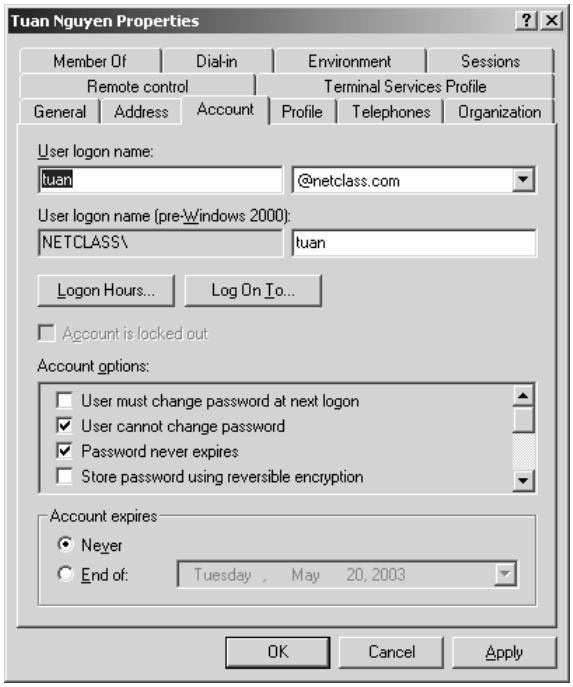


Tab **Organization** cho phép bạn khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban trực thuộc, tên công ty …

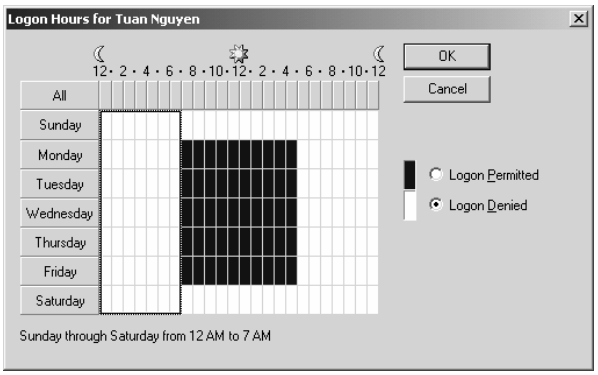


V.2.2 Tab Account.

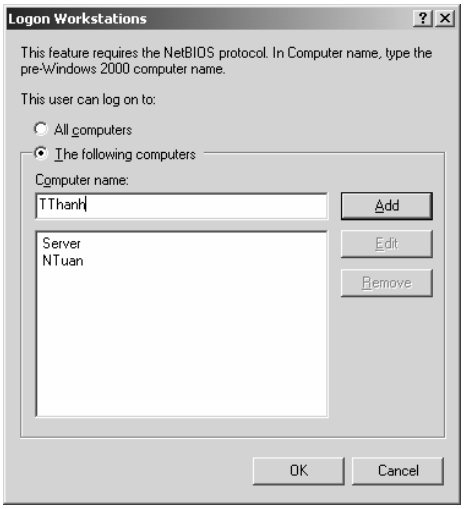
Tab **Account** cho phép bạn khai báo lại **username**, quy định giờ **logon** vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết hạn của tài khoản…



Điều khiển giờ **logon** vào mạng: bạn nhấp chuột vào nút **Logon Hours**, hộp thoại **Logon Hours** xuất hiện. Mặc định tất cả mọi người dùng đều được phép truy cập vào mạng 24 giờ mỗi ngày, trong tất cả 7 ngày của tuần. Khi một người dùng **logon** vào mạng thì hệ thống sẽ kiểm tra xem thời điểm này có nằm trong khoảng thời gian cho phép truy cập không, nếu không phù hợp thì hệ thống sẽ không cho vào mạng và thông báo lỗi **Unable to log you on because of an account restriction**. Bạn có thể thay đổi quy định giờ **logon** bằng cách chọn vùng thời gian cần thay đổi và nhấp chuột vào nút lựa chọn **Logon Permitted**, nếu ngược lại không cho phép thì nhấp chuột vào nút lựa chọn **Logon Denied**. Sau đây là hình ví dụ chỉ cho phép người dùng làm việc từ 7h sáng đến 5h chiều, từ thứ 2 đến thứ 6. Chú ý: mặc định người dùng không bị **logoff** tự động khi hết giờ đăng nhập nhưng bạn có thể điều chỉnh điều này tại mục **Automatically Log Off Users When Logon Hours Expire** trong **Group Policy** phần **Computer Configuration\ Windows Settings\Security Settings\ Local Policies\ Security Option**. Ngoài ra bạn cũng có cách khác để điều chỉnh thông tin **logoff** này bằng cách dùng công cụ **Domain Security Policy** hoặc **Local Security Policy** tùy theo bối cảnh.



Chọn lựa máy trạm được truy cập vào mạng: bạn nhấp chuột vào nút **Log On To**, bạn sẽ thấy hộp thoại **Logon Workstations** xuất hiện. Hộp thoại này cho phép bạn chỉ định người dùng có thể **logon** từ tất cả các máy tính trong mạng hoặc giới hạn người dùng chỉ được phép **logon** từ một số máy tính trong mạng. Ví dụ như người quản trị mạng làm việc trong môi trường bảo mật nên tài khoản người dùng này chỉ được chỉ định **logon** vào mạng từ một số máy tránh tình trạng người dùng giả dạng quản trị để tấn công mạng. Muốn chỉ định máy tính mà người dùng được phép **logon** vào mạng, bạn nhập tên máy tính đó vào mục **Computer Name** và sau đó nhấp chuột vào nút **Add**.



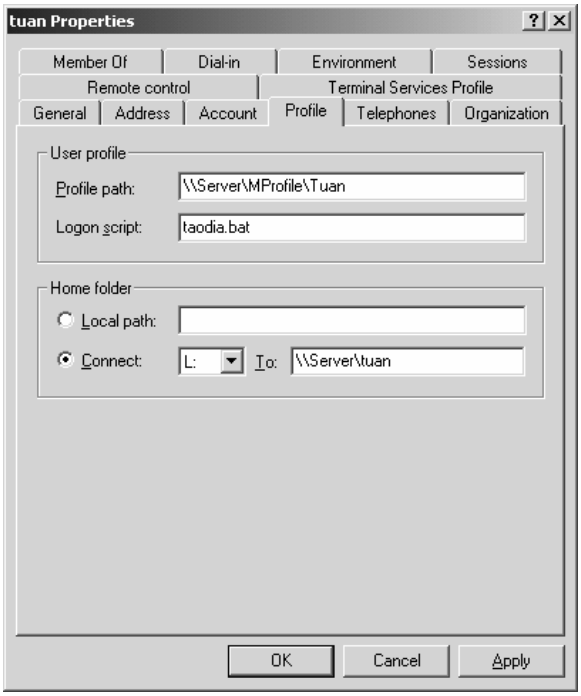
Bảng mô tả chi tiết các tùy chọn liên quan đến tài khoản người dùng:

Tùy Chọn	Ý Nghĩa
User must change password at next logon	Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn.
User cannot change password	Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu.
Password never expires	Nếu được chọn thì mật khẩu của tài khoản này không bao giờ hết hạn.
Store password using reversible encryption	Chỉ áp dụng tùy chọn này đối với người dùng đăng nhập từ các máy **Apple**.
Account is disabled	Nếu được chọn thì tài khoản này tạm thời bị khóa, không sử dụng được.
Smart card is required for interactive login	Tùy chọn này được dùng khi người dùng đăng nhập vào mạng thông qua một thẻ thông minh (**smart card**), lúc đó người dùng không nhập username và password mà chỉ cần nhập vào một số **PIN**.
Account is trusted for delegation	Chỉ áp dụng cho các tài khoản dịch vụ nào cần giành được quyền truy cập vào tài nguyên với vai trò những tài khoản người dùng khác
Account is sensitive and cannot be delegated	Dùng tùy chọn này trên một tài khoản khách vãng lai hoặc tạm để đảm bảo rằng tài khoản đó sẽ không được đại diện bởi một tài khoản khác.
Use DES encryption types for this account	Nếu được chọn thì hệ thống sẽ hỗ trợ **Data Encryption Standard** (**DES**) với nhiều mức độ khác nhau.
Do not require Kerberos preauthentication	Nếu được chọn hệ thống sẽ cho phép tài khoản này dùng một kiểu thực hiện giao thức **Kerberos** khác với kiểu của **Windows Server 2003**.

Mục cuối cùng trong **Tab** này là quy định thời gian hết hạn của một tài khoản người dùng. Trong mục **Account Expires**, nếu ta chọn **Never** thì tài khoản này không bị hết hạn, nếu chọn **End of: ngày tháng hết hạn** thì đến ngày này tài khoản này bị tạm khóa.

V.2.3 Tab Profile.

Tab Profile cho phép bạn khai báo đường dẫn đến **Profile** của tài khoản người dùng hiện tại, khai báo tập tin **logon script** được tự động thi hành khi người dùng đăng nhập hay khai báo **home folder**. Chú ý các tùy chọn trong **Tab Profile** này chủ yếu phục vụ cho các máy trạm trước **Windows 2000**, còn đối với các máy trạm từ **Win2K** trở về sau như: **Win2K Pro, WinXP, Windows Server 2003** thì chúng ta có thể cấu hình các lựa chọn này trong **Group Policy**.



Trước tiên chúng ta hãy tìm hiểu khái niệm **Profile**. **User Profiles** là một thư mục chứa các thông tin về môi trường của **Windows Server 2003** cho từng người dùng mạng. **Profile** chứa các qui định về màn hình **Desktop**, nội dung của menu **Start,** kiểu cách phối màu sắc, vị trí sắp xếp các **icon**, biểu tượng chuột…

Mặc định khi người dùng đăng nhập vào mạng, một **profile** sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một **profile** chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục **Documents and Settings**. Thư mục **profile** người dùng được tạo chứa một tập tin **ntuser.dat**, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong **Windows Server 2003** có ba loại **Profile**:

Local Profile: là **profile** của người dùng được lưu trên máy cục bộ và họ tự cấu hình trên **profile** đó.

Roaming Profile: là loại **Profile** được chứa trên mạng và người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, để tự động duy trì một bản sao của tài khoản người dùng trên mạng.

Mandatory Profile: người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, sau đó chép một profile đã cấu hình sẵn vào đường dẫn đó. Lúc đó các người dùng dùng chung **profile** này và không được quyền thay đổi profile đó.

Kịch bản đăng nhập (**logon script** hay **login script**) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xa từ **Server**). Bạn có thể dùng nhiều ngôn ngữ kịch bản để tạo ra **logon script** như: lệnh **shell** của **DOS/NT/Windows**, **Windows Scripting Host (WSH), VBScript, Jscript**…

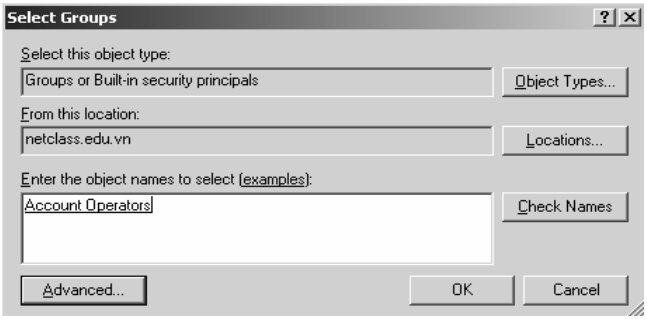
Đối với **Windows Server 2003** thì có hai cách để khai báo **logon script** là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ **Active Directory User and Computers**, khai báo thông qua **Group Policy**. Nhưng chú ý trong cả hai cách, các tập tin **script** và mọi tập tin cần thiết khác phải được đặt trong thư mục chia sẻ **SYSVOL**, nằm trong **\Windows\SYSVOL\sysvol**, nếu các tập tin script này phục vụ cho các máy tiền **Win2K** thì phải đặt trong thư mục **\Windows\Sysvol\sysvol\domainname\scripts**. Để các tập tin **script** thi hành được bạn nhớ cấp quyền cho các người dùng mạng có quyền **Read** và **Excute** trên các tập tin này. Sau đây là một ví dụ về một tập tin **logon script**.

```
@echo off
rem Taodia.bat Version 1.0
rem neu nguoi dung logon ngay tai server thi khong lam gi ca.
ff %computername%.== tvthanh. goto END
rem xoa cac o dia anh xa dang ton tai
net use h: /delete >nul
net use j: /delete >nul
rem anh xa o dia h va j
net use h: \\tvthanh\users  /yes >nul
net use j: \\tvthanh\apps  /yes >nul
rem dong bo thoi gian voi Server
net time \\tvthanh /set /yes
:END
```

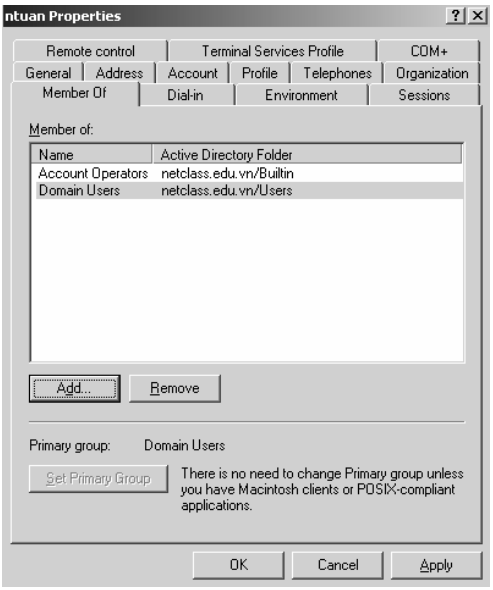
Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là "\\server\tuan", nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: "\\server\%username%".

V.2.4 Tab Member Of.

Tab Member Of cho phép bạn xem và cấu hình tài khoản người dùng hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấp chuột vào nút **Add**, hộp thoại chọn nhóm sẽ hiện ra.



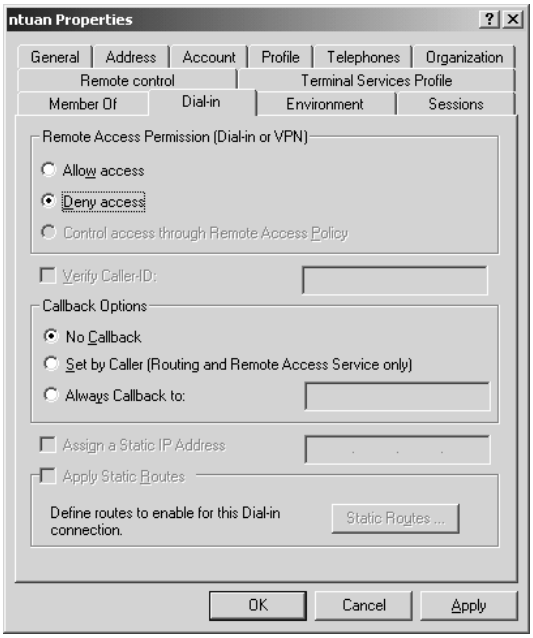
Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm kiếm và hiển thị hết tất cả các nhóm hiện có trong hệ thống. Nếu bạn không nhớ tên nhóm thì chấp nhận nhấp chuột vào nút **Advanced** và **Find Now** để tìm hết tất cả các nhóm.



Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

V.2.5 Tab Dial-in.

Tab **Dial-in** cho phép bạn cấu hình quyền truy cập từ xa của người dùng cho kết nối **dial-in** hoặc **VPN**, chúng ta sẽ khảo sát chi tiết ở chương **Routing and Remote Access**.



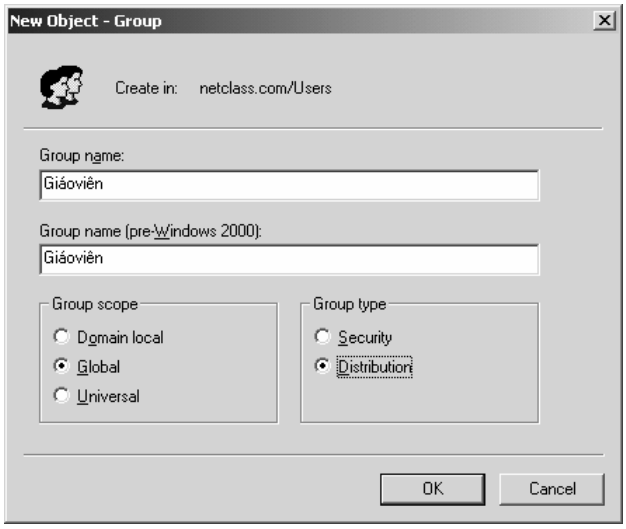
V.3. Tạo mới tài khoản nhóm.

Bạn tạo và quản lý tài khoản nhóm trên **Active Directory** thông qua công cụ **Active Directory Users and Computers**. Trước khi tạo nhóm bạn phải xác định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào. Sau khi chuẩn bị đầy đủ các thông tin bạn thực hiện các bước sau:

Chọn **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Active Directory Users and Computers** để mở công cụ **Active Directory Users and Computers** lên.

Nhấp phải chuột vào mục **Users**, chọn **New** trên **pop-up menu** và chọn **Group**.

Hộp thoại **New Object – Group** xuất hiện, bạn nhập tên nhóm vào mục **Group name**, trường tên nhóm cho các hệ điều hành trước **Windows 2000 (pre-Windows 2000)** tự động phát sinh, bạn có thể hiệu chỉnh lại cho phù hợp.



Nhấp chuột vào nút **OK** để hoàn tất và đóng hộp thoại.

V.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm.

So với **Windows 2000 Server** thì **Windows Server 2003** cung cấp thêm nhiều công cụ dòng lệnh mạnh mẽ, có thể được dùng trong các tập tin xử lý theo lô (**batch**) hoặc các tập tin kịch bản (**script**) để quản lý tài khoản người dùng như thêm, xóa, sửa. **Windows 2003** còn hỗ trợ việc nhập và xuất các đối tượng từ **Active Directory**. Hai tiện ích **dsadd.exe** và **admod.exe** với đối số **user** cho phép chúng ta thêm và chỉnh sửa tài khoản người dùng trong **Active Directory**. Tiện ích **csvde.exe** được dùng để nhập hoặc xuất dữ liệu đối tượng thông qua các tập tin kiểu **CSV** (**comma-separated values**). Đồng thời hệ thống mới này vẫn còn sử dụng hai lệnh **net user** và **net group** của **Windows 2000**.

V.4.1 Lệnh net user.

Chức năng: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng .

Cú pháp:

net user [username [password | *] [options]] [/domain]

net user username {password | *} /add [options] [/domain]

net user username [/delete] [/domain]

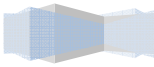
Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính
- [**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.
- [**Password**]: ấn định hoặc thay đổi mật mã của tài khoản người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows 2000** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **logon** vào mạng từ máy trạm dùng **Win9X**.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**/add**]: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.
- [**/delete**]: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.
- [**/active:{no | yes}**]: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (**active**).
- [**/comment:"text"**]: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.
- [**/countrycode:nnn**]: chỉ định mã quốc gia và mã vùng.
- [**/expires:{date | never}**]: quy định ngày hết hiệu lực của tài khoản người dùng.
- [**/fullname:"name"**]: khai báo tên đầy đủ của người dùng.
- [**/homedir:path**]: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.
- [**/passwordchg:{yes | no}**]: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.
- [**/passwordreq:{yes | no}**]: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.
- [**/profilepath:[path]**]: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **logon** đầu tiên.
- [**/scriptpath:path**]: khai báo đường dẫn và tập tin **logon script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).
- [**/times:{times | all}**]: quy định giờ cho phép người dùng logon vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự : M, T, W, Th, F, Sa, Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: “M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;”
- [**/workstations:{computername[,...] | *}**]: chỉ định các máy tính mà người dùng này có thể sử dụng để logon vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự ‘*’ thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.

V.4.2 Lệnh net group.

Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên **Windows 2000 Server**

domains, lệnh này chỉ có hiệu lực khi dùng trên máy **Windows 2000 Server Domain Controllers**.



Cú pháp:

net group [groupname [/comment:"text"]] [/domain]

net group groupname {/add [/comment:"text"] | /delete} [/domain]

net group groupname username[...] {/add | /delete} [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**username[...]**]: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.
- [**/add**]: thêm một nhóm hoặc thêm một người dùng vào nhóm.
- [**/delete**]: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.

V.4.3 Lệnh net localgroup.

Chức năng: thêm, hiển thị hoặc hiệu chỉnh nhóm cục bộ.

Cú pháp:

net localgroup [groupname [/comment:"text"]] [/domain]

net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]

net localgroup groupname name [...] {/add | /delete} [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng hiển thị tên server và tên các nhóm cục bộ trên máy tính hiện tại.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**name** [...]]: danh sách một hoặc nhiều tên người dùng hoặc tên nhóm cần thêm vào hoặc xóa khỏi nhóm cục bộ. Các tên này cách nhau bởi khoảng trắng.
- [**/add**]: thêm tên một nhóm toàn cục hoặc tên người dùng vào nhóm cục bộ.
- [**/delete**]: xóa tên một nhóm toàn cục hoặc tên người dùng khỏi nhóm cục bộ.

V.4.4 Các lệnh hỗ trợ dịch vụ Active Driectory trong môi trường Windows Server 2003.

Trên hệ thống **Windows Server 2003**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ

yếu trên các đối tượng **computer, contact, group, ou, user, quota**.

- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.
- **Dsrm**: xóa một đối tượng trong dịch vụ **Directory**.
- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.
- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**, **contact**, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.
- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.
- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.
- Ví dụ:
- Tạo một **user** mới: dsadd user “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn” –samid hv10 –pwd 123
- Xóa một **user**: dsrm “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn”
- Xem các **user** trong hệ thống: ***dsquery user***
- Gia nhập **user** mới vào nhóm: dsmod group “CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn” –addmbr “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn”

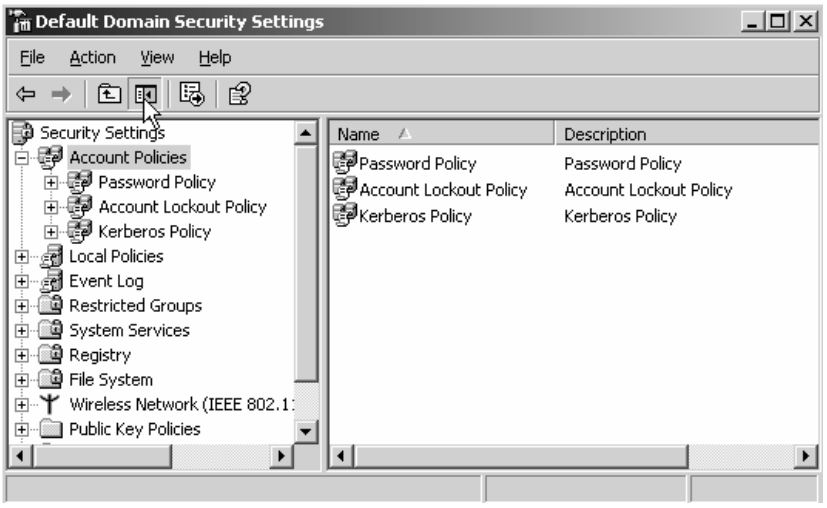
Tóm tắt

Lý thuyết 5 tiết - Thực hành 6 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về chính sách mật khẩu, chính sách khóa tài khoản người dùng, quyền hệ thống của người dùng, IPSec …	I. Chính sách tài khoản người dùng. II. Chính sách cục bộ. III. IPSec.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. CHÍNH SÁCH TÀI KHOẢN NGƯỜI DÙNG.

Chính sách tài khoản người dùng (**Account Policy**) được dùng để chỉ định các thông số về tài khoản người dùng mà nó được sử dụng khi tiến trình **logon** xảy ra. Nó cho phép bạn cấu hình các thông số bảo mật máy tính cho mật khẩu, khóa tài khoản và chứng thực **Kerberos** trong vùng. Nếu trên **Server** thành viên thì bạn sẽ thấy hai mục **Password Policy** và **Account Lockout Policy**, trên máy **Windows Server 2003** làm **domain controller** thì bạn sẽ thấy ba thư mục **Password Policy**, **Account Lockout Policy** và **Kerberos Policy**. Trong **Windows Server 2003** cho phép bạn quản lý chính sách tài khoản tại hai cấp độ là: cục bộ và miền. Muốn cấu hình các chính sách tài khoản người dùng ta vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Domain Security Policy** hoặc **Local Security Policy**.



I.1. Chính sách mật khẩu.

Chính sách mật khẩu (**Password Policies**) nhằm đảm bảo an toàn cho mật khẩu của người dùng để trách các trường hợp đăng nhập bất hợp pháp vào hệ thống. Chính sách này cho phép bạn qui định chiều dài ngắn nhất của mật khẩu, độ phức tạp của mật khẩu…

Các lựa chọn trong chính sách mật mã:

Chính sách	Mô tả	Mặc định
Enforce Password History	Số lần đặt mật mã không được trùng nhau	24
Maximum Password Age	Quy định số ngày nhiều nhất mà mật mã người dùng có hiệu lực	42.
Minimum Password Age	Quy số ngày tối thiểu trước khi người dùng có thể thay đổi mật mã.	1
Minimum Password Length	Chiều dài ngắn nhất của mật mã	7
Passwords Must Meet Complexity Requirements	Mật khẩu phải có độ phức tạp như: có ký tự hoa, thường, có ký số.	Cho phép
Store Password Using Reversible Encryption for All Users in the Domain	Mật mã người dùng được lưu dưới dạng mã hóa	Không cho phép

I.2. Chính sách khóa tài khoản.

Chính sách khóa tài khoản (**Account Lockout Policy**) quy định cách thức và thời điểm khóa tài khoản trong vùng hay trong hệ thống cục bộ. Chính sách này giúp hạn chế tấn công thông qua hình thức **logon** từ xa.

Các thông số cấu hình chính sách khóa tài khoản:

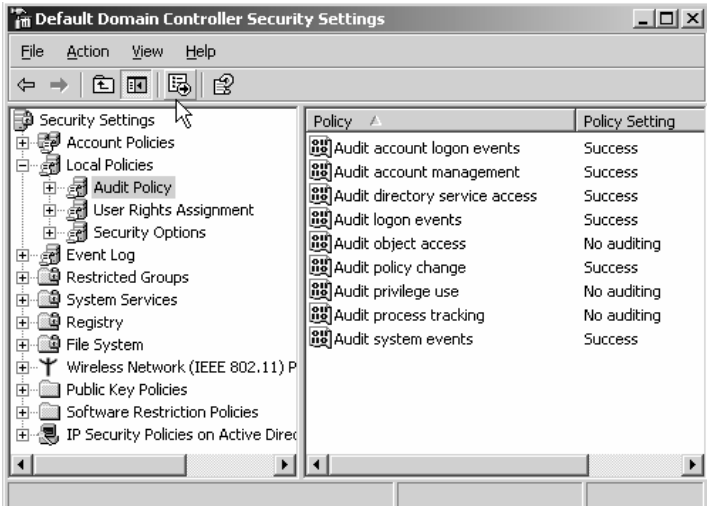
Chính sách	Mô tả	Giá trị mặc định
Account Lockout Threshold	Quy định số lần cố gắng đăng nhập trước khi tài khoản bị khóa	0 (tài khoản sẽ không bị khóa)
Account Lockout Duration	Quy định thời gian khóa tài khoản	Là 0, nhưng nếu Acc**ount Lockout Threshold** được thiết lập thì giá trị này là 30 phút.
Reset Account Lockout Counter After	Quy định thời gian đếm lại số lần đăng nhập không thành công	Là 0, nhưng nếu **Account Lockout Threshold** được thiết lập thì giá trị này là 30 phút.

II. CHÍNH SÁCH CỤC BỘ.

Chính sách cục bộ (**Local Policies**) cho phép bạn thiết lập các chính sách giám sát các đối tượng trên mạng như người dùng và tài nguyên dùng chung. Đồng thời dựa vào công cụ này bạn có thể cấp quyền hệ thống cho các người dùng và thiết lập các lựa chọn bảo mật.

II.1. Chính sách kiểm toán.

Chính sách kiểm toán (**Audit Policies**) giúp bạn có thể giám sát và ghi nhận các sự kiện xảy ra trong hệ thống, trên các đối tượng cũng như đối với các người dùng. Bạn có thể xem các ghi nhận này thông qua công cụ **Event Viewer**, trong mục **Security**.

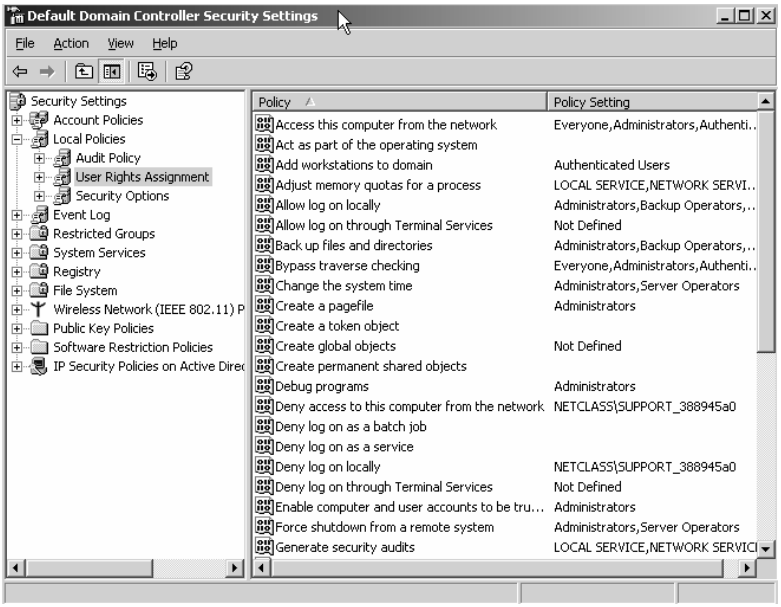


Các lựa chọn trong chính sách kiểm toán:

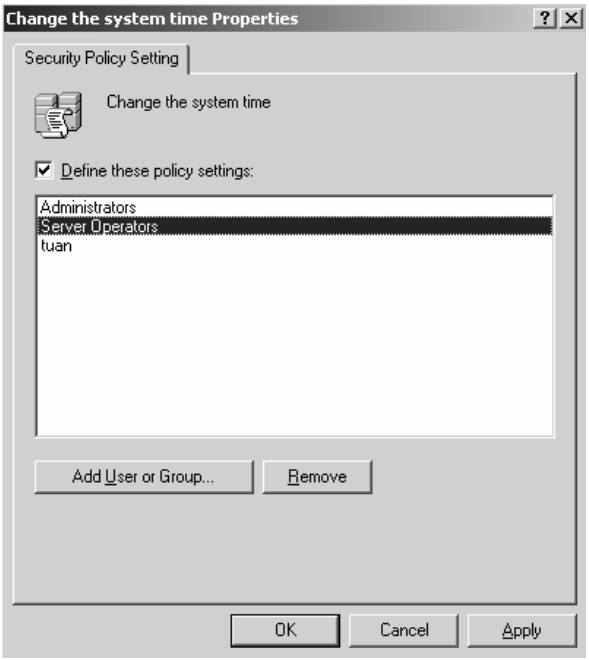
Chính sách	Mô tả
Audit Account Logon Events	Kiểm toán những sự kiện khi tài khoản đăng nhập, hệ thống sẽ ghi nhận khi người dùng **logon**, **logoff** hoặc tạo một kết nối mạng
Audit Account Management	Hệ thống sẽ ghi nhận khi tài khoản người dùng hoặc nhóm có sự thay đổi thông tin hay các thao tác quản trị liên quan đến tài khoản người dùng.
Audit Directory Service Access	Ghi nhân việc truy cập các dịch vụ thư mục
Audit Logon Events	Ghi nhân các sự kiện liên quan đến quá trình logon như thi hành một **logon script** hoặc truy cập đến một **roaming profile**.
Audit Object Access	Ghi nhận việc truy cập các tập tin, thư mục, và máy tin.
Audit Policy Change	Ghi nhận các thay đổi trong chính sách kiểm toán
Audit privilege use	Hệ thống sẽ ghi nhận lại khi bạn bạn thao tác quản trị trên các quyền hệ thống như cấp hoặc xóa quyền của một ai đó.
Audit process tracking	Kiểm toán này theo dõi hoạt động của chương trình hay hệ điều hành.
Audit system event	Hệ thống sẽ ghi nhận mỗi khi bạn khởi động lại máy hoặc tắt máy.

II.2. Quyền hệ thống của người dùng.

Đối với hệ thống **Windows Server 2003**, bạn có hai cách cấp quyền hệ thống cho người dùng là: gia nhập tài khoản người dùng vào các nhóm tạo sẵn (**built-in**) để kế thừa quyền hoặc bạn dùng công cụ **User Rights Assignment** để gán từng quyền rời rạc cho người dùng. Cách thứ nhất bạn đã biết sử dụng ở chương trước, chỉ cần nhớ các quyền hạn của từng nhóm tạo sẵn thì bạn có thể gán quyền cho người dùng theo yêu cầu. Để cấp quyền hệ thống cho người dùng theo theo cách thứ hai thì bạn phải dùng công cụ **Local Security Policy** (nếu máy bạn không phải **Domain Controller**) hoặc **Domain Controller Security Policy** (nếu máy bạn là **Domain Controller**). Trong hai công cụ đó bạn mở mục **Local Policy\ User Rights Assignment**.



Để thêm, bớt một quyền hạn cho người dùng hoặc nhóm, bạn nhấp đôi chuột vào quyền hạn được chọn, nó sẽ xuất hiện một hộp thoại chứa danh sách người dùng và nhóm hiện tại đang có quyền này. Bạn có thể nhấp chuột vào nút **Add** để thêm người dùng, nhóm vào danh sách hoặc nhấp chuột vào nút **Remove** để xóa người dùng khỏi danh sách. Ví dụ minh họa sau là bạn cấp quyền thay đổi giờ hệ thống (**change the system time**) cho người dùng "Tuan".



Danh sách các quyền hệ thống cấp cho người dùng và nhóm:

Quyền	Mô tả
Access This Computer from the Network	Cho phép người dùng truy cập máy tính thông qua mạng. Mặc định mọi người đều có quyền này.
Act as Part of the Operating System	Cho phép các dịch vụ chứng thực ở mức thấp chứng thực với bất kỳ người dùng nào.
Add Workstations to the Domain	Cho phép người dùng thêm một tài khoản máy tính vào vùng.
Back Up Files and Directories	Cho phép người dùng sao lưu dự phòng (**backup**) các tập tin và thư mục bất chấp các tập tin và thư mục này người đó có quyền không.
Bypass Traverse Checking	Cho phép người dùng duyệt qua cấu trúc thư mục nếu người dùng không có quyền xem (**list**) nội dung thư mục này.
Change the System Time	Cho phép người dùng thay đổi giờ hệ thống của máy tính.
Create a Pagefile	Cho phép người dùng thay đổi kích thước của **Page File**.
Create a Token Object	Cho phép một tiến trình tạo một thẻ bài nếu tiến trình này dùng **NTCreate Token API**.
Create Permanent Shared Objects	Cho phép một tiến trình tạo một đối tượng thư mục thông qua **Windows 2000 Object Manager**.

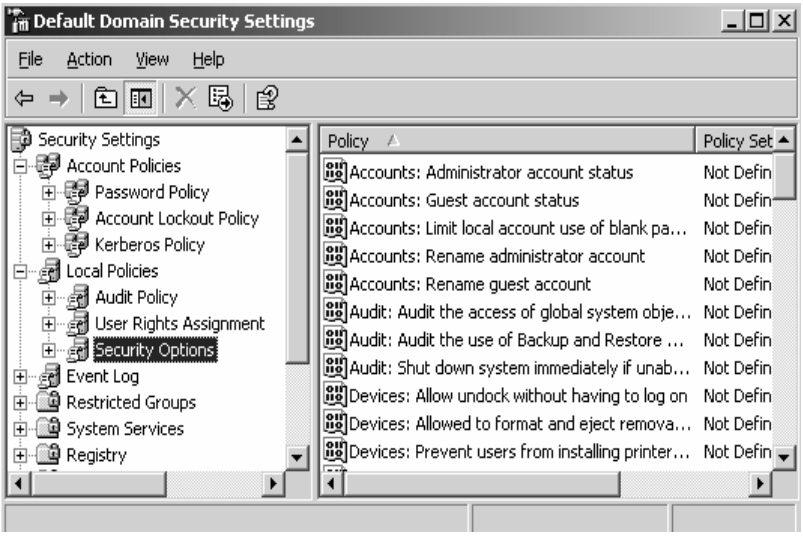
Debug Programs	Cho phép người dùng gắn một chương trình **debug** vào bất kỳ tiến trình nào.
Deny Access to This Computer from the Network	Cho phép bạn khóa người dùng hoặc nhóm không được truy cập đến các máy tính trên mạng.
Deny Logon as a Batch File	Cho phép bạn ngăn cản những người dùng và nhóm được phép logon như một **batch file**.
Deny Logon as a Service	Cho phép bạn ngăn cản những người dùng và nhóm được phép **logon** như một **services**.
Deny Logon Locally	Cho phép bạn ngăn cản những người dùng và nhóm truy cập đến máy tính cục bộ.
Enable Computer and User Accounts to Be Trusted by Delegation	Cho phép người dùng hoặc nhóm được ủy quyền cho người dùng hoặc một đối tượng máy tính.
Force Shutdown from a Remote System	Cho phép người dùng shut down hệ thống từ xa thông qua mạng
Generate Security Audits	Cho phép người dùng, nhóm hoặc một tiến trình tạo một **entry** vào **Security log**.
Increase Quotas	Cho phép người dùng điều khiển các hạn ngạch của các tiến trình.
Increase Scheduling Priority	Quy định một tiến trình có thể tăng hoặc giảm độ ưu tiên đã được gán cho tiến trình khác.
Load and Unload Device Drivers	Cho phép người dùng có thể cài đặt hoặc gỡ bỏ các driver của các thiết bị.
Lock Pages in Memory	Khóa trang trong vùng nhớ.
Log On as a Batch Job	Cho phép một tiến trình **logon** vào hệ thống và thi hành một tập tin chứa các lệnh hệ thống.
Log On as a Service	Cho phép một dịch vụ **logon** và thi hành một dịch vụ riêng.
Log On Locally	Cho phép người dùng **logon** tại máy tính **Server**.
Manage Auditing and Security Log	Cho phép người dùng quản lý **Security log**.

Modify Firmware Environment Variables	Cho phép người dùng hoặc một tiến trình hiệu chỉnh các biến môi trường hệ thống.

Profile Single Process	Cho phép người dùng giám sát các tiến trình bình thường thông qua công cụ **Performance Logs and Alerts**.
Profile System Performance	Cho phép người dùng giám sát các tiến trình hệ thống thông qua công cụ **Performance Logs and Alerts**.
Remove Computer from Docking Station	Cho phép người dùng gỡ bỏ một **Laptop** thông qua giao diện người dùng của **Windows 2000**.
Replace a Process Level Token	Cho phép một tiến trình thay thế một token mặc định mà được tạo bởi một tiến trình con.
Restore Files and Directories	Cho phép người dùng phục hồi tập tin và thư mục, bất chấp người dùng này có quyền trên tập tin và thư mục này hay không.
Shut Down the System	Cho phép người dùng **shut down** cục bộ máy **Windows 2000**.
Synchronize Directory Service Data	Cho phép người dùng đồng bộ dữ liệu với một dịch vụ thư mục.
Take Ownership of Files or Other Objects	Cho người dùng tước quyền sở hữu của một đối tượng hệ thống.

II.3. Các lựa chọn bảo mật.

Các lựa chọn bảo mật (**Security Options**) cho phép người quản trị **Server** khai báo thêm các thông số nhằm tăng tính bảo mật cho hệ thống như: không cho phép hiển thị người dùng đã **logon** trước đó hay đổi tên tài khoản người dùng tạo sẵn (**administrator, guest**). Trong hệ thống **Windows Server 2003** hỗ trợ cho chúng ta rất nhiều lựa chọn bảo mật, nhưng trong giáo trình này chúng ta chỉ khảo sát các lựa chọn thông dụng.



Một số lựa chọn bảo mật thông dụng:

Tên lựa chọn	Mô tả
Shutdown: allow system to be shut down without having to log on	Cho phép người dùng **shutdown** hệ thống mà không cần logon.
Audit : audit the access of global system objects	Giám sát việc truy cập các đối tượng hệ thống toàn cục.
Network security: force logoff when logon hours expires.	Tự động **logoff** khỏi hệ thống khi người dùng hết thời gian sử dụng hoặc tài khoản hết hạn.
Interactive logon: do not require CTRL+ALT+DEL	Không yêu cầu ấn ba phím **CTRL+ALT+DEL** khi logon.
Interactive logon: do not display last user name	Không hiển thị tên người dùng đã logon trên hộp thoại **Logon**.
Account: rename administrator account	Cho phép đổi tên tài khoản **Administrator** thành tên mới
Account: rename guest account	Cho phép đổi tên tài khoản **Guest** thành tên mới

III. IPSec.

IP Security (IPSec) là một giao thức hỗ trợ thiết lập các kết nối an toàn dựa trên **IP**. Giao thức này hoạt động ở tầng ba (**Network**) trong mô hình **OSI** do đó nó an toàn và tiện lợi hơn các giao thức an toàn khác ở tầng **Application** như **SSL**. **IPSec** cũng là một thành phần quan trọng hỗ trợ giao thức **L2TP** trong công nghệ mạng riêng ảo **VPN (Virtual Private Network).** Để sử dụng **IPSec** bạn phải tạo ra các qui tắc (**rule**), một qui tắc **IPSec** là sự kết hợp giữa hai thành phần là các bộ lọc **IPSec (filter)** và các tác động **IPSec (action).** Ví dụ nội dung của một qui tắc **IPSec** là "Hãy mã hóa tất cả những dữ liệu truyền **Telnet** từ máy có địa chỉ 192.168.0.10", nó gồm hai phần, phần bộ lọc là "qui tắc này chỉ hoạt động khi có dữ liệu được truyền từ máy có địa chỉ 192.168.0.10 thông qua cổng 23", phần hành động là "mã hóa dữ liệu.

III.1. Các tác động bảo mật.

IPSec của Microsoft hỗ trợ bốn loại tác động (**action**) bảo mật, các tác động bảo mật này giúp hệ thống có thể thiết lập những cuộc trao đổi thông tin giữa các máy được an toàn. Danh sách các tác động bảo mật trong hệ thống **Windows Server 2003** như sau:

- **Block transmissons**: có chức năng ngăn chặn những gói dữ liệu được truyền, ví dụ bạn muốn **IPSec** ngăn chặn dữ liệu truyền từ máy A đến máy B, thì đơn giản là chương trình **IPSec** trên máy B loại bỏ mọi dữ liệu truyền đến từ máy A.
- **Encrypt transmissions**: có chức năng mã hóa những gói dữ liệu được truyền, ví dụ chúng ta

muốn dữ liệu được truyền từ máy A đến máy B, nhưng chúng ta sợ rằng có người sẽ nghe trộm

trên đường truyền nối kết mạng giữa hai máy A và B. Cho nên chúng ta cần cấu hình cho **IPSec** sử dụng giao thức **ESP** (**encapsulating security payload**) để mã hóa dữ liệu cần truyền trước khi đưa lên mạng. Lúc này những người xem trộm sẽ thấy những dòng **byte** ngẫu nhiên và không hiểu được dữ liệu thật. Do **IPSec** hoạt động ở tầng **Network** nên hầu như việc mã hóa được trong suốt đối với người dùng, người dùng có thể gởi **mail**, truyền **file** hay **telnet** như bình thường.

- **Sign transmissions**: có chức năng ký tên vào các gói dữ liệu truyền, nhằm tránh những kẻ tấn công trên mạng giả dạng những gói dữ liệu được truyền từ những máy mà bạn đã thiết lập quan hệ tin cậy, kiểu tấn công này còn có cái tên là **main-in-the-middle**. **IPSec** cho phép bạn chống lại điều này bằng một giao thức **authentication header**. Giao thức này là phương pháp ký tên số hóa (**digitally signing**) vào các gói dữ liệu trước khi truyền, nó chỉ ngăn ngừa được giả mạo và sai lệnh thông tin chứ không ngăn được sự nghe trộm thông tin. Nguyên lý hoạt động của phương pháp này là hệ thống sẽ thêm một **bit** vào cuối mỗi gói dữ liệu truyền qua mạng, từ đó chúng ta có thể kiểm tra xem dữ liệu có bị thay đổi khi truyền hay không.
- **Permit transmissions**: có chức năng là cho phép dữ liệu được truyền qua, chúng dùng để tạo ra các qui tắc (**rule**) hạn chế một số điều và không hạn chế một số điều khác. Ví dụ một qui tắc dạng này "Hãy ngăn chặn tất cả những dữ liệu truyền tới, chỉ trừ dữ liệu truyền trên các cổng 80 và 443".

Chú ý: đối với hai tác động bảo mật theo phương pháp ký tên và mã hóa thì hệ thống còn yêu cầu bạn chỉ ra l**IPSec** dùng phương pháp chứng thực nào. **Microsoft** hỗ trợ ba phương pháp chứng thực: **Kerberos**, chứng chỉ (**certificate**) hoặc một khóa dựa trên sự thỏa thuận (**agreed-upon key**). Phương pháp **Kerberos** chỉ áp dụng được giữa các máy trong cùng một miền **Active Directory** hoặc trong những miền **Active Directory** có ủy quyền cho nhau. Phương pháp dùng các chứng chỉ cho phép bạn sử dụng các chứng chỉ **PKI** (**public key infrastructure**) để nhận diện một máy. Phương pháp dùng chìa khóa chia sẻ trước thì cho phép bạn dùng một chuỗi ký tự văn bản thông thường làm chìa khóa (**key**).

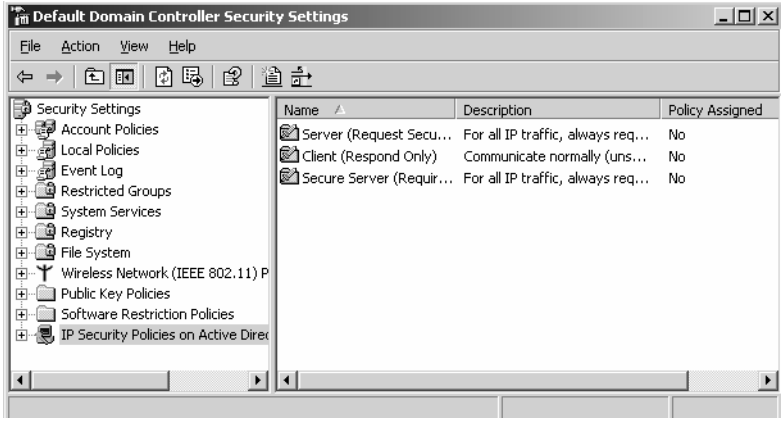
III.2. Các bộ lọc IPSec.

Để **IPSec** hoạt động linh hoạt hơn, **Microsoft** đưa thêm khái niệm bộ lọc (**filter**) **IPSec**, bộ lọc có tác dụng thống kê các điều kiện để qui tắc hoạt động. Đồng thời chúng cũng giới hạn tầm tác dụng của các tác động bảo mật trên một phạm vị máy tính nào đó hay một số dịch vụ nào đó. Bộ lọc **IPSec** chủ yếu dự trên các yếu tố sau:

- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy nguồn.
- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy đích.
- Theo số hiệu cổng (**port**) và kiển cổng (**TCP, UDP, ICMP**…)

III.3. Triển khai IPSec trên Windows Server 2003.

Trong hệ thống **Windows Server 2003** không hỗ trợ một công cụ riêng cấu hình **IPSec**, do đó để triển khai I**PSec** chúng ta dùng các công cụ thiết lập chính sách dành cho máy cục bộ hoặc dùng cho miền. Để mở công cụ cấu hình **IPSec** bạn nhấp chuột vào **Start** ◴ **Run** rồi gõ **secpol.msc** hoặc nhấp chuột vào **Start** ◴ **Programs** ◴ **Administrative Tools** ◴ **Local Security Policy**, trong công cụ đó bạn chọn **IP Security Policies on Local Machine**.



Tóm lại, các điều mà bạn cần nhớ khi triển khai **IPSec**:

- Bạn triển khai **IPSec** trên **Windows Server 2003** thông qua các chính sách, trên một máy tính bất kỳ nào đó vào tại một thời điểm thì chỉ có một chính sách **IPSec** được hoạt động.
- Mỗi chính sách **IPSec** gồm một hoặc nhiều qui tắc (**rule**) và một phương pháp chứng thực nào đó. Mặc dù các qui tắc **permit** và **block** không dùng đến chứng thực nhưng **Windows** vẫn đòi bạn chỉ định phương pháp chứng thực.
- **IPSec** cho phép bạn chứng thực thông qua **Active Directory**, các chứng chỉ **PKI** hoặc một khóa được chia sẻ trước.
- Mỗi qui tắc (**rule**) gồm một hay nhiều bộ lọc (**filter**) và một hay nhiều tác động bảo mật (**action**).
- Có bốn tác động mà qui tắc có thể dùng là: **block**, **encrypt**, **sign** và **permit**.

III.3.1 Các chính sách IPSec tạo sẵn.

Trong khung cửa sổ chính của công cụ cấu hình **IPSec**, bên phải chúng ta thấy xuất hiện ba chính sách được tạo sẵn tên là: **Client**, **Server** và **Secure**. Cả ba chính sách này đều ở trạng thái chưa áp dụng (**assigned**). Nhưng chú ý ngay cùng một thời điểm thì chỉ có thể có một chính sách được áp dụng và hoạt động, có nghĩa là khi bạn áp dụng một chính sách mới thì chính sách đang hoạt động hiện tại sẽ trở về trạng thái không hoạt động. Sau đây chúng ta sẽ khảo sát chi tiết ba chính sách tạo sẵn này.

- **Client (Respond Only)**: chính sách qui định máy tính của bạn không chủ động dùng **IPSec** trừ khi nhận được yêu cầu dùng **IPSec** từ máy đối tác. Chính sách này cho phép bạn có thể kết nối được cả với các máy tính dùng **IPSec** hoặc không dùng **IPSec**.
- **Server (Request Security)**: chính sách này qui định máy server của bạn chủ động cố gắng khởi tạo **IPSec** mỗi khi thiết lập kết nối với các máy tính khác, nhưng nếu máy **client** không thể dùng **IPSec** thì **Server** vẫn chấp nhận kết nối không dùng **IPSec**.
- **Secure Server (Require Security)**: chính sách này qui định không cho phép bất kỳ cuộc trao đổi dữ liệu nào với **Server** hiện tại mà không dùng **IPSec**.

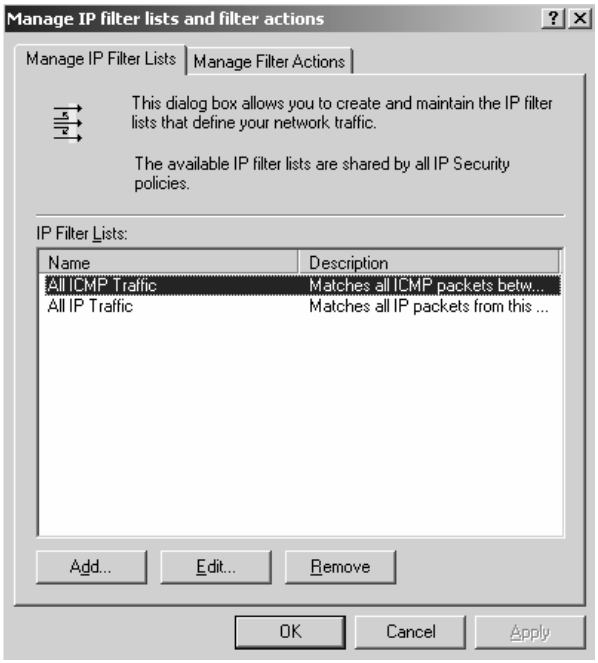
III.3.2 Ví dụ tạo chính sách IPSec đảm bảo một kết nối được mã hóa.

Trong phần này chúng ta bắt tay vào thiết lập một chính sách **IPSec** nhằm đảm bảo một kết nối được mã hóa giữa hai máy tính. Chúng ta có hai máy tính, máy A có địa chỉ 203.162.100.1 và máy B có địa chỉ 203.162.100.2. Chúng ta sẽ thiết lập chính sách I**PSec** trên mỗi máy thêm hai qui tắc (**rule**), trừ hai qui tắc của hệ thống gồm: một qui tắc áp dụng cho dữ liệu truyền vào máy và một qui tắc áp dụng cho dữ liệu truyền ra khỏi máy. Ví dụ qui tắc đầu tiên trên máy A bao gồm:

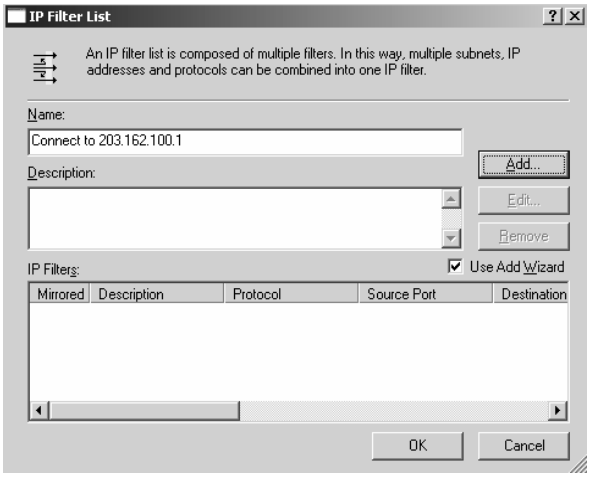
- Bộ lọc **(filter):** kích hoạt qui tắc này khi có dữ liệu truyền đến địa chỉ 203.162.100.1, qua bất kỳ cổng nào.
- Tác động bảo mật (**action**): mã hóa dữ liệu đó.
- Chứng thực: chìa khóa chia sẻ trước là chuỗi "quantri".

Qui tắc thứ hai áp dụng cho máy A cũng tương tự nhưng bộ lọc có nội dung ngược lại là "dữ liệu truyền đi từ địa chỉ 203.162.100.1". Chú ý: cách dễ nhất để tạo ra một qui tắc là trước tiên bạn phải qui định các bộ lọc và tác động bảo mật, rồi sau đó mới tạo ra qui tắc từ các bộ lọc và tác động bảo mật này. Các bước để thực hiện một chính sách **IPSec** theo yêu cầu như trên:

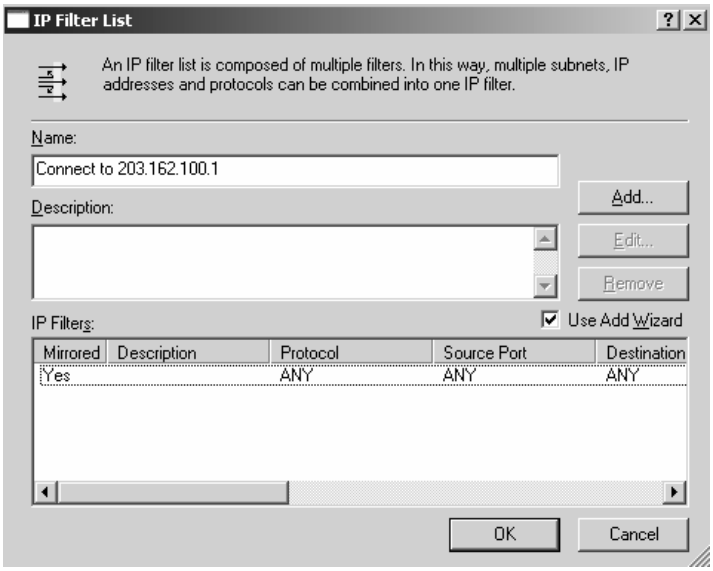
Trong công cụ **Domain Controller Security Policy**, bạn nhấp phải chuột trên mục **IP Security Policies on Active Directory**, rồi chọn **Manage IP filter lists and filter actions**.



Hộp thoại xuất hiện, bạn nhấp chuột vào nút **add** để thêm một bộ lọc mới. Bạn nhập tên cho bộ lọc này, trong ví dụ này chúng ta đặt tên là "**Connect to 203.162.100.1**". Bạn nhấp chuột tiếp vào nút **Add** để hệ thống hướng dẫn bạn khai báo các thông tin cho bộ lọc.

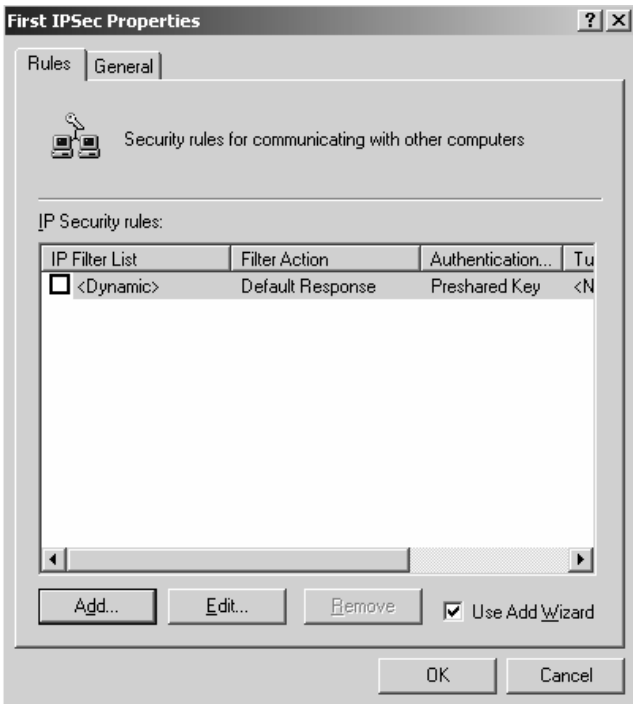


Bạn theo hướng dẫn của hệ thống để khai báo các thông tin, chú ý nên đánh dấu vào mục **Mirrored** để qui tắc này có ý nghĩa hai chiều bạn không phải tốn công để tạo ra hai qui tắc. Mục **Source address** chọn **My IP Address**, mục **Destination address** chọn **A specific IP Address** và nhập địa chỉ "203.162.100.1" vào, mục **IP Protocol Type** bạn để mặc định. Cuối cùng bạn chọn **Finish** để hoàn thành phần khai báo, bạn nhấp chuột tiếp vào nút **OK** để trở lại hộp thoại đầu tiên.

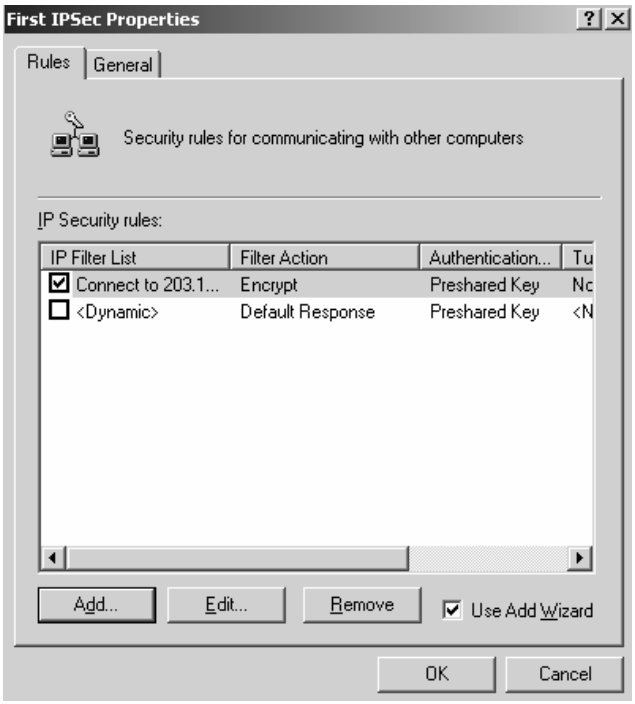


Tiếp theo bạn chuyển sang Tab **Manage Filter Actions** để tạo ra các tác động bảo mật. Bạn nhấp chuột vào nút **Add** hệ thống sẽ hướng dẫn bạn khai báo các thông tin về tác động. Trước tiên bạn đặt tên cho tác động này, ví dụ như là **Encrypt**.Tiếp tục trong mục **Filter Action** bạn chọn **Negotiate security**, trong mục **IP Traffic Security** bạn chọn **Integrity and encryption**. Đến đây bạn đã hoàn thành việc tạo một tác động bảo mật.

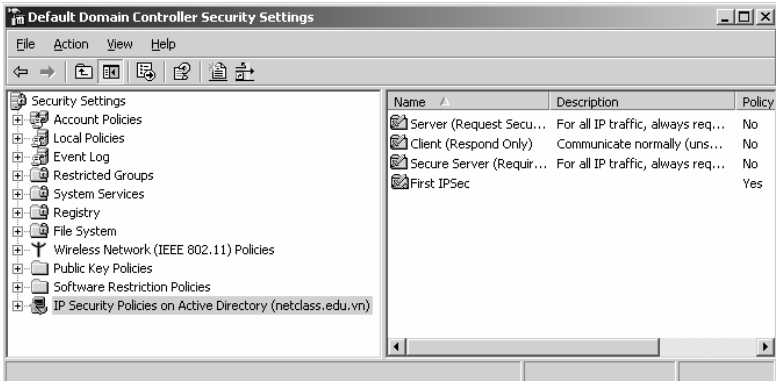
Công việc tiếp theo là bạn một chính sách **IPSec** trong đó có chứa một qui tắc kết hợp giữa bộ lọc và tác động vừa tạo ở phía trên. Trong công cụ **Domain Controller Security Policy**, bạn nhấp phải chuột trên mục **IP Security Policies on Active Directory**, rồi chọn **Create IP Security Policy**, theo hướng dẫn bạn nhập tên của chính vào, ví dụ là **First IPSec**, tiếp theo bạn phải bỏ đánh dấu trong mục **Active the default response rule**. Các giá trị còn lại bạn để mặc định vì qui tắc **Dynamic** này chúng ta không dùng và sẽ tạo ra một qui tắc mới.



Trong hộp thoại chính sách **IPSec**, bạn nhấp chuột vào nút **Add** để tạo ra qui tắc mới. Hệ thống sẽ hướng dẫn bạn từng bước thực hiện, đến mục chọn bộ lọc bạn chọn bộ lọc vừa tạo phía trên tên "**Connect to 203.162.100.1**", mục chọn tác động bạn chọn tác động vừa tạo tên **Encypt**. Đến mục chọn phương pháp chứng thực bạn chọn mục **Use this string to protect the key exchange** và nhập chuỗi làm khóa để mã hóa dữ liệu vào, trong ví dụ này là "quantri".



Đến bước này thì công việc thiết lập chính sách **IPSec** theo yêu cầu trên của bạn đã hoàn thành, trong khung của sổ chính của công cụ **Domain Controller Security Policy,** bạn nhấp phải chuột lên chính sách **First IPSec** và chọn **Assign** để chính sách này được hoạt động trên hệ thống **Server**.



Bài 12
CHÍNH SÁCH NHÓM

Tóm tắt

Lý thuyết 3 tiết - Thực hành 3 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về Group Policy, các chính sách đối với máy trạm, chính sách đối với người dùng…	I. Giới thiệu về chính sách nhóm. II. Triển khai một chính sách nhóm trên miền. III. Các ví dụ minh họa.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. GIỚI THIỆU.

I.1. So sánh giữa System Policy và Group Policy.

Vừa rồi ở chương trước, chúng ta đã tìm hiểu về chính sách hệ thống (**System Policy**), tiếp theo chúng ta sẽ tìm hiểu về chính sách nhóm (**Group Policy**). Vậy hai chính sách này khác nhau như thế nào.

- Chính sách nhóm chỉ xuất hiện trên miền **Active Directory** , nó không tồn tại trên miền **NT4**.
- Chính sách nhóm làm được nhiều điều hơn chính sách hệ thống. Tất nhiên chính sách nhóm chứa tất cả các chức năng của chính sách hệ thống và hơn thế nữa, bạn có thể dùng chính sách nhóm để triển khai một phần mềm cho một hoặc nhiều máy một cách tự động.
- Chính sách nhóm tự động hủy bỏ tác dụng khi được gỡ bỏ, không giống như các chính sách hệ thống.
- Chính sách nhóm được áp dụng thường xuyên hơn chính sách hệ thống. Các chính sách hệ thống chỉ được áp dụng khi máy tính đăng nhập vào mạng thôi. Các chính sách nhóm thì được áp dụng khi bạn bật máy lên, khi đăng nhập vào một cách tự động vào những thời điểm ngẫu nhiên trong suốt ngày làm việc.
- Bạn có nhiều mức độ để gán chính sách nhóm này cho người từng nhóm người hoặc từng nhóm đối tượng.
- Chính sách nhóm tuy có nhiều ưu điểm nhưng chỉ áp dụng được trên máy **Win2K**, **WinXP** và **Windows Server 2003**.

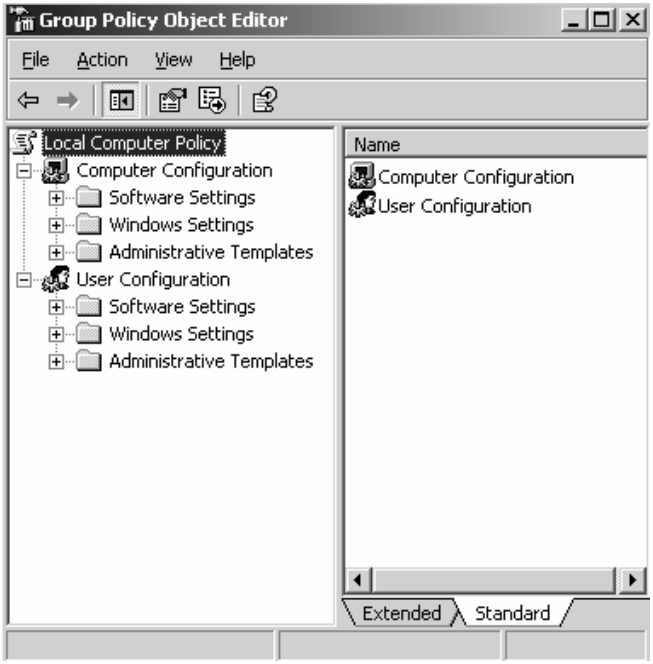
I.2. Chức năng của Group Policy.

- **Triển khai phần mềm ứng dụng**: bạn có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (**package**), đặt nó lên **Server**, rồi dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.
- **Gán các quyền hệ thống cho người dùng**: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt máy **server**, đổi giờ hệ thống hay **backup** dữ liệu…
- **Giới hạn những ứng dụng mà người dùng được phép thi hành**: chúng ta có thể kiểm soát máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: **Outlook Express**, **Word** hay **Internet Explorer**.
- **Kiểm soát các thiết lập hệ thống**: bạn có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.
- **Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy**: trong hệ thống NT4 thì chỉ hỗ trợ kịch bản đăng nhập (**logon script**), nhưng **Windows 2000** và **Windows Server 2003** thì hỗ trợ cả bốn sự kiện này được kích hoạt (**trigger**) một kịch bản (**script**). Bạn có thể dùng các **GPO** để kiểm soát những kịch bản nào đang chạy.
- **Đơn giản hóa và hạn chế các chương trình**: bạn có thể dùng **GPO** để gỡ bỏ nhiều tính năng khỏi Internet **Explorer**, **Windows Explorer** và những chương trình khác.

- Hạn chế tổng quát màn hình Desktop của người dùng: bạn có thể gỡ bỏ hầu hết các đề mục trên menu **Start** của một người dùng nào đó, ngăn chặn không cho người dùng cài thêm máy in, sửa đổi thông số cấu hình của máy trạm…

II. TRIỂN KHAI MỘT CHÍNH SÁCH NHÓM TRÊN MIỀN.

Chúng ta cấu hình và triển khai **Group Policy** bằng cách xây dựng các đối tượng chính sách (**GPO**). Các **GPO** là một vật chứa (**container**) có thể chứa nhiều chính sách áp dụng cho nhiều người, nhiều máy tính hay toàn bộ hệ thống mạng. Bạn dùng chương trình **Group Policy Object Editor** để tạo ra các đối tượng chính sách. Trong của sổ chính của **Group Policy Object Editor** có hai mục chính: cấu hình máy tính (**computer configuration**) và cấu hình người dùng (**user configuration**).



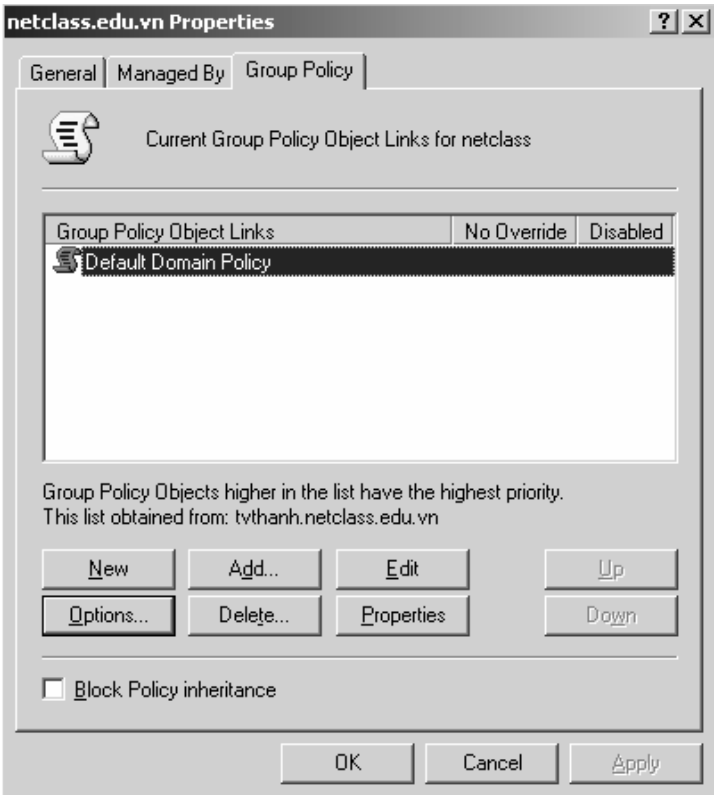
Điều kế tiếp bạn cũng chú ý khi triển khai **Group Policy** là các cấu hình chính sách của **Group Policy** được tích lũy và kề thừa từ các vật chứa (**container**) bên trên của **Active Directory**. Ví dụ các người dùng và máy tính vừa ở trong miền vừa ở trong **OU** nên sẽ nhận được các cấu hình từ cả hai chính sách cấp miền lẫn chính sách cấp **OU**. Các chính sách nhóm sau 90 phút sẽ được làm tươi và áp dụng một lần, nhưng các chính nhóm trên các **Domain Controller** được làm tươi 5 phút một lần. Các **GPO** hoạt động được không chỉ nhờ chỉnh sửa các thông tin trong **Registry** mà còn nhờ các thư viện liên kết động (**DLL**) làm phần mở rộng đặt tại các máy trạm. Chú ý nếu bạn dùng chính sách nhóm thì chính sách nhóm tại chỗ trên máy cục bộ sẽ xử lý trước các chính sách dành cho **site**, miền hoặc **OU**.

II.1. Xem chính sách cục bộ của một máy tính ở xa.

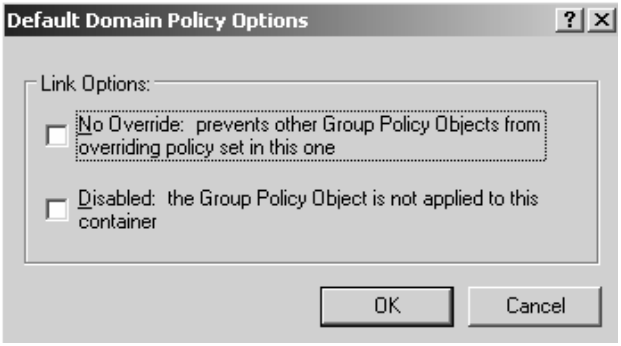
Để xem một chính sách cục bộ trên các máy tính khác trong miền, bạn phải có quyền quản trị trên máy đó hoặc quản trị miền. Lúc đó bạn có thể dùng lệnh **GPEDIT.MSC /gpcomputer:machinename**, ví dụ bạn muốn xem chính sách trên máy PCO1 bạn gõ lệnh **GPEDIT.MSC /gpcomputer: PCO1**. Chú ý là bạn không thể dùng cách này để thiết lập các chính sách nhóm ở máy tính ở xa, do tính chất bảo mật **Microsoft** không cho phép bạn ở xa thiết lập các chính sách nhóm.

II.2. Tạo các chính sách trên miền.

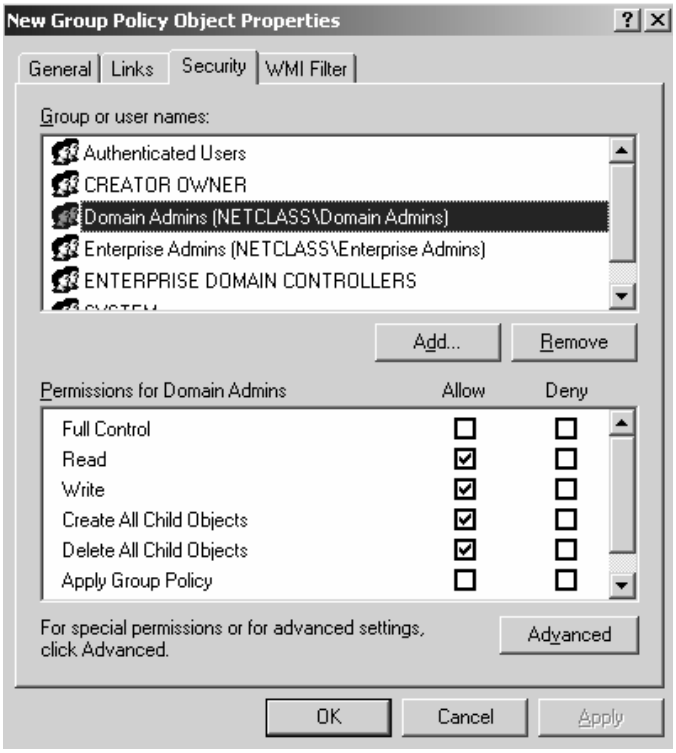
Chúng ta dùng **snap-in Group Policy** trong **Active Directory User and Computer** hoặc gọi trực tiếp tiện ích **Group Policy Object Editor** từ dòng lệnh trên máy **Domain Controller** để tạo ra các chính sách nhóm cho miền. Nếu bạn mở **Group Policy** từ **Active Directory User and Computer** thì trong khung cửa sổ chính của chương trình bạn nhấp chuột phải vào biểu tượng tên miền (trong ví dụ này là netclass.edu.vn), chọn **Properties**. Trong hộp thoại xuất hiện bạn chọn **Tab Group Policy**.



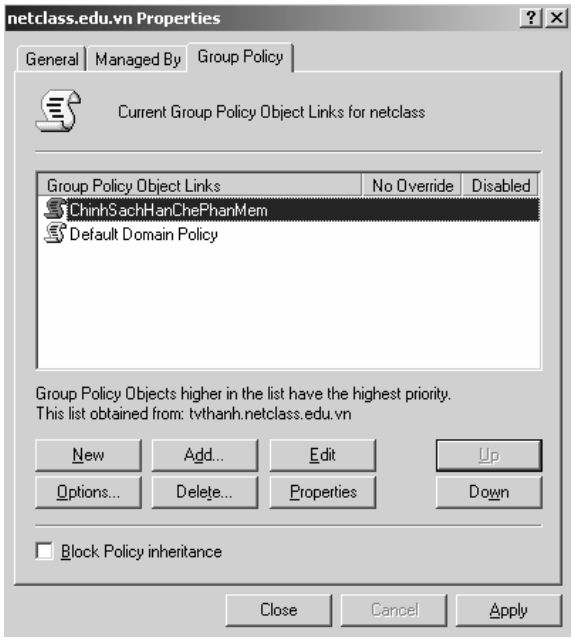
Nếu bạn chưa tạo ra một chính sách nào thì bạn chỉ nhìn thấy một chính sách tên **Default Domain Policy**. Cuối hộp thoại có một **checkbox** tên **Block Policy inheritance**, chức năng của mục này là ngăn chặn các thiết định của mọi chính sách bất kỳ ở cấp cao hơn lan truyền xuống đến cấp đang xét. Chú ý rằng chính sách được áp dụng đầu tiên ở cấp **site**, sau đó đến cấp miền và cuối cùng là cấp **OU**. Bạn chọn chính sách **Default Domain Policy** và nhấp chuột vào nút **Option** để cấu hình các lựa chọn việc áp dụng chính sách. Trong hộp thoại **Options**, nếu bạn đánh dấu vào mục **No Override** thì các chính sách khác được áp dụng ở dòng dưới sẽ không phủ quyết được những thiết định của chính sách này, cho dù chính sách đó không đánh dấu vào mục **Block Policy inheritance**. Tiếp theo nếu bạn đánh dấu vào mục **Disabled**, thì chính sách này sẽ không hoạt động ở cấp này, Việc **disbale** chính sách ở một cấp không làm **disable** bản thân đối tượng chính sách.



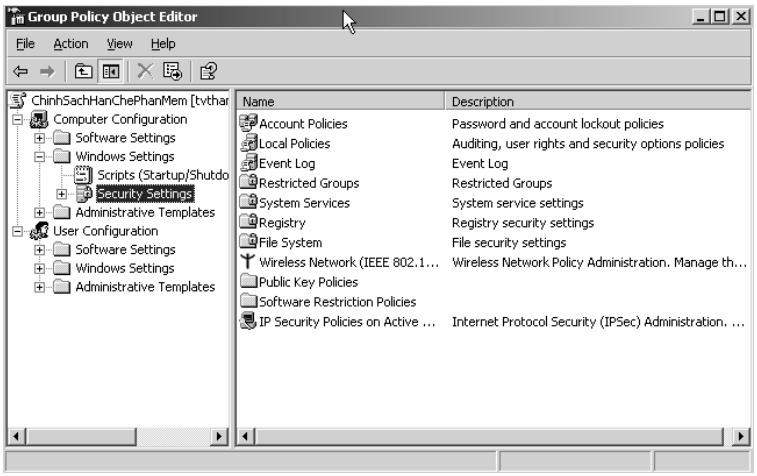
Để tạo ra một chính sách mới bạn nhấp chuột vào nút **New**, sau đó nhập tên của chính sách mới. Để khai báo thêm thông tin cho chính sách này bạn có thể nhấp chuột vào nút **Properties**, hộp thoại xuất hiện có nhiều **Tab**, bạn có thể vào **Tab Links** để chỉ ra các **site**, **domain** hoặc **OU** nào liên kết với chinh sách. Trong **Tab Security** cho phép bạn cấp quyền cho người dùng hoặc nhóm người dùng có quyền gì trên chính sách này.



Trong hộp thoại chính của **Group Policy** thì các chính sách được áp dụng từ dưới lên trên, cho nên chính sách nằm trên cùng sẽ được áp dụng cuối cùng. Do đó, các **GPO** càng nằm trên cao trong danh sách thì càng có độ ưu tiên cao hơn, nếu chúng có những thiết định mâu thuẫn nhau thì chính sách nào nằm trên sẽ thắng. Vì lý do đó nên **Microsoft** thiết kế hai nút **Up** và **Down** giúp chúng ta có thể di chuyển các chính sách này lên hay xuống.



Trong các nút mà chúng ta chưa khảo sát thì có một nút quan trọng nhất trong hộp thoại này đó là nút **Edit**. Bạn nhấp chuột vào nút **Edit** để thiết lập các thiết định cho chính sách này, dựa trên các khả năng của **Group Policy** bạn có thể thiết lập bất cứ thứ gì mà bạn muốn. Chúng ta sẽ khảo sát một số ví dụ minh họa ở phía sau.



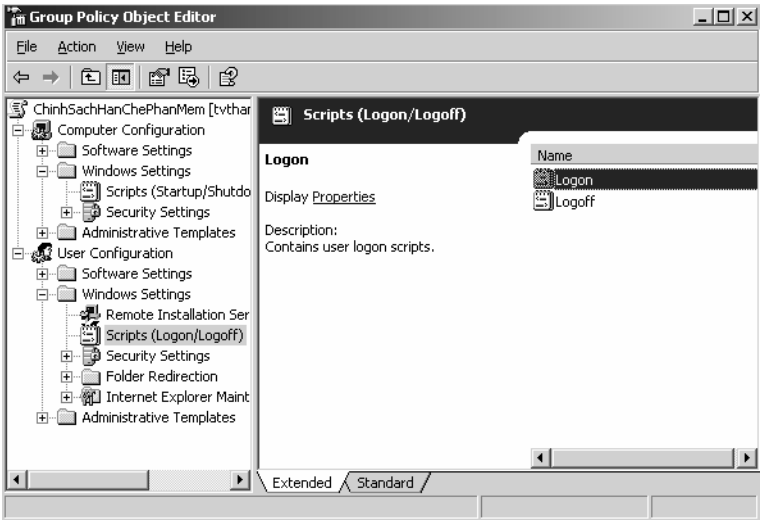
III. MỘT SỐ MINH HỌA GPO TRÊN NGƯỜI DÙNG VÀ CẤU HÌNH MÁY.

III.1. Khai báo một logon script dùng chính sách nhóm.

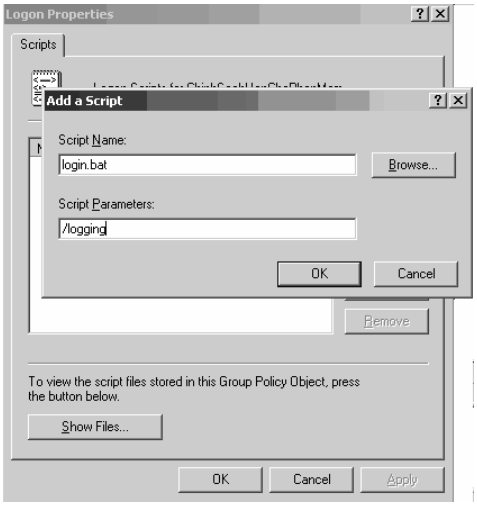
Trong **Windows Server 2003** hỗ trợ cho chúng ta bốn sự kiện để có thể kích hoạt các kịch bản (**script**) hoạt động là: **startup**, **shutdown, logon, logoff**. Trong công cụ **Group Policy Object Editor**, bạn có thể vào **Computer Configuration** 🕘 **Windows Setttings** 🕘 **Scripts** để khai báo các kịch bản sẽ hoạt động khi **startup, shutdown**. Đồng thời để khai báo các kịch bản sẽ hoạt động khi **logon, logoff** thì bạn vào **User Configuration** 🕘 **Windows Setttings** 🕘 **Scripts**. Trong ví dụ này chúng ta

tạo một **logon script**, quá trình gồm các bước sau:

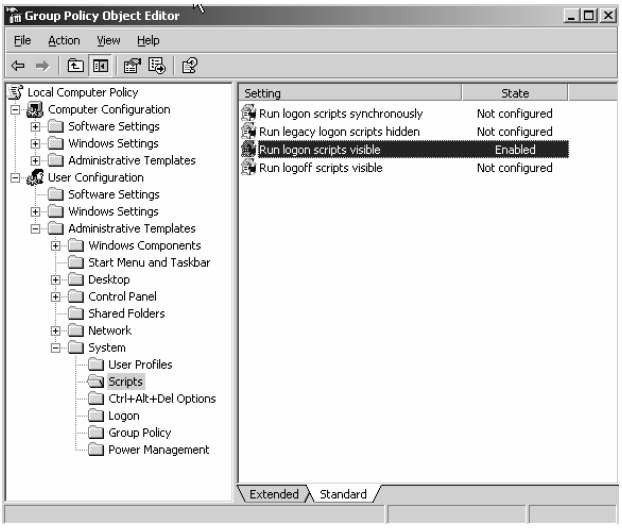
Mở công cụ **Group Policy Object Editor**, vào mục **User Configuration** ⏲ **Windows Setttings** ⏲ **Scripts**.



Nhấp đúp chuột vào mục **Logon** bên của sổ bên phải, hộp thoại xuất hiện, bạn nhấp chuột tiếp vào nút **Add** để khai báo tên tập tin kịch bản cần thi hành khi đăng nhập. Chú ý tập tin kịch bản này phải được chứa trong thư mục **c:\windows\system32\ grouppolicy\user\script\logon**. Thư mục này có thể thay đổi, tốt nhất bạn nên nhấp chuột vào nút **Show Files** phía dưới hộp thoại để xem thư mục cụ thể chứa các tập tin kịch bản này. Nội dung tập tin kịch bản có thể thay đổi tùy theo yêu cầu của bạn, bạn có thể tham khảo tập tin kịch bản ở chương trước.

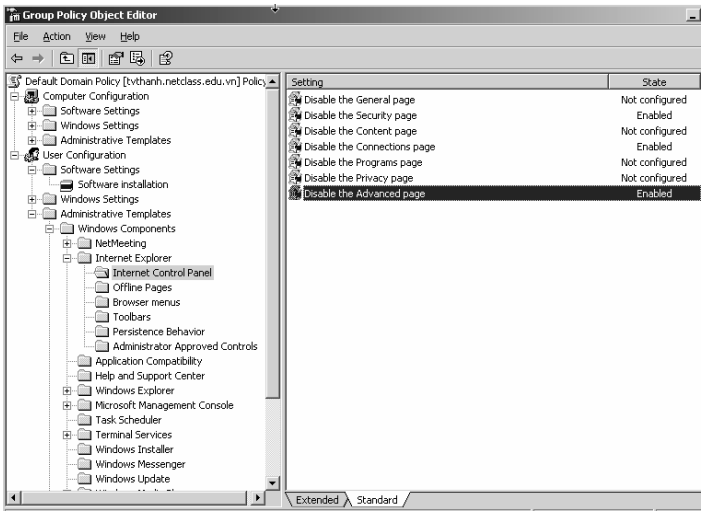


Tiếp theo để kiểm soát quá trình thi hành của tập tin kịch bản, bạn cần hiệu chỉnh chính sách **Run logon scripts visible** ở trạng thái **Enable**. Trạng thái này giúp bạn có thể phát hiện ra các lỗi phát sinh khi tập tin kịch bản thi hành từ đó chúng ta có thể sửa chữa. Để thay đổi chính sách này bạn nhấp chuột vào mục **User Configuration** ⏲ **Administrative Templates** ⏲ **System** ⏲ **Scripts,** sau đó nhấp đúp chuột vào mục **Run logon scripts visible** để thay đổi trạng thái.



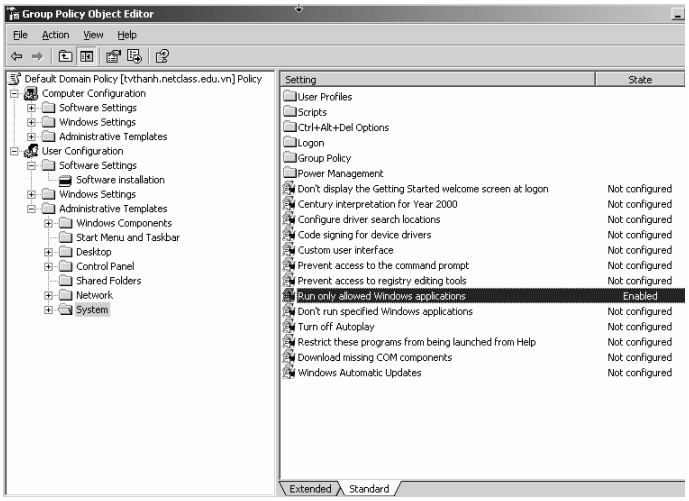
III.2. Hạn chế chức năng của Internet Explorer.

Trong ví dụ này chúng ta muốn các người dùng dưới máy trạm không được phép thay đổi bất kì thông số nào trong **Tab Security**, **Connection** và **Advanced** trong hộp thoại **Internet Options** của công cụ **Internet Explorer**. Để làm việc này, trong công cụ **Group Policy Object Editor**, bạn vào **User Configuration** 🕘 **Administrative Templates** 🕘 **Windows Components** 🕘 **Internet Explorer** 🕘 **Internet Control Panel**, chương trình sẽ hiện ra các mục chức năng của **IE** có thể giới hạn, bạn chọn khóa các chức năng cần thiết.



III.3. Chỉ cho phép một số ứng dụng được thi hành.

Để cấu hình **Group Policy** chỉ cho phép các người dùng dưới máy trạm chỉ sử dụng được một vài ứng dụng nào đó, trong công cụ **Group Policy Object Editor**, bạn vào **User Configuration** 🕘 **Administrative Templates**. Sau đó nhấp đúp chuột vào mục **Run only allowed windows applications** để chỉ định các phần mềm được phép thi hành.



Tóm tắt

Lý thuyết 3 tiết - Thực hành 5 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về các loại định dạng đĩa, công nghệ lưu trữ mới Dynamic Storage, kỹ thuật nén và mã hóa dữ liệu…	I. Các cấu hình hệ thống tập tin. II. Cấu hình đĩa lưu trữ. III. Sử dụng chương trình Disk Manager. IV. Quản lý việc nén dữ liệu V. Thiết lập hạn ngạch đĩa VI. Mã hóa dữ liệu bằng EFS	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. CẤU HÌNH HỆ THỐNG TẬP TIN.

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. **Windows Server 2003** hỗ trợ ba hệ thống tập tin khác nhau: **FAT16**, **FAT32** và **NTFS5**. Bạn nên chọn **FAT16** hoặc **FAT32** khi máy tính sử dụng nhiều hệ điều hành khác nhau. Nếu bạn định sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS5**. Bảng sau trình bày khả năng của từng hệ thống tập tin trên **Windows Server 2003**:

Khả năng	FAT16	FAT32	NTFS
Hệ điều hành hỗ trợ	Hầu hết các hệ điều hành	Windows 95 OSR2, Windows 98, Windows 2000, 2003	Windows 2000, 2003
Hỗ trợ tên tập tin dài	256 ký tự trên Windows, 8.3 trên Dos	256 ký tự	256 ký tự
Sử dụng hiệu quả đĩa	Không	Có	Có
Hỗ trợ nén đĩa	Không	Không	Có
Hỗ trợ hạn ngạch	Không	Không	Có
Hỗ trợ mã hoá	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật trên mạng	Có	Có	Có
Kích thước Volume tối đa được hỗ trợ	4GB	32GB	1024GB

Trên **Windows Server 2003/Windows 2000/NT**, bạn có thể sử dụng lệnh **CONVERT** để chuyển đổi hệ thống tập tin từ **FAT16, FAT32** thành **NTFS**. Cú pháp của lệnh như sau:

CONVERT [ổ đĩa:] /fs:ntfs

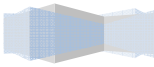
II. CẤU HÌNH ĐĨA LƯU TRỮ.

Windows Server 2003 hỗ trợ hai loại đĩa lưu trữ: **basic** và **dynamic**.

II.1. Basic storage.

Bao gồm các **partition primary** và **extended**. **Partition** tạo ra đầu tiên trên đĩa được gọi là **partition primary** và toàn bộ không gian cấp cho **partition** được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn **partition**. Bạn có thể tạo ba **partition primary** và một **partition extended**. Với **partition extended**,

bạn có thể tạo ra nhiều **partition logical**.



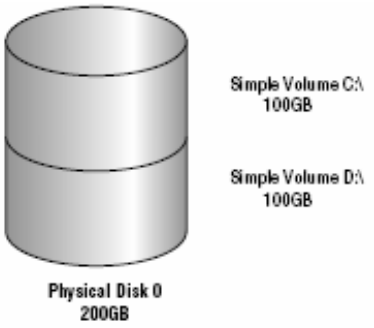
II.2. Dynamic storage

Đây là một tính năng mới của **Windows Server 2003**. Đĩa lưu trữ **dynamic** chia thành các **volume dynamic**. **Volume dynamic** không chứa **partition** hoặc ổ đĩa **logic**, và chỉ có thể truy cập bằng **Windows Server 2003** và **Windows 2000**. **Windows Server 2003/ Windows 2000** hỗ trợ năm loại **volume dynamic**: **simple**, **spanned**, **striped**, **mirrored** và **RAID-5**. Ưu điểm của công nghệ **Dynamic storage** so với công nghệ **Basic storage**:

- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa **logic** (**Volume**).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý để tạo ổ đĩa logic.
- Có thể tạo ra các ổ đĩa **logic** có khả năng dung lỗi cao và tăng tốc độ truy xuất…

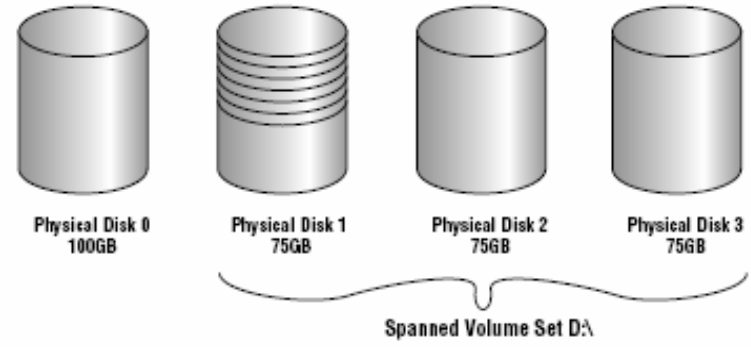
II.2.1 Volume simple.

Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục. Hình sau minh hoạ một đĩa vật lý được chia thành hai **volume** đơn giản.



II.2.2 Volume spanned.

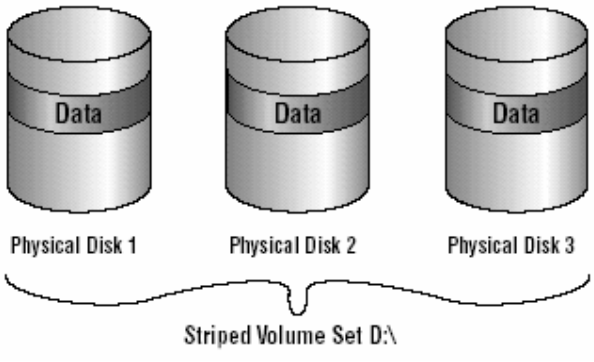
Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi bạn muốn tăng kích cỡ của **volume**. Dữ liệu ghi lên **volume** theo thứ tự, hết đĩa này đến đĩa khác. Thông thường người quản trị sử dụng **volume spanned** khi ổ đĩa đang sử dụng trong **volume** sắp bị đầy và muốn tăng kích thước của **volume** bằng cách bổ sung thêm một đĩa khác.



Do dữ liệu được ghi tuần tự nên **volume** loại này không tăng hiệu năng sử dụng. Nhược điểm chính của **volume spanned** là nếu một đĩa bị hỏng thì toàn bộ dữ liệu trên **volume** không thể truy xuất được.

II.2.3 Volume striped.

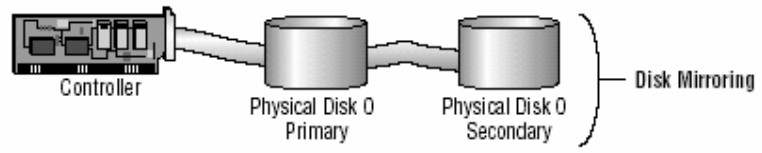
Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên bạn có thể thi hành nhiều tác vụ **I/O** đồng thời, làm tăng tốc độ truy xuất dữ liệu. Thông thường, người quản trị mạng sử dụng **volume striped** để kết hợp dung lượng của nhiều ổ đĩa vật lý thành một đĩa **logic** đồng thời tăng tốc độ truy xuất.



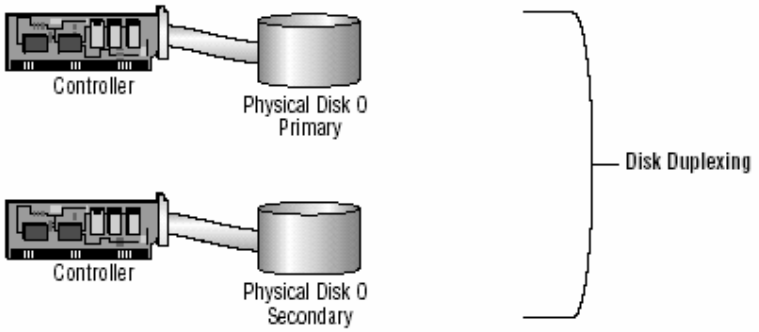
Nhược điểm chính của **volume striped** là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ **volume** mất giá trị.

II.2.4 Volume mirrored.

Là hai bản sao của một **volume** đơn giản. Bạn dùng một ổ đĩa chính và một ổ đĩa phụ. Dữ liệu khi ghi lên đĩa chính đồng thời cũng sẽ được ghi lên đĩa phụ. **Volume** dạng này cung cấp khả năng dung lỗi tốt. Nếu một đĩa bị hỏng thì ổ đĩa kia vẫn làm việc và không làm gián đoạn quá trình truy xuất dữ liệu. Nhược điểm của phương pháp này là bộ điều khiển đĩa phải ghi lần lượt lên hai đĩa, làm giảm hiệu năng.



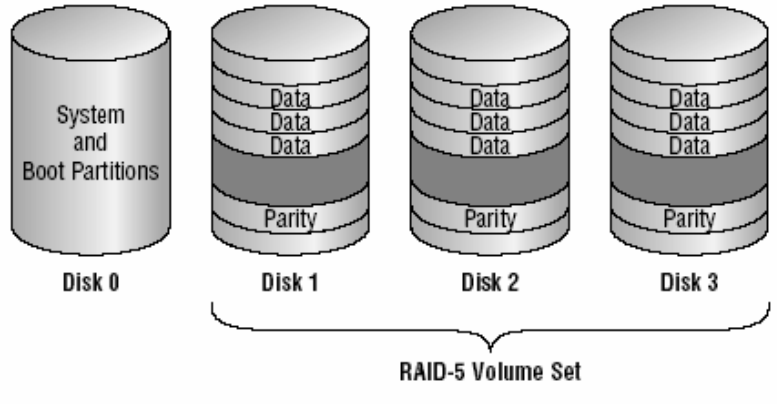
Để tăng tốc độ ghi đồng thời cũng tăng khả năng dung lỗi, bạn có thể sử dụng một biến thể của **volume mirrored** là **duplexing**. Theo cách này bạn phải sử dụng một bộ điều khiển đĩa khác cho ổ đĩa thứ hai.



Nhược điểm chính của phương pháp này là chi phí cao. Để có một **volume 4GB** bạn phải tốn đến **8GB** cho hai ổ đĩa.

II.2.5 Volume RAID-5.

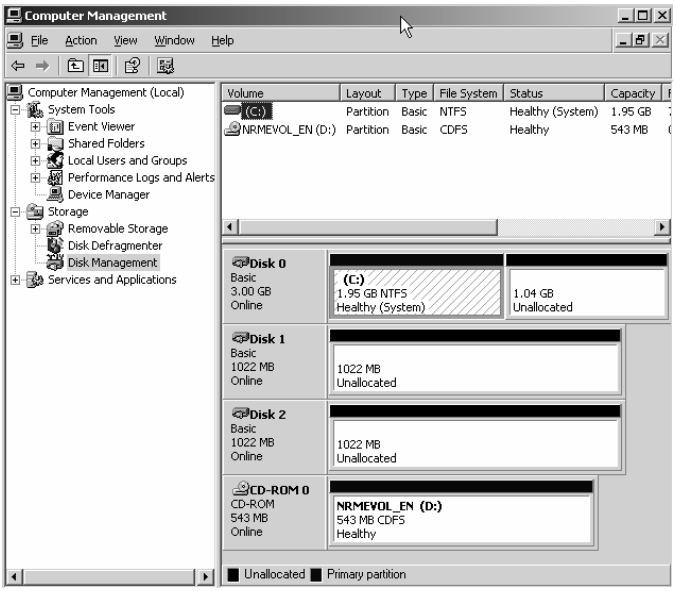
Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**. Nếu một đĩa của **volume** bị hỏng thì thông tin **parity** ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. **Volume RAID-5** sử dụng ít nhất ba ổ đĩa (tối đa là 32).



Ưu điểm chính của kỹ thuật này là khả năng dung lỗi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

III. SỬ DỤNG CHƯƠNG TRÌNH DISK MANAGER.

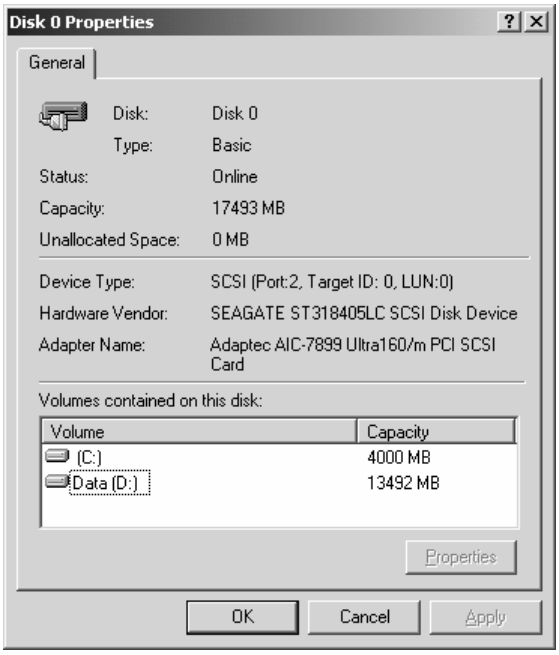
Disk Manager là một tiện ích giao diện đồ hoạ phục vụ việc quản lý đĩa và **volume** trên môi trường **Windows 2000** và **Windows Server 2003**. Để có thể sử dụng được hết các chức năng của chương trình, bạn phải đăng nhập vào máy bằng tài khoản **Administrator**. Vào **menu Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Computer Management**. Sau đó mở rộng mục **Storage** và chọn **Disk Management**. Cửa sổ **Disk Management** xuất hiện như sau:



Phần sau sẽ hướng dẫn bạn thực hiện các thao tác căn bản bằng **Disk Manager**.

III.1. Xem thuộc tính của đĩa.

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn **Properties**. Hộp thoại **Disk Properties** xuất hiện như sau:

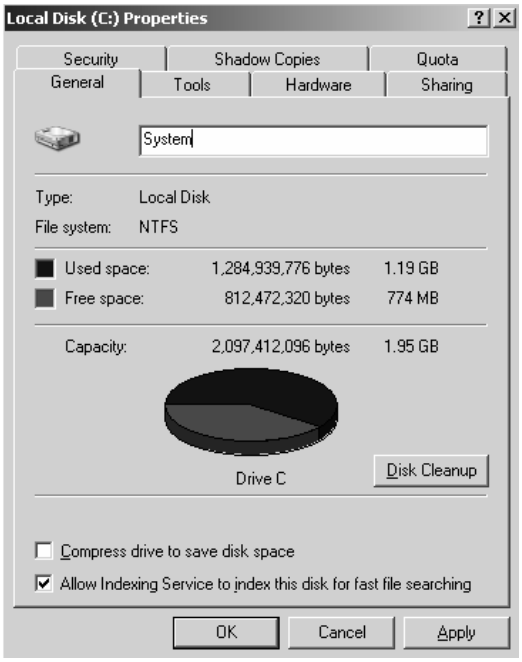


Hộp thoại cung cấp các thông tin:

- Số thứ tự của ổ đĩa vật lý
- Loại đĩa (**basic**, **dynamic**, **CD-ROM**, **DVD,** đĩa chuyển dời được, hoặc **unknown**)
- Trạng thái của đĩa (**online** hoặc **offline**)
- Dung lượng đĩa
- Lượng không gian chưa cấp phát
- Loại thiết bị phần cứng
- Nhà sản xuất thiết bị
- Tên của **adapter**
- Danh sách các **volume** đã tạo trên đĩa

III.2. Xem thuộc tính của volume hoặc đĩa cục bộ.

Trên một ổ đĩa **dynamic**, bạn sử dụng các **volume**. Ngược lại trên một ổ đĩa **basic**, bạn sử dụng các đĩa cục bộ (**local disk**). **Volume** và đĩa cục bộ đều có chức năng như nhau, do vậy các phần sau dựa vào đĩa cục bộ để minh hoạ. Để xem thuộc tính của một đĩa cục bộ, bạn nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties** và hộp thoại **Local Disk Properties** xuất hiện.

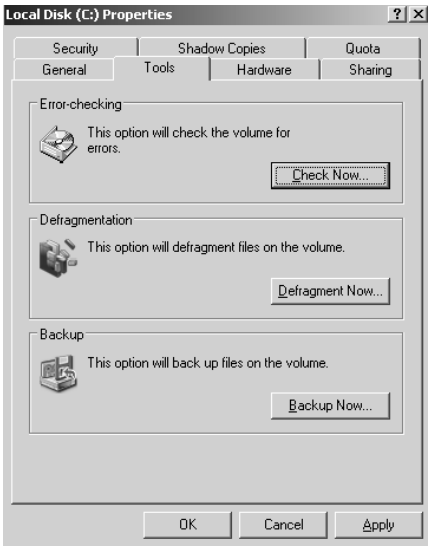


III.2.1 Tab General.

Cung cấp các thông tin như nhãn đĩa, loại, hệ thống tập tin, dung lượng đã sử dụng, còn trống và tổng dung lượng. Nút **Disk Cleanup** dùng để mở chương trình **Disk Cleanup** dùng để xoá các tập tin không cần thiết, giải phóng không gian đĩa.

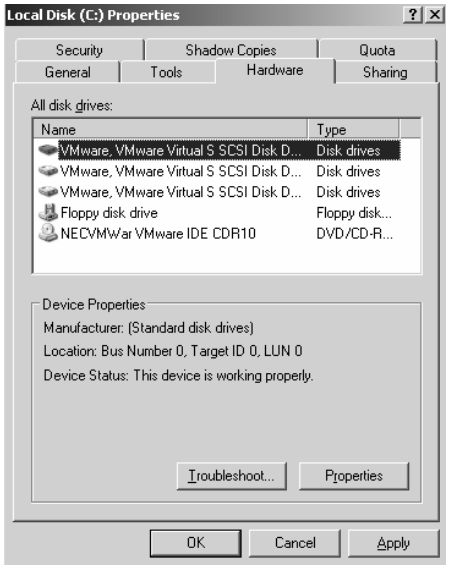
III.2.2 Tab Tools.

Bấm nút **Check Now** để kích hoạt chương trình **Check Disk** dùng để kiểm tra lỗi như khi không thể truy xuất đĩa hoặc khởi động lại máy không đúng cách. Nút **Backup Now** sẽ mở chương trình **Backup Wizard**, hướng dẫn bạn các bước thực hiện việc sao lưu các tập tin và thư mục trên đĩa. Nút **Defragment Now** mở chương trình **Disk Defragment**, dùng để dồn các tập tin trên đĩa thành một khối liên tục, giúp ích cho việc truy xuất đĩa.



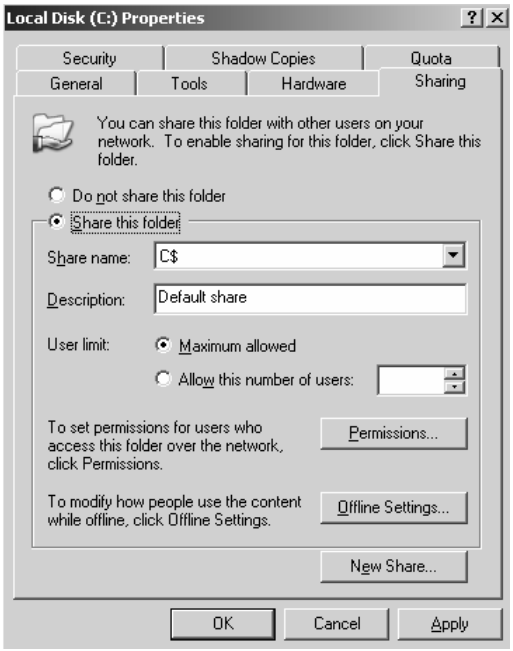
III.2.3 Tab Hardware.

Liệt kê các ổ đĩa vật lý **Windows Server 2003** nhận diện được. Bên dưới danh sách liệt kê các thuộc tính của ổ đĩa được chọn.



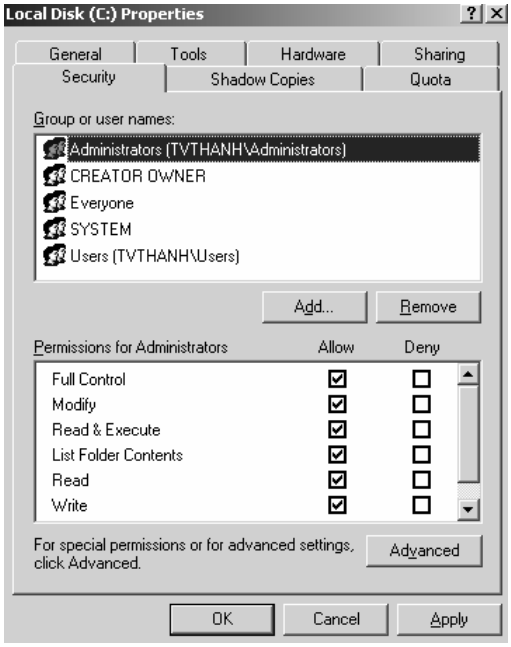
III.2.4 Tab Sharing.

Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này. Theo mặc định, tất cả các ổ đĩa cục bộ đều được chia sẻ dưới dạng ẩn (có dấu **$** sau tên chia sẻ).



III.2.5 Tab Security.

Chỉ xuất hiện khi đĩa cục bộ này sử dụng hệ thống tập tin **NTFS**. Dùng để thiết lập quyền truy cập lên đĩa. Theo mặc định, nhóm **Everyone** được toàn quyền trên thư mục gốc của đĩa.

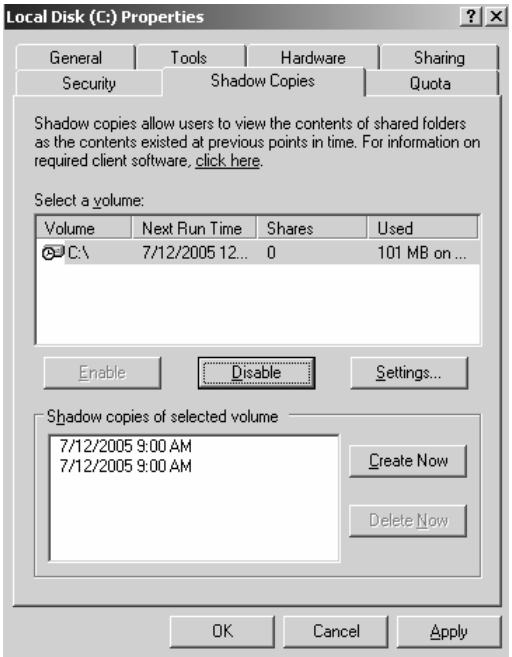


III.2.6 Tab Quota.

Chỉ xuất hiện khi sử dụng **NTFS**. Dùng để quy định lượng không gian đĩa cấp phát cho người dùng.

III.2.7 Shadow Copies.

Shadow Copies là dịch vụ cho phép người dùng truy cập hoặc khôi phục những phiên bản trước đây của những tập tin đã lưu, bằng cách dùng một tính năng ở máy trạm gọi là **Previous Versions**.



III.3. Bổ sung thêm một ổ đĩa mới.

III.3.1 Máy tính không hỗ trợ tính năng “hot swap”.

Bạn phải tắt máy tính rồi mới lắp ổ đĩa mới vào. Sau đó khởi động máy tính lại. Chương trình **Disk Management** sẽ tự động phát hiện và yêu cầu bạn ghi một chữ ký đặc biệt lên ổ đĩa, giúp cho **Windows Server 2003** nhận diện được ổ đĩa này. Theo mặc định, ổ đĩa mới được cấu hình là một đĩa **dynamic**.

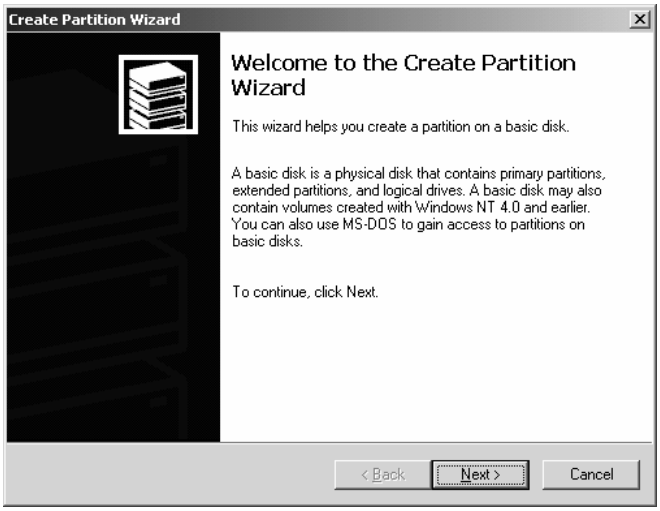
III.3.2 Máy tính hỗ trợ "hot swap".

Bạn chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng **Action** ◴ **Rescan Disk** của **Disk Manager** để phát hiện ổ đĩa mới này.

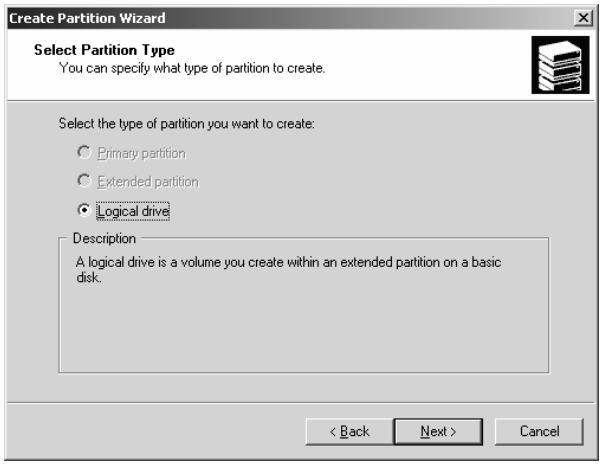
III.4. Tạo partition/volume mới.

Nếu bạn còn không gian chưa cấp phát trên một đĩa **basic** thì bạn có thể tạo thêm **partition** mới, còn trên đĩa **dynamic** thì bạn có thể tạo thêm **volume** mới. Phần sau hướng dẫn bạn sử dụng **Create Partition Wizard** để tạo một **partition** mới:

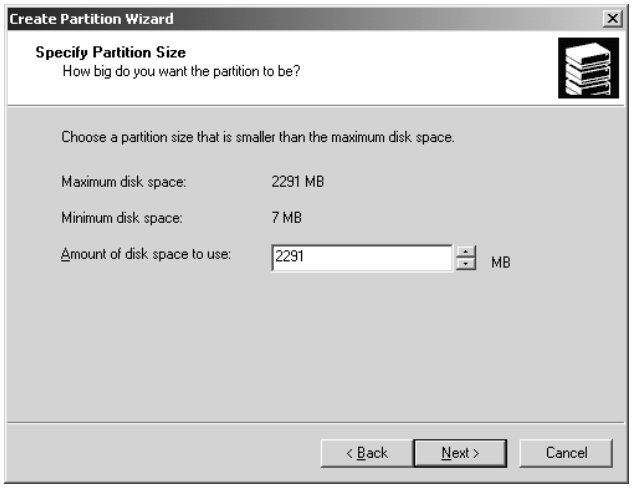
Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa **basic** và chọn **Create Logical Drive**.



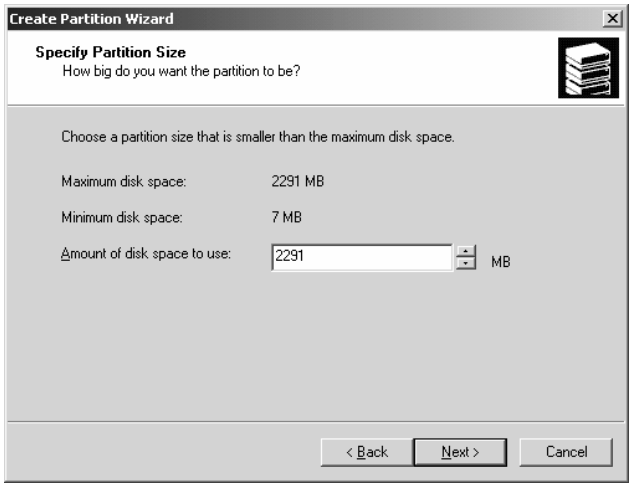
Xuất hiện hộp thoại **Create Partition Wizard**. Nhấn nút **Next** trong hộp thoại này.



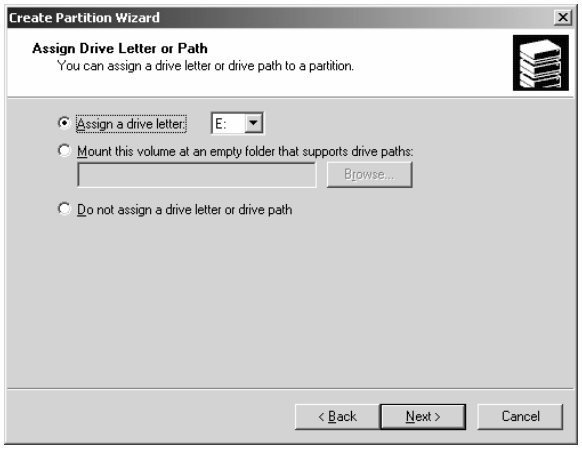
Trong hộp thoại **Select Partition Type**, chọn loại **partition** mà bạn định tạo. Chỉ có những loại còn khả năng tạo mới được phép chọn (tuỳ thuộc vào ổ đĩa vật lý của bạn). Sau khi chọn loại **partition** xong nhấn **Next** để tiếp tục.



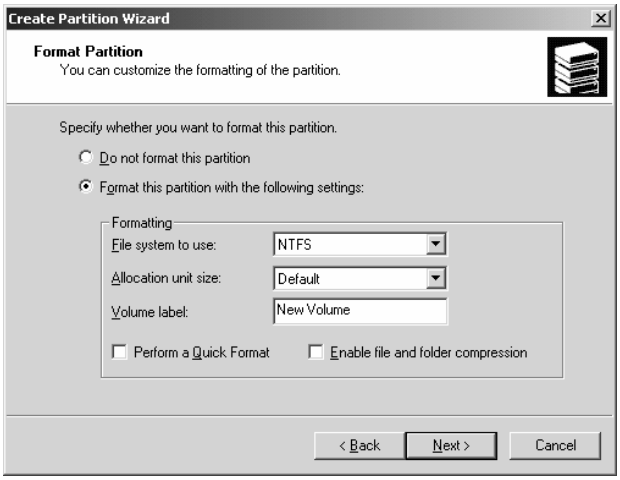
Tiếp theo, hộp thoại **Specify Partition Size** yêu cầu bạn cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn **Next**.



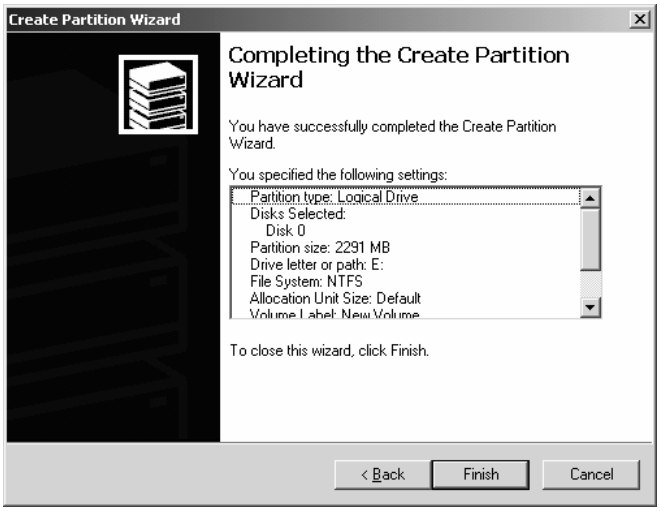
Trong hộp thoại **Assign Drive Letter or Path**, bạn có thể đặt cho **partition** này một ký tự ổ đĩa, hoặc gắn (**mount**) vào một thư mục rỗng, hoặc không làm đặt gì hết. Khi bạn chọn kiểu gắn vào một thư mục rỗng thì bạn có thể tạo ra vô số **partition** mới. Sau khi đã quyết định xong, nhấn **Next** để tiếp tục.



Hộp thoại **Format Partition** yêu cầu bạn quyết định có định dạng **partition** này không. Nếu có thì dùng hệ thống tập tin là gì? đơn vị cấp phát là bao nhiêu? nhãn của **partition** (**volume label**) là gì? có định dạng nhanh không? Có nén tập tin và thư mục không? Sau khi đã chọn xong, nhấn **Next** để tiếp tục.

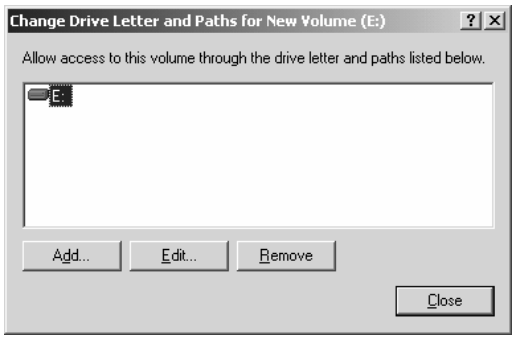


Hộp thoại **Completing** the **Create Partition Wizard** tóm tắt lại các thao tác sẽ thực hiện, bạn phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn **Finish** để bắt đầu thực hiện.



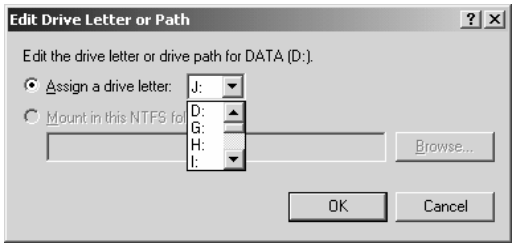
III.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn.

Muốn thay đổi ký tự ổ đĩa cho **partition/volume** nào, bạn nhấp phải chuột lên **volume** đó và chọn **Change Drive Letter and Path**. Hộp thoại **Change Drive Letter and Path** xuất hiện.



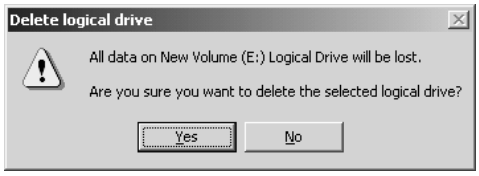
Trong hộp thoại này, nhấn nút **Edit** để mở tiếp hộp thoại **Edit Drive Letter and Path**, mở danh sách **Assign a drive letter** và chọn một ký tự ổ đĩa mới định đặt cho **partition/volume** này. Cuối cùng đồng

ý xác nhận các thay đổi đã thực hiện.



III.6. Xoá partition/volume.

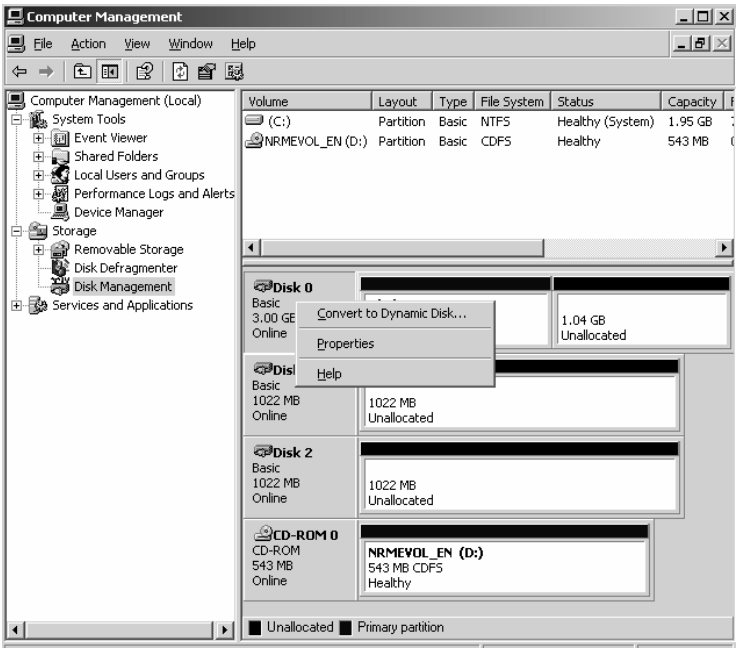
Để tổ chức lại một ổ đĩa hoặc huỷ các dữ liệu có trên một **partition/volume**, bạn có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, bạn nhấp phải chuột lên **partition/volume** muốn xoá và chọn **Delete Partition** (hoặc **Delete Volume**). Một hộp thoại cảnh báo xuất hiện, thông báo dữ liệu trên **partition** hoặc **volume** sẽ bị xoá và yêu cầu bạn xác nhận lại lần nữa thao tác này.



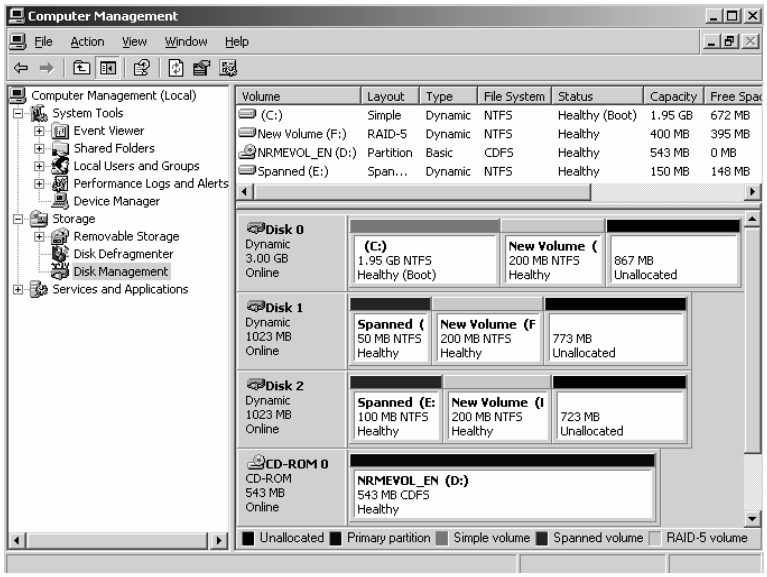
III.7. Cấu hình Dynamic Storage.

III.7.1 Chuyển chế độ lưu trữ.

Để sử dụng được cơ chế lưu trữ **Dynamic**, bạn phải chuyển đổi các đĩa cứng vật lý trong hệ thống thành **Dynamic Disk**. Trong công cụ **Computer Management** ⏲ **Disk Management**, bạn nhấp phải chuột trên các ổ đĩa bên của sổ bên phải và chọn **Convert to Dynamic Disk….** Sau đó đánh dấu vào tất cả các đĩa cứng vật lý cần chuyển đổi chế độ lưu trữ và chọn **OK** để hệ thống chuyển đổi. Sau khi chuyển đổi xong hệ thống sẽ yêu cầu bạn **restart** máy để áp dụng chế độ lưu trữ mới.

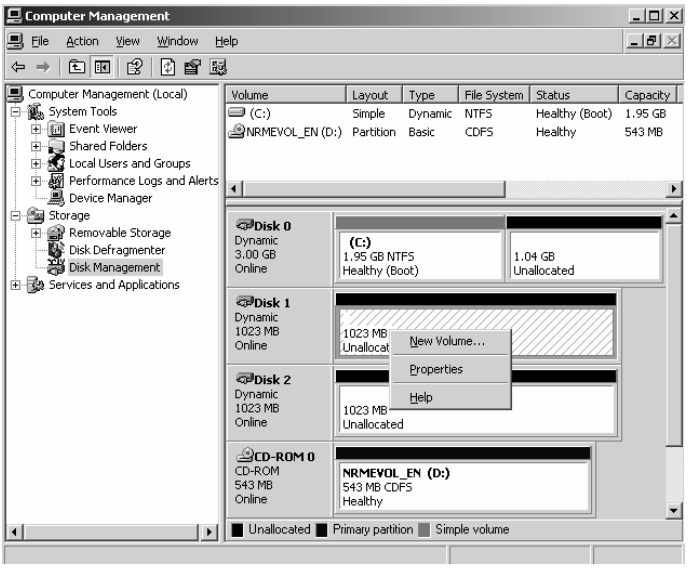


Các loại **Volume** mà chúng ta sẽ tạo ở phần sau:

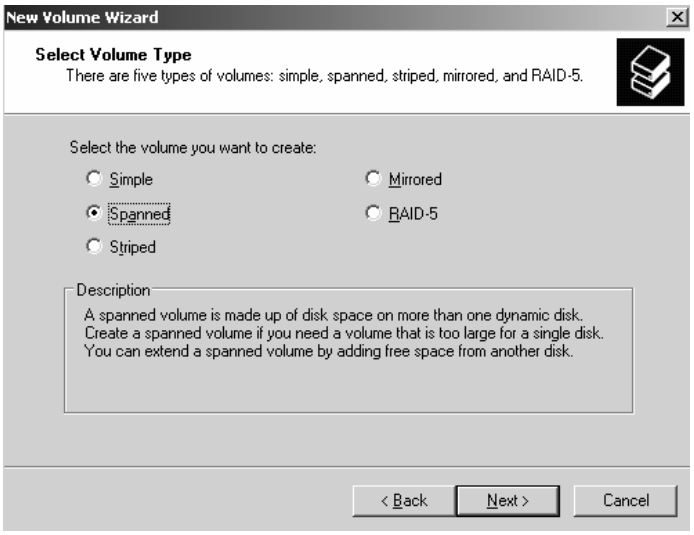


III.7.2 Tạo Volume Spanned.

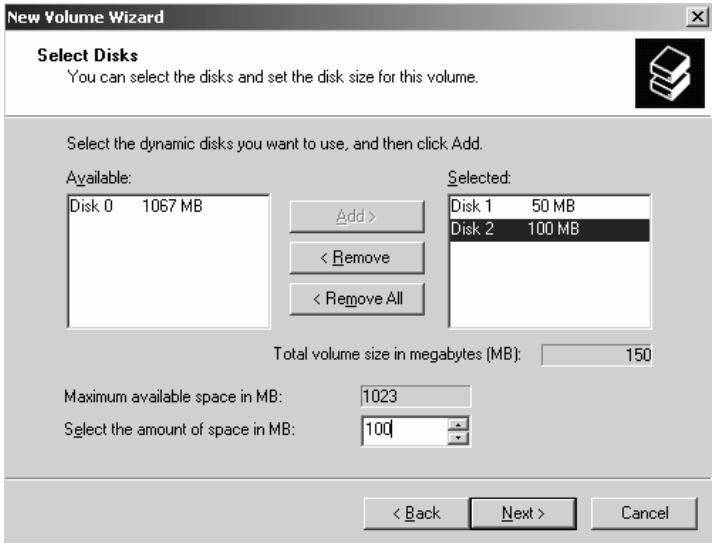
Trong công cụ **Disk Management**, bạn nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume**, sau đó chọn **New Volume.**



Tiếp theo, bạn chọn loại **Volume** cần tạo. Trong trường hợp này chúng ta chọn **Spanned**.

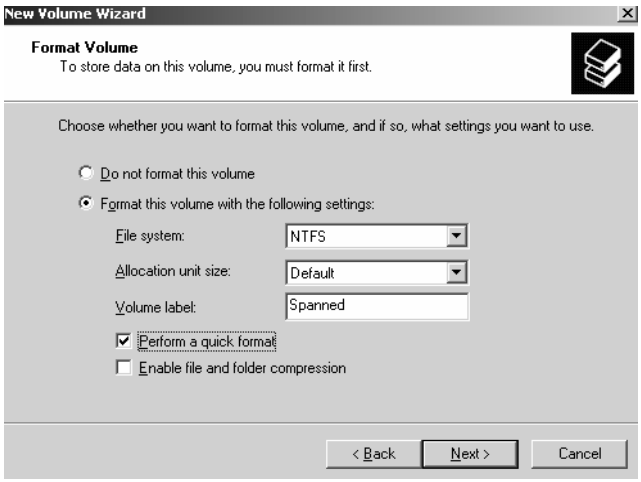


Bạn chọn những đĩa cứng dùng để tạo **Volume** này, đồng thời bạn cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**. Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau.



Bạn gán ký tự ổ đĩa cho **Volume**.

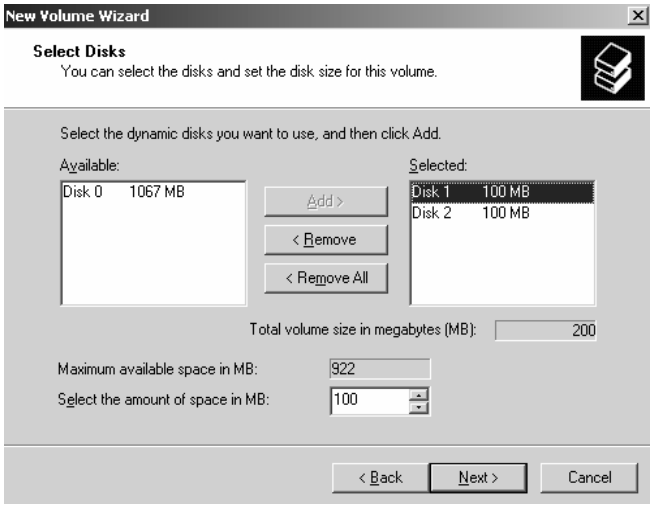
Bạn định dạng **Volume** mà bạn vừa tạo để có thể chứa dữ liệu.



Đến đây đã hoàn thành việc tạo **Volume**, bạn có thể lưu trữ dữ liệu trên **Volume** này theo cơ chế đã trình bày ở phần lý thuyết.

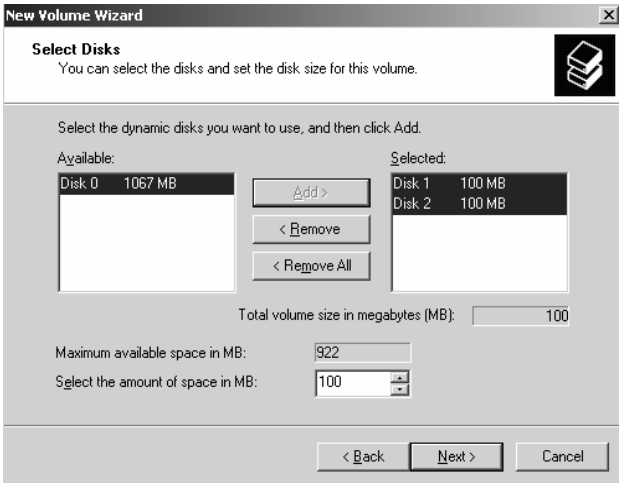
III.7.3 Tạo Volume Striped.

Các bước tạo **Volume Striped** cũng tương tự như việc tạo các **Volume** khác nhưng chú ý là kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng tổng các kích thước của các phần trên.



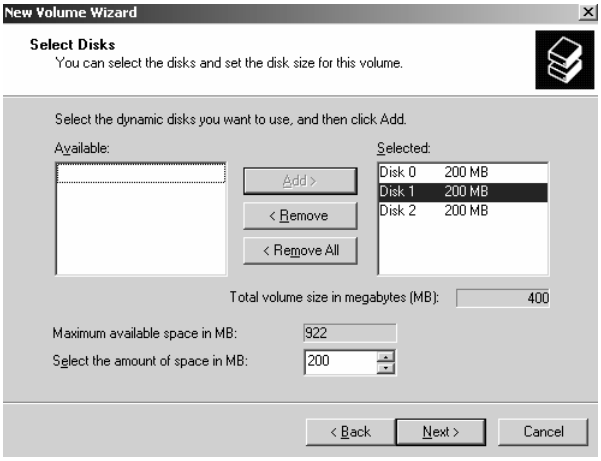
III.7.4 Tạo Volume Mirror.

Các bước tạo **Volume Mirror** cũng tương tự như trên, chú ý kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng chính kích thước của mỗi phần trên.



III.7.5 Tạo Volume Raid-5.

Các bước tạo **Volume Raid-5** cũng tương tự như trên nhưng chú ý là loại **Volume** yêu cầu tối thiểu đến 3 đĩa cứng. Kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng 2/3 kích thước của mỗi phần cộng lại.

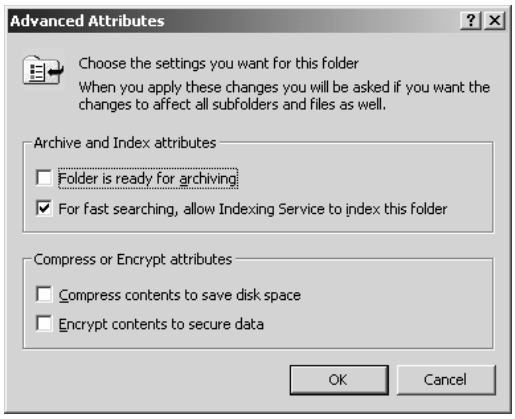


IV. QUẢN LÝ VIỆC NÉN DỮ LIỆU.

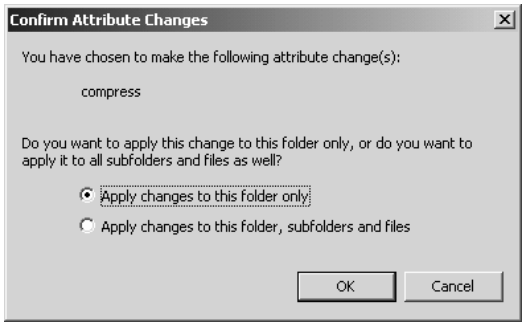
Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server 2003** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén khi mở tập tin và nén lại khi lưu tập tin lên đĩa. Khả năng này chỉ có trên các **partition NTFS**. Nếu bạn chép một tập tin/thư mục trên một **partition** có tính năng nén sang một partition **FAT** bình thường thì hệ điều hành sẽ giải nén tập tin/thư mục đó trước khi chép đi.

Để thi hành việc nén một tập tin/thư mục, bạn sử dụng chương trình **Windows Explorer** và thực hiện theo các bước sau:

- Trong cửa sổ **Windows Explorer**, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.
- Nhấp phải chuột lên đối tượng đó và chọn **Properties**.
- Trong hộp thoại **Properties**, nhấn nút **Advanced** trong **tab General**.
- Trong hộp thoại **Advanced Properties**, chọn mục "**Compress contents to save disk space**" và nhấn chọn **OK**.



Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu bạn định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu bạn lựa chọn hoặc là chỉ nén thư mục này thôi (**Apply changes to this folder only**) hoặc nén cả các thư mục con và tập tin có trong thư mục (**Apply changes to this folder, subfolders and files**). Thực hiện lựa chọn của bạn và nhấn **OK**.



Để thực hiện việc giải nén một thư mục/tập tin, bạn thực hiện tương tự theo các bước ở trên và bỏ chọn mục **Compress contents to save disk space** trong hộp thoại **Advanced Properties**.

V. THIẾT LẬP HẠN NGẠCH ĐĨA (DISK QUOTA).

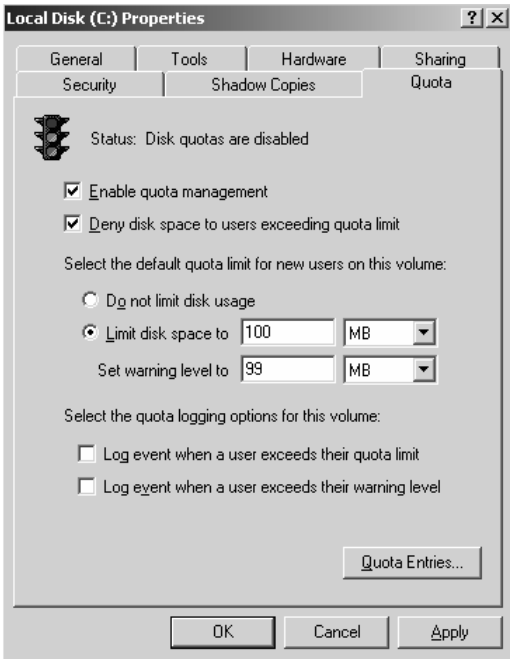
Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề bạn phải lưu ý khi thiết lập hạn ngạch đĩa:

- Chỉ có thể áp dụng trên các volume **NTFS**.
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.
- Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên **volume**.
- Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin/thư mục được nén.

V.1. Cấu hình hạn ngạch đĩa.

Bạn cấu hình hạn ngạch đĩa bằng hộp thoại **Volume Propertise** đã giới thiệu trong phần trên. Bạn cũng có thể mở hộp thoại này bằng cách nhấp phải chuột lên ký tự ổ đĩa trong **Windows Explorer** và chọn **Propertise**. Trong hộp thoại này nhấp chọn **tab Quota**. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.



Các mục trong hộp thoại có ý nghĩa như sau:

- **Enable quota management**: thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.
- **Deny disk space to users exceeding quota limit**: người dùng sẽ không thể tiếp tục sử dụng đĩa khi vượt quá hạn ngạch và nhận được thông báo **out of disk space.**
- **Select the default quota limit for new users on this volume**: định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm "không định nghĩa giới hạn" (**Do not limit disk space**), "giới hạn cho phép" (**Limit disk space to**) và "giới hạn cảnh báo" (**Set warning level to**).
- **Select the quota logging options for this volume**: có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.
- Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:
- Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.
- Đèn vàng cho biết **Windows Server 2003** đang xây dựng lại thông tin hạn ngạch.
- Đèn xanh cho biết tính năng quản lý đang có tác dụng.

V.2. Thiết lập hạn ngạch mặc định.

Khi bạn thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu bạn dự định áp đặt hạn ngạch cho tất cả các người dùng, bạn phải chỉ định hạn ngạch ngay từ khi tạo lập **volume**.

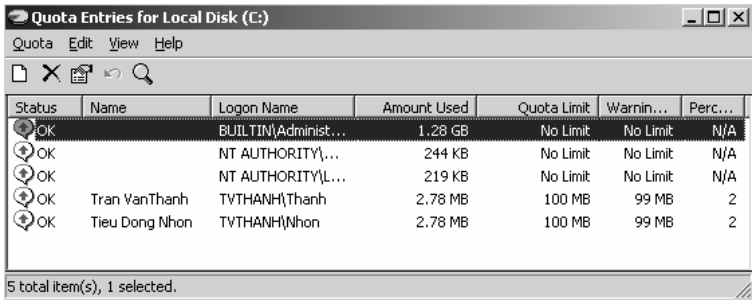
Để thực hiện, bạn mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

V.3. Chỉ định hạn ngạch cho từng cá nhân.

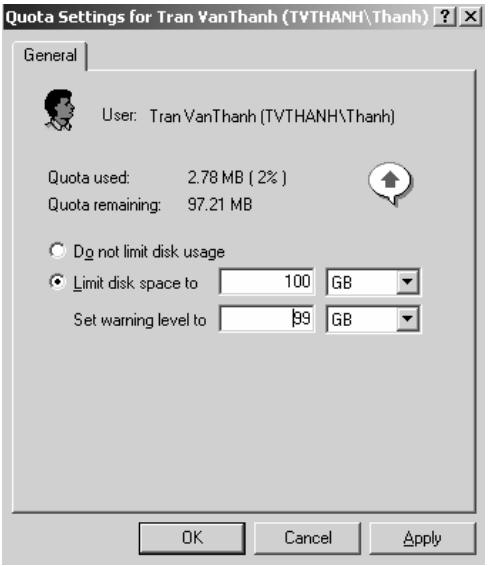
Trong một vài trường hợp, bạn cần phải chỉ định hạn ngạch cho riêng một người nào đó, chẳng hạn có thể là các lý do sau:

- Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.
- Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Bạn phải tạo riêng một giới hạn mới áp dụng cho người đó.

Để thiết lập, nhấn nút **Quota Entries** trong tab **Quota** của hộp thoại **Volume Properties**. Cửa sổ **Quota Entries** xuất hiện.



Chỉnh sửa thông tin hạn ngạch của một người dùng: nhấn đúp vào mục của người dùng tương ứng, hộp thoại **Quota Setting** xuất hiện cho phép bạn thay đổi các giá trị hạn ngạch.



Bổ sung thêm một mục quy định hạn ngạch: trong cửa sổ **Quota Entries**, vào menu **Quota** chọn mục **New Quota Entry** ⏲ xuất hiện hộp thoại **Select Users**, bạn chọn người dùng rồi nhấn **OK** ⏲ xuất hiện hộp thoại **Add New Quota Entry**, bạn nhập các giá trị hạn ngạch thích hợp và nhấn **OK**.

VI. MÃ HOÁ DỮ LIỆU BẰNG EFS.

EFS (Encrypting File System) là một kỹ thuật dùng trong **Windows Server 2003** dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì bị từ chối truy cập. Ngoài ra, người quản trị mạng còn có thể dùng tác nhân phục hồi (**recovery agent**) để truy xuất đến bất kỳ tập tin nào bị mã hoá. Để mã hoá các tập tin, tiến hành theo các bước sau:

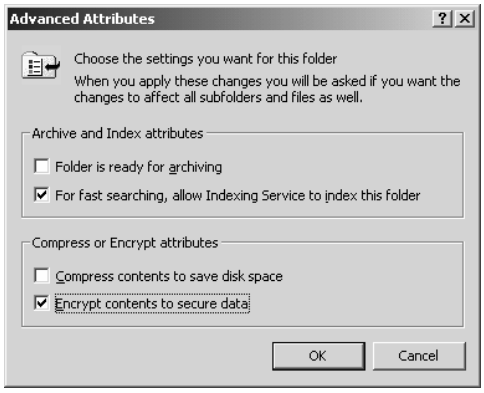
Mở cửa sổ **Windows Explorer**.

Trong cửa sổ **Windows Explorer**, chọn các tập tin và thực mục cần mã hoá.

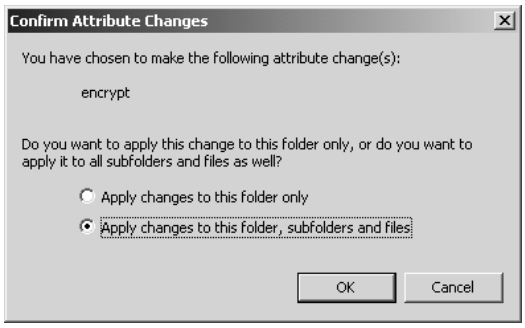
Nhấp phải chuột lên các tập tin và thư mục, chọn **Properties**.

Trong hộp thoại **Properties**, nhấn nút **Advanced**.

Hộp thoại **Advanced Properties** xuất hiện, đánh dấu mục **Encrypt contents to secure data** và nhấn OK.



Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cần bạn cho biết sẽ mã hoá chỉ riêng thư mục được chọn (**Apply changes to this folder only**) hoặc mã hoá toàn bộ thư mục kể các các thư mục con (**Apply changes to this folder, subfolders and files**). Sau đó nhấn **OK**.



Để thôi không mã hoá các tập tin, bạn thực hiện tương tự theo các bước trên nhưng bỏ chọn mục **Encrypt contents to secure data**.

Bài 14
TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG

Tóm tắt

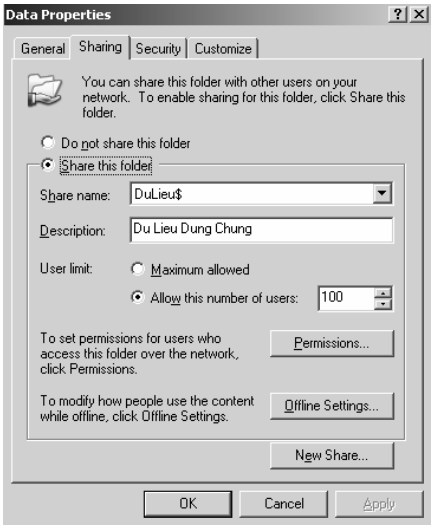
Lý thuyết 4 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về các loại quyền truy cập, tạo và quản lý các thư mục dùng chung trên mạng, NTFS, DFS…	I. Tạo các thư mục dùng chung. II. Quản lý các thư mục dùng chung. III. Quyền truy cập NTFS. IV. DFS.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. TẠO CÁC THƯ MỤC DÙNG CHUNG.

I.1. Chia sẻ thư mục dùng chung.

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, bạn phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** bạn nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.



Ý nghĩa của các mục trong **Tab Sharing**:

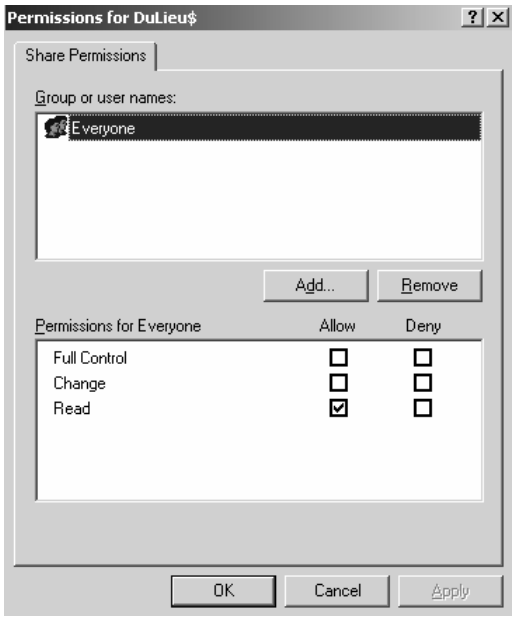
Mục	Mô tả
Do not share this folder	Chỉ định thư mục này chỉ được phép truy cập cục bộ
Share this folder	Chỉ định thư mục này được phép truy cập cục bộ và truy cập qua mạng
Share name	Tên thư mục mà người dùng mạng nhìn thấy và truy cập
Comment	Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này
User Limit	Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm
Permissions	Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng
Offline Settings	Cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ **Offline**.

I.2. Cấu hình Share Permissions.

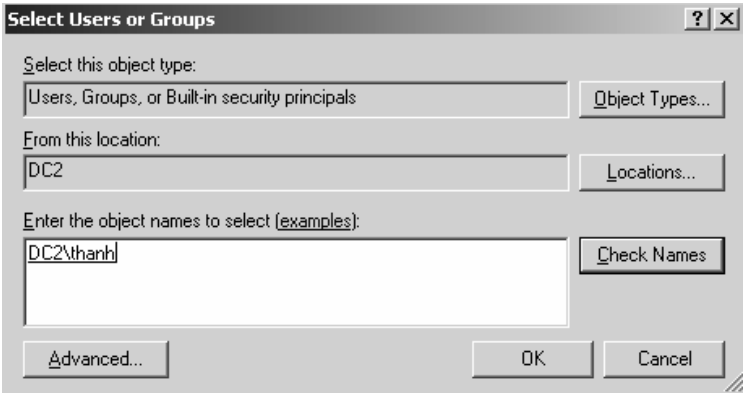
Bạn muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng **Share Permissions**. **Share Permissions** chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với **NTFS Permissions** là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa. Trong hộp thoại **Share Permissions**, chứa danh sách các quyền sau:

- **Full Control**: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- **Change**: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- **Read**: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ.

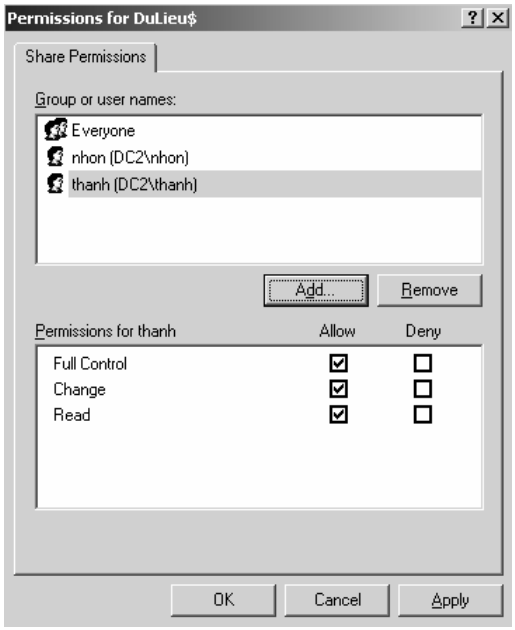
Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.



Hộp thoại chọn người dùng và nhóm xuất hiện, bạn nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**.



Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng bạn đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.



I.3. Chia sẻ thư mục dùng lệnh netshare.

Chức năng: tạo, xóa và hiển thị các tài nguyên chia sẻ.

Cú pháp:

net share sharename

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

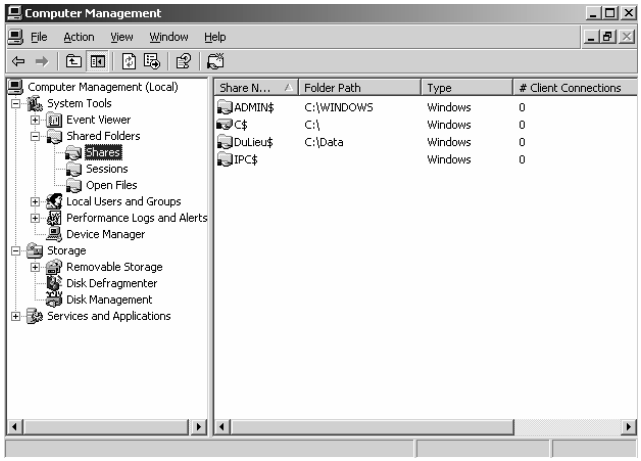
Ý nghĩa các tham số:

- [Không tham số]: hiển thị thông tin về tất cả các tài nguyên chia sẻ trên máy tính cục bộ
- [**Sharename**]: tên trên mạng của tài nguyên chia sẻ, nếu dùng lệnh **net share** với một tham số **sharename** thì hệ thống sẽ hiển thị thông tin về tài nguyên dùng chung này.
- [**drive:path**]: chỉ định đường dẫn tuyệt đối của thư mục cần chia sẻ.
- [**/users:number**]: đặt số lượng người dùng lớn nhất có thể truy cập vào tài nguyên dùng chung này.
- [**/unlimited**]: không giới hạn số lượng người dùng có thể truy cập vào tài nguyên dùng chung này.
- [**/remark:"text"**]: thêm thông tin mô tả về tài nguyên này.
- **/delete**: xóa thuộc tính chia sẻ của thư mục hiện tại.

II. QUẢN LÝ CÁC THƯ MỤC DÙNG CHUNG.

II.1. Xem các thư mục dùng chung.

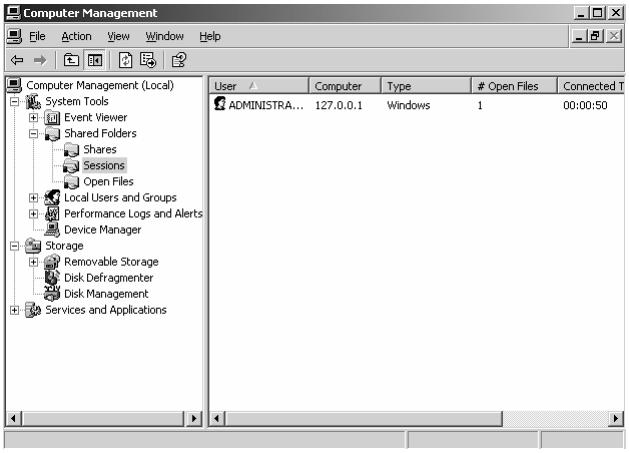
Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu **$** thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua **My Network Places** hoặc duyệt các tài nguyên mạng.



II.2. Xem các phiên làm việc trên thư mục dùng chung.

Muốn xem tất cả các người dùng đang truy cập đến các thư mục dùng chung trên máy tính bạn chọn mục **Session**. Mục **Session** cung cấp các thông tin sau:

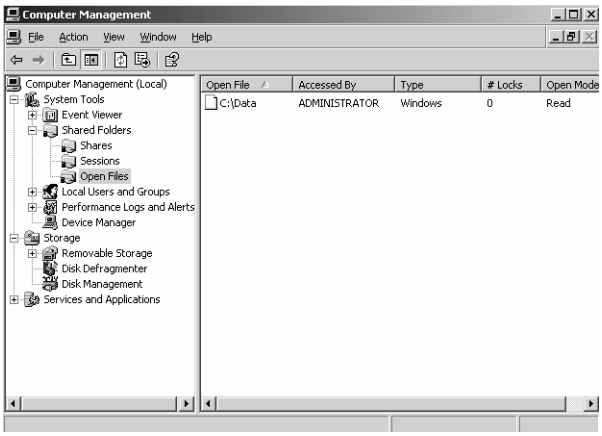
- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Phải là truy cập của người dùng **Guest** không?



II.3. Xem các tập tin đang mở trong các thư mục dùng chung.

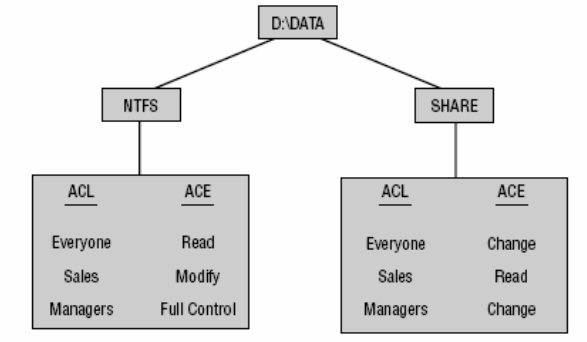
Muốn xem các tập đang mở trong các thư mục dùng chung bạn nhấp chuột vào mục **Open Files**. Mục **Open Files** cung cấp các thông tin sau:

- Đường dẫn và tập tin hiện đang được mở.
- Tên tài khoản người dùng đang truy cập tập tin đó.
- Hệ điều hành mà người dùng sử dụng để truy cập tập tin.
- Trạng thái tập tin có đang bị khoá hay không.
- Trạng thái mở sử dụng tập tin (**Read** hoặc **Write**).



III. QUYỀN TRUY CẬP NTFS.

Có hai loại hệ thống tập được dùng cho **partition** và **volume** cục bộ là **FAT** (bao gồm **FAT16** và **FAT32**). **FAT partition** không hỗ trợ bảo mật nội bộ, còn **NTFS partition** thì ngược lại có hỗ trợ bảo mật; có nghĩa là nếu đĩa cứng của bạn định dạng là **FAT** thì mọi người đều có thể thao tác trên các file chứa trên đĩa cứng này, còn ngược lại là định dạng **NTFS** thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống **Windows Server 2003** dùng các **ACL (Access Control List)** để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên **Active Directory**. Một **ACL** có thể chứa nhiều **ACE (Access Control Entry)** đại diện cho một người dùng hay một nhóm người.



III.1. Các quyền truy cập của NTFS.

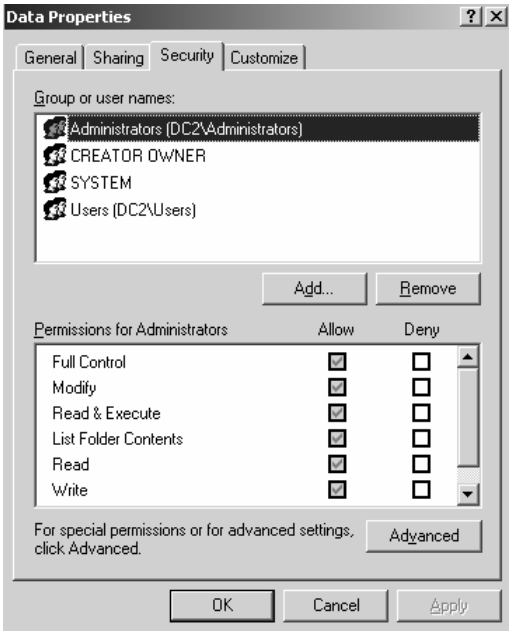
Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	Đọc các thuộc tính mở rộng của các tập tin và thư mục
Create File/Write Data	Tạo các tập tin mới và ghi dữ liệu lên các tập tin này
Create Folder/Append Data	Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin
Write Attributes	Thay đổi thuộc tính của các tập tin và thư mục
Write Extendd Attributes	Thay đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Delete	Xóa các tập tin
Read Permissions	Đọc các quyền trên các tập tin và thư mục
Change Permissions	Thay đổi quyền trên các tập tin và thư mục
Take Ownership	Tước quyền sở hữu của các tập tin và thư mục

III.2. Các mức quyền truy cập được dùng trong NTFS.

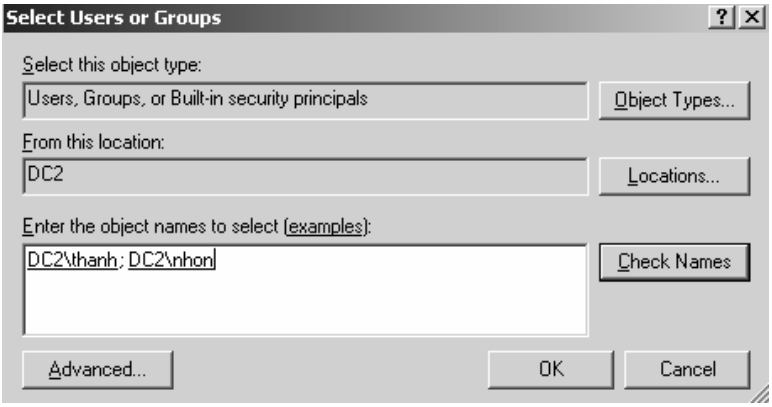
X	X	X	X	X	X	X	X	X	X	X	X	X	
		X	X		X	X	X	X	X	X	X	X	
									X	X	X	X	
		X							X	X	X	X	
		X							X	X	X		
		X			X	X	X						

III.3. Gán quyền truy cập NTFS trên thư mục dùng chung.

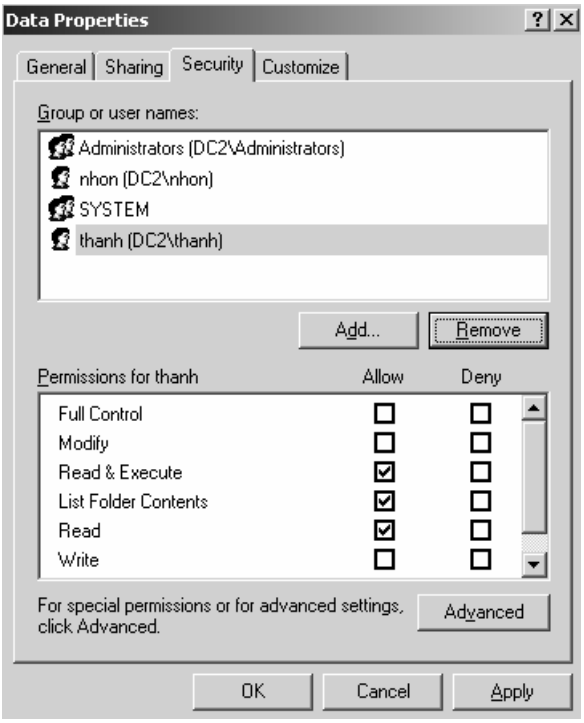
Bạn muốn gán quyền **NTFS**, thông qua **Windows Explorer** bạn nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn **Properties**. Hộp thoại **Properties** xuất hiện. Nếu ổ đĩa của bạn định dạng là **FAT** thì hộp thoại chỉ có hai **Tab** là **General** và **Sharing**. Nhưng nếu đĩa có định dạng là **NTFS** thì trong hộp thoại sẽ có thêm một **Tab** là **Security**. Tab này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người dùng lên các tập tin và thư mục. Bạn nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



Muốn cấp quyền truy cập cho một người dùng, bạn nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, bạn chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.

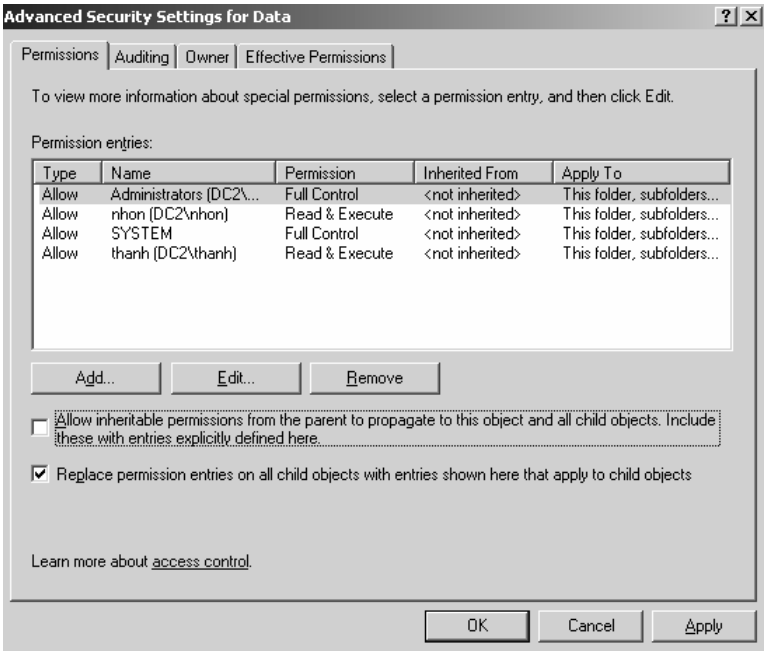


Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà bạn mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, bạn muốn cho người dùng đó có quyền gì thì bạn đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.

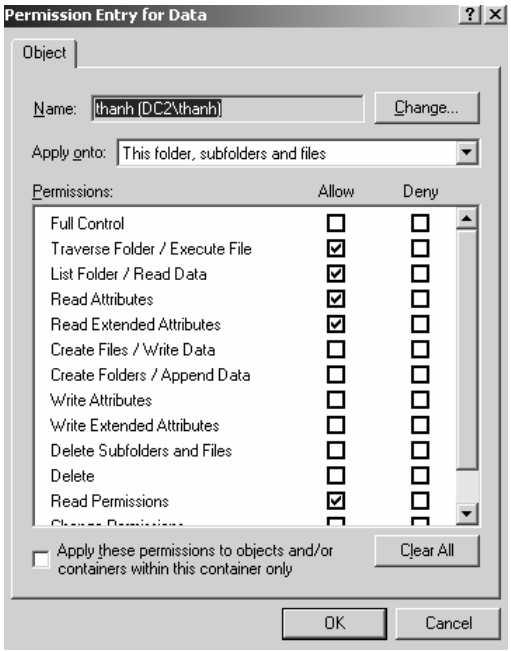


III.4. Kế thừa và thay thế quyền của đối tượng con.

Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút **Advanced** để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút **Advanced**, hộp thoại **Advanced Security Settings** xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục **Allow inheritable permissions from parent to propagate to this object and child objects** thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu bạn đánh dấu vào mục **Replace permission entries on all child objects with entries shown here that apply to child objects** thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cấp giống như các quyền đang hiển thị trong hộp thoại.



Trong hộp thoại này, **Windows Server 2003** cũng cho phép chúng ta kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, bạn chọn nhóm hay người dùng cần thao tác, sau đó nhấp chuột vào nút **Edit.**

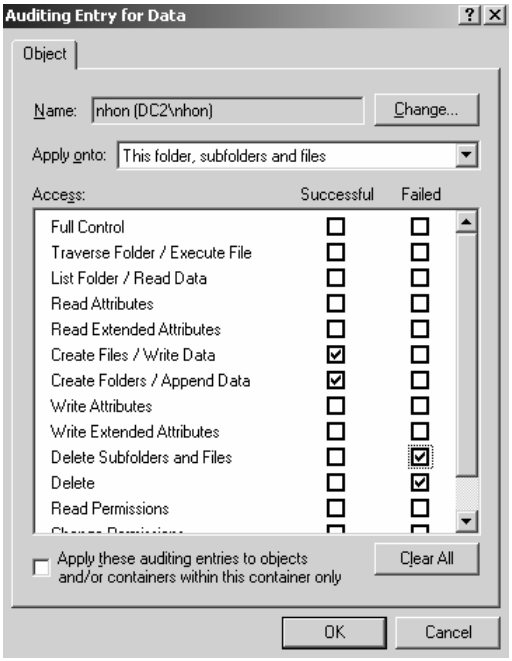


III.5. Thay đổi quyền khi di chuyển thư mục và tập tin.

Khi chúng ta sao chép (**copy**) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (**move**) một tập tin hay thư mục sang bất kì vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

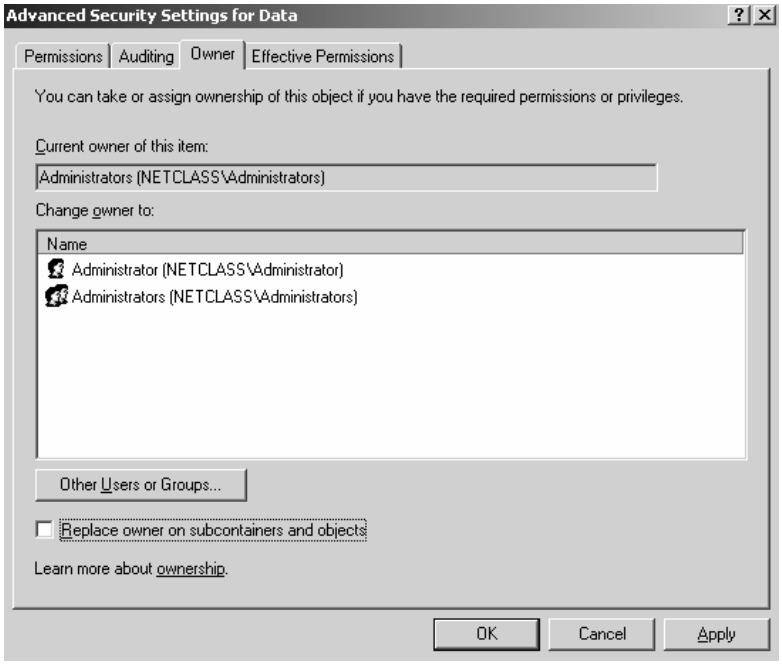
III.6. Giám sát người dùng truy cập thư mục.

Bạn muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó bạn muốn giám sát việc truy xuất thành công thì đánh dấu vào mục **Successful**, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục **Failed**.



III.7. Thay đổi người sở hữu thư mục.

Bạn muốn xem tài khoản người và nhóm người dùng sở hữa thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Owner.** Đồng thời bạn cũng có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút **Other Users or Groups**.



IV. DFS.

DFS (**Distributed File System**) là hệ thống tổ chức sắp xếp các thư mục, tập tin dùng chung trên mạng mà **Server** quản lý, ở đó bạn có thể tập hợp các thư mục dùng chung nằm trên nhiều **Server** khác nhau trên mạng với một tên chia sẻ duy nhất. Nhờ hệ thống này mà người dùng dễ dàng tìm kiếm một tài nguyên dùng chung nào đó trên mạng… **DFS** có hai loại **root**: **domain root** là hệ thống **root** gắn kết vào **Active Directory** được chứa trên tất cả **Domain Controller**, **Stand-alone root** chỉ chứa thông tin ngay tại máy được cấu hình. Chú ý **DFS** không phải là một **File Server** mà nó là chỉ là một "bảng mục lục" chỉ đến các thư mục đã được tạo và chia sẻ sẵn trên các **Server**. Để triển khai một hệ thống **DFS** trước tiên bạn phải hiểu các khái niệm sau:

- Gốc **DFS** (**DFS root**) là một thư mục chia sẻ đại diện cho chung cho các thư mục chia sẻ khác trên các **Server**.
- Liên kết **DFS** (**DFS link**) là một thư mục nằm trong **DFS root**, nó ánh xạ đến một tài nguyên chia sẻ các **Server** khác.

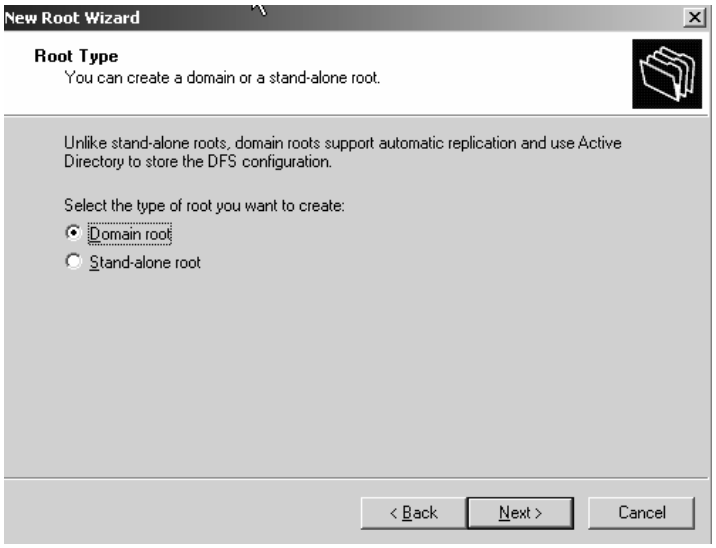
IV.1. So sánh hai loại DFS.

Stand-alone DFS	Fault-tolerant DFs
- Là hệ thống DFS trên một máy **Server Stand-alone**, không có khả năng dung lỗi. - Người dùng truy xuất hệ thống DFS thông qua đường dẫn \\servername\dfsname.	- Là hệ thống **DFS** dựa trên nền **Active Directory** nên có chính dung lỗi cao. - Hệ thống **DFS** sẽ tự động đồng bộ giữa các **Domain Controller** và người dùng có thể truy xuất đến **DFS** thông qua đường dẫn **\\domainname\dfsname**.

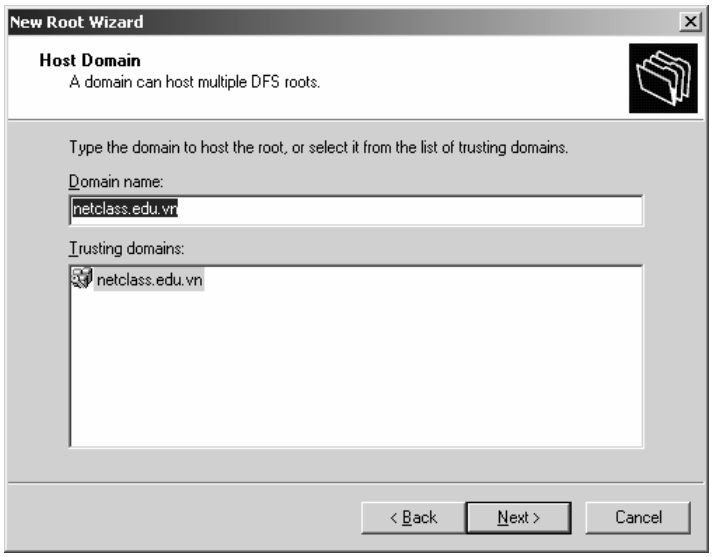
IV.2. Cài đặt Fault-tolerant DFS.

Để tạo một hệ thống **Fault-tolerant DFS** bạn làm theo các bước sau:

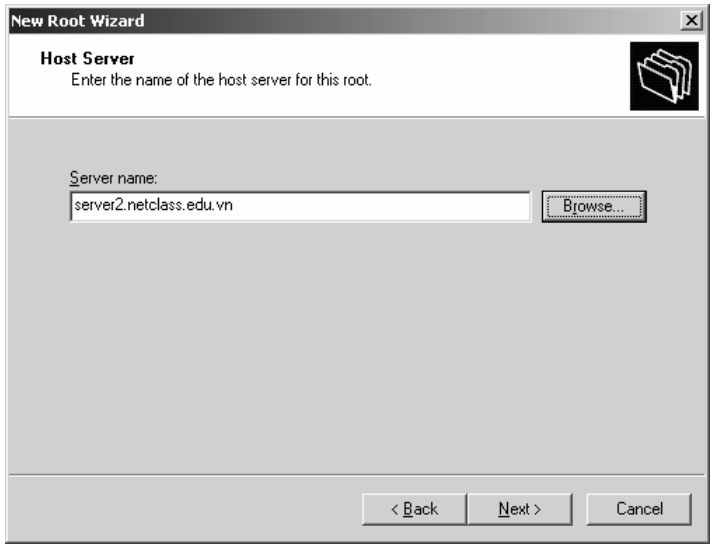
Bạn nhấp chuột vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Distributed File System**. Hộp thoại **Welcome** xuất hiện, bạn nhấn **Next** để tiếp tục. Hộp thoại **Root Type** xuất hiện, bạn chọn mục **Domain Root**, nhấn **Next** để tiếp tục.



Hệ thống yêu cầu bạn chọn tên miền **(domain name**) kết hợp với hệ thống **DFS** cần tạo.

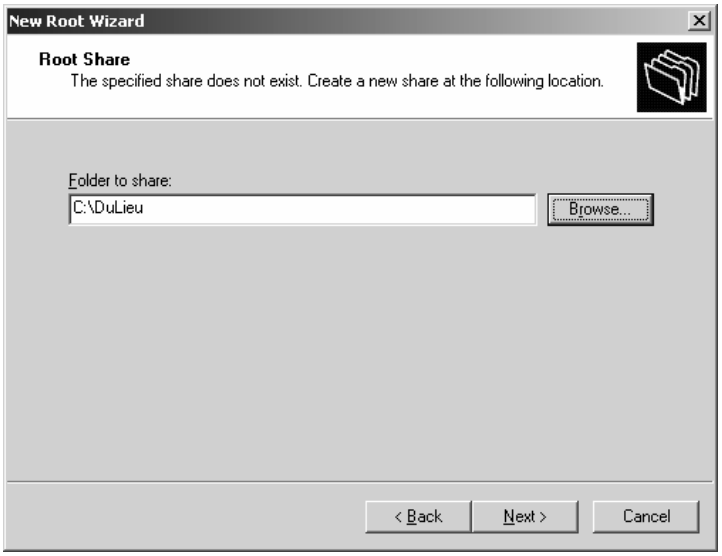


Tiếp theo bạn khai báo tên của **Domain Controller** chưa **root DFS** cần tạo.

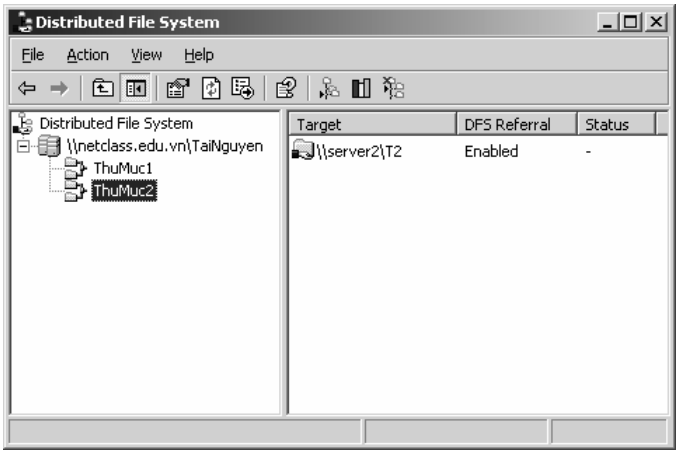


Đến đây bạn khai báo tên chia sẻ gốc (**Root Name**) của hệ thống **DFS**, đây chính là tên chia sẻ đại diện cho các tài nguyên khác trên mạng. Bạn nhập đầy đủ các thông tin chọn **Next** để tiếp tục.

Trong hộp thoại xuất hiện, bạn khai báo tên thư mục chia sẻ gốc của hệ thống **DFS**.



Sau khi cấu hình hệ thống **DFS** hoàn tất, tiếp theo bạn tạo các liên kết đến các tài nguyên dùng chung trên các **Server** khác trong mạng.



Để sử dụng hệ thống **DFS** này, tại máy trạm bạn ánh xạ (**map**) thư mục chia sẻ gốc thành một ổ đĩa mạng. Trong ổ đĩa mạng này bạn có thể nhìn thấy tất cả các thư mục chia sẻ trên các **Server** khác nhau trên hệ thống mạng.

Tương tự như **Fault-tolerant DFS**, bạn có thể tạo ra một **Stand-alone DFS** trên một máy **Server Stand-alone**, tất nhiên là hệ thống đó không có khả năng dung lỗi có nghĩa là khi **Server** chứa **DFS Root** hỏng thì các máy trạm sẽ không tìm thấy các tài nguyên chia sẻ trên các **Server** khác. Nhưng hệ thống **Stand-alone DFS** được sử dụng rộng rải vì nó đơn giản, tiện dụng.

Tóm tắt

Lý thuyết 2 tiết - Thực hành 3 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ cấp phát địa chỉ IP động cho các máy trạm …	I. Giới thiệu dịch vụ DHCP. II. Hoạt động của giao thức DHCP. III. Cài đặt dịch vụ DHCP. IV. Chứng thực dịch vụ DHCP trong Active Directory. V. Cấu hình dịch vụ DHCP	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. GIỚI THIỆU DỊCH VỤ DHCP.

Mỗi thiết bị trên mạng có dùng bộ giao thức **TCP/IP** đều phải có một địa chỉ **IP** hợp lệ, phân biệt. Để hỗ trợ cho vấn đề theo dõi và cấp phát các địa chỉ **IP** được chính xác, tổ chức **IETF** (**Internet Engineering Task Force**) đã phát triển ra giao thức **DHCP** (**Dynamic Host Configuration Protocol**). Giao thức này được mô tả trong các **RFC 1533, 1534, 1541** và **1542**. Bạn có thể tìm thấy các **RFC** này tại địa chỉ **http://www.ietf.org/rfc.html**. Để có thể làm một **DHCP Server**, máy tính **Windows Server 2003** phải đáp ứng các điều kiện sau:

- Đã cài dịch vụ **DHCP**.
- Mỗi **interface** phải được cấu hình bằng một địa chỉ **IP** tĩnh.
- Đã chuẩn bị sẵn danh sách các địa chỉ **IP** định cấp phát cho các máy **client**.

Dịch vụ **DHCP** này cho phép chúng ta cấp động các thông số cấu hình mạng cho các máy trạm (**client**). Các hệ điều hành của **Microsoft** và các hệ điều hành khác như **Unix** hoặc **Macintosh** đều hỗ trợ cơ chế nhận các thông số động, có nghĩa là trên các hệ điều hành này phải có một **DHCP Client**. Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

- Khắc phục được tình trạng đụng địa chỉ **IP** và giảm chi phí quản trị cho hệ thống mạng.
- Giúp cho các nhà cung cấp dịch vụ (**ISP**) tiết kiệm được số lượng địa chỉ **IP** thật (**Public IP**).
- Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.
- Kết hợp với hệ thống mạng không dây (**Wireless**) cung cấp các điểm **Hotspot** như: nhà ga, sân bay, trường học…

II. HOẠT ĐỘNG CỦA GIAO THỨC DHCP.

Giao thức **DHCP** làm việc theo mô hình **client/server**. Theo đó, quá trình tương tác giữa **DHCP client** và **server** diễn ra theo các bước sau:

- Khi máy **client** khởi động, máy sẽ gửi **broadcast** gói tin **DHCPDISCOVER**, yêu cầu một **server** phục vụ mình. Gói tin này cũng chứa địa chỉ **MAC** của máy **client.**
- Các máy **Server** trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ **IP**, đều gửi lại cho máy **Client** gói tin **DHCPOFFER**, đề nghị cho thuê một địa chỉ **IP** trong một khoản thời gian nhất định, kèm theo là một **subnet mask** và địa chỉ của **Server**. **Server** sẽ không cấp phát địa chỉ **IP** vừa đề nghị cho những **Client** khác trong suốt quá trình thương thuyết.
- Máy **Client** sẽ lựa chọn một trong những lời đề nghị (**DHCPOFFER**) và gửi **broadcast** lại gói tin **DHCPREQUEST** chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các **Server** rút lại và dùng để cấp phát cho **Client** khác.
- Máy **Server** được **Client** chấp nhận sẽ gửi ngược lại một gói tin **DHCPACK** như là một lời xác nhận, cho biết là địa chỉ **IP** đó, **subnet mask** đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra **Server** còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ của **gateway** mặc định, địa chỉ **DNS Server**, …

III. CÀI ĐẶT DỊCH VỤ DHCP.

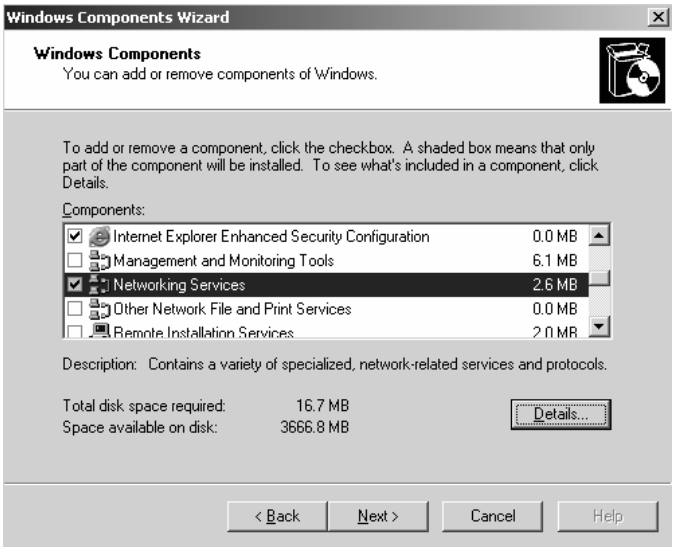
Thực hiện theo các bước sau:

Chọn menu **Start** 🕘 **Settings** 🕘 **Control Panel**.

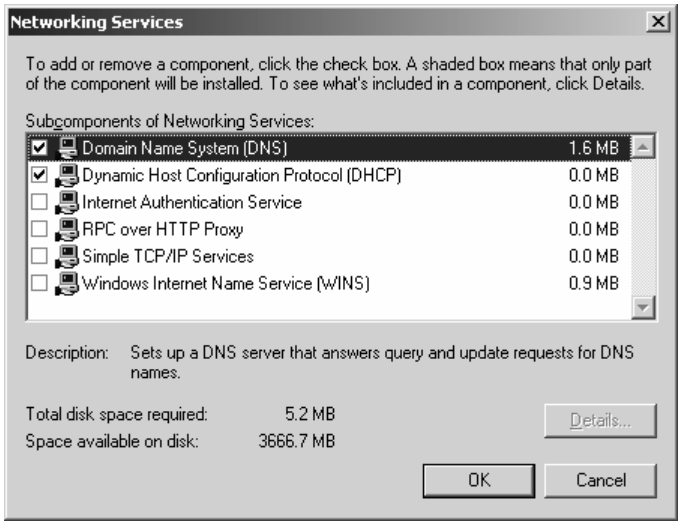
Trong cửa sổ **Control Panel**, nhấp đôi chuột vào mục **Add/Remove Programs.**

Trong hộp thoại **Add/Remove Programs**, nhấp chọn mục **Add/Remove Windows Components**.

Trong hộp thoại **Windows Components Wizard**, tô sáng **Networking Services** và nhấn nút **Details**.

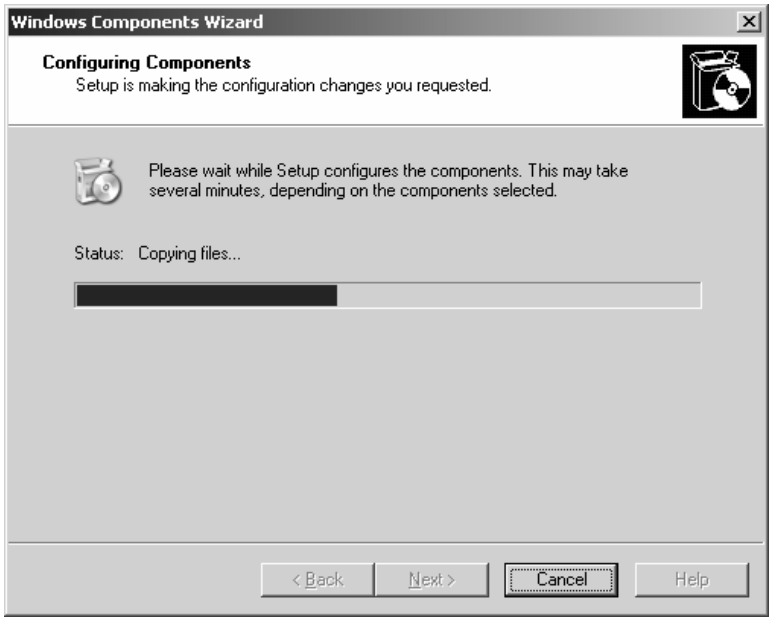


Trong hộp thoại **Networking Services**, nhấn chọn mục **Dynamic Host Configuration Protocol** (**DHCP**) và nhấn nút **OK**.



Trở lại hộp thoại **Windows Components Wizard**, nhấn chọn **Next**.

Windows 2000 sẽ cấu hình các thành phần và cài đặt dịch vụ **DHCP.**



Cuối cùng, trong hộp thoại **Completing the Windows Components Wizard**, nhấn chọn **Finish** để kết thúc.

IV. CHỨNG THỰC DỊCH VỤ DHCP TRONG ACTIVE DIRECTORY.

Nếu máy tính **Windows Server 2003** chạy dịch vụ **DHCP** trên đó lại làm việc trong một **domain** (có thể là một **Server** thành viên bình thường hoặc là một máy điều khiển vùng), dịch vụ muốn có thể hoạt động bình thường thì phải được chứng thực bằng **Active Directory**.

Mục đích của việc chứng thực này là để không cho các **Server** không được chứng thực làm ảnh hưởng đến hoạt động mạng. Chỉ có những **Windows 2003 DHCP seRver** được chứng thực mới được phép hoạt động trên mạng. Giả sử có một nhân viên nào đó cài đặt dịch vụ **DHCP** và cấp những thông tin **TCP/IP** không chính xác. **DHCP Server** của nhân viên này không thể hoạt động được (do không được quản trị mạng cho phép) và do đó không ảnh hưởng đến hoạt động trên mạng. Chỉ có **Windows 2003 DHCP Server** mới cần được chứng thực trong **Active Directory**. Còn các **DHCP server** chạy trên các hệ điều hành khác như **Windows NT, UNIX**, … thì không cần phải chứng thực.

Trong trường hợp máy **Windows Server 2003** làm **DHCP Server** không nằm trong một **domain** thì cũng không cần phải chứng thực trong **Active Directory**. Bạn có thể sử dụng công cụ quản trị **DHCP** để tiến hành việc chứng thực một **DHCP Server**. Các bước thực hiện như sau:

Chọn menu **Start** 🕘 **Administrative Tools** 🕘 **DHCP**.

Trong ô bên trái của cửa sổ **DHCP,** tô sáng **Server** bạn định chứng thực. Chọn **menu Action** 🕘 **Authorize.**

Đợi một hoặc hai phút sau, chọn lại menu **Action** 🕘 **Refresh.**

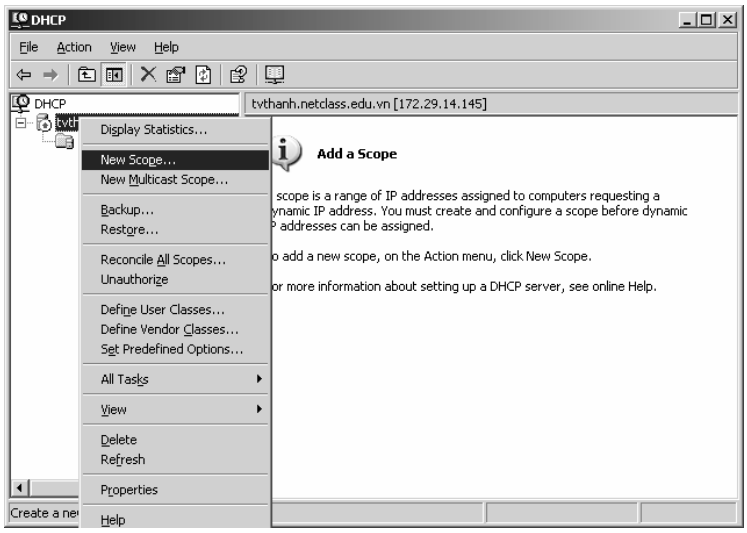
Bây giờ **DHCP** đã được chứng thực, bạn để ý biểu tượng kế bên tên **Server** là một mũi tên màu xanh hướng lên (thay vì là mũi tên màu đỏ hướng xuống).

V. CẤU HÌNH DỊCH VỤ DHCP.

Sau khi đã cài đặt dịch vụ **DHCP**, bạn sẽ thấy biểu tượng **DHCP** trong menu **Administrative Tools**. Thực hiện theo các bước sau để tạo một **scope** cấp phát địa chỉ:

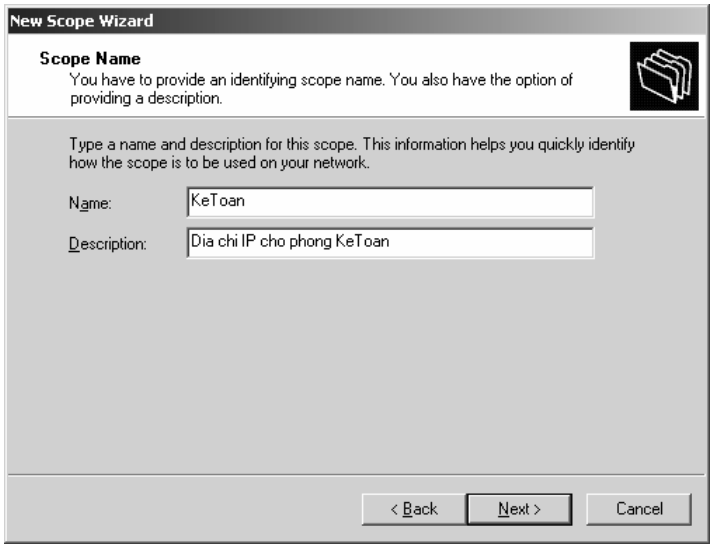
Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ **DHCP**.

Trong cửa sổ **DHCP**, nhấp phải chuột lên biểu tượng **Server** của bạn và chọn mục **New Scope** trong **popup menu**.

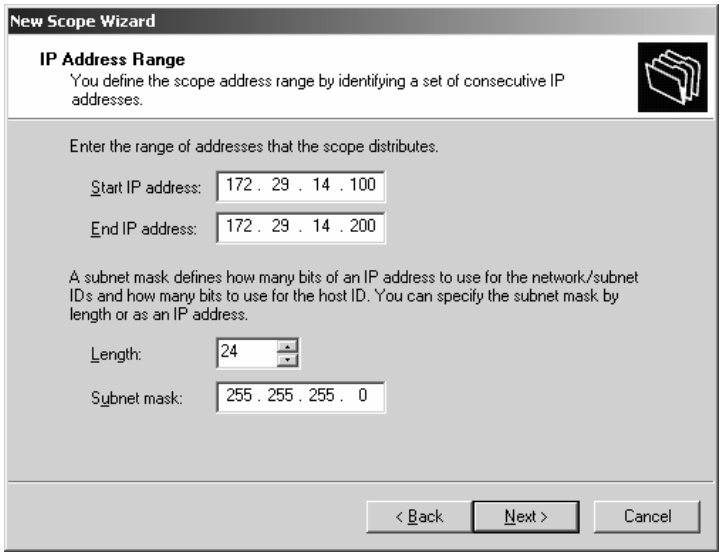


Hộp thoại **New Scope Wizard** xuất hiện. Nhấn chọn **Next**.

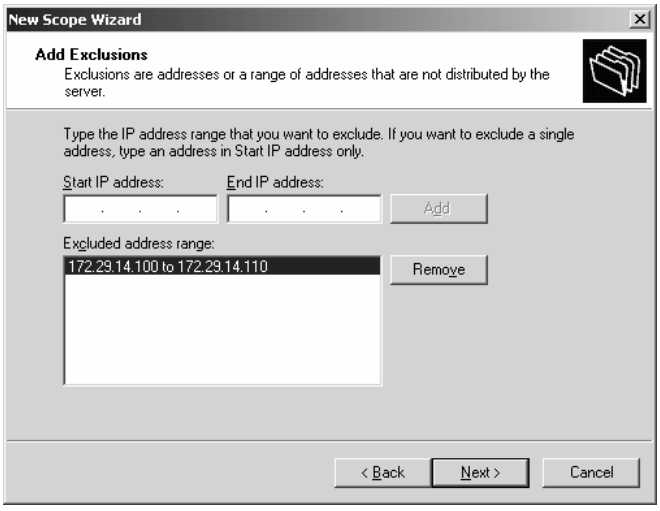
Trong hộp thoại **Scope Name**, bạn nhập vào tên và chú thích, giúp cho việc nhận diện ra **scope** này. Sau đó nhấn chọn **Next**.



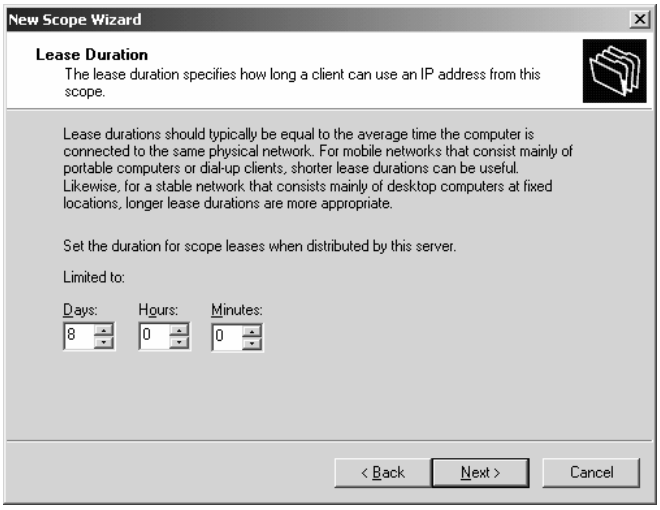
Hộp thoại **IP Address Range** xuất hiện. Bạn nhập vào địa chỉ bắt đầu và kết thúc của danh sách địa chỉ cấp phát. Sau đó bạn chỉ định **subnet mask** bằng cách cho biết số **bit** 1 hoặc hoặc nhập vào chuỗi số. Nhấn chọn **Next**.



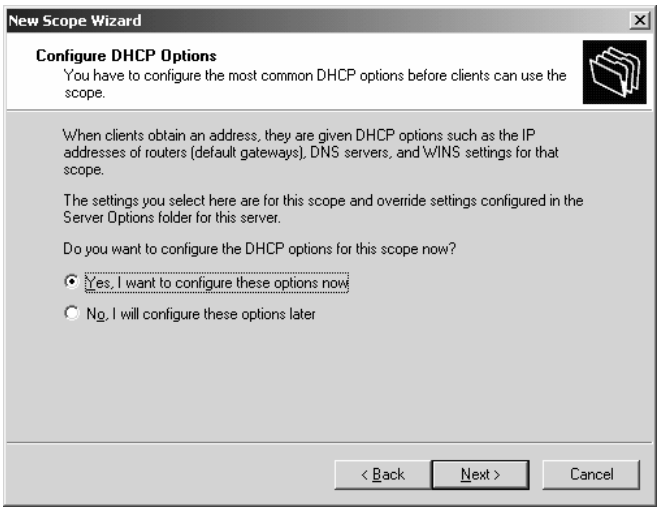
Trong hộp thoại **Add Exclusions**, bạn cho biết những địa chỉ nào sẽ được loại ra khỏi nhóm địa chỉ đã chỉ định ở trên. Các địa chỉ loại ra này được dùng để đặt cho các máy tính dùng địa chỉ tĩnh hoặc dùng để dành cho mục đích nào đó. Để loại một địa chỉ duy nhất, bạn chỉ cần cho biết địa chỉ trong ô **Start IP Address** và nhấn **Add**. Để loại một nhóm các địa chỉ, bạn cho biết địa chỉ bắt đầu và kết thúc của nhóm đó trong **Start IP Address** và **Stop IP Address**, sau đó nhấn **Add**. Nút **Remove** dùng để huỷ một hoặc một nhóm các địa chỉ ra khỏi danh sách trên. Sau khi đã cấu hình xong, bạn nhấn nút **Next** để tiếp tục.



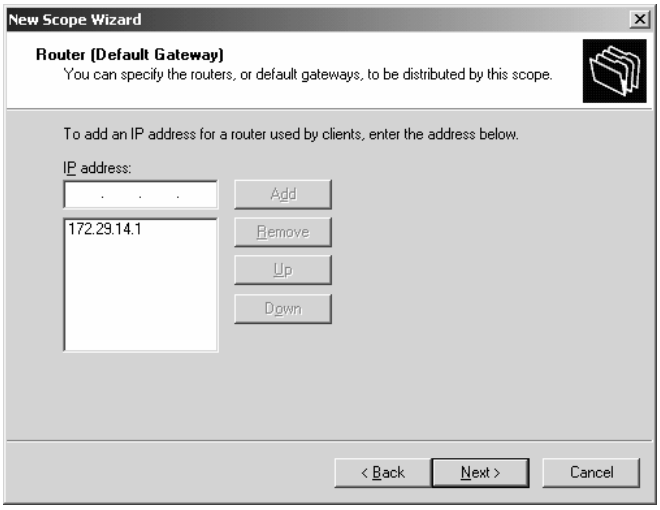
Trong hộp thoại **Lease Duration** tiếp theo, bạn cho biết thời gian các máy trạm có thể sử dụng địa chỉ này. Theo mặc định, một máy **Client** sẽ cố làm mới lại địa chỉ khi đã sử dụng được phân nửa thời gian cho phép. Lượng thời gian cho phép mặc định là 8 ngày. Bạn có thể chỉ định lượng thời gian khác tuỳ theo nhu cầu. Sau khi đã cấu hình xong, nhấn **Next** để tiếp tục.



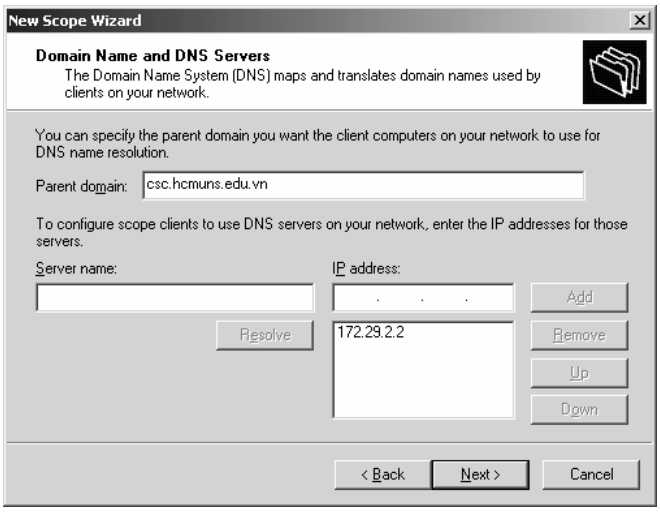
Hộp thoại **Configure DHCP Options** xuất hiện. Bạn có thể đồng ý để cấu hình các tuỳ chọn phổ biến (chọn **Yes, I want to configure these options now**) hoặc không đồng ý, để việc thiết lập này thực hiện sau (chọn **No, I will configure these options later**). Bạn để mục chọn đồng ý và nhấn chọn **Next**.



Trong hộp thoại **Router (Default Gateway)**, bạn cho biết địa chỉ **IP** của **default gateway** mà các máy **DHCP Client** sẽ sử dụng và nhấn **Add**. Sau đó nhấn **Next**.

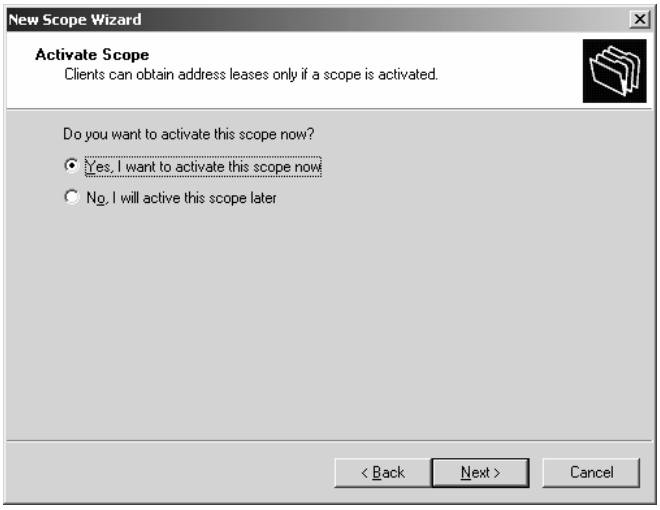


Trong hộp thoại **Domain Name and DNS Server**, bạn sẽ cho biết tên **domain** mà các máy **DHCP client** sẽ sử dụng, đồng thời cũng cho biết địa chỉ **IP** của **DNS Server** dùng phân giải tên. Sau khi đã cấu hình xong, nhấn **Next** để tiếp tục.



Trong hộp thoại **WINS SERVER** tiếp theo, bạn có thể cho biết địa chỉ của của **WINS Server** chính và phụ dùng phân giải các tên **NetBIOS** thành địa chỉ **IP**. Sau đó nhấn chọn **Next**. (Hiện nay dịch vụ **WINS** ít được sử dụng, do đó bạn có thể bỏ qua bước này, không nhập thông tin gì hết.)

Tiếp theo, hộp thoại **Activate Scope** xuất hiện, hỏi bạn có muốn kích hoạt **scope** này hay không. **Scope** chỉ có thể cấp địa chỉ cho các máy **Client** khi được kích hoạt. Nếu bạn định cấu hình thêm các thông tin tuỳ chọn cho **scope** thì chưa nên kích hoạt bây giờ. Sau khi đã lựa chọn xong, nhấn chọn **Next**.



Trong hộp thoại **Complete the New Scope Wizard**, nhấn chọn **Finish** để kết thúc.

VI. CẤU HÌNH CÁC TUỲ CHỌN DHCP.

Các tuỳ chọn **DHCP** là các thông tin phụ gửi kèm theo địa chỉ **IP** khi cấp phát cho các máy **Client**. Bạn có thể chỉ định các tuỳ chọn ở hai mức độ: **scope** và **Server**. Các tuỳ chọn mức scope chỉ áp dụng cho riêng **scope** đó, còn các tuỳ chọn mức **Server** sẽ áp đặt cho tất cả các **scope** trên toàn **Server**. Tuỳ chọn mức **scope** sẽ che phủ tuỳ chọn mức server cùng loại nếu có.

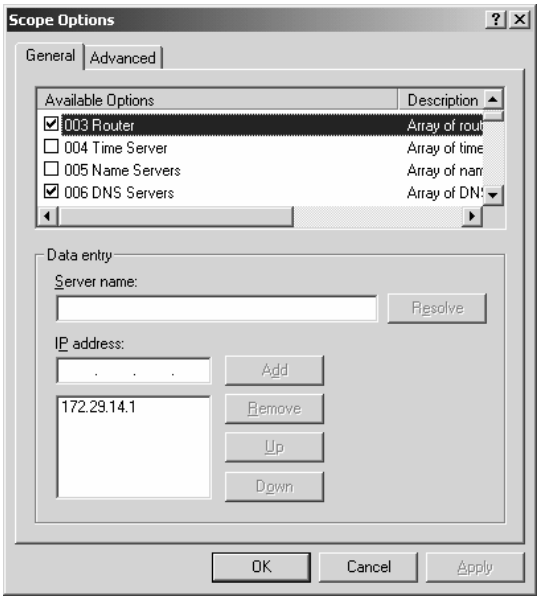
Các bước thực hiện:

Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ **DHCP**.

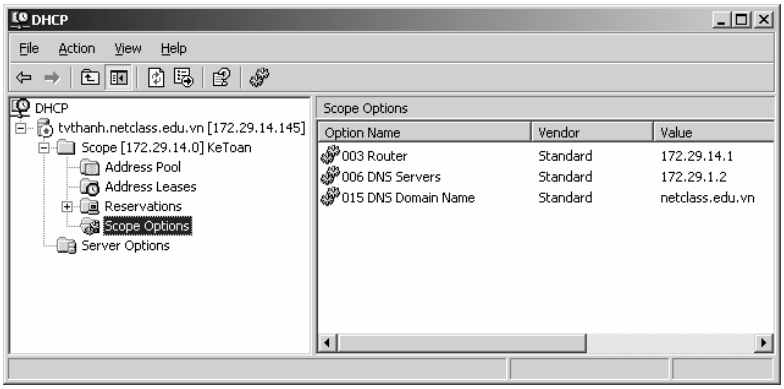
Trong cửa sổ **DHCP,** ở ô bên trái, mở rộng mục **Server** để tìm **Server Options** hoặc mở rộng một **scope** nào đó để tìm **Scope Options**.

Nhấn phải chuột lên mục tuỳ chọn tương ứng và chọn **Configure Options**.

Hộp thoại cấu hình các tuỳ chọn xuất hiện (mức **Server** hoặc **scope** đều giống nhau). Trong mục **Available Options**, chọn loại tuỳ chọn bạn định cấp phát và nhập các thông cấu hình kèm theo. Sau khi đã chọn xong hoặc chỉnh sửa các tuỳ chọn xong, nhấn **OK** để kết thúc.



Trong cửa sổ **DHCP**, mục tuỳ chọn tương ứng sẽ xuất hiện các thông tin định cấp phát.



VII. CẤU HÌNH DÀNH RIÊNG ĐỊA CHỈ.

Giả sử hệ thống mạng của bạn sử dụng việc cấp phát địa chỉ động, tuy nhiên trong đó có một số máy tính bắt buộc phải sử dụng một địa chỉ **IP** cố định trong một thời gian dài. Bạn có thể thực hiện được điều này bằng cách dành một địa chỉ **IP** cho riêng máy đó. Việc cấu hình này được thực hiện trên từng **scope** riêng biệt.

Các bước thực hiện:

Chọn menu **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **DHCP**.

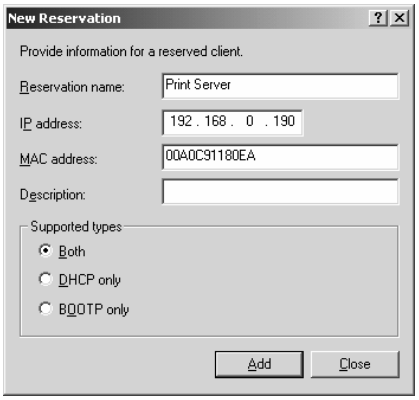
Trong ô bên trái của cửa sổ **DHCP**, mở rộng đến **scope** bạn định cấu hình, chọn mục **Reservation**, chọn menu **Action** 🕘 **New Reservation.**

Xuất hiện hộp thoại **New Reservation**. Đặt tên cho mục này dành riêng này trong ô **Reservation Name**, có thể là tên của máy tính được cấp địa chỉ đó. Trong mục **IP Address**, nhập vào địa chỉ **IP** định cấp cho máy đó. Tiếp theo, trong mục **MAC Address**, nhập vào địa chỉ **MAC** của máy tính đó (là một chuỗi liên tục 12 ký số thập lục phân). Bạn có thể ghi một dòng mô tả về địa chỉ vào mục **Description**. **Supported Types** có ý nghĩa:

DHCP only: chỉ cho phép máy **client DHCP** yêu cầu địa chỉ này bằng cách sử dụng giao thức **DHCP**.

BOOTP only: chỉ cho phép máy **client DHCP** yêu cầu địa chỉ này bằng cách sử dụng giao thức **BOOTP** (là tiền thân của giao thức **DHCP**).

Both: máy **client DHCP** có thể dùng giao thức **DHCP** hoặc **BOOTP** để yêu cầu địa chỉ này.



Lặp lại thao tác trên cho các địa chỉ dành riêng khác. Cuối cùng nhấn chọn **Close**.

Tóm tắt

Lý thuyết 2 tiết - Thực hành 2 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ in ấn trên mạng như cài đặt máy in mạng, quản lý, cấp quyền sử dụng máy in mạng …	I. Cài đặt máy in mạng. II. Quản lý thuộc tính máy in. III. Cấu hình thông số port. IV. Cấp quyền trên máy in mạng V. Cấu hình Print Server	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. CÀI ĐẶT MÁY IN.

Trước khi bạn có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành **Windows Server 2003** thì bạn phải tạo ra một máy in **logic**. Nếu máy in của bạn có tính năng **Plug and Play** thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành **Windows Server 2003**. Tiện ích **Found New Hardware Wizard** sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa **CD** được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in **logic** bằng cách sử dụng tiện ích **Add Printer Wizard**. Để có thể tạo ra một máy in **logic** trong **Windows Server 2003** thì trước hết bạn phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm **Administrators** hay nhóm **Power Users** (trong trường hợp đây là một **Server** thành viên) hay nhóm **Server Operators** (trong trường hợp đây là một **domain controller**).

Bạn có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị **Print Server**). Muốn thao tác bằng tay để tạo ra một máy in cục bộ hay một máy in mạng, chúng ta lần lượt thực hiện các thao tác sau đây:

Nhấp chuột chọn **Start**, rồi chọn **Printers And Faxes**.

Nhấp chuột vào biểu tượng **Add Printer**, tiện ích **Add Printer Wizard** sẽ được khởi động. Nhấp chuột vào nút **Next** để tiếp tục.

Hộp thoại **Local Or Network Printer** xuất hiện. Bạn nhấp vào tùy chọn **Local Printer Attached To This Computer** trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình. Nếu trường hợp ta đang tạo ra một máy in **logic** ứng với một máy in mạng thì ta nhấp vào tùy chọn **A Printer Attached To Another Computer**. Nếu máy in được gắn trực tiếp vào máy tính, bạn có thể chọn thêm tính năng **Automatically Detect And Install My Plug And Play Printer**. Tùy chọn này cho phép hệ thống tự động quét máy tính của bạn để phát hiện ra các máy in **Plug and Play**, và tự động cài đặt các máy in đó cho bạn. Khi đã hoàn tất việc chọn lựa, nhấp chuột vào nút **Next** để sang bước kế tiếp.

Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích **Found New Hardware Wizard**. Tiện ích này sẽ hướng dẫn bạn tiếp tục cài đặt **driver** máy in qua từng bước.

Hộp thoại **Print Test Page** xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính của bạn, bạn nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, nếu máy in là máy in mạng thì bạn nên bỏ qua bước này. Nhấp chuột vào nút **Next** để sang bước kế tiếp.

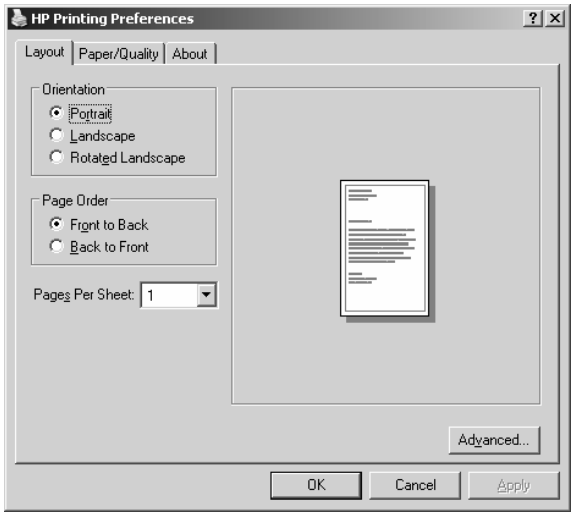
Hộp thoại **Completing The Add Printer Wizard** hiện ra. Hộp thoại này đem đến cho chúng ta một cơ hội để xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Nếu bạn phát hiện có thông tin nào không chính xác, hãy nhấp chuột vào nút **Back** để quay lại sửa chữa thông tin cho đúng. Còn nếu nhận thấy mọi thứ đều ổn cả thì bạn nhấp chuột vào nút **Finish**.

Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ **Printer And Faxes**. Theo mặc định, máy in sẽ được chia sẻ.

II. QUẢN LÝ THUỘC TÍNH MÁY IN.

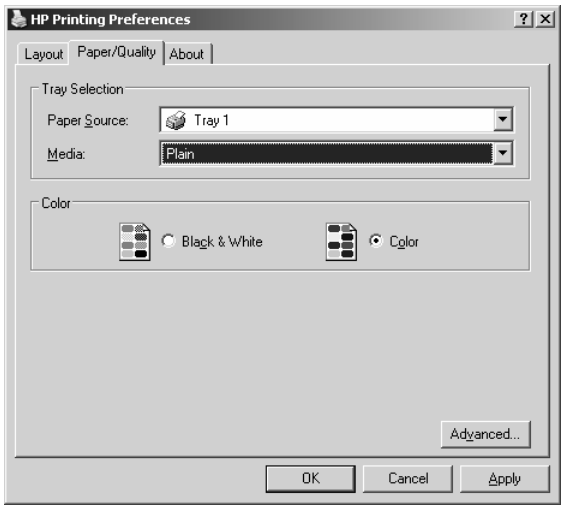
II.1. Cấu hình Layout.

Trong hộp thoại **Printing Preferences**, chọn **Tab Layout**. Sau đó trong mục **Orientation**, bạn chọn cách thức in trang theo chiều ngang hay chiều dọc. Trong mục **Page Order**, bạn chọn in từ trang đầu đến trang cuối của tài liệu hoặc in theo thứ tự ngược lại. Trong mục **Pages Per Sheet**, bạn chọn số trang tài liệu sẽ được in trên một trang giấy.



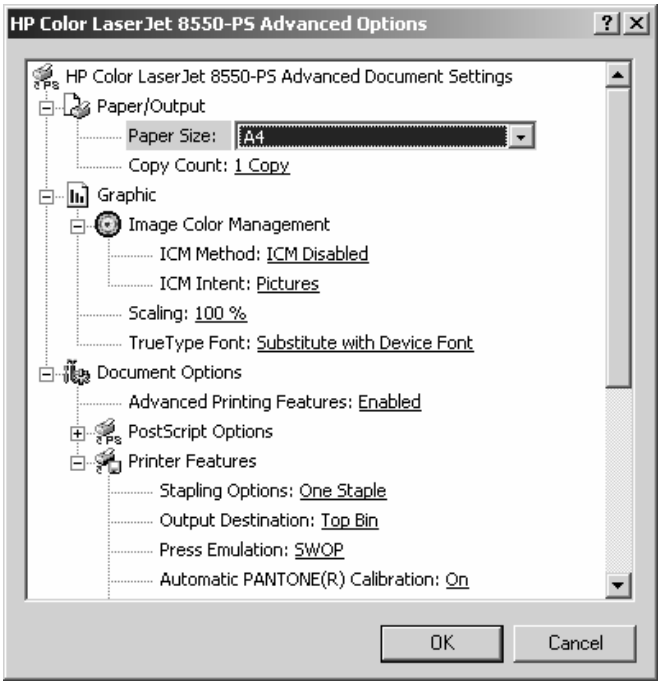
II.2. Giấy và chất lượng in.

Cũng trong hộp thoại **Printing Preferences,** để qui định giấy và chất lượng in, chúng ta chọn **Tab Paper/Quality**. Các tùy chọn trong **Tab Paper/Quality** phụ thuộc vào đặc tính của máy in. Ví dụ, máy in chỉ có thể cung cấp một tùy chọn là **Paper Source.** Còn đối với máy in **HP OfficeJet Pro Cxi,** chúng ta có các tùy chọn là: **Paper Source**, **Media, Quality Settings** và **Color**.



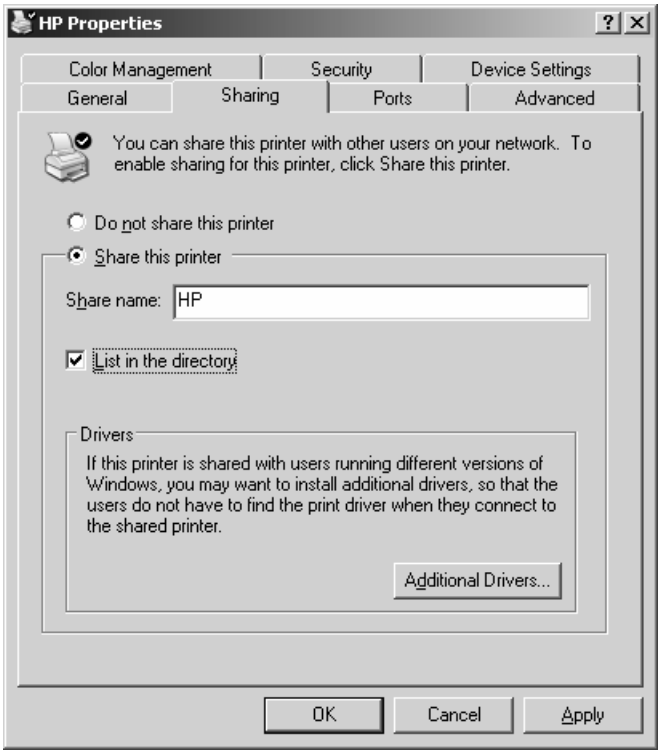
II.3. Các thông số mở rộng.

Nhấp chuột vào nút **Advanced** ở góc dưới bên phải của hộp thoại **Printing Preferences**. Hộp thoại **Advanced Options** xuất hiện cho phép bạn điều chỉnh các thông số mở rộng. Chúng ta có thể có các tùy chọn của máy in như: **Paper/Output, Graphic, Document Options, và Printer Features**. Các thông số mở rộng có trong hộp thoại **Advanced Options** phụ thuộc vào driver máy in mà bạn đang sử dụng.



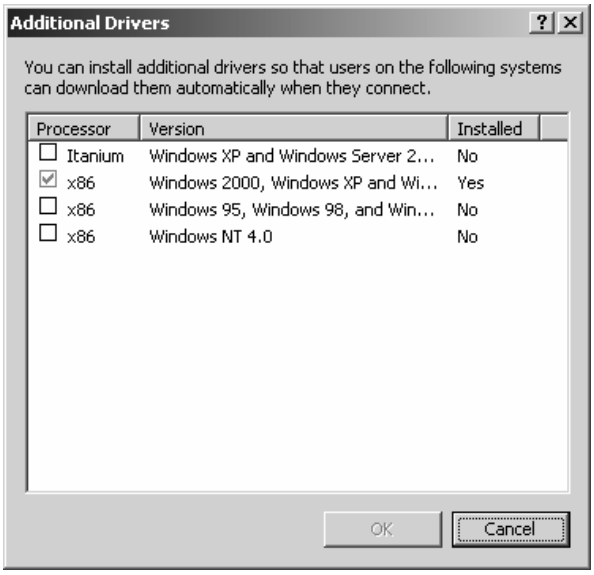
III. CẤU HÌNH CHIA SẺ MÁY IN.

Nhấp phải chuột lên máy in, chọn **Properties.** Hộp thoại **Properties** xuất hiện, bạn chọn **Tab Sharing**. Để chia sẻ máy in này cho nhiều người dùng, bạn nhấp chuột chọn **Share this printer**. Trong mục **Share name**, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể nhấp chọn mục **List In** The **Directory** để cho phép người dùng có thể tìm kiếm máy in thông qua **Active Directory** theo một vài thuộc tính đặc trưng nào đó.



Ngoài ra, trong **Tab Sharing**, ta có thể cấu hình **driver** hỗ trợ cho các máy trạm sử dụng máy in trong trường hợp máy trạm không phải là **Windows Server 2003**. Đây là một tính năng cần thiết vì nó cho phép chỉ định các **driver** hỗ trợ in để các máy trạm có thể tải về một cách tự động. Mặc định, **driver** duy nhất được nạp vào là **driver** của hãng **Intel** cho các máy trạm là **Windows 2000, Windows Server 2003**, và **Windows XP**. Để cung cấp thêm các **driver** cho máy trạm khác, bạn nhấp chuột vào nút **Additional Drivers** nằm phía dưới **Tab Sharing**. Hộp thoại **Additional Drivers** xuất hiện. **Windows Server 2003** hỗ trợ các **driver** thêm vào cho các **Client** là một trong những hệ điều hành sau:

- Itanium Windows XP hay Windows Server 2003.
- x86 Windows 2000, Windows XP, hay Windows Server 2003 (mặc định).
- x86 Windows 95, Windows 98, hay Windows Millennium Edition.
- x86 Windows NT 4.



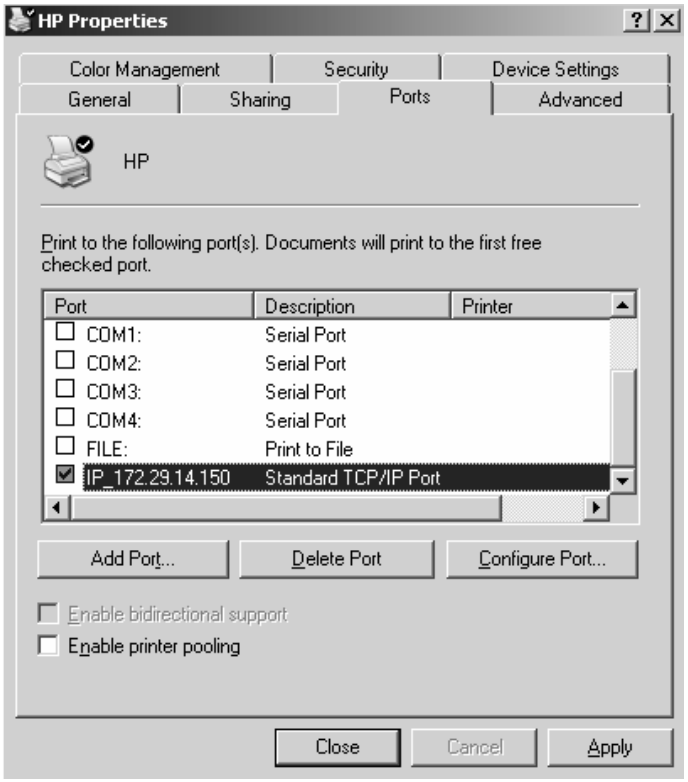
IV. CẤU HÌNH THÔNG SỐ PORT.

IV.1. Cấu hình các thông số trong Tab Port.

Trong hộp thoại **Properties**, bạn chọn **Tab Port** để cấu hình tất cả các **port** đã được định nghĩa cho máy in sử dụng. Một **port** được định nghĩa như một **interface** sẽ cho phép máy tính giao tiếp với thiết bị máy in. **Windows Server 2003** hỗ trợ các port vật lý (**local port**) và các **port TCP/IP** chuẩn (**port logic**).

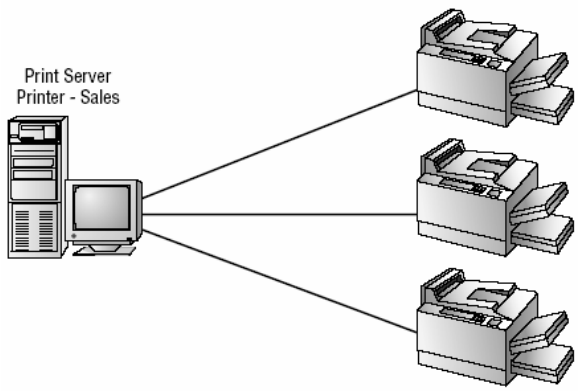
Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp **Windows Server 2003** đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn phải gắn máy in vào **port LPT1**.

Port TCP/IP chuẩn được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ **port RJ45)** và máy in này có một địa chỉ **IP** để nhận dạng. Ưu điểm của máy in mạng là tốc độ in nhanh hơn máy in cục bộ và máy in có thể đặt bất kì nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một port **TCP/IP** và khai báo địa chỉ **IP** của máy in mạng. Cùng với việc xoá và cấu hình lại một **port** đã tồn tại, bạn cũng có thể thiết lập **printer pooling** và điều hướng các công việc in ấn đến một máy in khác.

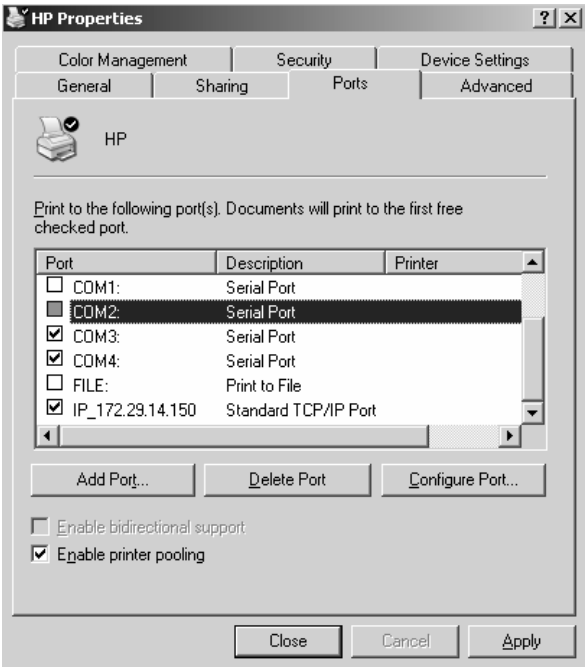


IV.2. Printer Pooling.

Printer pool được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in **logic**, được minh họa như hình bên dưới. Lợi ích của việc sử dụng **printer pool** là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng, ví dụ như là nhóm các thư ký.

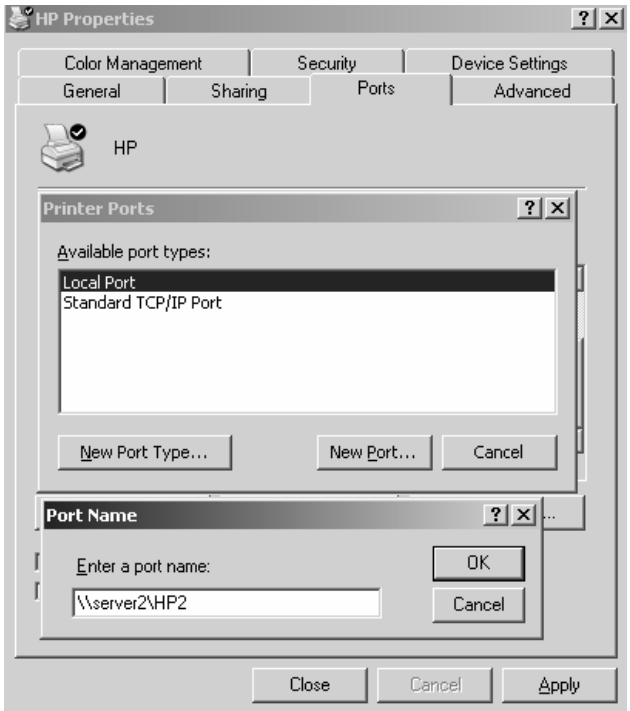


Để cấu hình một **printer pool**, bạn nhấp chuột vào tùy chọn **Enable Printer Pooling** nằm ở phía dưới **Tab Port** trong hộp thoại **Properties**. Sau đó, kiểm tra lại tất cả các **port** mà ta dự định gắn các máy in vật lý trong **printer pool** vào. Nếu ta không chọn tùy chọn **Enable Printer Pooling** thì ta chỉ có một port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một **printer pool** phải sử dụng cùng một **driver** máy in.



IV.3. Điều hướng tác vụ in đến một máy in khác.

Nếu một máy in vật lý của bạn bị hư, bạn có thể chuyển tất cả các tác vụ in ấn của máy in bị hư sang một máy in khác. Để làm được điều này, trước hết bạn phải đảm bảo máy in mới phải có **driver** giống với máy in cũ. Sau đó, trong **Tab Port**, bạn nhấp chuột vào nút **Add Port**, chọn **Local port** rồi chọn tiếp **New Port**. Hộp thoại **Port Name** xuất hiện, gõ vào tên **UNC** của máy in mới theo định dạng: **\\computername\printer_sharename.**

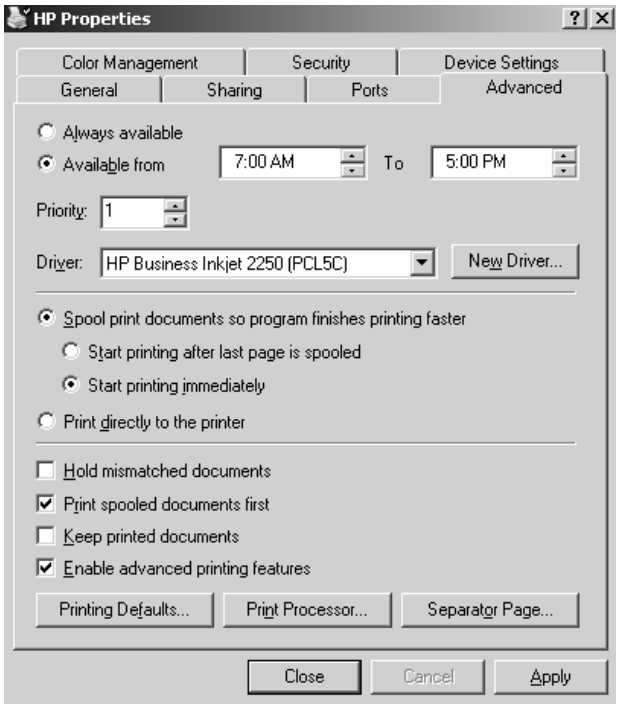


V. CẤU HÌNH TAB ADVANCED.

V.1. Các thông số của Tab Advanced.

Trong hộp thoại **Properties**, bạn nhấp chuột vào **Tab Advanced** để điều khiển các đặc tính của máy in. Bạn có thể cấu hình các thuộc tính sau:

- Khả năng của máy in
- Độ ưu tiên của máy in
- Driver mà máy in sẽ sử dụng
- Các thuộc tính đồng tác (**spooling**) của máy in
- Cách thức in tài liệu theo biểu mẫu
- Chế độ in mặc định
- Sử dụng bộ xử lý in ấn nào
- Các trang độc lập



V.2. Khả năng sẵn sàng phục vụ của máy in.

Thông thường, chúng ta cần kiểm tra khả năng sẵn sàng phục vụ của máy in trong trường hợp chúng ta có nhiều máy in cùng sử dụng một thiết bị in. Mặc định thì tùy chọn **Always Available** luôn được bật lên. Do đó, người dùng có thể sử dụng máy in 24 tiếng một ngày. Để giới hạn khả năng phục vụ của máy in, bạn chọn **Available From** và chỉ định khoảng thời gian mà máy in sẽ phục vụ. Ngoài khoảng thời gian này, máy in sẽ không phục vụ cho bất kì người dùng nào.

V.3. Độ ưu tiên (Printer Priority).

Khi bạn đặt độ ưu tiên, bạn sẽ định ra bao nhiêu công việc sẽ được gửi trực tiếp vào thiết bị in. Ví dụ, bạn có thể sử dụng tùy chọn này khi 2 nhóm người dùng cùng chia sẻ một máy in và bạn cần điều khiển độ ưu tiên đối với các thao tác in ấn trên thiết bị in này. Trong **Tab Advanced** của hộp thoại **Properties**, bạn sẽ đặt độ ưu tiên bằng các giá trị từ 1 đến 99, với 1 là có độ ưu tiên thấp nhất và 99 là có độ ưu tiên cao nhất.

Ví dụ: giả sử có một máy in được phòng kế toán sử dụng. Những người quản lý trong phòng kế toán luôn luôn muốn tài liệu của họ sẽ được ưu tiên in ra trước các nhân viên khác. Để cấu hình cho việc sắp xếp thứ tự này, ta tạo ra một máy in tên là **MANAGERS** gắn vào **port LPT1** với độ ưu tiên là 99. Sau đó, cũng trên port **LPT1**, ta tạo thêm một máy in nữa tên là **WORKERS** với độ ưu tiên là 1. Sau đó, ta sẽ sử dụng **Tab Security** trong hộp thoại **Properties** để giới hạn quyền sử dụng máy in **MANAGERS** cho những người quản lý. Đối với các nhân viên còn lại trong phòng kế toán, ta cho phép họ sử dụng máy in **WORKERS** (chúng ta sẽ tìm hiểu rõ hơn về **Security** trong phần sau). Khi các tác vụ in xuất phát từ máy in **MANAGERS**, nó sẽ đi vào hàng đợi của của máy in vật lý với độ ưu tiên cao hơn là các tác vụ xuất phát từ máy in **WORKERS**. Do đó, tài liệu của những người quản lý sẽ được ưu tiên in trước.

V.4. Print Driver.

Mục **Drive**r trong **Tab Advanced** cho phép bạn chỉ định driver sẽ dùng cho máy in. Nếu bạn đã cấu hình nhiều máy in trên một máy tính thì bạn có thể chọn bất kì **driver** nào trong các **driver** đã cài đặt. Thao tác thực hiện như sau: Nhấp chuột vào nút **New Driver** để khởi động **Add Printer Driver Wizard**. **Add Printer Driver Wizard** cho phép bạn thực hiện cập nhật cũng như thêm driver mới.

V.5. Spooling.

Khi bạn cấu hình tùy chọn **spooling**, bạn cần chỉ định rõ các tác vụ in ấn sẽ được đẩy ra đường ống máy in hay được gửi trực tiếp đến thiết bị máy in. **Spooling** có nghĩa là các thao tác in ấn sẽ được lưu trữ xuống đĩa thành một hàng đợi trước khi các thao tác in này được gửi đến máy in. Có thể xem **spooling** giống như là bộ điều phối in ấn nếu như tại một thời điểm có nhiều người dùng cùng lúc gởi yêu cầu đến máy in. Theo chế độ mặc định, tùy chọn **spooling** sẽ được bật lên sẵn.

V.6. Print Options.

Phía dưới **Tab Advance** có chứa bốn tùy chọn in ấn. Đó là các tùy chọn:

- **Hold Mismatched Documents**: tùy chọn này hữu dụng trong trường hợp bạn sử dụng chế độ nhiều biểu mẫu trong một máy in. Mặc định thì tùy chọn này sẽ không được bật lên. Các tác vụ sẽ được in theo chế độ **first-in-first-out (FIFO).** Nếu bạn bật tùy chọn này lên, hệ thống sẽ chọn ưu tiên in trước những tác vụ có chung một biểu mẫu.
- **Print Spooled Documents First**: tùy chọn này qui định rằng các tác vụ in ấn được điều hướng xong trước các loại tác vụ lớn khác. Điều này có nghĩa là các tác vụ in ấn sẽ có độ ưu tiên lớn hơn các loại tác vụ khác trong quá trình điều hướng. Mặc định thì tùy chọn này luôn được bật lên giúp gia tăng hiệu quả làm việc của máy in.
- **Keep Printed Documents**: tùy chọn này qui định rằng các tác vụ in ấn phải được xóa khỏi hàng đợi điều hướng in ấn khi các tác vụ này đã hoàn tất quá trình in. Thông thường, bạn muốn xóa các

tác vụ in ấn ngay khi nó bắt đầu in bởi vì nếu chúng ta tiếp tục lưu trữ các tác vụ này trong hàng

đợi điều hướng và đợi cho đến khi chúng được in xong mới xóa thì sẽ phải tốn dung lượng ổ đĩa cho việc lưu trữ. Mặc định thì tùy chọn này sẽ không được bật lên.

- **Enable Advanced Printing Features**: tùy chọn này qui định rằng bất kì các tính năng mở rộng nào mà máy in của bạn có hỗ trợ ví dụ như **Page Order** và **Pages Per Sheet** nên được bật lên. Mặc định thì tùy chọn này luôn được bật lên. Chỉ trong trường hợp xảy ra các vấn đề về tương thích thì bạn có thể tắt tùy chọn này. Ví dụ như bạn đang sử dụng **driver** cho một thiết bị máy in tương tự nhưng nó không hỗ trợ tất cả các tính năng của máy in. Trong trường hợp đó, bạn nên tắt tùy chọn này đi.

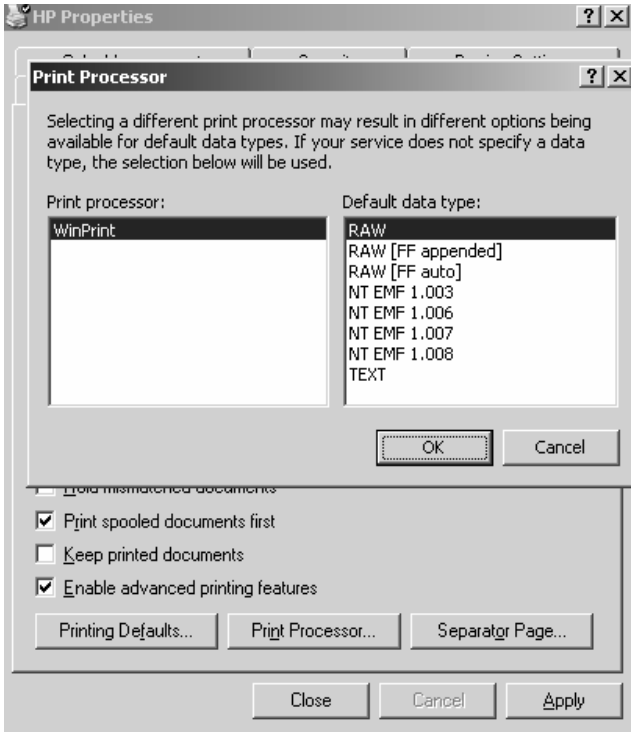
V.7. Printing Defaults.

Nút **Printing Defaults** nằm ở góc trái phía dưới của **Tab Advance**. Nếu bạn nhấp chuột vào nút **Printing Defaults**, hộp thoại **The Printing Preferences** sẽ xuất hiện. Đây cũng chính là hộp thoại sẽ xuất hiện khi bạn nhấp chuột vào nút **Printing Preferences** trong **Tab General**.

V.8. Print Processor.

Bộ xử lý in ấn được sử dụng để qui định **Windows Server 2003** có cần phải thực hiện các xử lý bổ sung trong công việc in ấn hay không. Bộ xử lý in ấn **WinPrint** mặc định được cài đặt và được **Windows Server 2003** sử dụng. Bộ xử lý in ấn **WinPrint** có thể hỗ trợ một vài kiểu dữ liệu.

Theo mặc định thì hầu hết các ứng dụng trên nền **Window** sử dụng chuẩn **EMF (enhanced metafile)** để gởi các tác vụ đến máy in. Chuẩn **EMF** dùng kiểu dữ liệu **RAW**. Kiểu dữ liệu này sẽ báo với bộ xử lý in ấn là tác vụ này không cần phải sửa đổi độ ưu tiên khi in. Điều này là do nhà sản xuất phần mềm qui định.



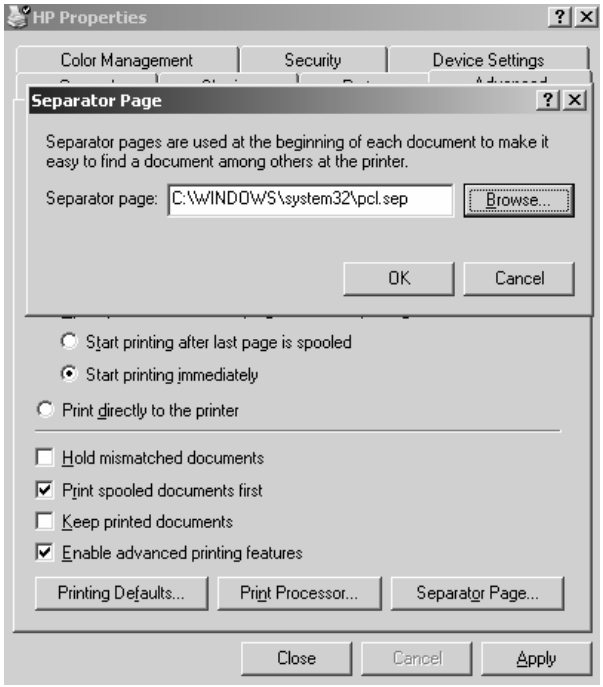
Bảng danh sách các kiểu dữ liệu được bộ xử lý in ấn trong **Windows Server 2003** hỗ trợ:

Kiểu dữ liệu	Mô tả
RAW	Không làm thay đổi tài liệu in ấn
RAW (FF appended)	Không làm thay đổi tài liệu in ấn ngoại trừ việc thêm vào một kí tự **form-feed**
RAW (FF Auto)	Không làm thay đổi tài liệu in ấn ngoại trừ việc kiểm tra xem có cần thêm vào một kí tự **form-feed** hay không
NT EMF 1.00x	Thường điều hướng các tài liệu được gửi từ các máy tính **Window** khác
TEXT	Phiên dịch tất cả các kiểu dữ liệu văn bản đơn giản và máy in sẽ thực hiện in bằng cách sử dụng các lệnh văn bản chuẩn.

V.9. Separator Pages.

Separator pages được sử dụng tại thời điểm bắt đầu của mỗi tài liệu nhằm mục đích định dạng rõ người dùng nào đã thực hiện việc in tài liệu này. Nếu như máy in không được chia sẻ thì chế độ **Separator pages** vô hình chung sẽ gây ra lãng phí giấy in. Nếu trong trường hợp máy in được chia sẻ cho nhiều người dùng thì chế độ **Separator pages** sẽ hữu dụng trong việc phân phối các tác vụ in ấn đã hoàn tất.

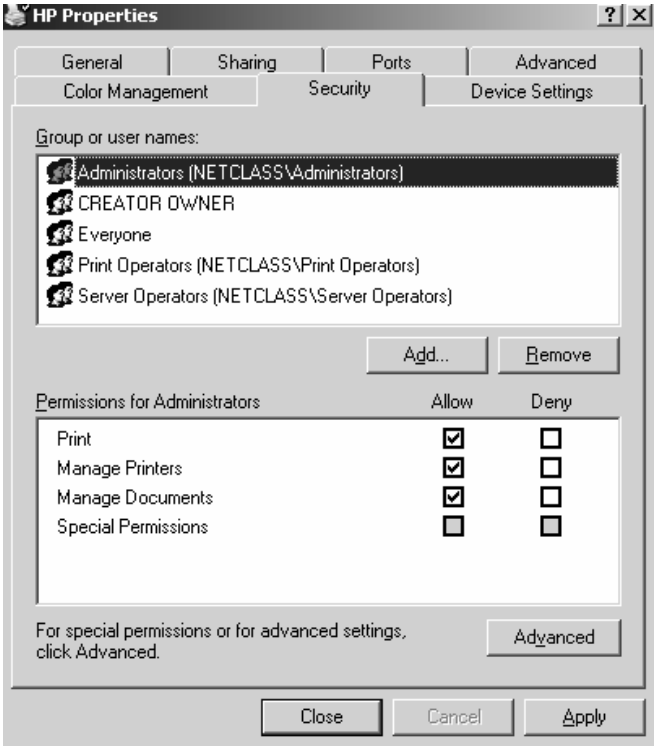
Để thêm một **Separator page**, bạn thực hiện như sau: nhấp chuột vào nút **Separator page** nằm ở góc phải phía **dưới Tab Advance**. Hộp thoại **Separator page** hiện ra, bạn nhấp chuột vào nút **Browse** để chọn tập tin **Separator page** nào bạn muốn sử dụng.



VI. CẤU HÌNH TAB SECURITY.

VI.1. Giới thiệu Tab Security.

Chúng ta có thể kiểm soát quyền truy cập vào máy in **Windows Server 2003** của người dùng cũng như các nhóm người dùng bằng cách cấu hình quyền in ấn. Chúng ta có thể cho phép hoặc không cho phép người dùng truy xuất máy in. Chúng ta cấp quyền in ấn cho người dùng và nhóm người dùng thông qua **Tab Security** trong hộp thoại **Properties** của máy in.



Bảng phân quyền in ấn cho người dùng

Quyền hạn	Mô tả
Print	Cho phép người dùng hoặc một nhóm người dùng có thể kết nối và gửi tác vụ in ấn đến máy in.
Manage Printers	Cho phép thực hiện thao tác điều khiển, quản lý máy in. Với quyền này, người dùng hoặc nhóm người dùng có thể dừng hoặc khởi động lại máy in, thay đổi cấu hình của bộ điều tác, chia sẻ hoặc không chia sẻ máy in, thay đổi quyền in ấn, và quản trị các thuộc tính của máy in.
Manage Documents	Cho phép người dùng quản lý các tài liệu in qua các thao tác dừng việc in, khởi động lại, phục hồi lại, hoặc là xoá tài liệu ra khỏi hàng đợi máy in. Người dùng không thể điều khiển trạng thái của máy in.

Special Permissions	Bằng cách chọn **Tab Advanced** trong hộp thoại **Print Permissions**, bạn có thể quản lý các quyền đặc biệt.

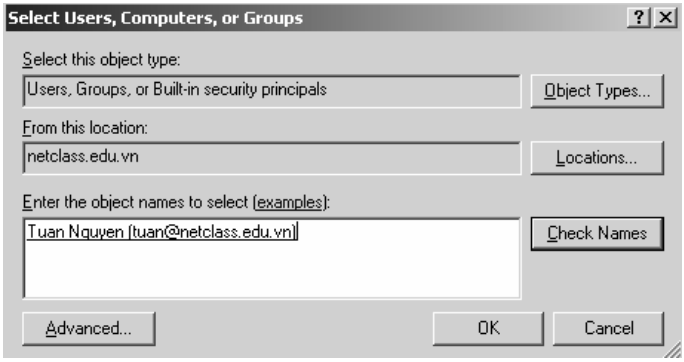
Theo mặc định, bất kì khi nào một máy in được tạo ra, các quyền in ấn mặc định sẽ được thiết lập. Bảng các quyền in ấn mặc định:

Nhóm quyền	Được phép in	Quản lý máy in	Quản lý tài liệu in
Administrators	✓	✓	✓
Creator Owner			✓
Everyone	✓		
Print Operators	✓	✓	✓
Server Operators	✓	✓	✓

VI.2. Cấp quyền in cho người dùng/nhóm người dùng.

Thông thường, bạn có thể chấp nhận quyền in ấn mặc định đã được thiết lập sẵn. Tuy nhiên, trong một số trường hợp đặc biệt, bạn cần phải hiệu chỉnh lại các quyền in cho thích hợp. Ví dụ: Công ty của bạn vừa trang bị cho phòng **Marketing** một máy in **laser** màu đắt tiền, bạn không muốn ai cũng được phép sử dụng máy in này. Trong trường hợp này, trước tiên bạn phải bỏ tùy chọn **Allow checkbox for the Everyone group**. Sau đó, thêm nhóm **Marketing** vào trong danh sách của **Tab Security**. Cuối cùng bạn cấp cho nhóm **Marketing** quyền **Print**. Muốn thêm các quyền in ấn, bạn thực hiện các bước sau:

1. Ở **Tab Security** trong hộp thoại **Properties** của máy in, nhấp chuột vào nút **Add.**
2. Hộp thoại **Select Users**, **Computers**, **Or Groups** xuất hiện, bạn nhập vào tên của người dùng hoặc nhóm người dùng mà bạn định cấp quyền in ấn rồi nhấp chuột vào nút **Add**. Sau đó, bạn chọn tất cả các người dùng mà bạn muốn cấp quyền và nhấp chuột vào nút **OK**

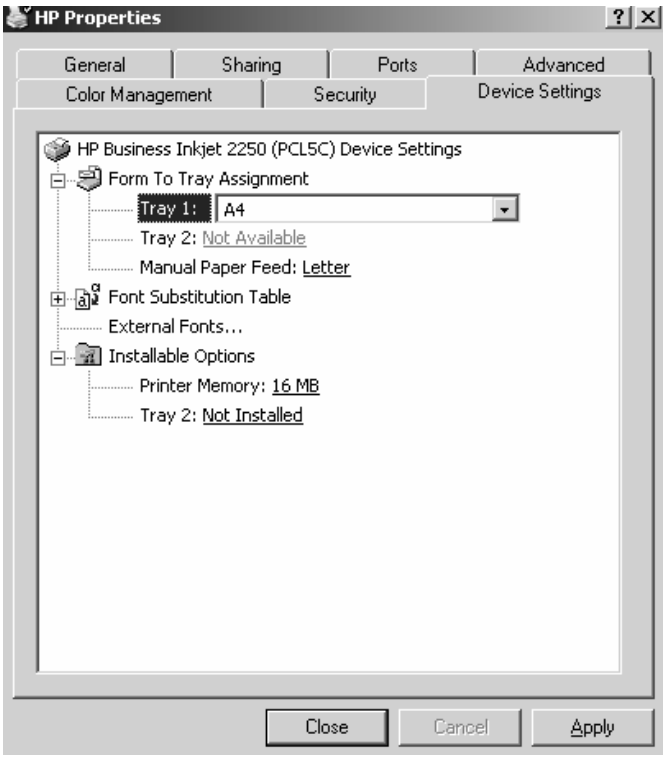


3. Chọn người dùng hoặc nhóm người dùng từ danh sách các phân quyền, sau đó chọn **Allow** để cấp quyền hoặc chọn **Deny** để không cấp quyền in ấn, các quyền quản lý máy in hay các quyền quản lý tài liệu in.

Để loại bỏ một nhóm có sẵn trong danh sách phân quyền, ta sẽ chọn nhóm đó và nhấp chuột vào nút **Remove.** Nhóm vừa chọn sẽ không còn được liệt kê trong **Tab Security** nữa và không thể được cấp bất kì quyền hạn in ấn nào.

VII. CẤU HÌNH TAB DEVICES.

Trong hộp thoại **Properties**, chọn mở **Tab Devices**. Các thuộc tính hiển thị trong **Tab Devices** phụ thuộc vào đặc tính của máy in và **driver** máy in mà bạn đã cài đặt.

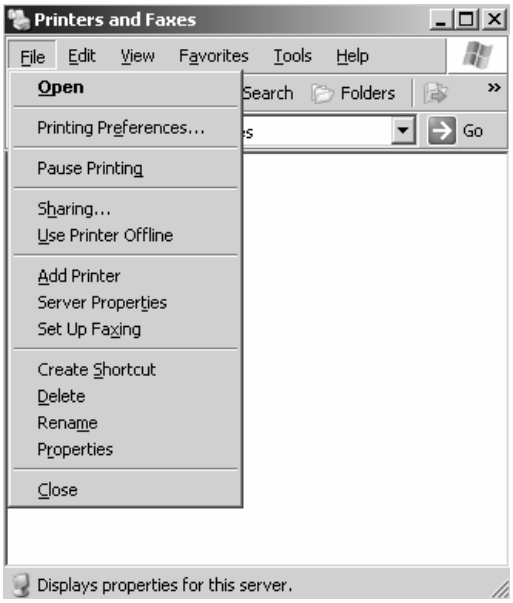


VIII. QUẢN LÝ PRINT SERVER.

VIII.1. Hộp thoại quản lý Print Server.

Print Server là một một máy tính trên đó có định nghĩa sẵn các máy in. Khi người dùng gửi một yêu cầu in ấn đến một máy in mạng, thì trước tiên, yêu cầu đó phải được gửi đến **Print Server**. Nói cách khác **Print Server** sẽ có nhiệm vụ quản lý tất cả các máy in **logic** đã được tạo ra trên máy tính. Với tư cách là một **Print Server**, máy tính này phải đủ mạnh để hỗ trợ cho việc đón nhận các tác vụ in ấn và nó cũng phải đủ không gian đĩa trống để chứa các tác vụ in trong hàng đợi.

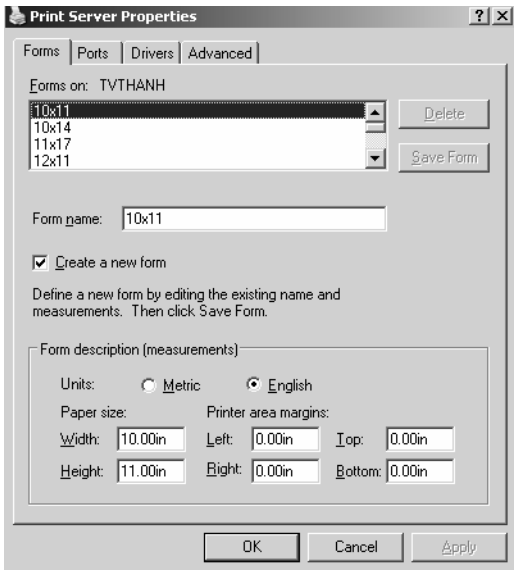
Bạn có thể quản lý **Print Server** bằng cách cấu hình các thuộc tính trong hộp thoại **Print Server Properties**. Chúng ta mở hộp thoại **Print Server Properties** bằng cách: mở hộp thoại **Printers And Faxes**, chọn **File** rồi chọn tiếp **Server Properties**. Hộp thoại **Print Server Properties** bao gồm các **Tab: Forms, Ports, Drivers** và **Advanced.**



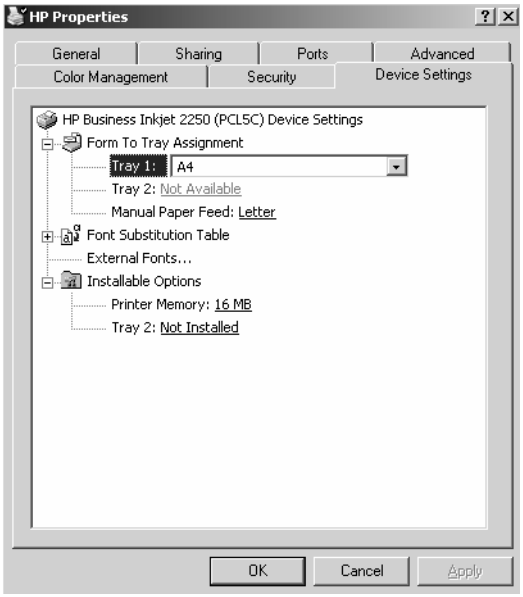
VIII.2. Cấu hình các thuộc tính của biểu mẫu in.

Nếu máy in của bạn có nhiều khay giấy và ở mỗi khay, bạn đặt vào đó các loại giấy khác nhau, bạn có thể cấu hình các thuộc tính trong **Tab Form** để tạo ra và quản lý nhiều biểu mẫu cho máy in. Một biểu mẫu chủ yếu được cấu hình dựa vào kích cỡ. Muốn tạo ra một biểu mẫu mới, ta thực hiện theo bốn bước sau:

(1) Trong **Tab Forms**, bạn nhấp chuột vào tùy chọn **Create A New Form**.
(2) Trong mục **Form Name**, bạn nhập vào tên của biểu mẫu.
(3) Trong mục **Form Description**, bạn lựa chọn kích thước cho biểu mẫu
(4) Nhấp chuột vào nút **Save Form** để hoàn tất việc tạo biểu mẫu



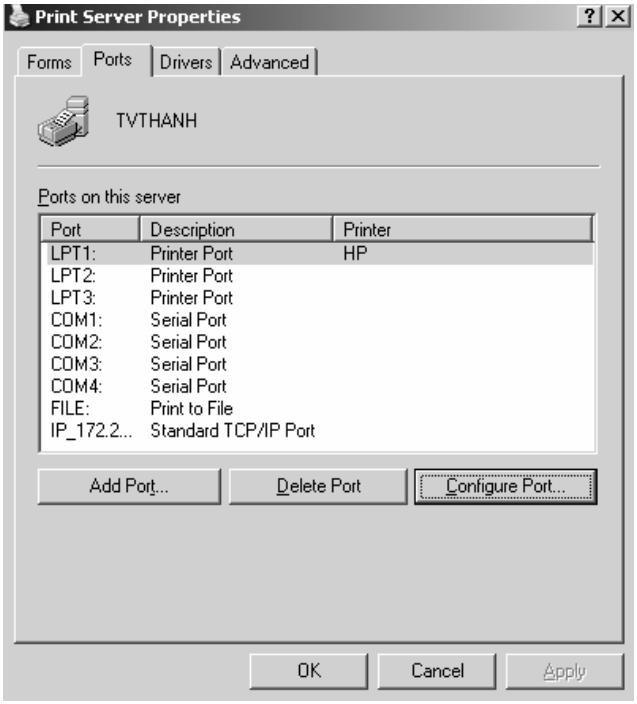
Chúng ta vừa tạo ra một biểu mẫu. Tiếp theo, chúng ta cần kết hợp biểu mẫu với khay giấy của máy in. Để làm được điều này, chúng ta phải sử dụng **Tab Devices** trong hộp thoại **Properties** của máy in.



Phía dưới phần **Form To Tray Assignment**, trước tiên bạn chọn khay giấy, rồi chọn biểu mẫu để kết hợp với khay giấy đó.

VIII.3. Cấu hình các thuộc tính Port của Print Server.

Trong hộp thoại **Printer Server Properties**, bạn mở **Tab Port**. **Tab** này cũng tương tự như **Tab Port** trong hộp thoại **Properties** của máy in. Sự khác nhau giữa hai **Tab Port** là: **Tab Port** trong hộp thoại **Print Server Properties** được sử dụng để quản lý tất cả các port trên **Print Server**. Còn **Tab port** trong hộp thoại **Properties** của máy in quản lý các **port** của thiết bị máy in vật lý.

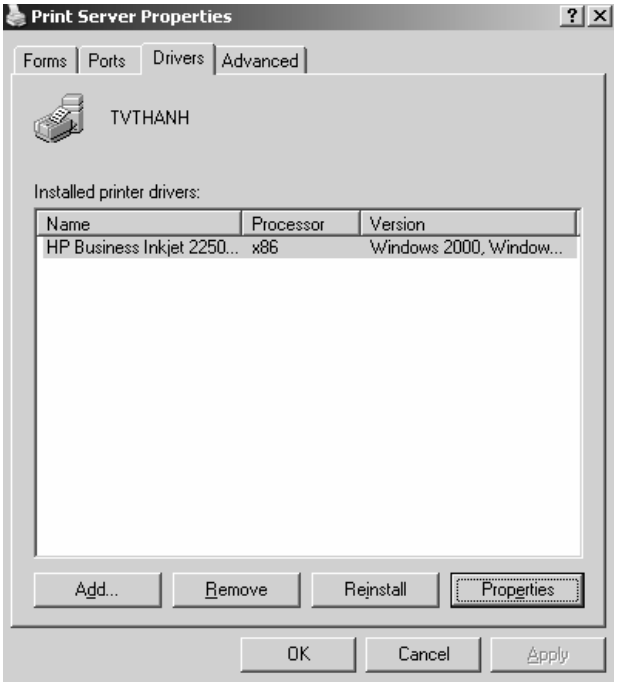


VIII.4. Cấu hình Tab Driver.

Trong hộp thoại **Printer Server Properties**, bạn mở **tab Driver**. **Tab Driver** cho phép bạn quản lý các **driver** máy in đã được cài đặt trên **Print Server**. Đối với mỗi **driver** máy in, **Tab** này sẽ hiển thị tên, môi trường và hệ điều hành mà **driver** hỗ trợ.

Sử dụng các tùy chọn trong **Tab Driver**, bạn có thể thêm vào hay loại bỏ hay cập nhật **driver** máy in. Để nhìn thấy các thuộc tính của một **driver** máy in, ta chọn **driver** cần hiển thị và nhấp chuột vào nút **Properties**. Các thuộc tính của một **driver** máy in gồm có:

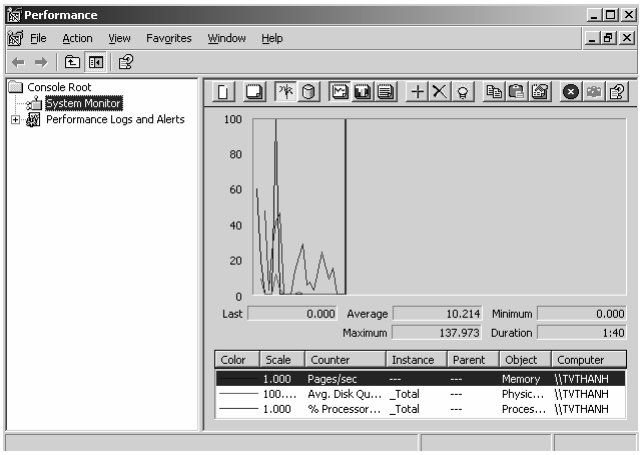
- Tên **driver**.
- Phiên bản.
- Bộ xử lý.
- Ngôn ngữ.
- Loại dữ liệu mặc định.
- Đường dẫn của **driver**.



IX. GIÁM SÁT TRẠNG THÁI HÀNG ĐỢI MÁY IN.

Chúng ta có thể dùng tiện ích **System Monitor** để quản lý hàng đợi máy in. **System Monitor** được dùng để theo dõi các **counter** liên quan đến thao tác thực hiện cho nhiều đối tượng máy tính. Muốn quản lý hàng đợi máy in bằng **System Monitor**, ta thực hiện theo các bước sau:

1. Chọn **Start** ⏲ **Administrative Tools** ⏲ **Performance**.
2. Hộp thoại **Performance** sẽ xuất hiện. Mặc định thì tiện ích **System Monitor** sẽ được chọn như hình sau:



3. Nhấp chuột vào nút **Add** (có biểu tượng dấu +) để truy xuất vào hộp thoại **Add Counters**. Sau đó, nhấp chọn **Print Queue Performance Object.**

4. Trong hộp thoại **Add Counters**, bạn có thể chỉ định ra máy tính mà bạn muốn giám sát (cả máy tính cục bộ và máy tính ở xa). **Performance Object** mà bạn cần theo dõi (trong trường hợp này là hàng đợi - **Print Queue**), các **counter** mà bạn muốn theo dõi, và bạn cũng chỉ ra là bạn có muốn theo dõi tất cả các thể hiện hay là bạn chỉ muốn theo dõi một số thể hiện của **counter** được bạn lựa chọn. Nếu bạn chọn tất cả các thể hiện được lựa chọn sẽ cho phép tất cả dữ liệu của tất cả các hàng đợi in ấn đã được định nghĩa trong máy in. Còn nếu bạn chọn chỉ theo dõi một số thể hiện của **counter** thì bạn chỉ theo dõi được dữ liệu từ một số hàng đợi in ấn cá nhân.

Bảng danh sách các hàng đợi in ấn đã được định nghĩa:

Print Queue Counter	Mô tả
Add Network Printer Calls	Counter này sẽ chỉ ra bao nhiêu **Print Server** đã được thêm vào các máy in được chia sẻ trong mạng. Con số này được tích lũy từ lần khởi động cuối cùng của **server.**
Bytes Printed/Sec	Số **byte** trong thực tế đã được in trên một hàng đợi trong mỗi giây
Enumerate Network Printer Calls	Chỉ ra có bao nhiêu yêu cầu đã được gửi đến **Print Server** từ các danh sách duyệt mạng. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Job Errors	Tổng số các lỗi thao tác đã được tường trình bởi hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Jobs	Chỉ ra con số hiện tại các thao tác in ấn vẫn còn trong hàng đợi chưa được xử lý.
Job Spooling	Chỉ ra con số hiện tại các thao tác in ấn đã được điều hướng đến hàng đợi in ấn..

Max Jobs Spooling	Chỉ ra con số tối đa các thao tác in ấn đã được lưu trữ trong hàng đợi in

	ấn kể từ lần khởi động cuối cùng của **Server**.
Max References	Chỉ ra con số tối đa các tác vụ mở (tham chiếu) đã được gửi đến máy in kể từ lần khởi động cuối cùng của **Server**.
Not Ready Errors	Chỉ ra số lượng các lỗi máy in "chưa sẵn sàng phục vụ" đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Out of Paper Errors	Chỉ ra số lượng các lỗi máy in không có giấy đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Total Jobs Printed	Được sử dụng để hiển thị bao nhiêu tác vụ in ấn đã được thực hiện thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Total Pages Printed	Được sử dụng để hiển thị bao nhiêu trang đã được in thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.

Bài 17
DỊCH VỤ TRUY CẬP TỪ XA

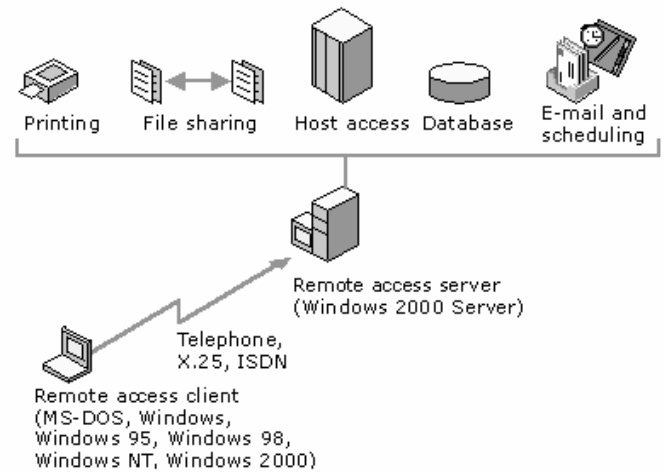
Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ truy cập từ xa, cho phép máy trạm ở xa có thể quay số kết nối vào công ty thông qua đường dây điện thoại, chia sẻ Internet đơn giản …	I. Xây dựng một Remote Access Server. II. Xây dựng một Internet Connection Server.	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.

I. XÂY DỰNG MỘT REMOTE ACCESS SERVER.

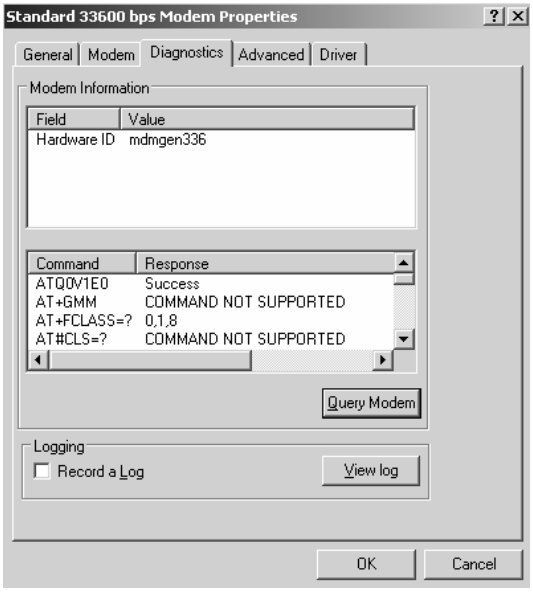
Giả sử bạn định xây dựng một hệ thống mạng cho phép các người dùng di động (**mobile user**) hoặc các văn phòng chi nhánh ở xa kết nối về. Để đáp ứng được nhu cầu trên bạn phải thiết lập một **Remote Access Server** (**RAS**). Khi máy tính **Client** kết nối thành công vào **RAS**, máy tính này có thể truy xuất đến toàn bộ hệ thống mạng phía sau **RAS**, nếu được cho phép, và thực hiện các thao tác như thể máy đó đang kết nối trực tiếp vào hệ thống mạng.



I.1. Cấu hình RAS server.

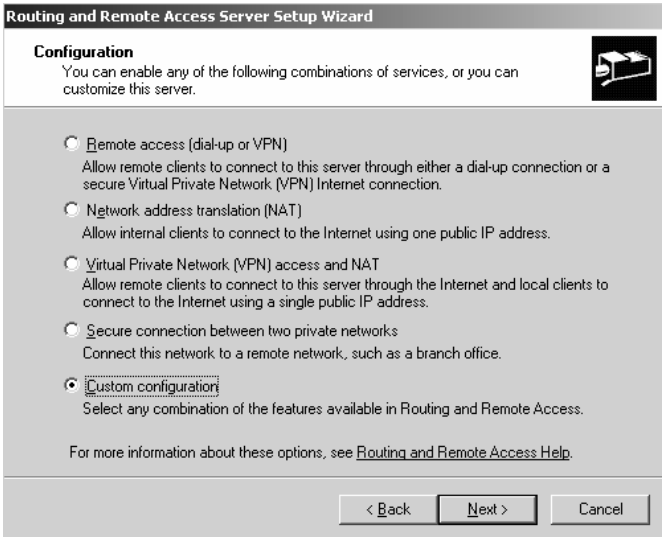
Sau đây là các bước xây dựng một **RAS Server** dùng các kết nối quay số.

Đầu tiên, bạn phải đảm bảo đã cài **driver** cho các modem định dùng để nhận các cuộc gọi vào. Để kiểm tra, bạn vào **Start** ◴ **Settings** ◴ **Control Panel** ◴ **Phone and Modem Options**, trong hộp thoại **Phone and Modem Options**, bạn chọn **Modem** cần kiểm tra và nhấp chuột vào nút **Properties**. Tại hộp thoại **Properties**, bạn chọn **Tab Diagnostics** và nhấp chuột vào nút **Query Modem** để hệ thống kiểm tra **Modem** hiện tại, nếu có lỗi thì hệ thống sẽ thông báo.

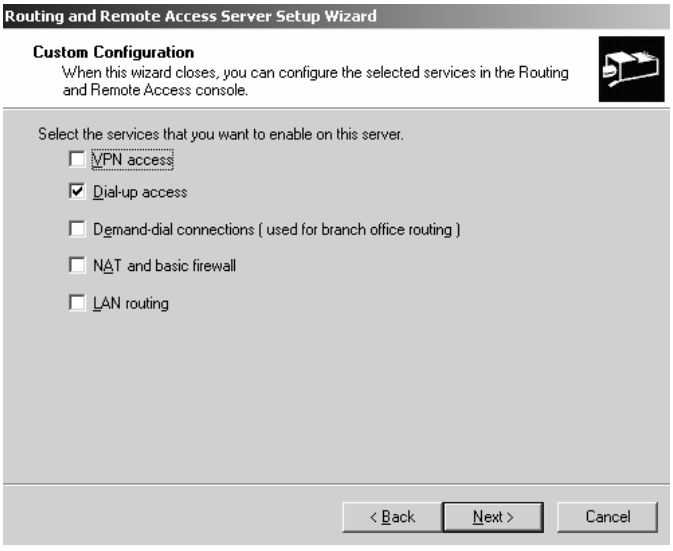


Tiếp theo bạn cần kích hoạt dịch vụ **Routing and Remote Access** trên **Windows Server 2003**. Bạn nhấp chuột vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Routing and Remote Access**, hộp thoại mở ra bạn nhấp phải chuột lên biểu tượng server của bạn, chọn **Configure and Enable Routing and Remote Access**. Chương trình sẽ xuất hiện hộp thoại **Welcome to the Routing and Remote Access Server Setup Wizard**. Nhấn **Next** để tiếp tục.

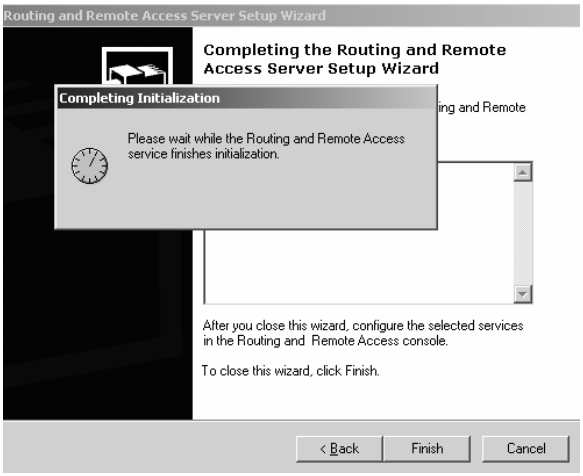
Trong hộp thoại tiếp theo, **Configuration**, bạn chọn **Custom configuration** và chọn **Next**.



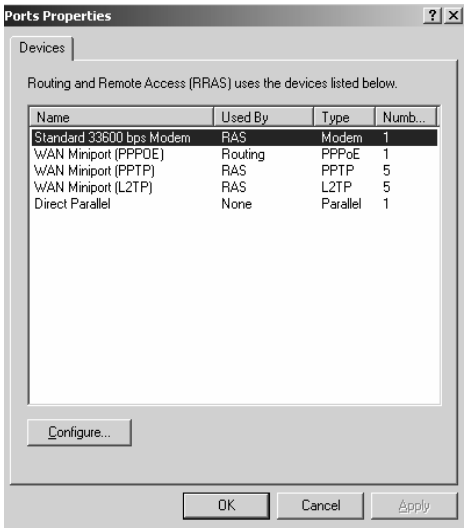
Tiếp theo hộp thoại **Custom Configuration** xuất hiện, bạn chọn mục **Dial-up access** vì chúng ta cần xây dựng một **Server** cho phép các máy tính ở xa truy cập vào. Sau đó bạn nhấp chuột vào nút **Next** để tiếp tục. Hộp thoại **Completing the Routing and Remote Access Server Setup Wizard** xuất hiện, chọn **Finish** để kết thúc.



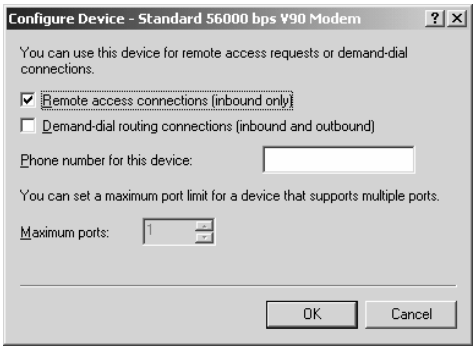
Một hộp thoại cảnh báo xuất hiện, yêu cầu bạn cho biết có khởi động dịch vụ này lên hay không? Bạn chọn **Yes** để khởi động dịch vụ.



Trong cửa sổ chính của chương trình, bạn cấu hình cho phép hệ thống dùng **modem** để nhận các cuộc gọi. Nhấp phải chuột lên mục **Ports**, chọn **Properties**. Hộp thoại **Ports Properties** xuất hiện. Trong hộp thoại này, chọn một thiết bị **Modem** và nhấn **Configure** để cấu hình.

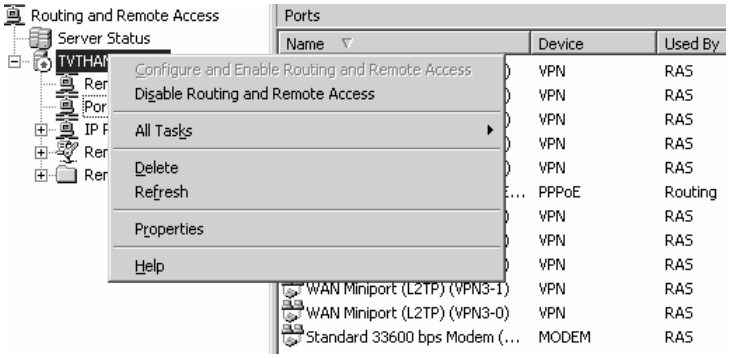


Xuất hiện hộp thoại **Configure Device**. Trong hộp thoại này, chọn vào mục **Remote access connections (inbound only)**, chỉ chấp nhận các cuộc gọi hướng vào. Sau đó nhấn nút **OK**.

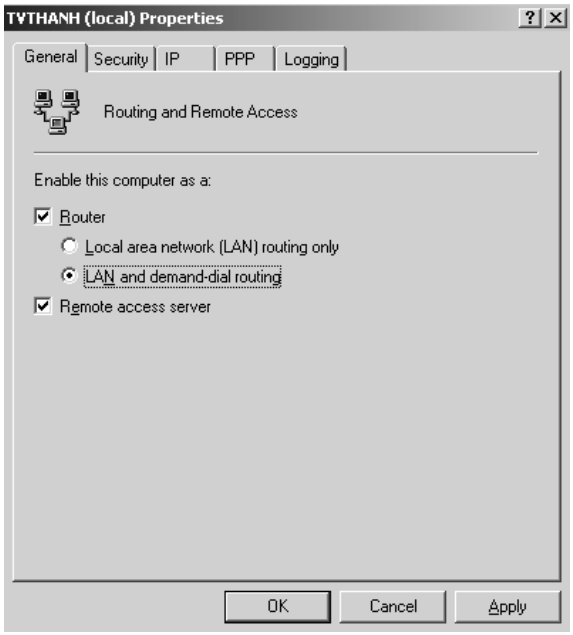


Lặp lại bước (7) cho các thiết bị **modem** khác. Sau khi đã thực hiện xong, nhấn nút **OK** để đóng hộp thoại **Ports Properties** lại. Tiếp theo, bạn sẽ cấu hình để **Server** thực hiện chức năng RAS. Nhấn phải

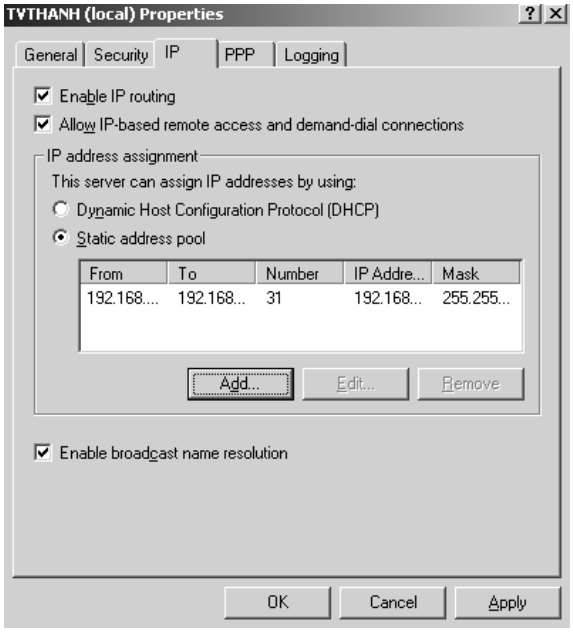
chuột lên biểu tượng **Server** và chọn **Properties**.



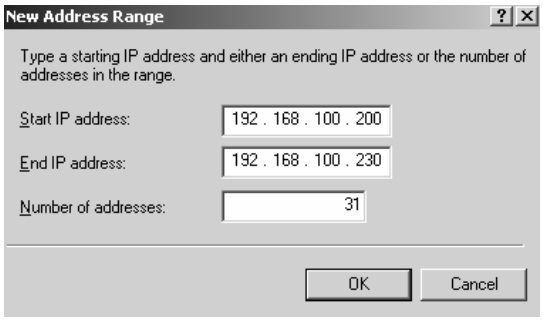
Hộp thoại **Server Properties** xuất hiện. Trong **Tab General**, bạn chọn các mục **Router**, **LAN and dial-demand routing** và mục **Remote access server**.



Tiếp theo, bạn chọn Tab **IP**. Tab này chỉ xuất hiện khi hệ thống mạng của bạn có sử dụng bộ giao thức TCP/IP. Phần **IP address assignment** chỉ định cách cấp phát địa chỉ IP cho các **RAS Client** khi quay số vào. Nếu hệ thống mạng đã thiết lập một **DHCP Server** thì bạn có thể nhờ **DHCP Server** này cấp phát địa chỉ cho các **RAS Client** (chọn mục **Dynamic Host Configuration Protocol**). Nếu không có, bạn phải chỉ định danh sách các địa chỉ sẽ cấp phát (chọn mục **Static address pool**). Trong ví dụ này, bạn sẽ nhập vào danh sách địa chỉ **IP**.



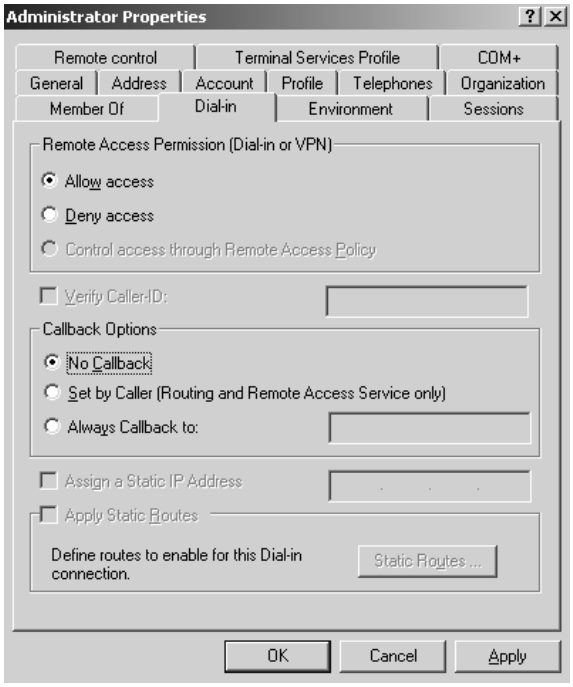
Để bổ sung danh sách địa chỉ, chọn mục **Static address pool** và nhấn **Add**. Xuất hiện hộp thoại **New Address Range**. Trong hộp thoại này, bạn nhập vào địa chỉ bắt đầu và địa chỉ kết thúc của danh sách. Các địa chỉ này nên lấy từ đường mạng của **RAS Server**. Nếu bạn sử dụng đường mạng khác, bạn phải đặt các đường đi tĩnh cho từng đường mạng mới đó. Sau đó nhấn **OK** để đồng ý tạo.



Các Tab khác chúng ta để mặc định, sau khi đã cấu hình xong, nhấn **OK** để đóng hộp thoại **Server Properties** lại.

Bước tiếp theo là cấu hình các tài khoản dùng để quay số. Bạn có thể tạo trong **local security database** nếu **RAS Server** nằm trong **workgroup** hoặc tạo trên **Active Directory database** nếu là thành viên của một **domain**. Kích hoạt chương trình **Local User and Group** (hoặc **Active Directory Users and Computers** tuỳ theo ví trị tạo tài khoản), nhấp phải chuột lên tài khoản định cấu hình và chọn **Properties**.

Hộp thoại **User Properties** xuất hiện. Bạn chọn Tab **Dial-in** và chọn mục **Allow Access** để cho phép người dùng này được phép truy cập từ xa thông qua quay số. Ngoài ra trong hộp thoại này cũng cho phép bạn chọn chế độ quay số, nếu chọn mặc định (**No Callback**) thì phía máy trạm sẽ trả phí điện thoại, nhưng nếu bạn chọn chế độ **Callback** thì phía Server sẽ trả chi phí điện thoại trong quá trình quay số để truyền dữ liệu. Sau đó nhấn **OK** để đóng hộp thoại lại.



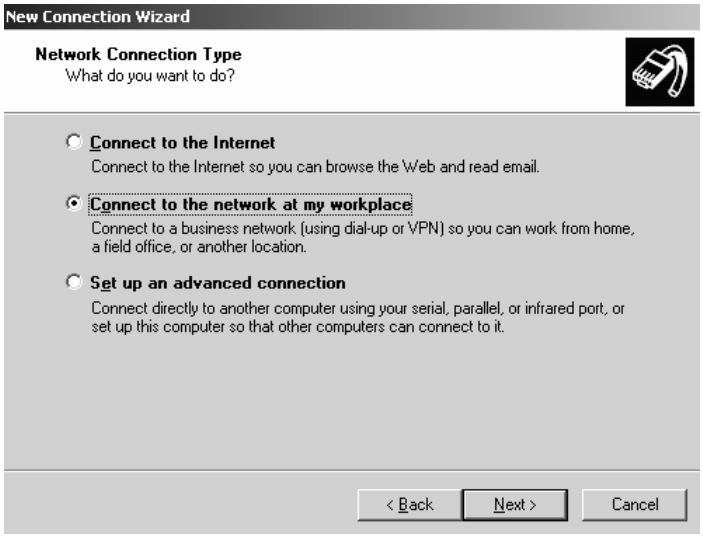
Như vậy là bạn đã cấu hình xong một **RAS Server**. Người dùng có thể bắt đầu dùng tài khoản đã cấp thực hiện kết nối từ xa qua đường quay số, truy xuất vào hệ thống mạng ở cơ quan.

I.2. Cấu hình RAS client.

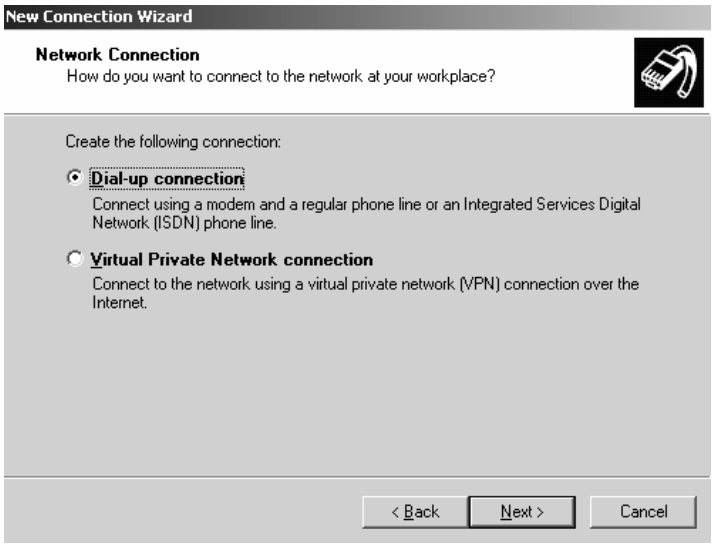
Tiếp theo chúng ta tạo một **network connection** trên máy trạm để quay số đến một **RAS Server**. Máy trạm có thể sử dụng hệ điều hành **Win98**, **WinME**, **Win2000**, **WinXP**… Để kết nối đến một **RAS Server**, bạn cần tối thiểu ba thông tin như: số điện thoại của **RAS Server**, **username** và **passwork** do **RAS Server** cấp. Trong ví dụ này chúng ta dùng máy **Windows Server 2003 Stand-alone** để minh họa, các bước thực hiện như sau:

Mở menu **Start** ⏲ **Settings** ⏲ **Network and Dial-up Connections**. Trong cửa sổ **Network and Dial-up Connections**, nhấp đôi chuột vào **Make New Connection**. Xuất hiện hộp thoại **Welcome to the Network Connection Wizard**, bạn nhấn **Next** để tiếp tục.

Trong hộp thoại **Network Connection Type**, bạn chọn mục **Connect to the network at my workplace** vì ở đây chúng ta kết nối với **RAS Server** nội bộ của công ty, không kết nối **Internet**. Sau đó nhấn nút **Next** để tiếp tục.



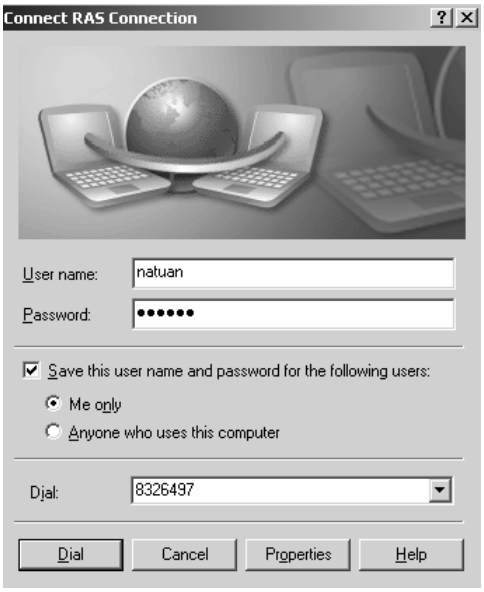
Tiếp theo bạn chọn loại kết nối là **Dial-up** hay **VPN**, ở đây chúng ta chọn kết nối kiểu quay số dùng **Modem**.



Theo hướng dẫn của chương trình, bạn sẽ nhập tên của kết nối này, số điện thoại cần gọi đến của **RAS Server**, kết nối này chỉ dùng cho người dùng hiện tại hay cho mọi người.

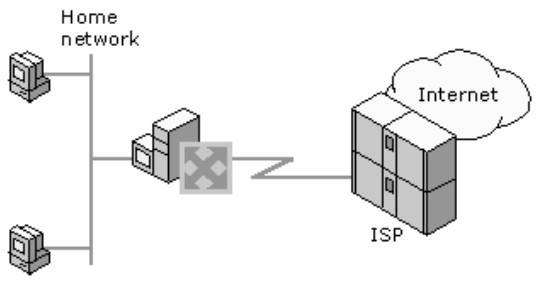
Cuối cùng, hộp thoại **Completing the Network Connection Wizard** xuất hiện bạn nhấn nút **Finish** để hoàn thành quá trình tạo kết nối.

Khi muốn thiết lập kết nối, bạn kích hoạt biểu tượng của **Connection** mới tạo, hộp thoại **Connect** xuất hiện, bạn nhập vào **username** và **password** đã được tạo ra trên **RAS Server** (hay nói cách khác là đã được quản trị **RAS Server** cấp phát), kiểm tra lại số điện thoại của **RAS Server** và nhấn nút **Dial**.



II. XÂY DỰNG MỘT INTERNET CONNECTION SERVER.

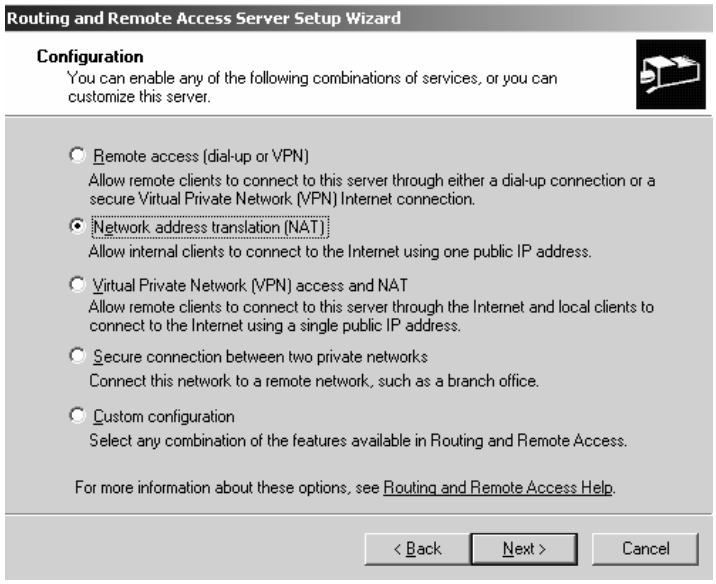
Bạn đang quản lý một hệ thống mạng nhỏ, sử dụng giao thức **TCP/IP** và bạn định thiết lập kết nối Internet cho hệ thống mạng của mình. Thông thường, các hệ thống mạng như vậy sử dụng địa chỉ riêng (**private address**). Để các máy tính bên trong mạng có thể truy xuất ra mạng **Internet**, bạn cần phải có một máy tính đóng vai trò như một **Router** hỗ trợ **NAT** (**Network Address Translation**).



II.1. Cấu hình trên server.

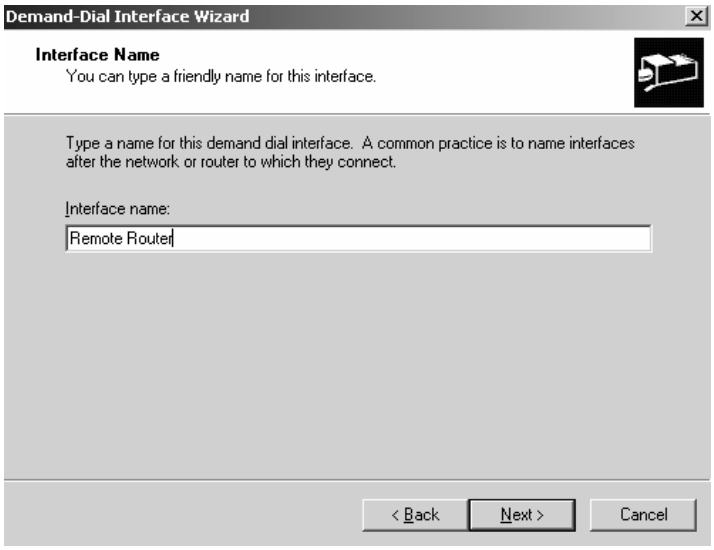
Bạn có thể sử dụng dịch vụ **Routing and Remote Access** để xây dựng một **Internet Connection Server** hỗ trợ **NAT**, phục vụ cho mục đích trên. Cách thực hiện như sau:

Đầu tiên, bạn phải đảm bảo đã cài driver cho các modem. Thực hiện kiểm tra như hướng dẫn trong phần trên. Cấu hình để các **Modem** này chấp nhận các cuộc gọi ra ngoài khi có nhu cầu (**demand-dial**). Thực hiện theo các bước như trong mục trên nhưng đến hộp thoại **Configuration**, bạn chọn trong **Network address translation (NAT)**.

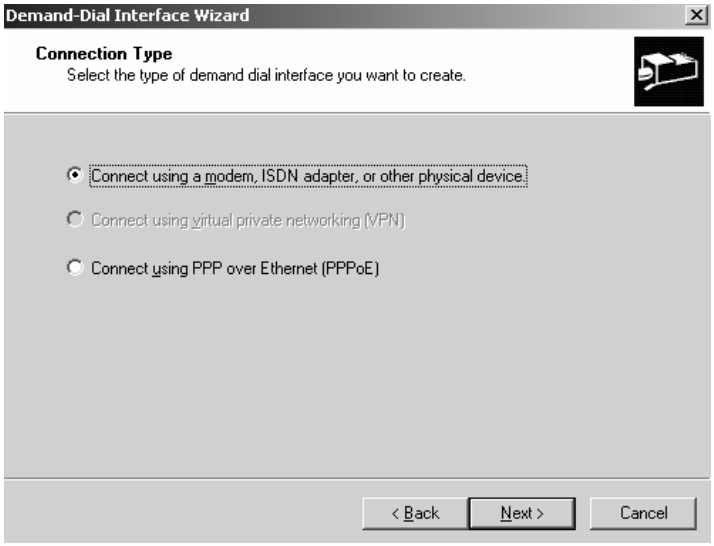


Tiếp theo hộp thoại **NAT Internet Connection** xuất hiện, bạn để mặc định vì chúng ta cần tạo một **demand-dial interface**. Bạn nhấn **Next** để chương trình tiếp tục.

Hộp thoại **Interface Name** yêu cầu bạn đặt cho **interface** mới này một cái tên. Thông thường bạn nên đặt tên của **Router** ở xa để dễ quản lý.

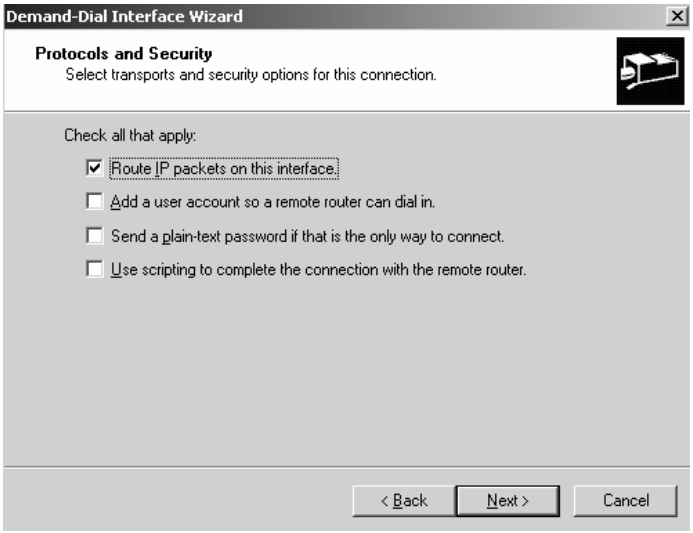


Hộp thoại **Connection Type** yêu cầu bạn chọn loại kết nối mà **interface** này sử dụng.

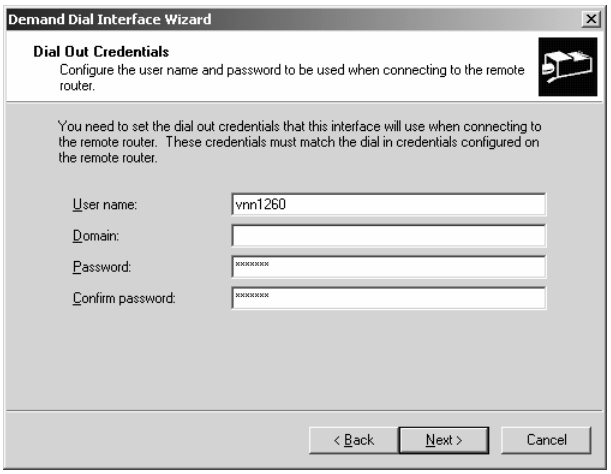


Hộp thoại **Select a device** yêu cầu bạn chọn loại thiết bị kết nối dùng cho **interface**.

Trong hộp thoại **Phone Number**, bạn nhập vào số điện thoại mà **ISP** cung cấp cho bạn. Hộp thoại **Protocols and Security** yêu cầu bạn chọn loại giao thức chuyển vận và các tuỳ chọn an toàn cho kết nối. Thông thường, bạn nên chọn **Route IP packets on this interface**.

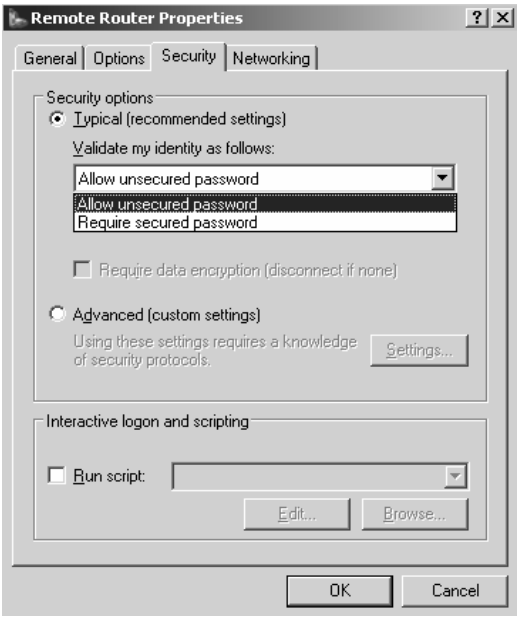


Trong hộp thoại **Dial Out Credentials**, bạn nhập vào thông tin tài khoản dùng để kết nối đến **ISP** (cũng chính **ISP** sẽ cung cấp cho bạn).

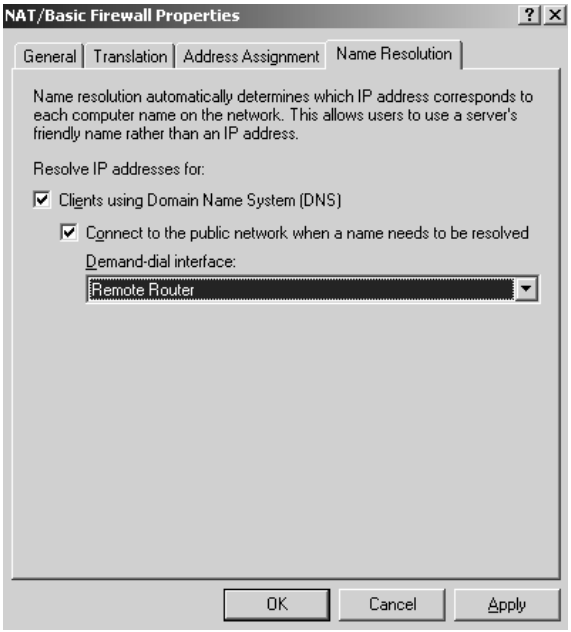


Cuối cùng hộp thoại **Completing the demand dial interface wizard** cho biết kết thúc quá trình cấu hình. Bạn nhấn **Finish** để kết thúc.

Sau khi đã tạo xong **demand-dial interface**, tuỳ theo **ISP** có chấp nhận việc thiết lập kết nối an toàn hoặc không an toàn. Hiện tại các nhà cung cấp dịch vụ ở Việt Nam cung cấp các kết nối không mã hóa. Trong mục **Network Interfaces**, nhấn phải chuột lên **demand-dial interface** mới tạo, chọn **Properties**. Trong hộp thoại **Properties**, chọn Tab **Security**. Trong phần **Security options**, mục **Validate my identity as follows**, bạn có thể chọn **Require secured password** hoặc **Allow unsecured password** (nếu quay số vào **ISP** thông thường thì nên chọn mục này).



Mở rộng mục **IP Routing** trong cửa sổ **Routing and Remote Access**, nhấn phải chuột lên mục **NAT** và chọn **Properties**. Trong hộp thoại **NAT Properties**, bạn chọn Tab **Name Resolution**. Trong Tab này, bạn chọn mục **Clients using Domain Name System (DNS)**. Nếu muốn mỗi khi có yêu cầu phân giải tên thì **Server** sẽ kết nối vào mạng thì bạn chọn luôn mục **Connect to the public network when a name needs to be resolved** và chọn **demand-dial interface** vừa tạo. Sau khi chọn xong nhấn **OK** để kết thúc.



II.2. Cấu hình trên máy trạm.

Do server bạn vừa thiết lập trên đây là một **NAT router** và một **Forwarder DNS Server**, cho nên trên các máy trạm, ngoài việc cấu hình TCP/IP về địa chỉ **IP**, **subnet mask**, bạn phải chỉ định **default gateway** và **DNS Server** là địa chỉ của **Server** trên.

Tóm tắt

Lý thuyết 6 tiết - Thực hành 12 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học giúp học viên hiểu nguyên tắc hoạt động, tổ chức, cài đặt và quản trị dịch vụ phân giải tên miền DNS, hiểu được mô hình phân giải tên trên hệ thống mạng Internet.	I. Tổng quan về DNS II. Cách phân bổ dữ liệu quản lý Domain Name. III. Cơ chế phân giải tên miền IV. Một số khái niệm cơ bản. V. Phân loại Domain Name Server. VI. Resource Record (RR) VII. Cài đặt và cấu hình dịch vụ DNS	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

I. Tổng quan về DNS.

I.1. Giới thiệu DNS.

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết rõ địa chỉ **IP** của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ **IP** này rất là khó khăn.

Mỗi máy tính ngoài địa chỉ **IP** ra còn có một tên (hostname). Đối với con người việc nhớ tên máy dù sao cũng dễ dàng hơn vì chúng có tính trực quan và gợi nhớ hơn địa chỉ **IP**. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ **IP** thành tên máy tính.

Ban đầu do quy mô mạng **ARPA NET** (tiền thân của mạng **Internet**) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ **IP**. Trong đó tên máy chỉ là 1 chuỗi văn bản không phân cấp (**flat name**). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin **HOSTS.TXT** có các nhược điểm như sau:

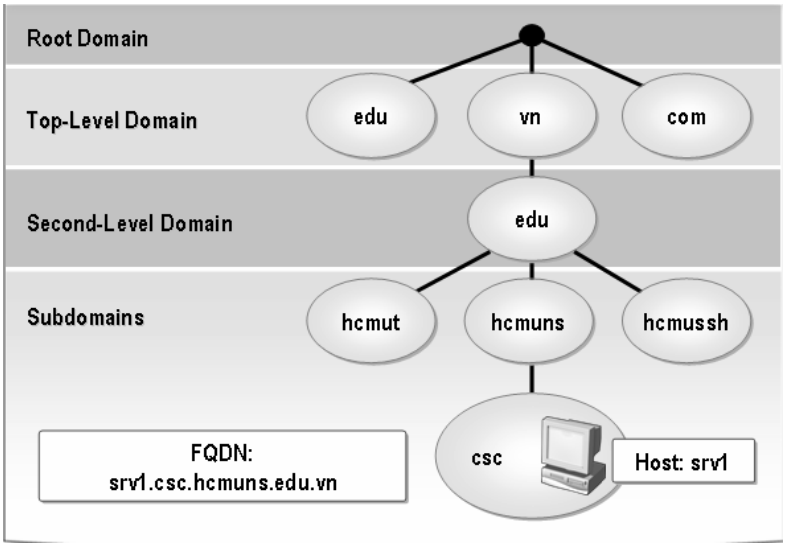
- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng “cổ chai”.
- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT . Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

Tóm lại việc dùng tập tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó, dịch vụ **DNS** ra đời nhằm khắc phục các nhược điểm này. Người thiết kế cấu trúc của dịch vụ **DNS** là **Paul Mockapetris** - **USC's Information Sciences Institute**, và các khuyến nghị **RFC** của **DNS** là **RFC** 882 và 883, sau đó là **RFC** 1034 và 1035 cùng với 1 số **RFC** bổ sung như bảo mật trên hệ thống **DNS**, cập nhật động các bản ghi **DNS** …

Lưu ý: Hiện tại trên các máy chủ vẫn sử dụng được tập tin hosts.txt để phân giải tên máy tính thành địa chỉ **IP** (trong Win**d**ows tập tin này nằm trong thư mục **WINDOWS\system32\drivers\etc**)

Dịch vụ **DNS** hoạt động theo mô hình **Client-Server**: phần **Server** gọi là máy chủ phục vụ tên hay còn gọi là **Name Server**, còn phần **Client** là trình phân giải tên - **Resolver**. **Name Server** chứa các thông tin CSDL của **DNS**, còn **Resolver** đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (**query**) và gửi chúng qua đến **Name Server**. **DNS** được thi hành như một giao thức tầng **Application** trong mạng **TCP/IP**.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình **Client-Server**. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (**replication**) và lưu tạm (**caching**). Một **hostname** trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).



Hình 1.1: Sơ đồ tổ chức DNS

Cơ sở dữ liệu(CSDL) của **DNS** là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL **DNS** gọi là 1 miền (**domain**). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (**subdomain**).

Mỗi **domain** có 1 tên (**domain name**). Tên **domain** chỉ ra vị trí của nó trong CSDL **DNS**. Trong **DNS** tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm.

Tên nhãn bên phải trong mỗi **domain name** được gọi là **top-level domain**. Trong ví dụ trước srv1.csc.hcmuns.edu.vn, vậy miền ".vn" là **top-level domain**. Bảng sau đây liệt kê **top-level domain**.

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Vì sự quá tải của những **domain name** đã tồn tại, do đó đã làm phát sinh những **top-level domain**

mới. Bảng sau đây liệt kê những **top-level domain** mới.

Tên miền	Mô tả
.arts	Những tổ chức liên quan đến nghệ thuật và kiến trúc
.nom	Những địa chỉ cá nhân và gia đình
.rec	Những tổ chức có tính chất giải trí, thể thao
.firm	Những tổ chức kinh doanh, thương mại.
.info	Những dịch vụ liên quan đến thông tin.

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-leveldomain** của Việt Nam là .vn, Mỹ là .us, ta có thể tham khảo thêm thông tin địa chỉ tên miền tại địa chỉ: **http://www.thrall.org/domains.htm**

Ví dụ về tên miền của một số quốc gia.

Tên miền quốc gia	Tên quốc gia
.vn	Việt Nam
.us	Mỹ
.uk	Anh
.jp	Nhật Bản
.ru	Nga
.cn	Trung Quốc
…	…

I.2. Đặt điểm của DNS trong Windows 2003.

- **Conditional forwarder**: Cho phép **Name Server** chuyển các yêu cầu phân giải dựa theo tên domain trong yêu cầu truy vấn.
- **Stub zone**: hỗ trợ cơ chế phân giải hiệu quả hơn.
- Đồng bộ các **DNS zone** trong **Active Directory** (**DNS zone replication in Active Directory**).
- Cung cấp một số cơ chế bảo mật tốt hơn trong các hệ thống **Windows** trước đây.
- Luân chuyển (**Round robin**) tất cả các loại **RR**.

- Cung cấp nhiêu cơ chế ghi nhận và theo dõi sự cố lỗi trên **DNS**.

- Hỗ trợ giao thức **DNS Security Extensions** (**DNSSEC**) để cung cấp các tính năng bảo mật cho việc lưu trữ và nhân bản (**replicate**) **zone**.
- Cung cấp tính năng **EDNS0** (**Extension Mechanisms for DNS**) để cho phép **DNS Requestor** quản bá những **zone transfer packet** có kích thước lớn hơn 512 byte.

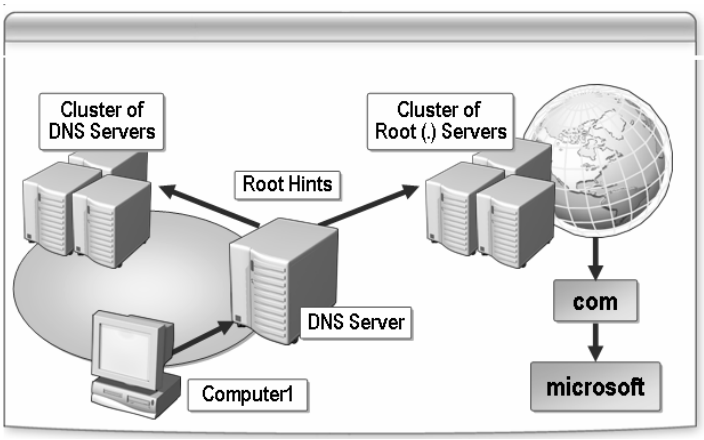
II. Cách phân bổ dữ liệu quản lý domain name.

Những **root name server** (.) quản lý những **top-level domain** trên **Internet**. Tên máy và địa chỉ **IP** của những **name server** này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những **name server** này cũng có thể đặt khắp nơi trên thế giới.

Tên máy tính	Địa chỉ IP
H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107
C.ROOT-SERVERS.NET	192.33.4.12
D.ROOT-SERVERS.NET	128.8.10.90
E.ROOT-SERVERS.NET	192.203.230.10
I.ROOT-SERVERS.NET	192.36.148.17
F.ROOT-SERVERS.NET	192.5.5.241
F.ROOT-SERVERS.NET	39.13.229.241
G.ROOT-SERVERS.NET	192.112.88.4
A.ROOT-SERVERS.NET	198.41.0.4

Thông thường một tổ chức được đăng ký một hay nhiều **domain name**. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều **name server** và duy trì cơ sở dữ liệu cho tất cả những máy tính trong **domain**. Những **name server** của tổ chức được đăng ký trên **Internet**. Một trong những **name server** này được biết như là **Primary Name Server**. Nhiều **Secondary Name Server** được dùng để làm **backup** cho **Primary Name Server**. Trong trường hợp **Primary** bị lỗi, **Secondary** được sử dụng để phân giải tên.

Primary Name Server có thể tạo ra những **subdomain** và ủy quyền những **subdomain** này cho những **Name Server** khác.



Hình 1.2: **Root hints**.

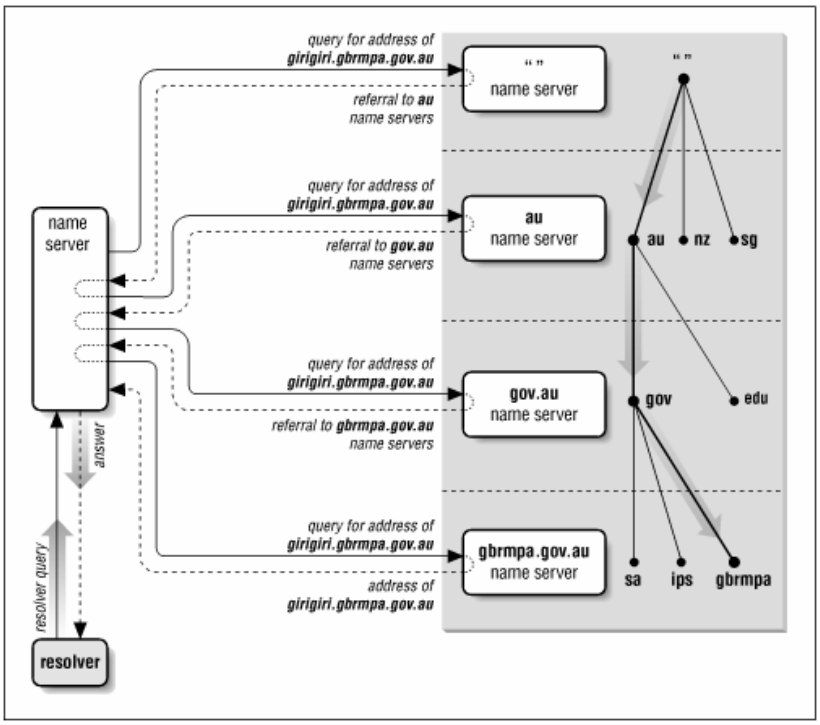
III. Cơ chế phân giải tên.

III.1. Phân giải tên thành IP.

Root name server : Là máy chủ quản lý các **name server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp tên và địa chỉ **IP** của **name server** quản lý **top-level domain** (Thực tế là hầu hết các **root server** cũng chính là máy chủ quản lý **top-level domain**) và đến lượt các **name server** của **top-level domain** cung cấp danh sách các **name server** có quyền trên các **second-level domain** mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

Qua trên cho thấy vai trò rất quan trọng của **root name server** trong quá trình phân giải tên miền. Nếu mọi **root name server** trên mạng **Internet** không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được.

Hình vẽ dưới mô tả quá trình phân giải grigiri.gbrmpa.gov.au trên mạng **Internet**

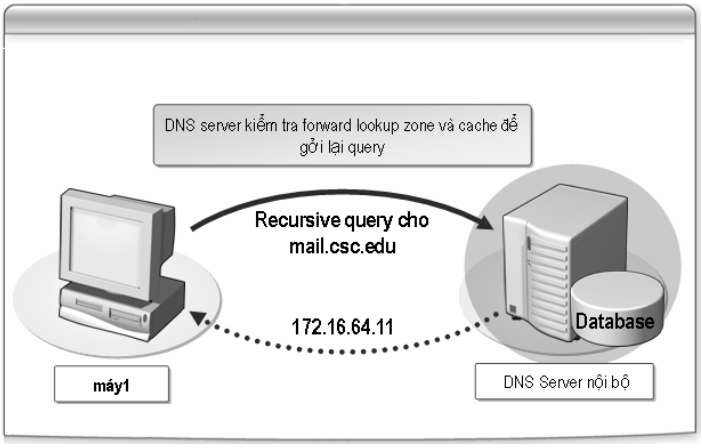


Hình 1.3: Phân giải **hostname** thành địa **IP**.

Client sẽ gửi yêu cầu cần phân giải địa chỉ **IP** của máy tính có tên girigiri.gbrmpa.gov.au đến **name server** cục bộ. Khi nhận yêu cầu từ **Resolver**, **Name Server** cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu như tên miền do **Server** cục bộ quản lý, nó sẽ trả lời địa chỉ **IP** của tên máy đó ngay cho **Resolver**. Ngược lại, server cục bộ sẽ truy vấn đến một **Root Name Server** gần nhất mà nó biết được. **Root Name Server** sẽ trả lời địa chỉ IP của **Name Server** quản lý miền au. Máy chủ **name server** cục bộ lại hỏi tiếp **name server** quản lý miền au và được tham chiếu đến máy chủ quản lý miền gov.au. Máy chủ quản lý gov.au chỉ dẫn máy **name server** cục bộ tham chiếu đến máy chủ quản lý miền gbrmpa.gov.au. Cuối cùng máy **name server** cục bộ truy vấn máy chủ quản lý miền gbrmpa.gov.au và nhận được câu trả lời.

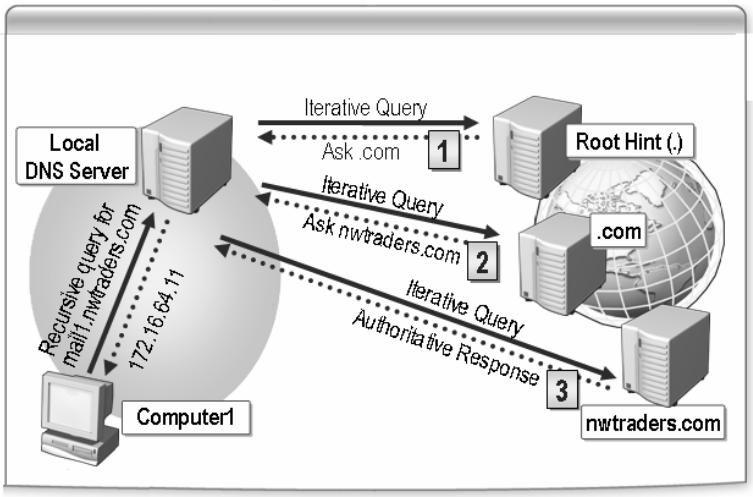
Các loại truy vấn : Truy vấn có thể ở 2 dạng :

- Truy vấn đệ quy (**recursive query**) : khi **name server** nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. **Name server** không thể tham chiếu truy vấn đến một **name server** khác. **Name server** có thể gửi truy vấn dạng đệ quy hoặc tương tác đến **name server** khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi.



Hình 1.4: **Recursive query**.

- Truy vấn tương tác (**Iteractive query**): khi **name server** nhận được truy vấn dạng này, nó trả lời cho **Resolver** với thông tin tốt nhất mà nó có được vào thời điểm lúc đó. Bản thân **name server** không thực hiện bất cứ một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy từ dữ liệu cục bộ (kể cả **cache**). Trong trường hợp **name server** không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của **name server** gần nhất mà nó biết.



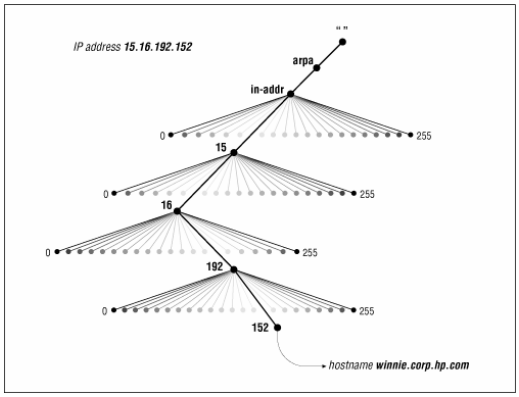
Hình 1.5: Iteractive query

III.2. Phân giải IP thành tên máy tính.

Ánh xạ địa chỉ **IP** thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống **UNIX** (kiểm tra các tập tin .rhost hay host.equiv). Trong không gian tên miền đã nói ở trên dữ liệu -bao gồm cả địa chỉ **IP**- được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ **IP** khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ **IP**, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ **IP**. Phần không gian này có tên miền là **in-addr.arpa**.

Mỗi nút trong miền **in-addr.arpa** có một tên nhãn là chỉ số thập phân của địa chỉ **IP**. Ví dụ miền **in-addr.arpa** có thể có 256 **subdomain**, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi **subdomain** lại có 256 **subdomain** con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ **IP** tương ứng.



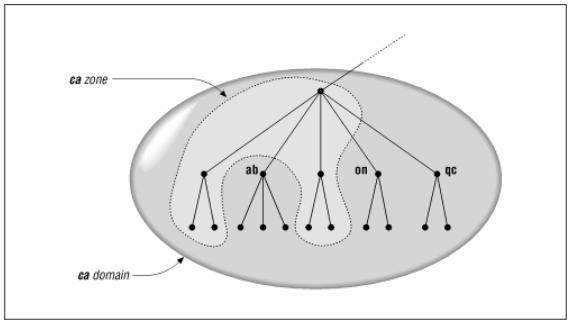
Hình 1.6: **Reverse Lookup Zone**.

- Lưu ý khi đọc tên miền địa chỉ **IP** sẽ xuất hiện theo thứ tự ngược. Ví dụ nếu địa chỉ **IP** của máy winnie.corp.hp.com là 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.in-addr.arpa.

IV. Một số Khái niệm cơ bản.

IV.1. Domain name và zone.

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (**subdomain**). Ví dụ, miền **ca** bao gồm nhiều miền con như **ab.ca, on.ca, qc.ca,...**(như Hình 1.7). Bạn có thể ủy quyền một số miền con cho những **DNS Server** khác quản lý. Những miền và miền con mà **DNS Server** được quyền quản lý gọi là **zone**. Như vậy, một **Zone** có thể gồm một miền, một hay nhiều miền con. Hình sau mô tả sự khác nhau giữa **zone** và **domain**.



Hình 1.7: **Zone** và **Domain**

Các loại **zone**:

- **Primary zone** : Cho phép đọc và ghi cơ sở dữ liệu.
- **Secondary zone** : Cho phép đọc bản sao cơ sở dữ liệu.
- **Stub zone** : chứa bản sao cơ sở dữ liệu của **zone** nào đó, nó chỉ chứa chỉ một vài **RR**.

IV.2. Fully Qualified Domain Name (FQDN).

Mỗi nút trên cây có một tên gọi(không chứa dấu chấm) dài tối đa 63 ký tự. Tên rỗng dành riêng cho gốc (**root**) cao nhất và biểu diễn bởi dấu chấm. Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiện tại đi ngược lên nút gốc, mỗi tên gọi cách nhau bởi dấu chấm. Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (**absolute**) khác với tên tương đối là tên không kết thúc bằng dấu chấm. Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (**Fully Qualified Domain Name – FQDN**).

IV.3. Sự ủy quyền(Delegation).

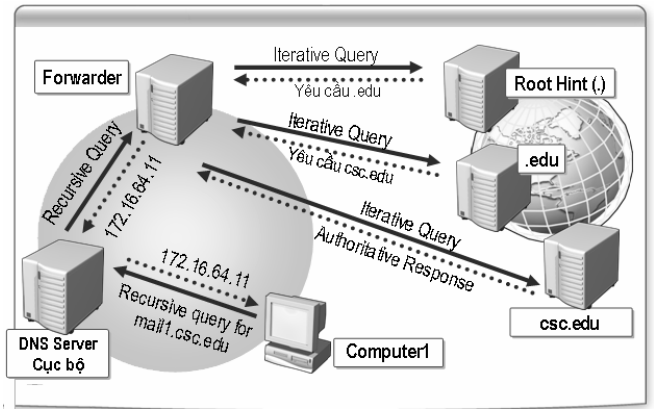
Một trong các mục tiêu khi thiết kế hệ thống **DNS** là khả năng quản lý phân tán thông qua cơ chế uỷ quyền (**delegation**). Trong một miền có thể tổ chức thành nhiều miền con, mỗi miền con có thể được uỷ quyền cho một tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong miền con này. Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.

Không phải một miền luôn luôn tổ chức miền con và uỷ quyền toàn bộ cho các miền con này, có thể chỉ có vài miền con được ủy quyền. Ví dụ miền **hcmuns.edu.vn** của Trường ĐHKHTN chia một số miền con như **csc.hcmuns.edu.vn** (Trung Tâm Tin Học), **fit.hcmuns.edu.vn** (Khoa CNTT) hay math.hcmuns.edu.vn (Khoa Toán), nhưng các máy chủ phục vụ cho toàn trường thì vẫn thuộc vào miền **hcmuns.edu.vn.**

IV.4. Forwarders.

Là kỹ thuật cho phép **Name Server** nội bộ chuyển yêu cầu truy vấn cho các **Name Server** khác để phân giải các miền bên ngoài.

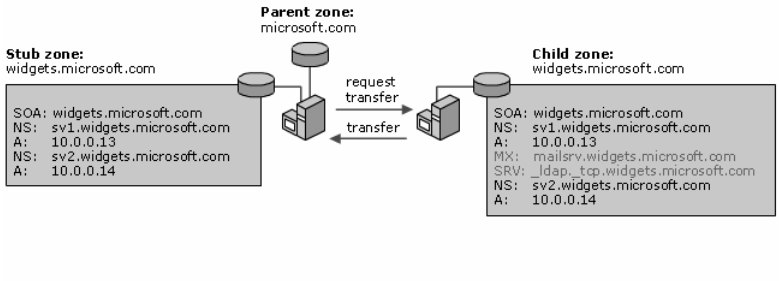
Ví dụ: Trong Hình 1.8, ta thấy khi **Internal DNS Servers** nhận yêu cầu truy vấn của máy trạm nó kiểm tra xem có thể phân giải được yêu cầu này hay không, nếu không thì nó sẽ chuyển yêu cầu này lên **Forwarder DNS server** (**multihomed**) để nhờ **name server** này phân giải dùm, sau khi xem xét xong thì **Forwarder DNS server** (**multihomed**) sẽ trả lời yêu cầu này cho **Internal DNS Servers** hoặc nó sẽ tiếp tục **forward** lên các **name server** ngoài **Internet**.



Hình 1.8: **Forward DNS queries**.

IV.5. Stub zone.

Là **zone** chứa bảng sao cơ sở dữ liệu **DNS** từ **master name server**, **Stub zone** chỉ chứa các **resource record** cần thiết như : **A**, **SOA**, **NS**, một hoặc vài địa chỉ của **master name server** hỗ trợ cơ chế cập nhật **Stub zone**, chế chứng thực **name server** trong **zone** và cung cấp cơ chế phân giải tên miền được hiệu quả hơn, đơn giản hóa công tác quản trị (Tham khảo Hình 1.9).

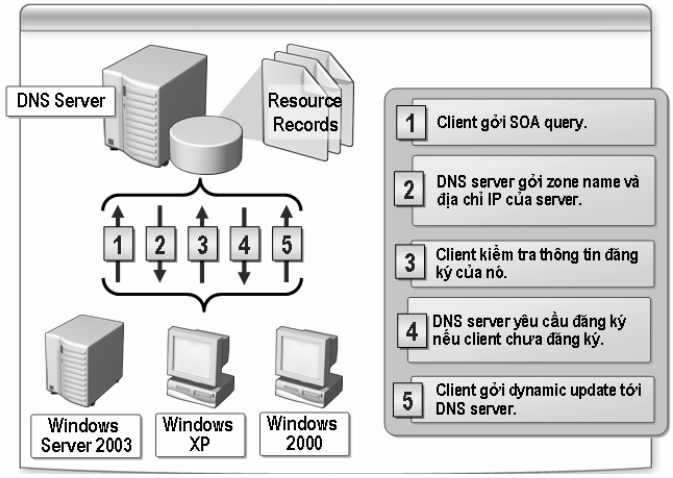


Hình 1.9: **Stub zone**.

IV.6. Dynamic DNS.

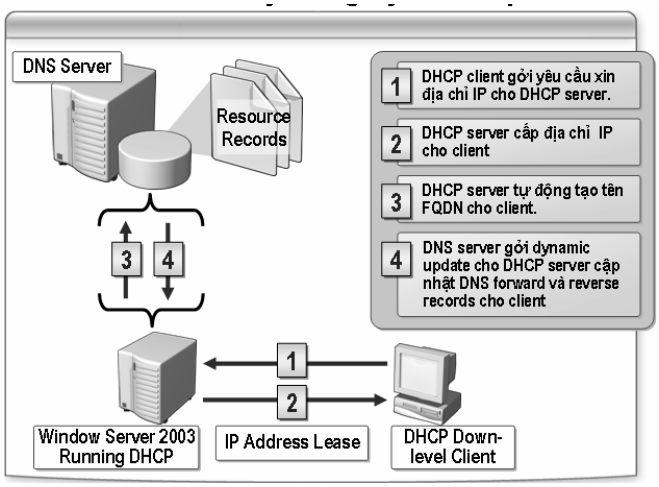
Dynamic DNS là phương thức ánh xạ tên miền tới địa chỉ **IP** có tần xuất thay đổi cao. Dịch vụ **DNS** động (**Dynamic DNS**) cung cấp một chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ **dynamic DNS** gọi là **Dynamic Dns Client**. Chương trình này giám sát sự thay đổi địa chỉ **IP** tại **host** và liên hệ với hệ thống **DNS** mỗi khi địa chỉ **IP** của **host** thay đổi và sau đó **update** thông tin vào cơ sở dữ liệu **DNS** về sự thay đổi địa chỉ đó.

DNS Client đăng ký và cập nhật **resource record** của nó bằng cách gởi **dynamic update**.



Hình 1.10: **Dynamic update**.

Các bước **DHCP Server** đăng ký và cập nhật **resource record** cho **Client**.



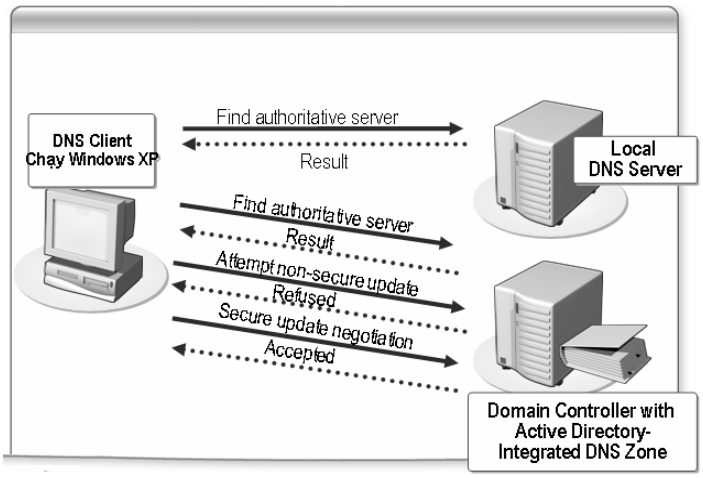
Hình 1.11: DHCP server cập nhật dynamic update.

IV.7. Active Directory-integrated zone.

Sử dụng **Active Directory-integrated zone** có một số thuận lợi sau:

- **DNS zone** lưu trữ trong trong **Active Directory**, nhờ cơ chế này mà dữ liệu được bảo mật hơn.
- Sử dụng cơ chế nhân bản của **Active Directory** để cập nhận và sao chép cơ sở dữ liệu **DNS**.
- Sử dụng **secure dynamic update**.
- Sử dụng nhiều **master name server** để quản lý tên miền thay vì sử dụng một **master name server**.

Mô hình **Active Directory-integrated zone** sử dụng **secure dynamic update**.



Hình 1.12: Secure dynamic update

V. Phân loại Domain Name Server.

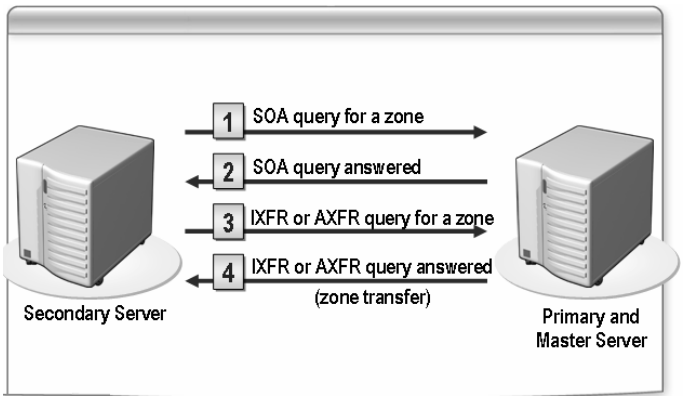
Có nhiều loại **Domain Name Server** được tổ chức trên Internet. Sự phân loại này tùy thuộc vào nhiệm vụ mà chúng sẽ đảm nhận. Tiếp theo sau đây mô tả những loại **Domain Name Server**.

V.1. Primary Name Server.

Mỗi miền phải có một **Primary Name Server**. **Server** này được đăng kí trên **Internet** để quản lý miền. Mọi người trên **Internet** đều biết tên máy tình và địa chỉ **IP** của **Server** này. Người quản trị **DNS** sẽ tổ chức những tập tin CSDL trên **Primary Name Server**. **Server** này có nhiệm vụ phân giải tất cả các máy trong miền hay **zone**.

V.2. Secondary Name Server.

Mỗi miền có một **Primary Name Server** để quản lý CSDL của miền. Nếu như **Server** này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ **IP** và ngược lại xem như bị gián đoạn. Việc gián đoạn này làm ảnh hưởng rất lớn đến những tổ chức có nhu cầu trao đổi thông tin ra ngoài **Internet** cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một **Server** dự phòng gọi là **Secondary**(hay **Slave**) **Name Server**. **Server** này có nhiệm vụ sao lưu tất cả những dữ liệu trên **Primary Name Server** và khi **Primary Name Server** bị gián đoạn thì nó sẽ đảm nhận việc phân giải tên máy tính thành địa chỉ **IP** và ngược lại. Trong một miền có thể có một hay nhiều **Secondary Name Server**. Theo một chu kỳ, **Secondary** sẽ sao chép và cập nhật CSDL từ **Primary Name Server**. Tên và địa chỉ **IP** của **Secondary Name Server** cũng được mọi người trên **Internet** biết đến.

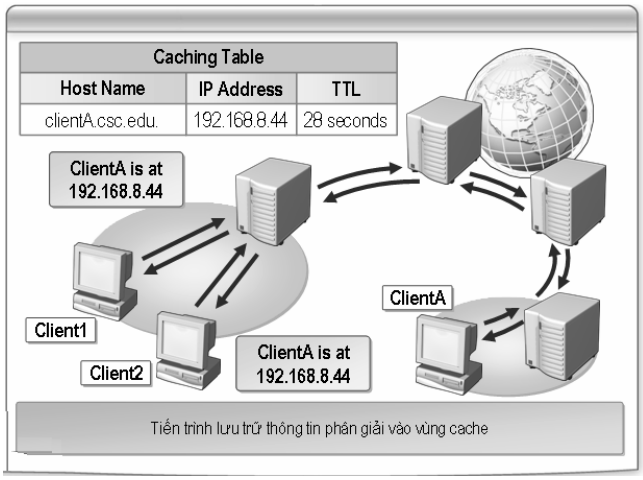


Hình 1.13: Zone tranfser

V.3. Caching Name Server.

Caching Name Server không có bất kỳ tập tin CSDL nào. Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những **Name Server** khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:

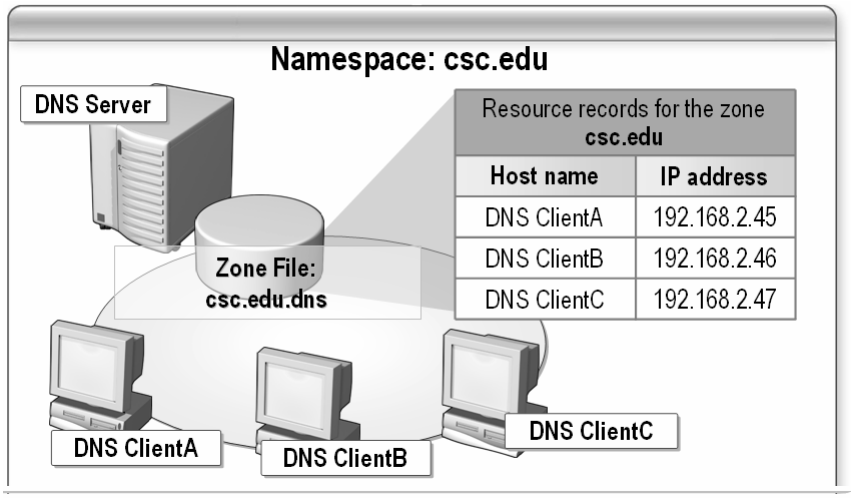
- Làm tăng tốc độ phân giải bằng cách sử dụng **cache**.
- Giảm bớt gánh nặng phân giải tên máy cho các **Name Server**.
- Giảm việc lưu thông trên những mạng lớn.



Hình .1.14: Bảng cache

VI. Resource Record (RR).

RR là mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu **DNS**, các mẫu tin này được lưu trong các file cơ sở dữ liệu **DNS** (**\systemroot\system32\dns**).



Hình 1.15: cơ sở dữ liệu

VI.1. SOA(Start of Authority).

Trong mỗi tập tin CSDL phải có một và chỉ một **record SOA** (**start of authority**). **Record SOA** chỉ ra rằng máy chủ **Name Server** là nơi cung cấp thông tin tin cậy từ dữ liệu có trong **zone**. Cú pháp của **record SOA**.

[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (

serial number;

refresh number;

retry number;

experi number;

Time-to-live number)

- **Serial :** Áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này bắt đầu từ 1 nhưng thông thường người ta sử dụng theo định dạng thời gian như 1997102301. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày và NN số lần sửa đổi dữ liệu **zone** trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu **zone**. Khi máy máy chủ **Secondary** liên lạc với máy chủ **Primary**, trước tiên nó sẽ hỏi số **serial**. Nếu số **serial** của máy **Secondary** nhỏ hơn số serial của máy **Primary** tức là dữ liệu **zone** trên **Secondary** đã cũ và sau đó máy **Secondary** sẽ sao chép dữ liệu mới từ máy **Primary** thay cho dữ liệu đang có hiện hành.
- **Refresh:** Chỉ ra khoảng thời gian máy chủ **Secondary** kiểm tra dữ liệu **zone** trên máy **Primary** để cập nhật nếu cần. Trong ví dụ trên thì cứ mỗi 3 giờ máy chủ **Secondary** sẽ liên lạc với máy chủ **Primary** để cập nhật dữ liệu nếu có. Giá trị này thay đổi tuỳ theo tần suất thay đổi dữ liệu trong zone.
- **Retry:** nếu máy chủ **Secondary** không kết nối được với máy chủ **Primary** theo thời hạn mô tả trong **refresh** (ví dụ máy chủ **Primary** bị **shutdown** vào lúc đó thì máy chủ **Secondary** phải tìm cách kết nối lại với máy chủ **Primary** theo một chu kỳ thời gian mô tả trong **retry**. Thông thường giá trị này nhỏ hơn giá trị **refresh**.

- **Expire:** Nếu sau khoảng thời gian này mà máy chủ **Secondary** không kết nối được với máy chủ **Primary** thì dữ liệu **zone** trên máy **Secondary** sẽ bị quá hạn. Một khi dữ liệu trên **Secondary** bị quá hạn thì máy chủ này sẽ không trả lời mọi truy vấn về **zone** này nữa. Giá trị **expire** này phải lớn hơn giá trị **refresh** và giá trị **retry**.
- **TTL:** Viết tắt của **time to live**. Giá trị này áp dụng cho mọi record trong **zone** và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ **Name Server** khác **cache** lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn **DNS** trên mạng.

VI.2. NS (Name Server).

Record tiếp theo cần có trong **zone** là **NS** (**name server**) **record**. Mỗi **Name Server** cho **zone** sẽ có một **NS record**.

Cú pháp:

[domain_name] IN NS [DNS-Server_name]

Ví dụ 2: Record NS sau:

t3h.com. IN NS dnsserver.t3h.com.

t3h.com. IN NS server.t3h.com.

chỉ ra 2 name servers cho miền t3h.com

VI.3. A (Address) và CNAME (Canonical Name).

Record A (**Address**) ánh xạ tên máy (**hostname**) vào địa chỉ **IP**. **Record CNAME** (**canonical name**) tạo tên bí danh **alias** trỏ vào một tên **canonical**. Tên **canonical** là tên **host** trong **record A** hoặc lại trỏ vào 1 tên **canonical** khác.

Cú pháp record A:

[tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ 1: record A trong tập tin db.t3h

server.t3h.com. IN A 172.29.14.1

diehard.t3h.com. IN A 172.29.14.4

// Multi-homed hosts

server.t3h.com. IN A 172.29.14.1

server.t3h.com. IN A 192.253.253.1

VI.4. AAAA.

Ánh xạ tên máy (**hostname**) vào địa chỉ **IP version 6**

Cú pháp:

[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ:

```
Server    IN AAAA 1243:123:456:789:1:2:3:456ab
```

VI.5. SRV.

Cung cấp cơ chế định vị dịch vụ, **Active Directory** sử dụng **Resource Record** này để xác định **domain controllers**, **global catalog servers**, **Lightweight Directory Access Protocol** (**LDAP**) **servers**.

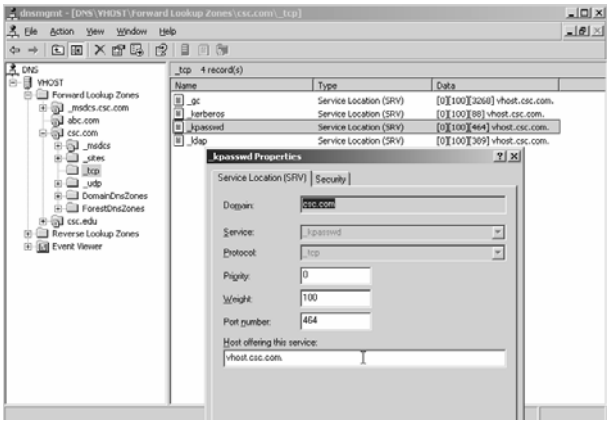
Các **field** trong **SVR**:

- Tên dịch vụ ***service.***
- Giao thức sử dụng.
- Tên miền (**domain name**).
- **TTL** và **class.**
- **Priority**.
- **Weight** (hỗ trợ **load balancing**).
- Port của dịch vụ.
- **Target** chỉ định **FQDN** cho **host** hỗ trợ dịch vụ.

Ví dụ:

_ftp._tcp.somecompany.com. IN SRV 0 0 21 ftpsvr1.somecompany.com.

_ftp._tcp.somecompany.com. IN SRV 10 0 21 ftpsvr2.somecompany.com.(Tham khảo hình 1.16)

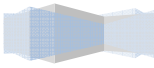


Hình 1.16: Thông tin về RR SRV

VI.6. MX (Mail Exchange).

DNS dùng **record MX** trong việc chuyển **mail** trên mạng **Internet**. Ban đầu chức năng chuyển **mail** dựa trên 2 **record**: **record MD** (**mail destination**) và **record MF** (**mail forwarder**) **records**. **MD** chỉ ra đích cuối cùng của một thông điệp **mail** có tên miền cụ thể. **MF** chỉ ra máy chủ trung gian sẽ chuyển tiếp **mail** đến được máy chủ đích cuối cùng. Tuy nhiên, việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành một **record** là **MX**. Khi nhận được mail, trình chuyển **mail** (**mailer**) sẽ dựa vào **record MX** để quyết định đường đi của mail. **Record MX** chỉ ra một mail **exchanger** cho một miền - **mail exchanger** là một máy chủ xử lý (chuyển **mail** đến **mailbox** cục bộ hay làm **gateway** chuyển sang một giao thức chuyển **mail** khác như **UUCP**) hoặc chuyển tiếp **mail** đến một **mail exchanger** khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng hơn dùng giao thức

SMTP (**Simple Mail Transfer Protocol**).



Để tránh việc gửi **mail** bị lặp lại, **record MX** có thêm 1 giá trị bổ sung ngoài tên miền của **mail exchanger** là 1 số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các **mail exchanger**.

Cú pháp **record MX**:

[domain_name] IN MX [priority] [mail-host]

Ví dụ record MX sau :

t3h.com. IN MX 10 mailserver.t3h.com.

Chỉ ra máy chủ **mailserver.t3h.com** là một **mail exchanger** cho miền **t3h.com** với số thứ tự tham chiếu 10.

Chú ý: các giá trị này chỉ có ý nghĩa so sánh với nhau. Ví dụ khai báo 2 record MX:

t3h.com. IN MX 1 listo.t3h.com.

t3h.com. IN MX 2 hep.t3h.com.

Trình chuyển thư **mailer** sẽ thử phân phát thư đến **mail exchanger** có số thứ tự tham chiếu nhỏ nhất trước. Nếu không chuyển thư được thì **mail exchanger** với giá trị kế sau sẽ được chọn. Trong trường hợp có nhiều **mail exchanger** có cùng số tham chiếu thì **mailer** sẽ chọn ngẫu nhiên giữa chúng.

VI.7. PTR (Pointer).

Record PTR (**pointer**) dùng để ánh xạ địa chỉ **IP** thành **Hostname**.

Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR [tên-máy-tính]

Ví dụ:

Các **record PTR** cho các host trong mạng 192.249.249:

1.**14.29.172.in-addr.arpa.** IN PTR server.t3h.com.

VII. Cài đặt và cấu hình dịch vụ DNS.

Có nhiều cách cài đặt dịch vụ **DNS** trên môi trường **Windows** như: Ta có thể cài đặt **DNS** khi ta nâng cấp máy chủ lên **domain controllers** hoặc cài đặt **DNS** trên máy **stand-alone Windows 2003 Server** từ tùy chọn **Networking services** trong thành phần **Add/Remove Program**.

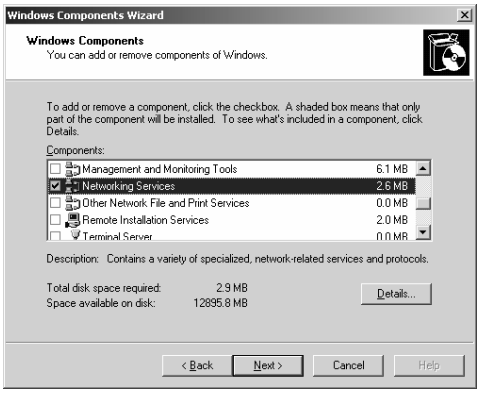
VII.1. Các bước cài đặt dịch vụ DNS.

Khi cài đặt dịch vụ **DNS** trên **Windows 2003 Server** đòi hỏi máy này phải được cung cấp địa chỉ **IP** tĩnh, sau đây là một số bước cơ bản nhất để cài đặt dịch vụ **DNS** trên **Windows 2003 stand-alone Server.**

Chọn **Start** | **Control Panel** | **Add/Remove Programs.**

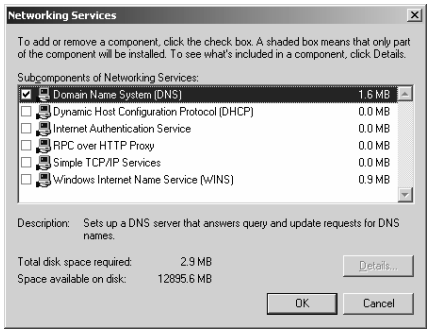
Chọn **Add or Remove Windows Components** trong hộp thoại **Windows components.**

Từ hộp thoại ở bước 2 ta chọn **Network Services** sau đó chọn nút **Details** (Tham khảo hình 1.17)



Hình 1.17: Thêm các dịch vụ mạng trong **Windows**.

Chọn tùy chọn **Domain Name System**(**DNS**), sau đó chọn nút **OK**(Tham khảo hình 1.18)



Hình 1.18: Thêm dịch vụ DNS

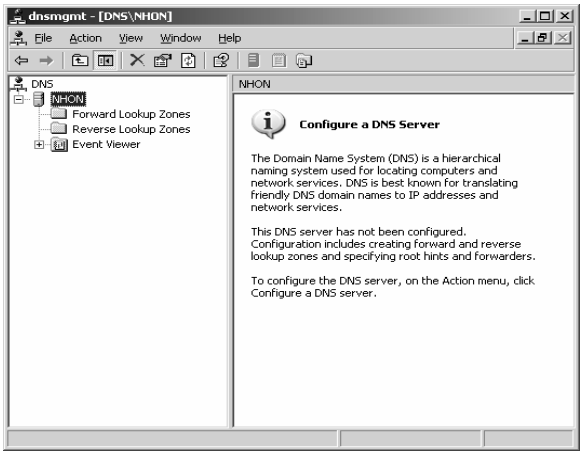
Chọn **Next** sau đó hệ thống sẽ chép các tập tin cần thiết để cài đặt dịch vụ (bạn phải đảm bảo có đĩa **CDROM Windows 2003** trên máy cục bộ hoặc có thể truy xuất tài nguyên này từ mạng).

Chọn nút **Finish** để hoàn tất quá trình cài đặt.

VII.2. Cấu hình dịch vụ DNS

Sau khi ta cài đặt thành công dịch vụ **DNS**, ta có thể tham khảo trình quản lý dịch vụ này như sau:

Ta chọn **Start** | **Programs** | **Administrative Tools** | **DNS**. Nếu ta không cài **DNS** cùng với quá trình cài đặt **Active Directory** thì không có **zone** nào được cấu hình mặc định. Một số thành phần cần tham khảo trong **DNS Console** (Tham khảo hình 1.19)



Hình 1.19: DNS console

- **Event Viewer**: Đây trình theo dõi sự kiện nhật ký dịch vụ **DNS**, nó sẽ lưu trữ các thông tin về: cảnh giác (**alert**), cảnh báo (**warnings**), lỗi (**errors**).
- **Forward Lookup Zones**: Chứa tất cả các **zone** thuận của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.
- **Reverse Lookup Zones**: Chứa tất cả các **zone** nghịch của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.

VII.2.1 Tạo Forward Lookup Zones.

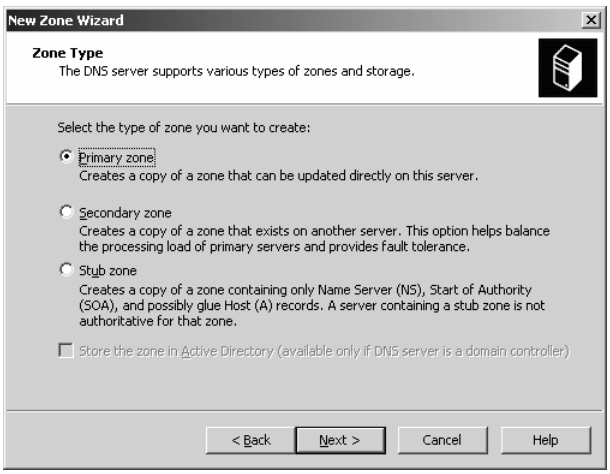
Forward Lookup Zone để phân giải địa chỉ Tên máy (**hostname**) thành địa chỉ **IP**. Để tạo **zone** này ta thực hiện các bước sau:

Chọn nút **Start** | **Administrative Tools** | **DNS**.

Chọn tên **DNS server**, sau đó Click chuột phải chọn **New Zone**.

Chọn **Next** trên hộp thoại **Welcome to New Zone Wizard**.

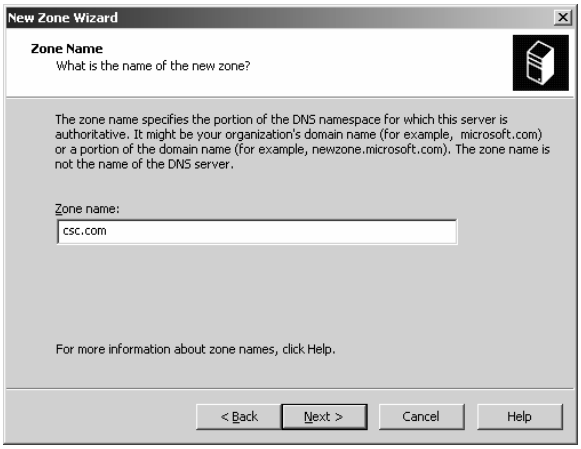
Chọn **Zone Type** là **Primary Zone** | **Next**.



Hình 1.20: Hộp thoại Zone Type

Chọn **Forward Lookup Zone** | **Next**.

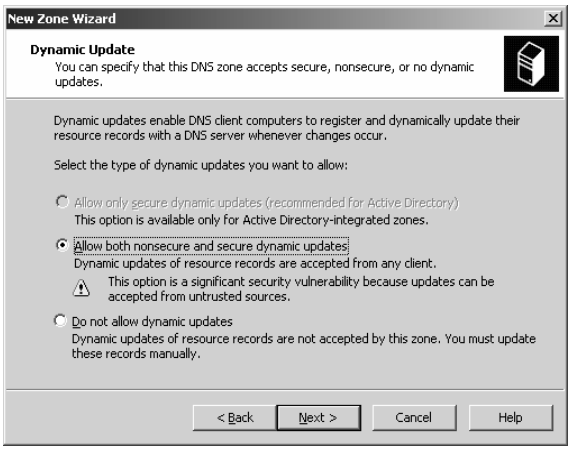
Chỉ định **Zone Name** để khai báo tên **Zone** (Ví dụ: csc.com), chọn **Next**.



Hình 1.21: Chỉ định tên zone

Từ hộp thoại **Zone File**, ta có thể tạo file lưu trữ cơ sở dữ liệu cho **Zone**(**zonename.dns**) hay ta có thể chỉ định **Zone File** đã tồn tại sẵn (tất cả các file này được lưu trữ tại **%systemroot%\system32\dns**), tiếp tục chọn **Next**.

Hộp thoại **Dynamic Update** để chỉ định **zone** chấp nhận **Secure Update**, **nonsecure Update** hay chọn không sử dụng **Dynamic Update**, chọn **Next**.



Hình 1.22: Chỉ định **Dynamic Update**.

Chọn **Finish** để hoàn tất.

VII.2.2 Tạo Reverse Lookup Zone.

Sau khi ta hoàn tất quá trình tạo **Zone** thuận ta sẽ tạo **Zone** nghịch (**Reverse Lookup Zone**) để hỗ trợ cơ chế phân giải địa chỉ **IP** thành tên máy(**hostname**).

Để tạo **Reverse Lookup Zone** ta thực hiện trình tự các bước sau:

Chọn **Start** | **Programs** | **Administrative Tools** | **DNS**.

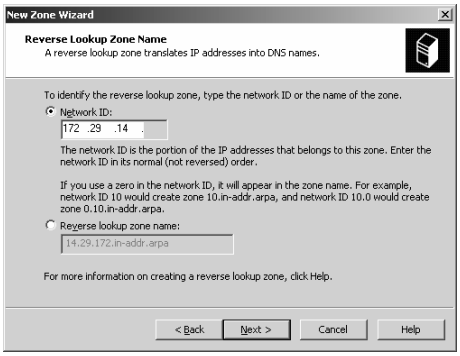
Chọn tên của **DNS server**, Click chuột phải chọn **New Zone**.

Chọn **Next** trên hộp thoại **Welcome to New Zone Wizard**.

Chọn **Zone Type** là **Primary Zone** | **Next**.

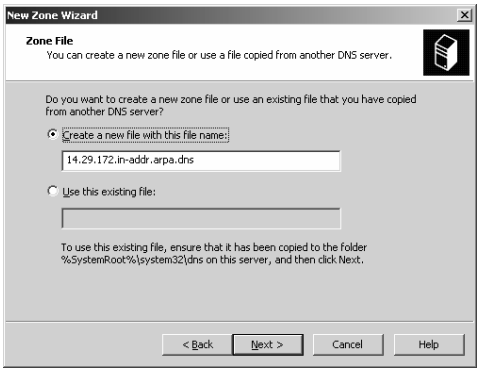
Chọn **Reverse Lookup Zone** | **Next**.

Gõ phần địa chỉ mạng(**NetID**) của địa chỉ **IP** trên **Name Server** | **Next**.



Hình 1.23: Chỉ định **zone** ngược.

Tạo mới hay sử dụng tập tin lưu trữ cơ sở dữ liệu cho **zone** ngược, sau đó chọn **Next**.



Hình 1.24: Chỉ định zone file.

Hộp thoại **Dynamic Update** để chỉ định **zone** chấp nhận **Secure Update**, **nonsecure Update** hay chọn không sử dụng **Dynamic Update**, chọn **Next**.

Chọn **Finish** để hoàn tất.

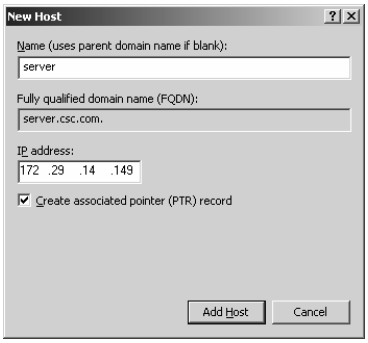
VII.2.3 Tạo Resource Record(RR).

Sau khi ta tạo **zone** thuận và **zone** nghịch, mặc định hệ thống sẽ tạo ra hai **resource record NS** và **SOA**.

Tạo **RR A**.

Để tạo **RR A** để ánh xạ **hostname** thành tên máy, để làm việc này ta Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Host** (tham khảo hình 1), sau đó ta cung cấp một số thông tin về **Name**, **Ip address,** sau đó chọn **Add Host.**

Chọn **Create associated pointer (PTR) record** để tạo **RR PTR** trong **zone** nghịch (trong ví dụ Hình 1.25 ta tạo **hostname** là **server** có địa chỉ **IP** là 172.29.14.149).

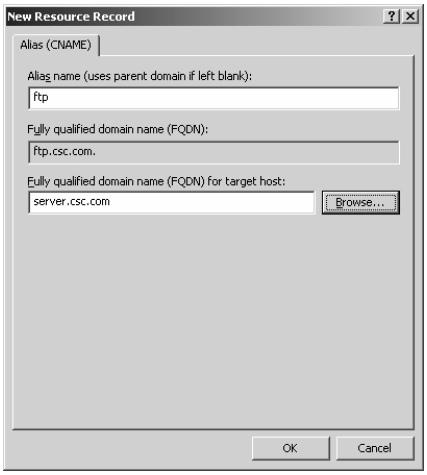


Hình 1.25: Tạo **Resource record A**.

Tạo **RR CNAME**.

Trong trường hợp ta muốn máy chủ **DNS Server** vừa có tên **server.csc.com** vừa có tên **ftp.csc.com** để phản ánh đúng chức năng là một **DNS Server**, **FTP server**,…Để tạo **RR Alias** ta thực hiện như sau:

- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Alias (CNAME)** (tham khảo Hình 1.26), sau đó ta cung cấp một số thông tin về:
- **Alias Name**: Chỉ định tên **Alias** (ví dụ ftp).
- **Full qualified domain name(FQDN) for target host:** chỉ định tên **host** muốn tạo **Alias**(ta có thể gõ tên **host** vào mục này hoặc ta chọn nút **Browse** sau đó chọn tên host).



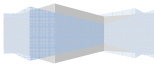
Hình 1.26: Tạo RR CNAME

Tạo **RR MX** (**Mail Exchanger**).

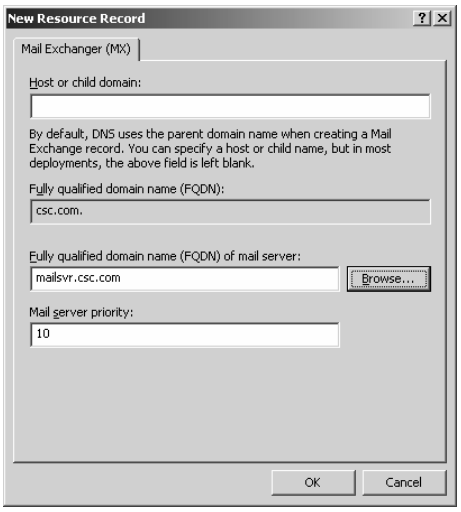
Trong trường hợp ta tổ chức máy chủ **Mail** hỗ trợ việc cung cấp hệ thống thư điện tử cho miền cục bộ, ta phải chỉ định rõ địa chỉ của **Mail Server** cho tất cả các miền bên ngoài biết được địa chỉ này thông qua việc khai báo **RR MX**. Mục đích chính của **RR** này là giúp cho hệ thống bên ngoài có thể chuyển thư vào bên trong miền nội bộ. Để tạo **RR** này ta thực hiện như sau:

- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Mail Exchanger (MX) …** (tham khảo hình 3), sau đó ta cung cấp một số thông tin về:
- **Host or child domain:** Chỉ định tên máy hoặc địa chỉ miền con mà **Mail Server** quản lý, thông

thường nếu ta tạo **MX** cho miền hiện tại thì ta không sử dụng thông số này.



- **Full qualified domain name(FQDN) of mail server:** Chỉ định tên của máy chủ **Mail Server** quản lý mail cho miền nội bộ hoặc miền con.
- **Mail server priority:** Chỉ định độ ưu tiên của **Mail Server** (Chỉ định máy nào ưu tiên xử lý **mail** trước máy nào).
- Trong Hình 1.27 ta tạo một **RR MX** để khai báo máy chủ **mailsvr.csc.com** là máy chủ quản lý **mail** cho miền **csc.com**.

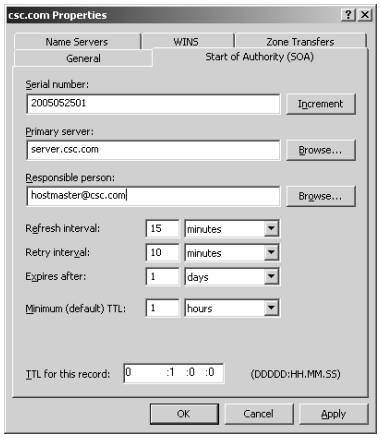


Hình 1.27: Tạo RR MX

Thay đổi thông tin về **RR SOA** và **NS**.

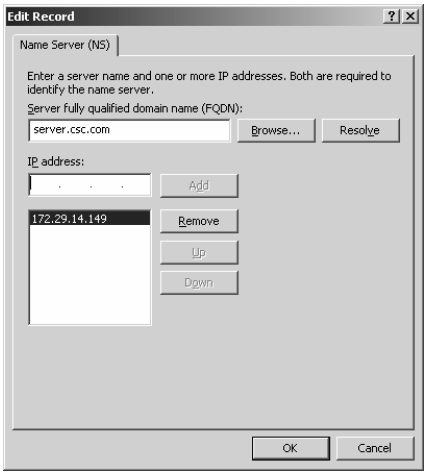
Hai **RR NS** và **SOA** được tạo mặc định khi ta tạo mới một **Zone**, nếu như ta cài đặt **DNS** cùng với **Active Directory** thì ta thường không thay đổi thông tin về hai **RR** này, tuy nhiên khi ta cấu hình **DNS Server** trên **stand-alone server** thì ta phải thay đổi một số thông tin về hai **RR** này để đảm bảo tính đúng đắn, không bị lỗi. Để thay đổi thông tin này ta thực hiện như sau:

- Click chuột **Forward Lookup Zone**, sau đó Click vào tên **zone** sẽ hiển thị danh sách các **RR**, Click đôi vào **RR SOA** (tham khảo Hình 1.28).
- **Serial number:** Chỉ định chỉ số thay đổi thao cú pháp (năm_tháng_ngày_sốlầnthayđổitrongngày)
- **Primary server:** Chỉ định tên **FQDN** cho máy chủ **Name Server**(ta có thể click và nút **Browse…** để chỉ định tên của **Name Server** tồn tại sẵn trong **zone**).
- **Responsible person:** Chỉ định địa chỉ **email** của người quản trị hệ thống **DNS**.



Hình 1.28: Thay đổi thông tin về RR SOA.

- Từ hộp thoại (ở Hình 1.28) ta chọn **Tab Name Servers | Edit** để thay đổi thông tin về **RR NS** (Tham khảo Hình 1.29).
- **Server Full qualified domain name(FQDN):** Chỉ định tên đầy đủ của **Name Server**, ta có thể chọn nút **Browser** để chọn tên của **Name Server** tồn tại trong **zone file**(khi đó ta không cần cung cấp thông tin về địa chỉ **IP** cho **server** này).
- **IP address:** Chỉ định địa chỉ **IP** của máy chủ **Name Server**, sau đó chọn nút **Add**.

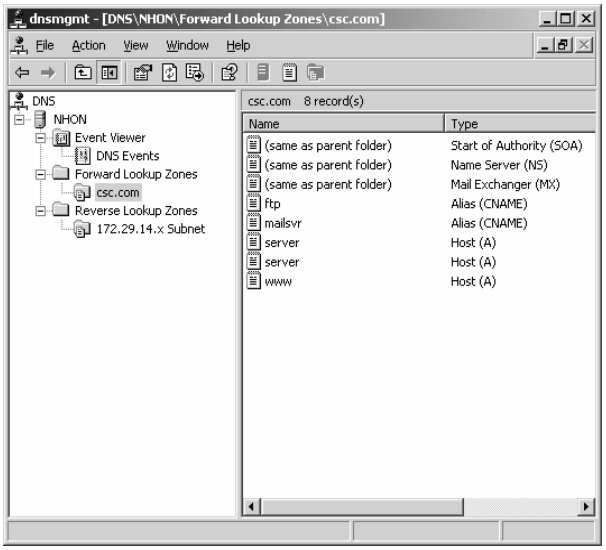


Hình 1.29: Thay đổi thông tin về RR NS

- Thay đổi thông tin về **RR SOA** và **NS** trong **zone** nghịch (**Reverse Lookup Zone**) ta thực hiện tương tự như ta đã làm trong **zone** nghịch.

VII.2.4 Kiểm tra hoạt động dịch vụ DNS.

Sau khi ta hoàn tất quá trình tạo **zone** thuận, **zone** nghịch, và mô tả một số **RR** cần thiết (tham khảo Hình 1.30).

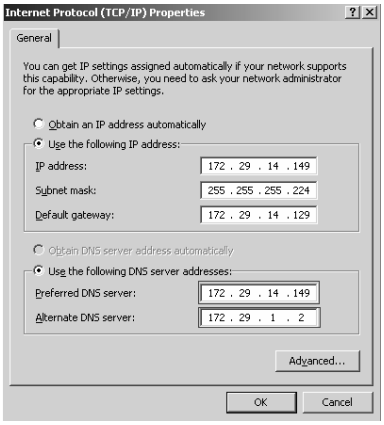


Hình 1.30: Một số cơ sở dữ liệu cơ bản của dịch vụ **DNS**.

Muốn kiểm tra quá trình hoạt động của dịch vụ **DNS** ta thực hiện các bước sau:

Khai báo **Resolver**:

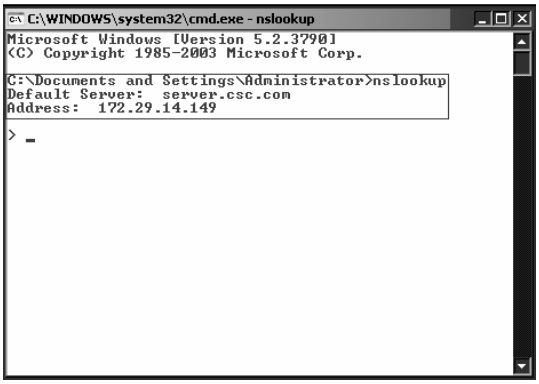
- Để chỉ định rõ cho **DNS Client** biết địa chỉ máy chủ **DNS Server** hỗ trợ việc phân giải tên miền.
- Để thực hiện khai báo **Resolver** ta chọn **Start | Settings | Network Connections** | Chọn **Properties** của **Local Area Connection** | Chọn **Properties** của **Internet Control (TCP/IP)** (ta tham khảo Hình 1.31), sau đó chỉ định hai thông số .
- **Referenced DNS server**: Địa chỉ của máy chủ **Primary DNS Server**.
- **Alternate DNS server**: Địa chỉ của máy chủ **DNS** dự phòng hoặc máy chủ **DNS** thứ hai.



Hình 1.31: Khai báo Resolver cho máy trạm.

Kiểm tra hoạt động.

Ta có thể dùng công cụ **nslookup** để kiểm tra quá trình hoạt động của dịch vụ **DNS**, phân giải **resource record** hoặc phân giải tên miền. để sử dụng được công cụ **nslookup** ta vào **Start | Run | nslookup**.



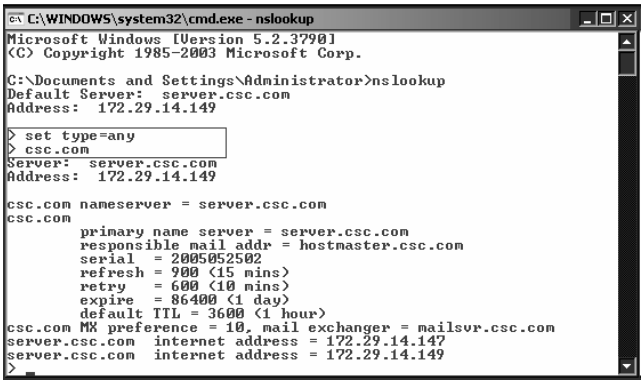
Hình 1.32: Kiểm tra **DNS**.

Cần tìm hiểu một vài tập lệnh của công cụ **nslookup**.

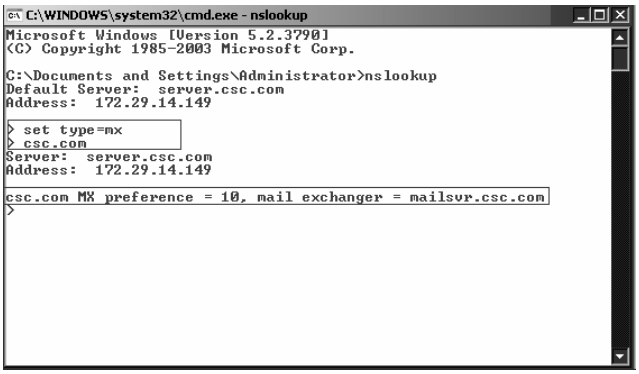
>set type=<RR_Type>

Trong đó <**RR_Type**> là loại **RR** mà ta muốn kiểm tra, sau đó gõ tên của **RR** hoặc tên miền cần kiểm tra

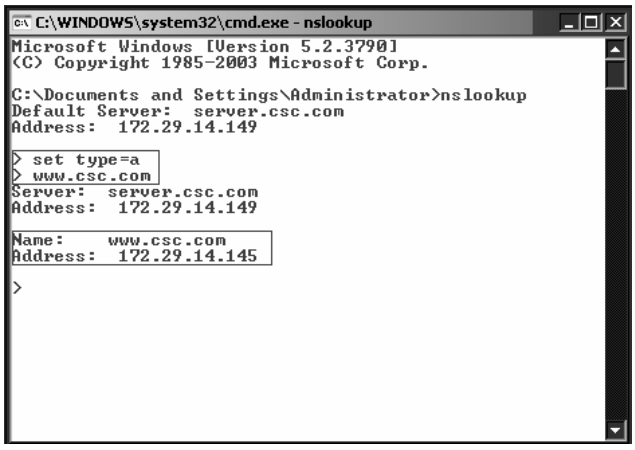
>set type=any: Để xem mọi thông tin về **RR** trong miền, sau đó ta gõ <**domain name**> để xem thông tin về các **RR** như **A**, **NS**, **SOA**, **MX** của miền này.



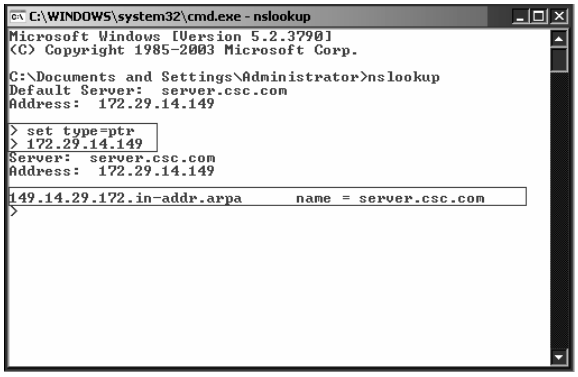
Hình 1.33: Ví dụ về **nslookup**.



Hình 1.34: Xem **RR MX**.

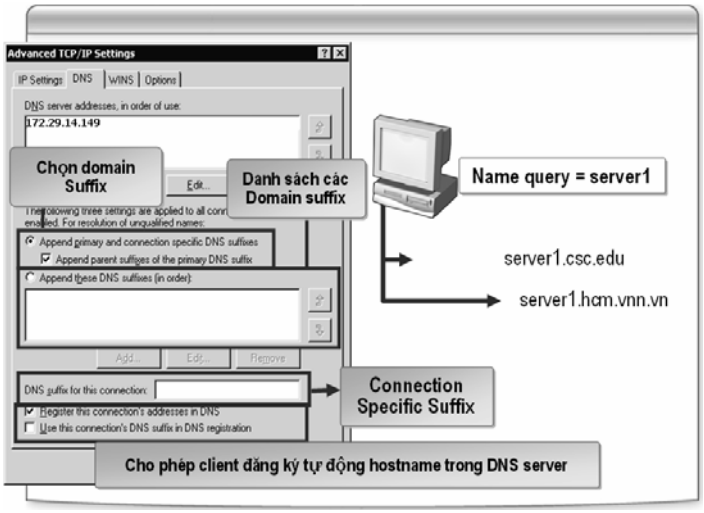


Hình 1.35: Xem địa chỉ **IP** của một **hostname**.



Hình 1.36: Kiểm tra phân giải ngược.

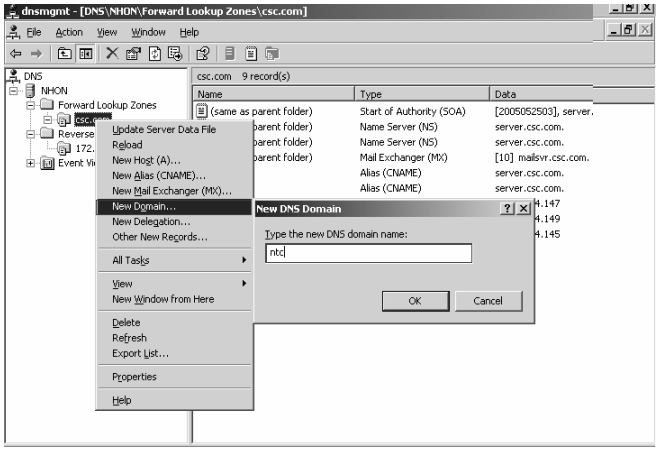
Một số thông số cấu hình cần thiết cho **DNS Client**:



Hình 1.37: Một số thông tin cấu hình khác.

VII.2.5 Tạo miền con(Subdomain).

Trong miền có thể có nhiều miền con, việc tạo miền con giúp cho người quản trị cung cấp tên miền cho các tổ chức, các bộ phận con trong miền của mình thông qua đó nó cho phép người quản trị có thể phân loại và tổ chức hệ thống dễ dàng hơn. Để tạo miền con ta chọn **Forward Lookup Zone**, sau đó ta click chuột phải vào tên **Zone** chọn **New Domain**…(tham khảo Hình 1.38)

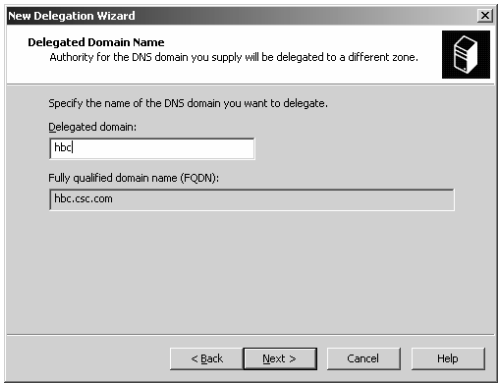


Hình 1.38: Tạo miền con.

VII.2.6 Ủy quyền cho miền con.

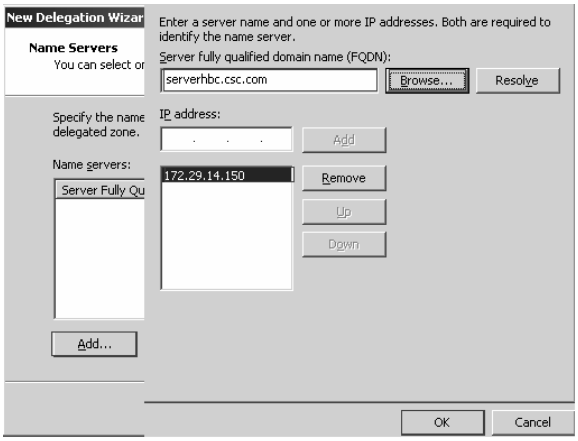
Giả sử ta ủy quyền tên miền **subdomain hbc.csc.com** cho **server serverhbc** có địa chỉ 172.29.14.150 quản lý, ta thực hiện các thao tác sau:

- Tạo **resource record A** cho **serverhbc** trong miền **csc.com**(tham khảo trong phần tạo RR A).
- Chọn **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone** chọn **New delegation… | Next** (tham khảo Hình 1.39),.



Hình 1.39: **delegation domain**.

- **Add Name Server** quản lý cơ cở dữ liệu cho miền con **hbc.csc.com** trong hộp thoại **Name Server** (tham khảo Hình 1.40).



Hình 1.40: **Add Name Server**.

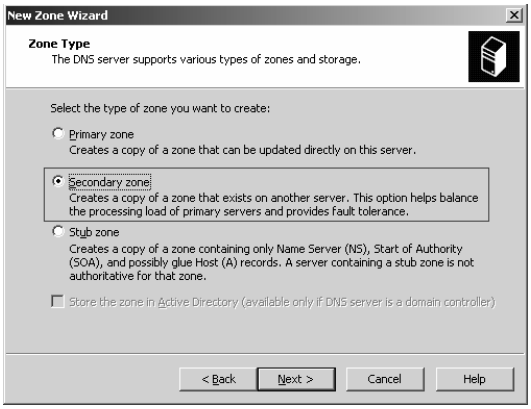
- Sau khi add xong **Name Server** ở bước trên ta chọn **Next | Finish** để hoàn tất.

VII.2.7 Tạo Secondary Zone.

Thông thường trong một **domain** ta có thể tổ chức một **Primary Name Server**(**PNS**) và một **Secondary Name Server**(**SNS**), **SNS** đóng vai trò là máy dự phòng, nó lưu trữ bảng sao dữ liệu từ máy **PNS**, một khi **PNS** bị sự cố thì ta có thể sử dụng **SNS** thay cho máy **PNS**.

Sau đây ta sử dụng máy chủ **server1** có địa chỉ 172.29.14.151 làm máy chủ dự phòng (**SNS**) cho miền **csc.edu** từ **Server** chính (**PNS**) có địa chỉ 172.29.14.149.

- Click chuột phải vào tên **Name Server** trong giao diện **DNS management console** chọn **New Zone** | **Next** | **Secondary Zone** (tham khảo Hình 1.41)
- **Secondary Zone** : Khi ta muốn sao chép dự phòng cơ sở dữ liệu **DNS** từ **Name Server** khác, **SNS** hỗ trợ cơ chế chứng thực, cân bằng tải với máy **PNS**, cung cấp cơ chế dung lỗi tốt.
- **Stub Zone**: Khi ta muốn sao chép cơ sở dữ liệu chỉ từ **PNS**, **Stub Zone** sẽ chỉ chứa một số **RR** cần thiết như **NS**, **SOA**, **A** hỗ trợ cơ chế phân giải được hiệu quả hơn.

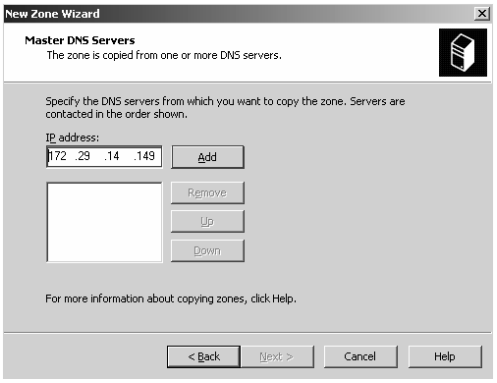


Hình 1.41: Tạo Secondary Zone

- Chọn **Forward Lookup Zone** nếu ta muốn tạo sao chép **Zone** thuận, chọn **Reverse Lookup Zone** nếu ta muốn sao chép **Zone** nghịch. Trong trường hợp này ta chọn **Forward Lookup Zone |**

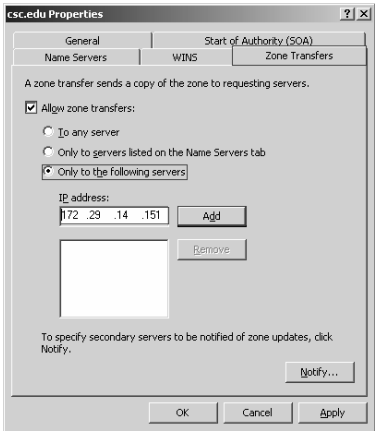
Next.

- Chỉ định **Zone Name** mà ta muốn sao chép (ví dụ **csc.edu**), tiếp theo ta chọn **Next**.
- Chỉ định địa chỉ của máy chủ **Master Name Server**(còn gọi là **Primary Name Server**), sao đó chọn **Add** | **Next** (tham khảo Hình 1.42).



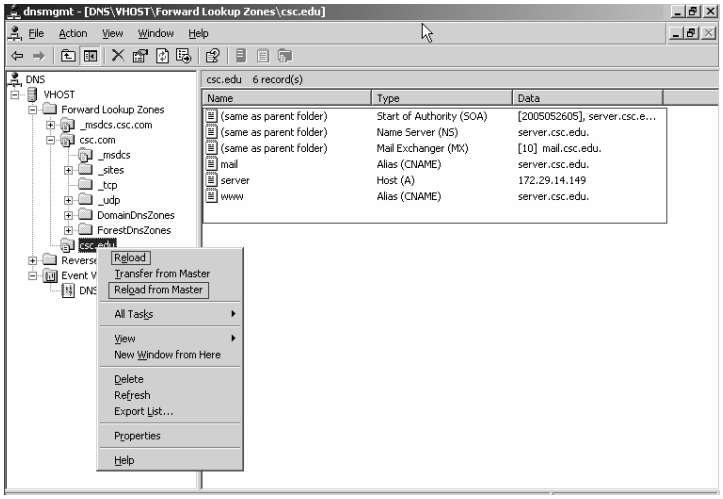
Hình 1.42: Tạo Secondary Zone

- Chọn **Finish** để hoàn tất quá trình. ta kiểm tra xem trong **Zone** csc.edu mới tạo sẽ có cơ sở dữ liệu được sao chép từ **PNS**, ngược lại trong **zone csc.edu** không có cơ sở dữ liệu thì ta hiệu chỉ lại thông số **Zone Transfer** trên máy **Master Name Server** để cho phép máy **SNS** được sao chép cơ sở dữ liệu, ta thực hiện điều này bằng cách Click chuột phải vào **Zone csc.edu** trên máy **Master Name Server**, chọn **Properties** | chọn **Tab Zone Transfer** (Tham khảo Hình 1.43).



Hình 1.43: Allow Zone Transfer.

- Sau khi ta hiệu chỉ xong thông tin **Zone Transfer ta Reload** cơ sở dữ liệu từ máy **SNS** để cho máy **SNS** sao chép lại cơ sở dữ liệu từ **PNS** (Tham khảo hình 1.44)

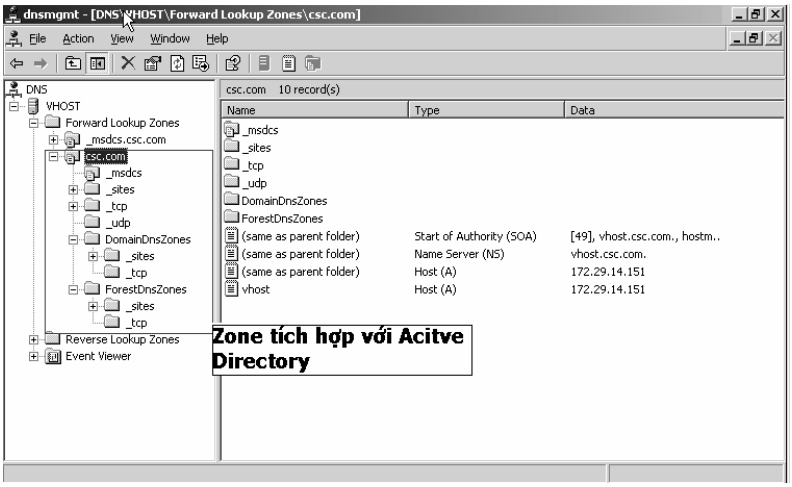


Hình 1.44: **Reload Secondary Zone**.

VII.2.8 Tạo zone tích hợp với Active Directory.

Trong quá trình nâng cấp máy **Stand-Alone Server** thành **Domain Controller** bằng cách cài **Active Directory** ta có thể chọn cơ chế cho phép hệ thống tự động cài đặt và cấu hình dịch vụ **DNS** tích hợp chung với **Active Directory**, nếu ta chọn theo cách này thì sau khi quá trình nâng cấp hoàn tất, ta có thể tham khảo cơ sở dữ liệu của **DNS** tích hợp chung với **Active Directory** thông qua trình quản lý dịch vụ **DNS**(tham khảo Hình 1.45).

Trong Hình 1.45 này ta tham khảo cơ sở dữ liệu của **DNS** quản lý tên miền **csc.com** được tích hợp chung với **Active Directory**.



Hình 1.45: **Active Integrated zone**.

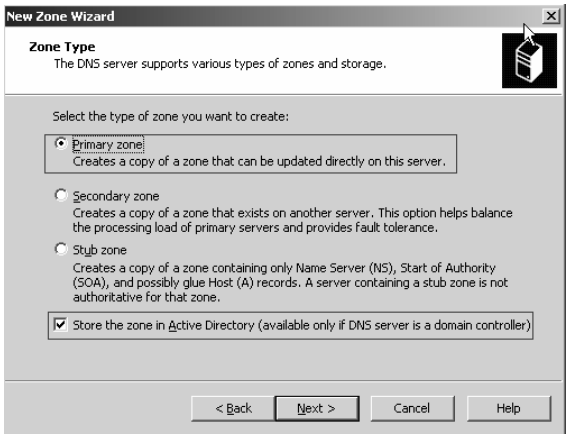
Tuy nhiên khi ta cho hệ thống tự động cấu hình cơ sở dữ liệu cho **zone** thì nó chỉ tạo một số cơ sở dữ liệu cần thiết ban đầu để nó thực hiện một số thao tác truy vấn và quản lý cơ sở dữ liệu cho **Active Directory**. Để cho **DNS** hoạt động tốt hơn thì ta mô tả thêm thông tin **resource record** cần thiết vào, điều cần thiết nhất là ta tạo **Reverse Lookup Zone** cho **Active Integrated Zone** vì ban đầu hệ thống không tạo ra **zone** này, mô tả thêm thông tin **record PTR** cho từng **resource record A** trong **Forward**

Lookup Zone.

Ta có thể tạo một **zone** mới tích hợp với **Active Directory** theo các bước sau:

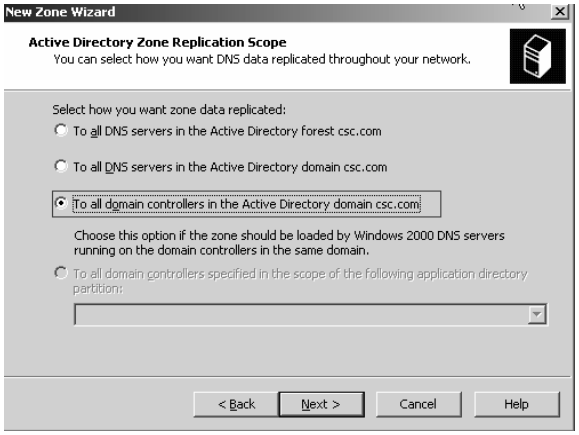
Bấm chuột phải vào tên **DNS Server** trong **DNS management console**, chọn **New Zone**…| chọn **Next**.

Trong hộp thoại **zone type** ta chọn **Primary Zone** với cơ chế lưu trữ zone trong **AD**(tham khảo hình 1.46), tiếp tục chọn **Next**.



Hình 1.46: Chọn zone type

Chọn cơ chế nhân bản dữ liệu tới tất cả các **Domain Controller** trong **Active Directory Zone** | **Next** (tham khảo Hình 1.47)

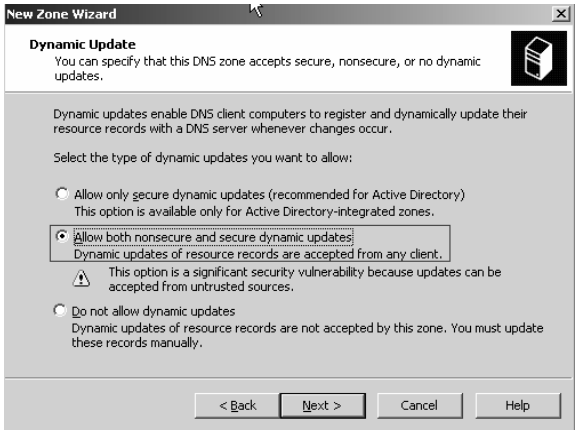


Hình 1.47: Nhân bản dữ liệu cho **zone**.

Chọn tạo **zone** thuận (**Forward Lookup Zone**) | **Next**.

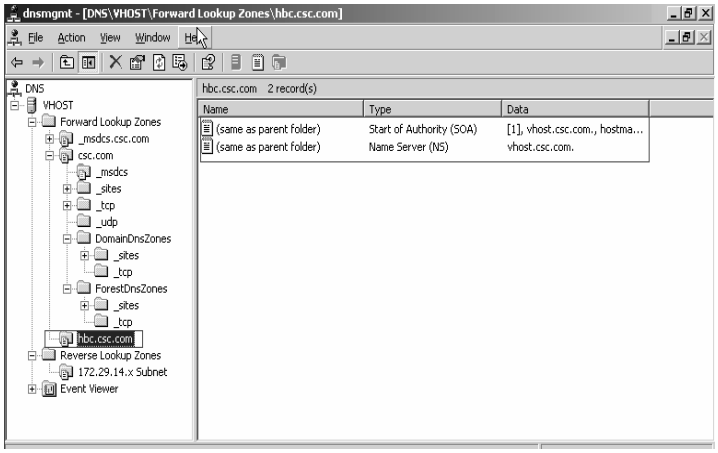
Chỉ định tên **zone** (**Zone Name**) | **Next**.

Chỉ định **Dynamic Update** trong trường hợp ta muốn tạo **DDNS** cho **zone** này (tham khảo Hình 1.48), trong trường hợp này ta chọn **Allow both nonsecure and secure dynamic updates | Next**.



Hình 1.48: Dynamic update

Chọn **Finish** để hoàn tất quá trình, sau khi hoàn thành ta có thể mô tả **resource record** cho **zone** này, tạo thêm **Reverse Lookup Zone** trong trường hợp ta muốn hỗ trợ phân giải nghịch.



Hình 1.49: Cơ sở dữ liệu **zone**.

VII.2.9 Thay đổi một số tùy chọn trên Name Server.

Trong phần này ta khảo sát một vài tùy chọn cần thiết để tạo hiệu chỉnh thông tin cấu hình cho **DNS**. Thông thường có ba phần chính trong việc thay đổi tùy chọn.

- Tùy chọn cho **Name Server**.
- Tùy chọn cho từng **zone name**.
- Tùy chọn cho từng **RR** trong **zone name**.

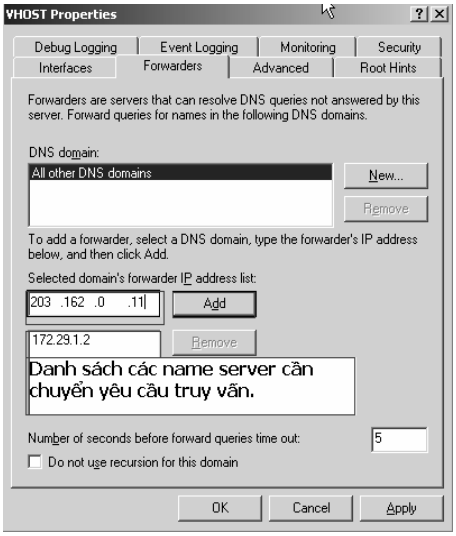
Tùy chọn cho **Name Server**.

Cho phép thay đổi một số tùy chọn chính của **Name Server** bao gồm: Cấu hình **Forwarder**, Cấu hình **Root hints**, đặt một số tùy chọn cho phép theo dõi **log** (**Event Logging**), quản lý các truy vấn (**Monitoring query**), **debug logging**,... và một số hiệu chỉnh khác.

Để sử dụng tùy chọn này ta chọn **Properties** của tên **server** trong **DNS management console** (tham khảo Hình 1.50).

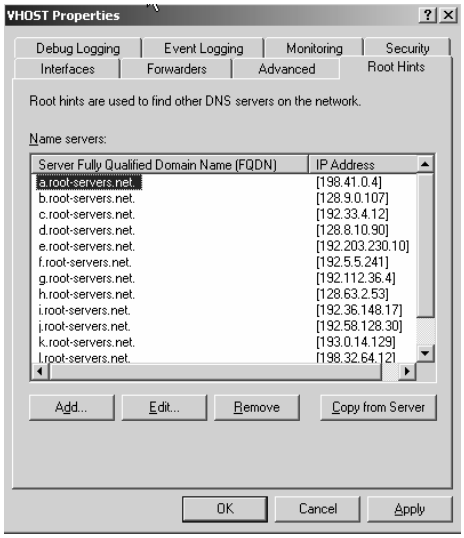
Hình 1.50: **Name server properties**.

- **Cấu hình Forwader**: Chọn **Tab Forwarders** từ màn hình **properties** của **Name Server** (tham khảo hình 1.51).



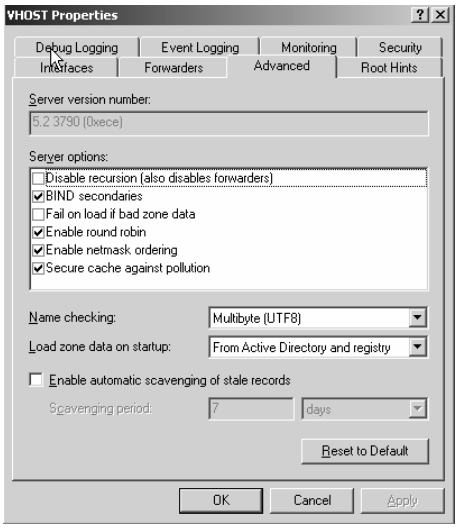
Hình 1.51: Cấu hình **Forwarder**.

- **Cấu hình Root hints:** Ta có thể tham khảo danh sách các **Root name server** quản lý các **Top-Level domain**, thông qua hộp thoại này ta có thể thêm, xóa, hiệu chỉnh địa chỉ của **Root hints**, thông thường các địa chỉ này hệ thống có thể tự nhận biết (tham khảo hình 1.52).



Hình 1.52: **Root Name Server**.

- Hiệu chỉnh một số thông số cấu hình nâng cao như (tham khảo Hình 1.53):
- **Disable recursion:** bỏ cơ chế truy vấn đệ qui, nếu ta chọn tùy chọn này thì **Forwarder** cũng bị **disable**.
- **BIND secondaries:** Cho phép **secondary** là **Name server** trên môi trường **Unix**.
- **Fail on load if bad zone data** : Nếu **zone data** bị lỗi thì không cho **name server load** dữ liệu.
- **Enable round robin**: Cho phép cơ chế luân chuyển giữa các **server** trong quá trình phân giải tên miền.
- **Enable netmask ordering**: Cho phép **client** dựa vào **local subnet** để nó lựa chọn **host** gần với **client** nhất (một khi **client** nhận được câu trả lời truy vấn ánh xạ một **hostname** có nhiều địa chỉ IP)
- **Secure cache agianst pollution**: Bảo mật vùng nhớ tạm lưu trữ các **RR** đã phân giải trước.

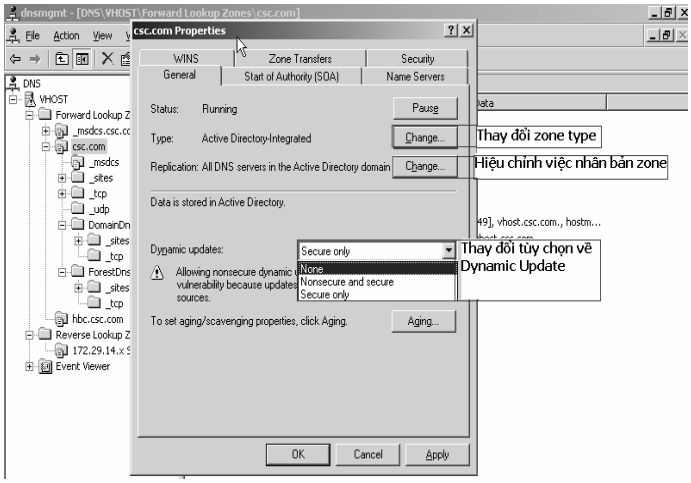


Hình 1.53: Tùy chọn nâng cao.

Tùy chọn cho từng **Zone**.

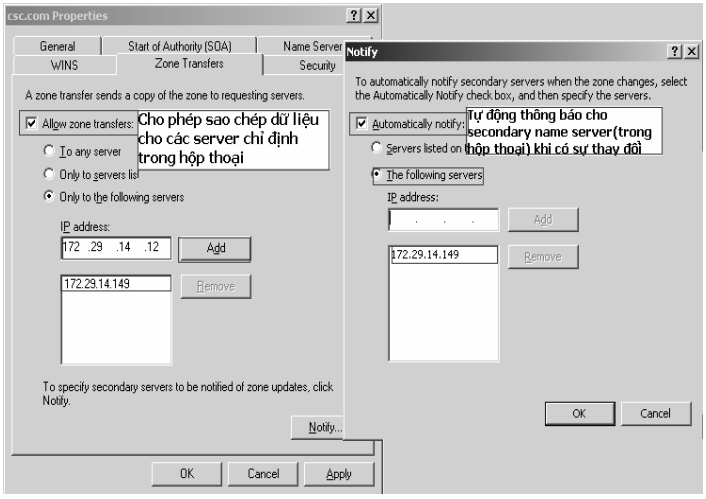
Để sử dụng tùy chọn này ta chọn **Properties** của tên **zone** trong **DNS management console**.

- Trong phần này ta có thể :
- Thay đổi **Zone Type**, cho phép **zone** hỗ trợ hay không hỗ trợ **Dynamic update** (**DDNS**) (tham khảo Hình 1.54)



Hình 1.54: Tùy chọn chung của **zone name**.

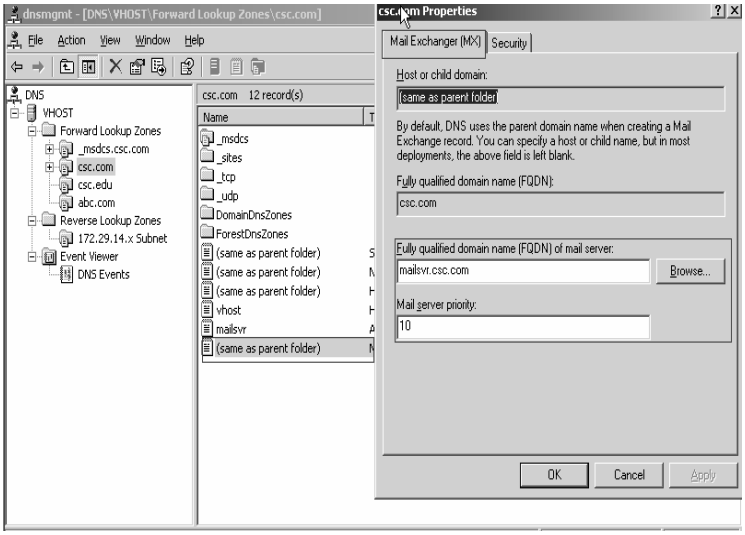
- Thay đổi thông tin **resource record SOA**, **NS** (ta có thể tham khảo trong phần cấu hình trước)
- Cho phép hay không cho phép sao chép dữ liệu **zone** giữa các **Name Server** (tham khảo hình 1.55).



Hình 1.55: **Zone transfer**.

Tùy chọn cho từng **Resource Record**.

Thông qua tùy chọn này ta có thể thay đổi thông tin của từng **resource record** cho **zone name**, mỗi một **resource record** có thông tin khác nhau: để thực hiện điều này ta chỉ cần bấm đôi vào tên **resource record** tương ứng (tham khảo ví dụ trong Hình 1.56 về **RR MX**)



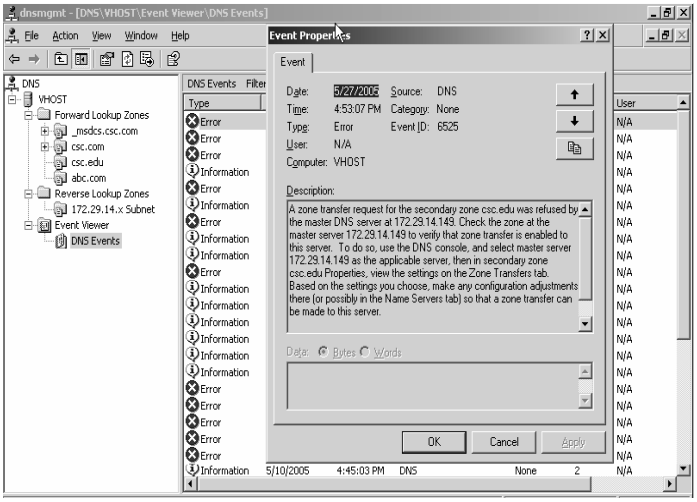
Hình 1.56: Thuộc tính của **MX record**.

VII.2.10 Theo dõi sự kiện log trong DNS.

Khi quản trị dịch vụ **DNS**, việc ghi nhận và theo dõi sự kiện xảy ra cho dịch vụ **DNS** là rất quan trọng, thông qua đó ta có thể đưa ra một số giả pháp khác phục một khi có sự cố xảy ra,…Trong **DNS** management console cung cấp mục **Event Viewer** để cho ta có thể thực hiện điều này, trong phần này ta cần lưu ý một số biểu tượng như:

Theo dõi sự kiện:

- Error : Chỉ thị lỗi nghiêm trọng, đối với lỗi này ta cần theo xử lý nhanh chóng.



Hình 1.57: Theo dõi sự kiện lỗi

- Information : Thông tin ghi nhận các sự kiện bình thường như **shutdown**, **start**, **stop DNS**,….

Tóm tắt

Lý thuyết 3 tiết - Thực hành 6 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học giúp học viên hiểu nguyên tắc hoạt động của dịch vụ FTP và thiết lập một FTP Server hỗ trợ cho việc truyền file trên mạng.	I. Giới thiệu FTP II. Chương trình FTP client. III. Giới thiệu FTP server.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

I. Giới thiệu về FTP.

I.1. Giao thức FTP.

FTP là từ viết tắt của **File Transfer Protocol**. Giao thức này được xây dựng dựa trên chuẩn **TCP**, **FTP** cung cấp cơ chế truyền tin dưới dạng tập tin (**file**) thông qua mạng **TCP/IP**, **FTP** là 1 dịch vụ đặc biệt vì nó dùng đến 2 cổng: cổng 20 dùng để truyền dữ liệu (**data port**) và cổng 21 dùng để truyền lệnh (**command port**).

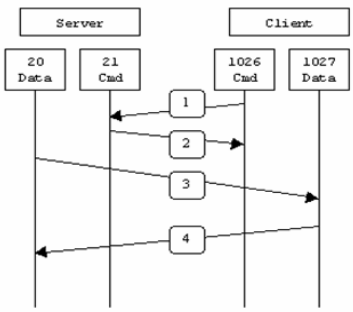
I.1.1 Active FTP.

Ở chế độ chủ động (**active**), máy khách **FTP** (**FTP client**) dùng 1 cổng ngẫu nhiên không dành riêng (cổng N > 1024) kết nối vào cổng 21 của **FTP Server**. Sau đó, máy khách lắng nghe trên cổng N+1 và gửi lệnh **PORT** N+1 đến **FTP Server**. Tiếp theo, từ cổng dữ liệu của mình, **FTP Server** sẽ kết nối ngược lại vào cổng dữ liệu của **Client** đã khai báo trước đó (tức là N+1)

Ở khía cạnh **firewall**, để **FTP Server** hỗ trợ chế độ **Active** các kênh truyền sau phải mở:

- Cổng 21 phải được mở cho bất cứ nguồn gửi nào (để **Client** khởi tạo kết nối)
- **FTP Server's** port 21 to **ports** > 1024 (**Server** trả lời về cổng điều khiển của **Client**)
- Cho kết nối từ cổng 20 của **FTP Server** đến các cổng > 1024 (**Server** khởi tạo kết nối vào cổng dữ liệu của **Client**)
- Nhận kết nối hướng đến cổng 20 của **FTP Server** từ các cổng > 1024 (**Client** gửi xác nhận **ACKs** đến cổng **data** của **Server**)

Sơ đồ kết nối:



Hình 2.1: Mô hình hoạt động của **Active FTP**.

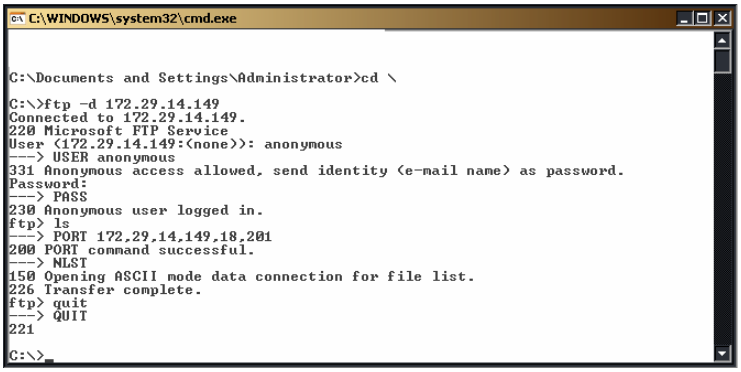
- Bước 1: **Client** khởi tạo kết nối vào cổng 21 của **Server** và gửi lệnh PORT 1027.
- Bước 2: **Server** gửi xác nhận **ACK** về cổng lệnh của **Client**.
- Bước 3: **Server** khởi tạo kết nối từ cổng 20 của mình đến cổng dữ liệu mà **Client** đã khai báo trước đó.
- Bước 4: **Client** gửi **ACK** phản hồi cho **Server**.

Khi **FTP Server** hoạt động ở chế độ chủ động, **Client** không tạo kết nối thật sự vào cổng dữ liệu của **FTP server**, mà chỉ đơn giản là thông báo cho **Server** biết rằng nó đang lắng nghe trên cổng nào và **Server** phải kết nối ngược về **Client** vào cổng đó. Trên quan điểm **firewall** đối với máy **Client** điều này giống như 1 hệ thống bên ngoài khởi tạo kết nối vào hệ thống bên trong và điều này thường bị ngăn chặn trên hầu hết các hệ thống **Firewall**.

Ví dụ phiên làm việc **active FTP**:

Trong ví dụ này phiên làm việc **FTP** khởi tạo từ máy **testbox1.slacksite.com** (192.168.150.80), dùng chương trình **FTP Client** dạng dòng lệnh, đến máy chủ **FTP testbox2.slacksite.com** (192.168.150.90). Các dòng có dấu --> chỉ ra các lệnh **FTP** gửi đến **Server** và thông tin phản hồi từ các lệnh này. Các thông tin người dùng nhập vào dưới dạng chữ đậm.

Lưu ý là khi lệnh **PORT** được phát ra trên **Client** được thể hiện ở 6 byte. 4 byte đầu là địa chỉ IP của máy **Client** còn 2 byte sau là số cổng. Giá trị cổng được tính bằng (byte_5*256) + byte_6, ví dụ ((14*256) + 178) là 3762.



Phiên làm việc active FTP.

I.1.2 Passive FTP.

Để giải quyết vấn đề là **Server** phải tạo kết nối đến **Client**, một phương thức kết nối **FTP** khác đã được phát triển. Phương thức này gọi là **FTP** thụ động (**passive**) hoặc **PASV** (là lệnh mà **Client** gửi cho **Server** để báo cho biết là nó đang ở chế độ **passive**).

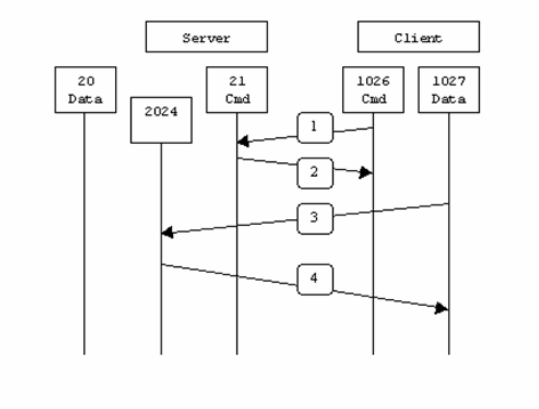
Ở chế độ thụ động, **FTP Client** tạo kết nối đến **Server**, tránh vấn đề **Firewall** lọc kết nối đến cổng của máy bên trong từ **Server**. Khi kết nối **FTP** được mở, client sẽ mở 2 cổng không dành riêng N, N+1 (N > 1024). Cổng thứ nhất dùng để liên lạc với cổng 21 của **Server**, nhưng thay vì gửi lệnh **PORT** và sau đó là server kết nối ngược về **Client**, thì lệnh **PASV** được phát ra. Kết quả là **Server** sẽ mở 1 cổng không dành riêng bất kỳ P (P > 1024) và gửi lệnh **PORT P** ngược về cho **Client**.. Sau đó client sẽ khởi tạo kết nối từ cổng N+1 vào cổng P trên **Server** để truyền dữ liệu.

Từ quan điểm **Firewall** trên **Server FTP**, để hỗ trợ **FTP** chế độ **passive**, các kênh truyền sau phải được mở:

- Cổng FTP 21 của **Server** nhận kết nối từ bất nguồn nào (cho **Client** khởi tạo kết nối)
- Cho phép trả lời từ cổng 21 **FTP Server** đến cổng bất kỳ trên 1024 (**Server** trả lời cho cổng **control** của **Client**)
- Nhận kết nối trên cổng **FTP server** > 1024 từ bất cứ nguồn nào (**Client** tạo kết nối để truyền dữ

liệu đến cổng ngẫu nhiên mà **Server** đã chỉ ra)

- Cho phép trả lời từ cổng **FTP Server** > 1024 đến các cổng > 1024 (**Server** gửi xác nhận **ACKs** đến cổng dữ liệu của **Client**)



Hình 2.2: Mô hình hoạt động của **Active FTP**.

- Bước 1: **Client** kết nối vào cổng lệnh của **Server** và phát lệnh **PASV**.
- Bước 2: **Server** trả lời bằng lệnh **PORT** 2024, cho **Client** biết cổng 2024 đang mở để nhận kết nối dữ liệu.
- Bước 3: **Client** tạo kết nối truyền dữ liệu từ cổng dữ liệu của nó đến cổng dữ liệu 2024 của **Server**.
- Bước 4: **Server** trả lời bằng xác nhận **ACK** về cho cổng dữ liệu của **Client**.

Trong khi **FTP** ở chế độ thụ động giải quyết được vấn đề phía **Client** thì nó lại gây ra nhiều vấn đề khác ở phía **Server**. Thứ nhất là cho phép máy ở xa kết nối vào cổng bất kỳ > 1024 của **Server**. Điều này khá nguy hiểm trừ khi FTP cho phép mô tả dãy các cổng >= 1024 mà **FTP Server** sẽ dùng (ví dụ WU-FTP **Daemon**).

Vấn đề thứ hai là một số **FTP Client** lại không hỗ trợ chế độ thụ động. Ví dụ tiện ích **FTP Client** mà **Solaris** cung cấp không hỗ trợ **FTP** thụ động. Khi đó cần phải có thêm trình **FTP Client**. Một lưu ý là hầu hết các trình duyệt **Web** chỉ hỗ trợ **FTP** thụ động khi truy cập **FTP Server** theo đường dẫn URL ftp://.

Ví dụ phiên làm việc **passive FTP**:

Trong ví dụ này phiên làm việc **FTP** khởi tạo từ máy **testbox1.slacksite.com** (192.168.150.80), dùng chương trình **FTP Client** dạng dòng lệnh, đến máy chủ **FTP testbox2.slacksite.com** (192.168.150.90), máy chủ **Linux** chạy **ProFTPd 1.2.2RC2**. Các dòng có dấu --> chỉ ra các lệnh **FTP** gửi đến **Server** và thông tin phản hồi từ các lệnh này. Các thông tin người nhập vào dưới dạng chữ đậm.

Lưu ý: đối với **FTP** thụ động, cổng mà lệnh **PORT** mô tả chính là cổng sẽ được mở trên **Server**. Còn đối với **FTP** chủ động cổng này sẽ được mở ở **Client**.

```
bash-2.05# ftp -d localhost
Connected to localhost.
220 nhon FTP server ready.
Name (localhost:root): hv
---> USER hv
331 Password required for hv.
Password:
---> PASS XXXX
230-No directory! Logging in with home=/
230 User hv logged in.
---> SYST
215 UNIX Type: L8 Version: SUNOS
Remote system type is UNIX.
---> TYPE I
200 Type set to I.
Using binary mode to transfer files.
ftp> cd /home
---> CWD /home
250 CWD command successful.
ftp> ls
---> EPSV
229 Entering Extended Passive Mode (|||64948|)
---> TYPE A
200 Type set to A.
---> NLST
550 *: No such file or directory.
---> TYPE I
200 Type set to I.
ftp>
```

Phiên giao dịch **Passive FTP**.

I.1.3 Một số lưu ý khi truyền dữ liệu qua FTP.

IIS hỗ trợ cả hai chế độ kết nối **Active** và **Passive**, do đó việc kết nối theo phương thức **Active** hay **passive** tùy thuộc vào từng **Client**. **IIS** không hỗ trợ cơ chế vô hiệu hóa (**disable**) chế độ kết nối **Active** hay **Passive**.

Khi ta sử dụng dịch vụ **FTP** để truyền dữ liệu trên mạng **Internet** thông qua một hệ thống bảo mật như **Proxy**, **Firewall**, **NAT**, thông thường các hệ thống bảo mật này chỉ cho phép kết nối **TCP** theo cổng dịch vụ 21 do đó **user** gặp vấn đề trong việc sử dụng các lệnh **DIR**, **LS**, **GET**, or **PUT** để truyền dữ liệu vì các lệnh này đòi hỏi hệ thống bảo mật phải cho phép sử dụng cổng TCP 20. Cho nên khi sử dụng **FTP** để truyền tin trên mạng Internet thông qua mạng các hệ thống bảo mật (**Proxy**, **Firewall**, **NAT**) thì những hệ thống này phải mở **TCP port** 20 của **FTP**.

Danh sách các ứng dụng **Microsoft** cung cấp làm **FTP Client**.

FTP Client	Transfer Mode
Command-line	Active
Internet Explorer 5.1 và các phiên bản trước đó	Passive
Internet Explorer 5.5 và các phiên bản sau này	Active and Passive
Từ FrontPage 1.1 tới FrontPage 2002	Active

I.1.4 Cô lập người dùng truy xuất FTP Server (FTP User Isolation).

FTP User Isolation đặc tính mới trên **Windows 2003**, hỗ trợ cho **ISP** và **Aplication Service Provider** cung cấp cho người dùng **upload** và cập nhật nội dung **Web**, chứng thực cho từng người dùng. **FTP user Isolation** cấp mỗi người dùng một thư mục riêng rẻ, người dùng chỉ có khả năng xem, thay đổi,

xóa nội dung trong thư mục của mình.

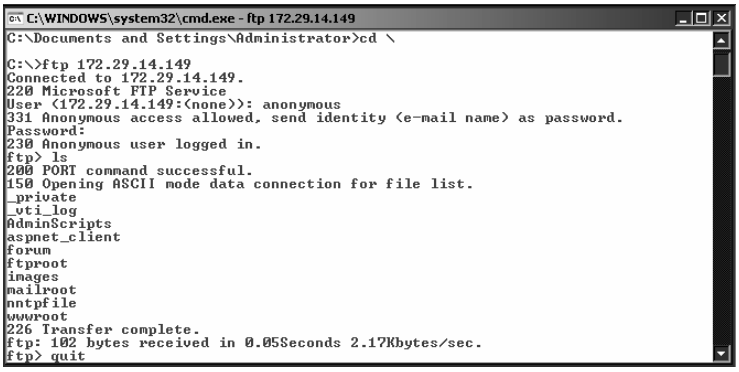
Isolation Mode	Chức năng
Do not isolate users	Đây là chế độ không sử dụng **FTP User Isolation**, ở **mode** này không giới hạn truy xuất của người dùng. Thông thường ta sử dụng **mode** này để tạo một **public FTP Site**.
Isolate users	Mode này chứng thực người dùng cục bộ (**Local User**) và người dùng miền (**Domain User**) truy xuất vào **FTP Site**. Đối với **mode** người quản trị phải tạo cho mỗi người dùng một thư mục con của thư mục **FTP Root**, với tên thư mục này là **username** của người dùng.
Isolate users using Active Directory	Sử dụng **Active Directory** để tách lập từng **user** truy xuất vào **FTP Server**.

II. Chương trình FTP client.

Là chương trình giao tiếp với **FTP Server**, hầu hết các hệ điều hành đều hỗ trợ **FTP Client**, trên **Linux** hoặc **Windows** để mở kết nối tới **FTP Server** ta dùng lệnh #ftp <ftp_address>.

Để thiết lập một phiên giao dịch, ta cần phải có địa chỉ **IP** (hoặc tên máy tính), một tài khoản (**username**, **password**). **Username** mà **FTP** hỗ trợ sẵn cho người dùng để mở một giao dịch **FTP** có tên là **anonymous** với **password** rỗng.

Sau đây là một ví dụ về mở một phiên giao dịch đến **FTP Server**:



Hình 2.3: Sử dụng **FTP Client**.

Một số tập lệnh của **FTP Client**:

Tên lệnh	Cú pháp	Ý nghĩa
? hoặc lệnh help	? [command]	Hiển thị giúp đỡ về [**command**].
append	append local-file [remote-file]	Ghép một tập tin cục bộ với 1 tập tin trên **Server**.

ascii	ASCII	Chỉ định kiểu truyền file là **ascii** (đây là kiểu

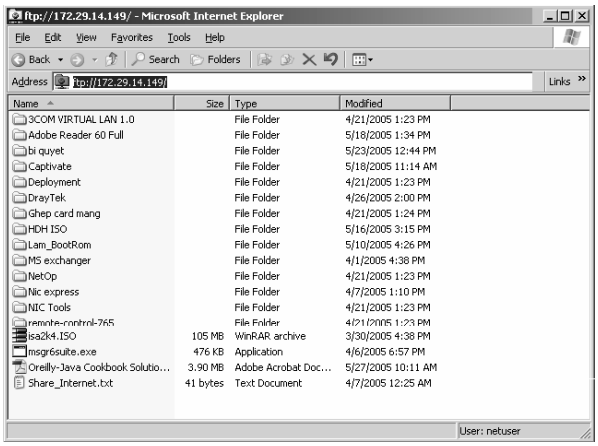
		truyền mặc định).
binary	Binary	Chỉ định kiểu truyền file là **binary**(đây là kiểu truyền mặc định).
Bye	Bye	Kết thúc **ftp session**.
Cd	cd remote-directory	Thay đổi đường dẫn thư mục trên **FTP Server.**
delete	delete remote-file	Xóa file trên **FTP Server**.
Dir	dir remote-directory	Liệt kê danh sách tập tin.
Get	get remote-file [local-file]	**Download** tập tin từ **FTP Server** về máy cục bộ.
Lcd	lcd [directory]	Thay đổi thư mục trên máy cục bộ.
Ls	ls [remote-directory] [local-file]	Liệt kê các tập tin và thư mục.
mdelete	mdelete remote-files [...]	Xóa nhiều tập tin.
Mget	mget remote-files [...]	**Download** nhiều tập tin.
Mkdir	mkdir directory	Tạo thư mục.
Put	put local-file [remote-file]	**Upload** tập tin.
Mput	mput local-files [...]	**Upload** nhiều tập tin.
Open	open computer [port]	Kết nối tới **ftp server**.
prompt	Prompt	Tắt cơ chế **confirm** sau mỗi lần **download** tập tin.
disconnect	Disconnect	Hủy kết nối **FTP**.
Pwd	Pwd	Xem thư mục hiện tại.
Quit	Quit	Thoát khỏi **ftp session**.
Recv	recv remote-file [local-file]	Copy tập tin từ **remote** về local.
Rename	rename filename newfilename	Thay đổi tên tập tin.
Rmdir	rmdir directory	Xóa thư mục.

Send	send local-file [remote-file]	Copy tập tin từ **local** đến **remote**.

User	user user-name [password] [account]		Chuyển đổi **user** khác.

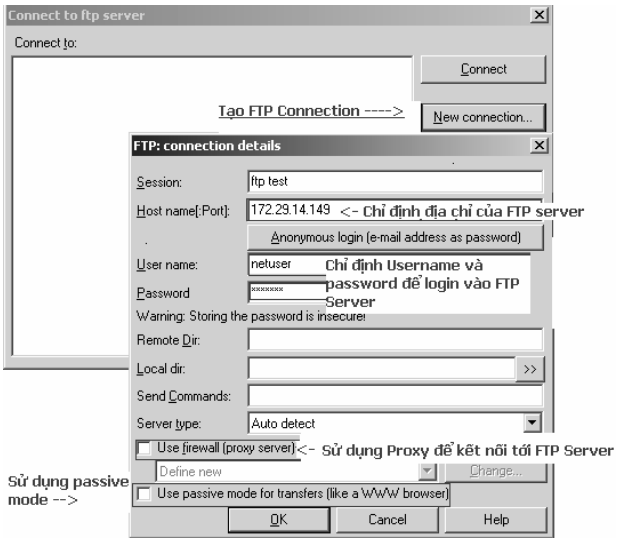
Ta có thể sử dụng chương trình Internet **Explorer** để kết nối với **FTP Server** theo cú pháp sau:

ftp://<username:password>@<Địa chỉ **FTP_Server**>



Hình 2.4: Sử dụng **IE** làm **FTP Client**.

Dùng **Windows commander** làm **FTP Client** để kết nối vào **FTP Server**, để thực hiện điều này ta mở chương trình **Windows Commander** | **Command** | **FTP Connect**…



Hình 2.5: Sử dụng **Windows commander** để kết nối vào **FTP Server**.

III. Giới thiệu FTP Server.

Là máy chủ lưu trữ tập trung dữ liệu, cung cấp dịch vụ **FTP** để hỗ trợ cho người dùng có thể cung cấp, truy xuất tài nguyên qua mạng **TCP/IP**. **FTP** là một trong các dịch vụ truyền file rất thông dụng, người dùng có thể **upload** và **download** thông tin một cách dễ dàng hơn.

III.1. Cài đặt dịch vụ FTP.

Để cài đặt dịch vụ **FTP** trên **Windows 2003** ta thực hiện các bước sau:

Chọn **Start** | **Control Panel**.

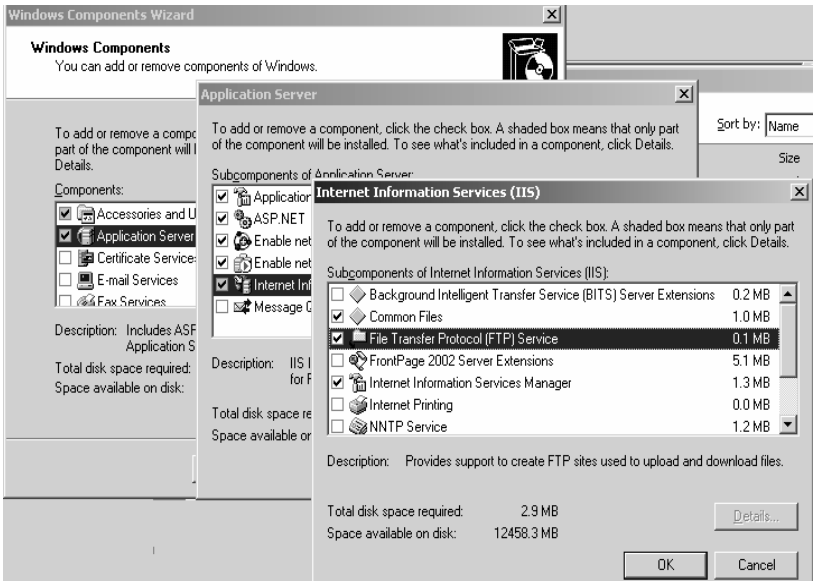
Bấm đôi vào **Add or Remove Programs**.

Từ ô vuông bên trái(pane) của cửa sổ "**Add or Remove Programs**" chọn **Add/Remove Windows Components**.

Từ danh sách **Components**, chọn **Application Server** và chọn nút **Details**.

Từ danh sách các **Application Server** chọn **Internet Information Services** và chọn nút **Details**.

Chọn mục **File Transfer Protocol** (**FTP**) **Service**.



Hình 2.6: Cài đặt **FTP Service**.

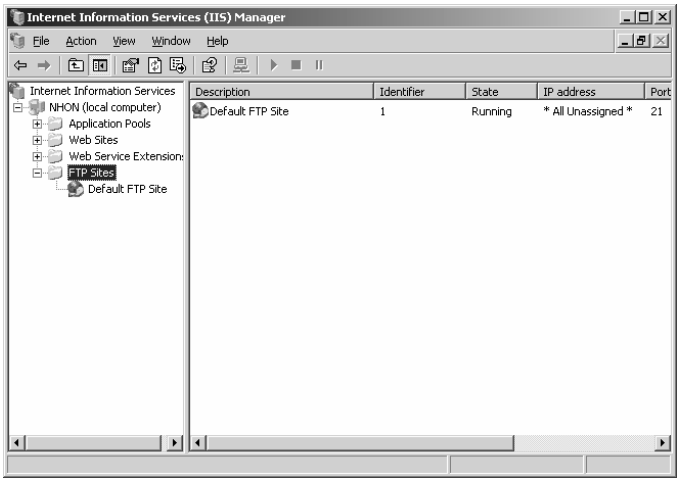
Bấm nút **OK**.

Click vào nút **Next** để hệ thống cài đặt dịch vụ **FTP** (đôi khi hệ thống yêu cầu chỉ bộ nguồn **I386** hoặc đường dẫn có chứa thư mục này để hệ thống chép một số file cần thiết khi cài đặt).

Bấm vào nút **Finish** để hoàn tất quá trình cài đặt.

III.2. Cấu hình dịch vụ FTP.

Sau khi ta cài đặt hoàn tất dịch vụ **FTP**, để quản lý dịch vụ này ta chọn **Start** | **Programs** | **Administrative Tools** | **Internet Information Services**(**IIS**) **Manager** | **Computer name** | **FTP sites** (tham khảo Hình 2.7).



Hình 2.7: **IIS Manager**.

Mặc định khi cài xong dịch vụ **FTP**, hệ thống tự tạo một **FTP site** có tên **Default FTP Site** với một số thông tin sau:

- **FTP name: Default FTP Site**.
- **TCP Port**: 21
- **Connection Limited to:** Giới hạn tối đa 100.000 kết nối.
- **Enable logging:** để cho phép ghi nhận log vào file **\systemRoot \system32\LogFiles**
- Cho phép **Anonymous** và người dùng cục bộ được đăng nhập vào **FTP Server**.
- Thư mục gốc của **FTP server** là **<ổ đĩa>\Inetpub\ftproot.**
- Quyền hạn truy xuất (cho **Anonymous** và **user** cục bộ) là **read** và **log visits**.
- Cho phép tất cả các máy tính được phép truy xuất vào **FTP Server**.

Do đó khi ta cài đặt xong ta có thể sử dụng dịch vụ **FTP** ngay mà không cần cấu hình, tuy nhiên chỉ sử dụng được một số chức năng cơ bản mà hệ thống cấu hình ban đầu. Điều tốt nhất là ta xóa đi rồi tạo **FTP Site** mới để cấu hình lại từ đầu.

III.2.1 Tạo mới FTP site.

Để tạo mới một **FTP site** ta thực hiện các bước sau:

Trong **IIS Manager** ta bấm chuột phải vào vào thư mục **FTP Sites** | **New** | **FTP Site**…| **Next**.

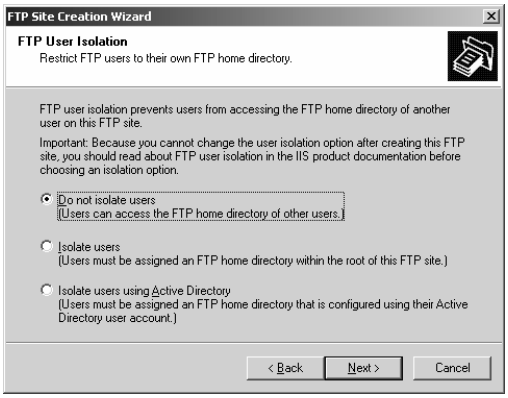
Mô tả tên **FTP site** trong hộp thoại "**FTP Site Desciption**" | **Next**.

Chỉ định **IP Address** và **Port** sử dụng cho **FTP Site**, trong phần này ta để mặc định, tiếp theo chọn **Next**.

Trong hộp thoại "**FTP User Isolation**", chọn tùy chọn **Do not isolate users** để cho phép mọi người dùng được sử dụng **FTP server**, chọn **Next** (tham khảo hình 2.8), ta cần tham khảo một số mục chọn sao

- **Do not isolate users**: Không giới hạn truy xuất tài nguyên cho từng người dùng.
- **Isolate users**: Giới hạn truy xuất tài nguyên **FTP** cho từng người dùng (tham khảo trong cấu hình **FTP User Isolation**).

- **Isolate users using Active Directory**: Dùng **AD** để giới hạn việc sử dụng tài nguyên cho từng người (tham khảo trong mục cấu hình **FTP User Isolation**).



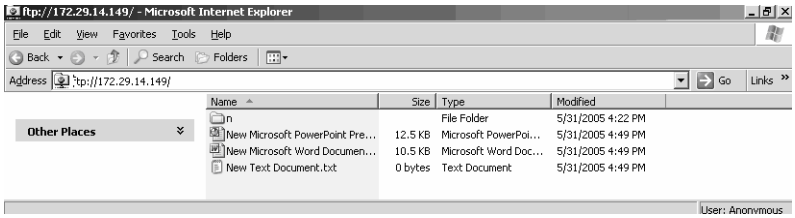
Hình 2.8: FTP User Isolation

Chọn đường dẫn chỉ định **Home Directory** cho **FTP Site**, chọn **Next**.

Chọn quyền hạn truy xuất cho **FTP site**, mặc định hệ thống chọn quyền **Read**, chọn **Next**.

Chọn **Finish** để hoàn tất quá trình tạo **FTP Site**.

Ta có thể kiểm tra bằng cách vào **Internet Explorer** đánh địa chỉ **URL** sau: ftp://172.29.14.149 (tham khảo Hình 2.9)



Hình 2.9: Truy xuất **FTP Server** bằng **IE**.

III.2.2 Tạo và xóa FTP Site bằng dòng lệnh.

Để tạo một **FTP Site** ta dùng lệnh:

iisftp /create <Home Dir> "Description" /i <IP address>

Trong đó <**IP address**> để cho **FTP** lắng nghe tại port 21.

Xóa ftp dùng lệnh:

iisftp /delete "<Tên FTP>"

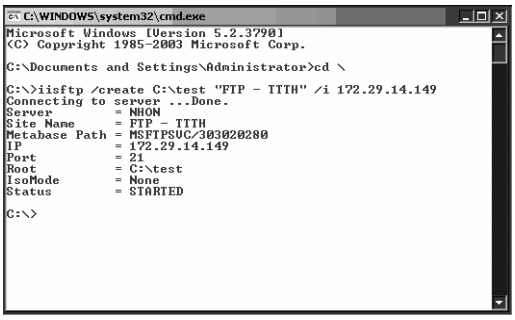
Ta tham khảo **Hình 2.10** cung cấp một số thông tin khi tạo như:

- "Connecting to server ...Done"
- "Server = NHON" : Tên FTP Server
- "Site Name= FTP – TTTH" : Tên FTP Site
- **"Metabase Path = MSFTPSVC/303020280"**: biểu diễn registry key cho thư mục Home Directory.
- **"IP = 172.29.14.149"** : Địa chỉ IP listen port 21

- “Port= 21” : TCP port

- **"Root= C:\test" :** Home directory của FTP Site.
- **"IsoMode= None" :** Không sử dụng Isolation mode.
- **"Status= STARTED" :** Mô tả trạng thái hoạt động.

Ví dụ: Tạo **FTP Site** bằng lệnh:

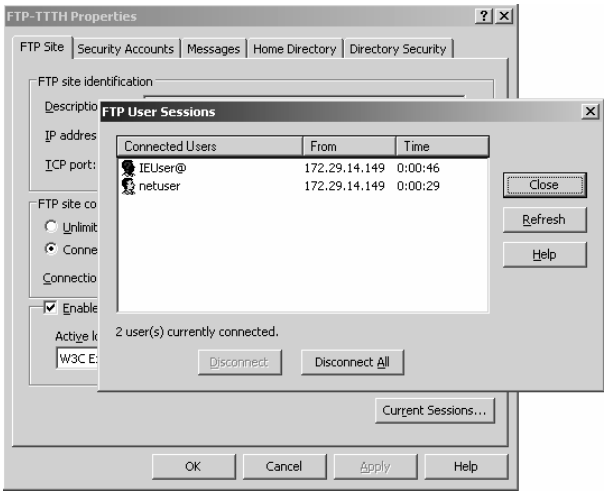


Hình 2.10: Tạo **FTP** bằng lệnh.

III.2.3 Theo dõi các user login vào FTP Server.

Để theo dõi các **user** đăng nhập vào **FTP Server** ta bấm chuột phải vào **FTP site** | **Properties** | **General** | **Current sessions**…(tham khảo Hình 2.10)

- **Connected Users**: để chỉ định tên người dùng đang **login** vào **FTP Server** (IEUser@ là **Anonymous user**).
- **From**: Chỉ địa chỉ máy trạm đăng nhập vào **FTP Server**.
- **Time**: Thời gian đăng nhập.
- Nút **Disconect** : Để hủy kết nối của **user** đang login.
- Nút **Disconect All**: Để hủy tất cả các kết nối của **user** đang **login**.



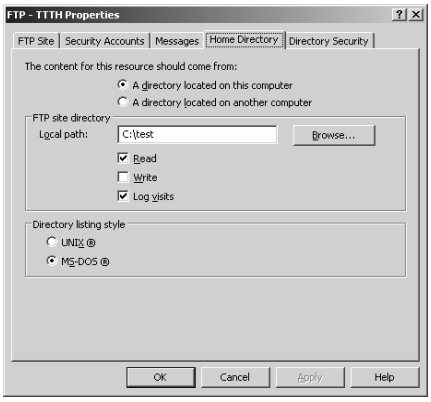
Hình 2.11: Theo dõi **user session**.

III.2.4 Điều khiển truy xuất đến FTP Site.

Ta có 4 cách điều khiển việc truy xuất đến **FTP Site** trên **IIS** như sau:

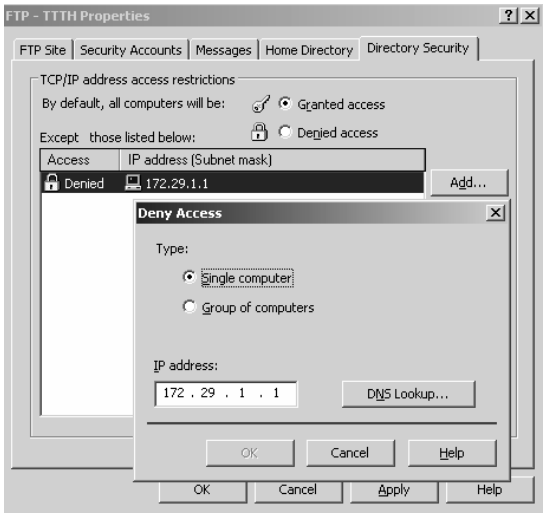
- **NTFS Permissions**: áp đặt quyền **NTFS** vào các thư mục liên quan đến **FTP Site**.

- **IIS Permissions**: Gán quyền **FTP** cho thư mục, thông thường chỉ có quyền **Read** và **Write**. Để gán quyền này ta chọn **properties** của **FTP Site** | **Tab Home Directory**(tham khảo Hình 2.12).



Hình 2.12: Gán quyền **FTP** cho thư mục.

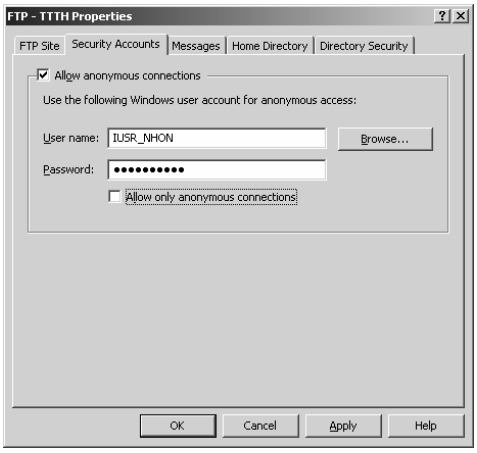
- **IP address restrictions**: Giới hạn việc truy xuất vào **FTP** theo địa chỉ **IP**. Để gán quyền này ta chọn **properties** của **FTP Site** | **Tab Home Directory** (tham khảo Hình 2.13).
- Nếu ta chọn **Granted access: FTP Server** cho phép tất các **host** khác truy xuất, trừ các **host** được mô tả trong hộp thoại.
- Nếu ta chọn **Denied access: FTP Server** chỉ cho phép các **host** trong hộp thoại được truy xuất.



Hình 2.13: Giới hạn truy xuất **FTP** cho **host**.

- **Authentication**: **Tab Security Account** để cho chứng thực người dùng **Anonymous** và người dùng cục bộ được phép hay không được phép truy xuất vào **FTP Server**.
- Mặc định **Anonymous** được login vào **FTP Server**. Ta chọn mục này khi ta muốn **public FTP** cho mọi người khác được sử dụng.
- Nếu ta chọn mục **"Allow only anonymous connections"** có nghĩa ta chỉ cho phép **Anonymous** truy xuất vào **FTP Server**.
- Thông thường để tổ chức một **FTP Server** riêng biệt và ta không muốn **public FTP** cho mọi người sử dụng thì ta bỏ tùy chọn **Allow anonymous connections"**, lúc này **FTP Server** chỉ cho phép

các người dùng cục bộ truy xuất.



Hình 2.14: Cấp truy xuất cho **Account**.

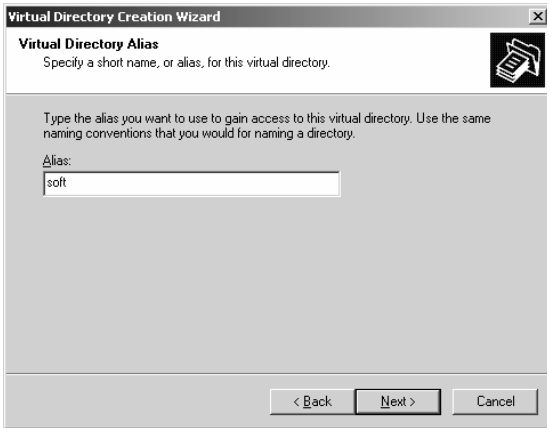
III.2.5 Tạo Virtual Directory.

Thông thường các thư mục con của **FTP r**oot đều có thể truy xuất thông qua đường dẫn **URL** của dịch vụ **FTP** như: "ftp://<địa_chỉ_của_FTP_server>/<tên_thư_mục_con>", để cho phép người dùng có thể truy xuất một tài nguyên bên ngoài **FTP root** thì ta phải làm cách nào? **FTP server** cung cấp tính năng **virtual directory** để cho phép ta có thể giải quyết trường hợp này, thông **virtual directory** ta tạo một thư mục ảo bên trong **FTP Site** ánh xạ vào bất kỳ một thư mục nào đó trên ổ đĩa cục bộ hoặc ánh xạ vào một tài nguyên chia sẻ trên mạng. sao khi ánh xạ xong ta có thể truy xuất tài nguyên theo địa chỉ "ftp://<địa_chỉ_của_FTP_server>/<tên_thư_mục_ảo >"

Các bước tạo thư mục ảo (**virtual directory**):

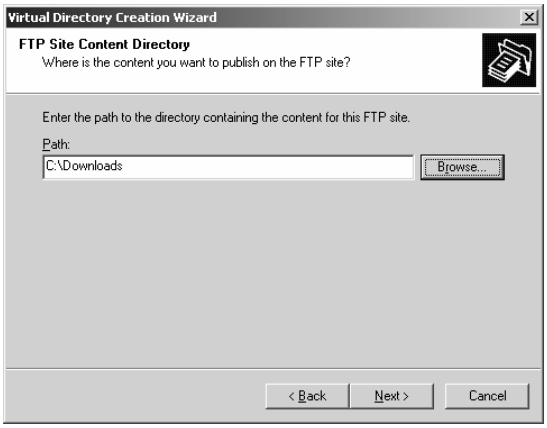
Bấm chuột phải vào **FTP Site** chọn **New** | **Virtual Directory**…| **Next**.

Enter vào tên **virtual directory** trong ô **Alias** (tham khảo hình 2.15)



Hình 2.15: Tạo tên **Alias**.

Chỉ định tên thư mục trong ổ đĩa.



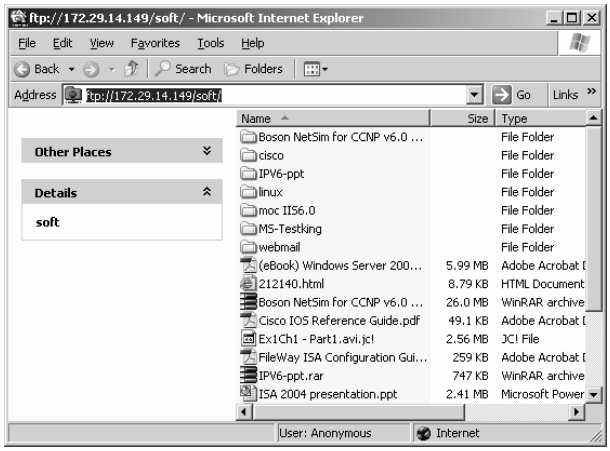
Hình 2.16: Chỉ định thư mục.

Chỉ định quyền hạn truy xuất vào thư mục.

Hình 2.17: Đặt quyền truy xuất vào **Virtual Directory**.

Chọn **Finish** để hoàn tất quá trình.

Truy xuất **Virtual directory** (minh họa ở Hình 2.18)



Hình 2.18: Truy xuất **Virtual Directory**.

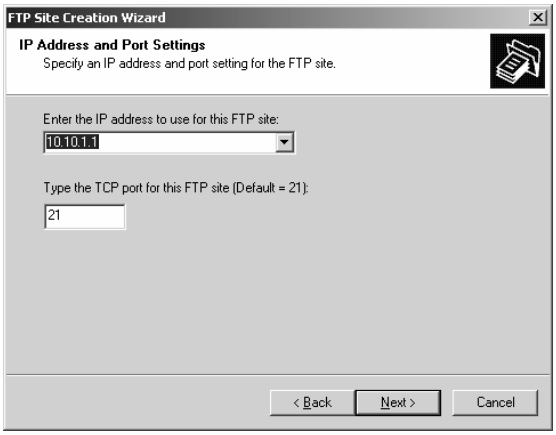
III.2.6 Tạo nhiều FTP Site.

Ta có thể tạo nhiều **FTP Site** trên một **FTP Server** bằng cách sử dụng nhiều địa chỉ **IP** và nhiều **FTP port**.

Các bước thực hiện:

Bấm đôi vào tên máy tính cục bộ trong **IIS manager**, sau đó bấm chuột phải **FTP Sites** | **New** | **FTP Site**…| **Next** | **Description** | **Next**.

Trong hộp thoại "**IP Address and Port Settings**" ta chọn địa chỉ **IP** cụ thể từ hộp thoại "**Enter IP address to use for this FTP site**" (tham khảo hình 2.19), chọn Next.



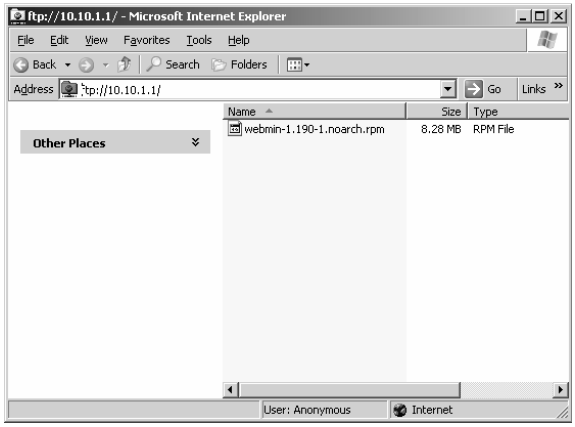
Hình 2.19: Chọn **IP address** và **Port**.

Chọn "**do not isolate user**" trong hộp thoại "**FTP User Isolation**", chọn **Next**.

Chọn đường dẫn thư mục gốc của **FTP**, chọn **Next**.

Chọn quyền truy xuất, sau đó chọn **Next** | **Finish** để hoàn tất.

Truy xuất **FTP site**:

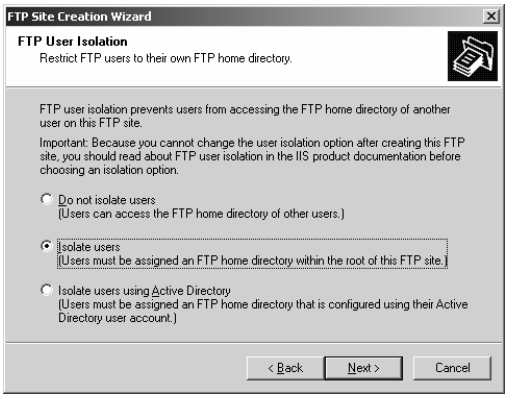


Hình 2.20: Truy xuất **vftp**.

III.2.7 Cấu hình FTP User Isolate.

Tạo **FTP Site** dùng **User Isolate**.

- Trong **IIS Manager**, Bấm chuột phải vào **FTP Sites folder** | **New** | **FTP Site**.
- Cung cấp các thông tin về "**FTP Site Description**" và "**IP Address and Port Settings**", chọn **Next**.
- Chọn **Isolate users**, chọn **Next** (tham khảo hình 2.21).



Hình 2.21: Tạo **FTP** sử dụng **Isolate Users**.

- Sau đó ta chỉ định thư mục gốc của **FTP**, quyền hạn truy xuất thư mục, sau cùng chọn **Finish** để hoàn tất quá trình.
- Nếu ta cho phép **User Anonymous** truy xuất vào **FTP Site** này thì trong thư mục gốc của **FTP Site** ta tạo một thư mục con có tên **LocalUser** (hoặc tên miền (tên **domain**) trong trường hợp máy chủ là **domain controller**), sau đó tạo **LocalUser\Public** (hoặc **domain_name\Public**) để **anonymous** truy xuất vào thư mục này.
- Nếu cho phép mỗi **người dùng cục bộ** truy xuất vào **FTP** thì ta tạo thư mục con của thư mục **FTP Root** với tên **LocalUser** và **LocalUser*username*.**
- Nếu cho phép mỗi **người dùng trong domain** truy xuất vào **FTP** thì ta tạo thư mục con của thư mục **FTP Root** với tên **<domain_name>** và thư mục con **<domain_name>\username.**

Tạo **FTP Site** dùng **Isolate User** với **Active Directory**.

Khi ta cấu hình **FTP Server** để cô lập các người dùng (**isolate users**) với **Active Directory**, khi tạo ta cần hiệu chỉnh hai thông số:

- **FTPRoot**: Chỉ định thông số **UNC** (**Universal Naming Convention**) của máy chủ chia sẻ tài nguyên (ví dụ **\\servername\sharename**), tuy nhiên ta cũng có thể chỉ định **FTP root** trên ổ đĩa cục bộ.
- **FTPDir**: Chỉ định đường dẫn thư mục cho từng user trong **Active Directory**.

Với **Windows 2003 family** hoặc **Windows 2003 enterprise** Để chỉ định hai thông số **FTPRoot** và FTPDir ta có thể vào **Properties** của từng người dùng hiệu chỉ hai thông số **msIIS-FTPRoot, msIIS-FTPDir** (trên **windows 2003 standard** không tồn tại cơ chế hiệu chỉnh này, ta phải dùng dòng lệnh để định nghĩa). Ta cũng có thể dùng lệnh **iisftp.vbs** để thay đổi hai thông số này.

Cú pháp lệnh như sau:

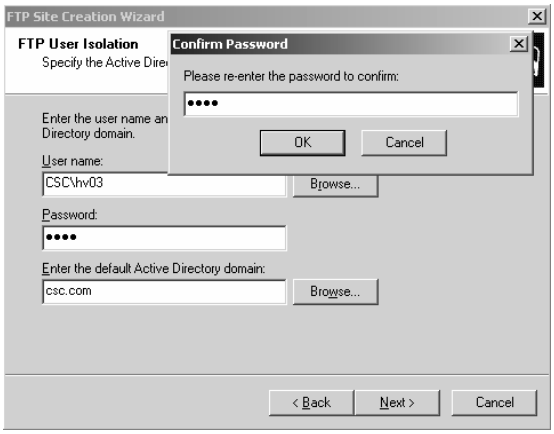
Định FTP Root:

```
<cmd_prompt>iisftp.vbs /SetADProp <username> FTPRoot <Local_dir>
```

<cmd_prompt>iisftp.vbs /SetADProp <user_name> FTPDir <sub_FTPRoot>

Sau đây là các bước tạo **FTP User Isolate** với **Active Directory**:

- Bấm chuột phải vào **FTP Sites** folder | **New** | **FTP Site**.
- Cung cấp các thông tin về **FTP Site Description**, chọn cụ thể địa chỉ **IP** trong hộp thoại "**IP Address and Port Settings**", chọn **Next**.
- Trong hộp thoại "**FTP User Isolation**", ta chọn "**Isolate users using Active Directory**", chọn **Next**.
- Cung cấp thông tin về **username**, **password**, **domain name**, sau đó chọn **Next** để xác nhập lại mật khẩu của người dùng (tham khảo Hình 2.22 ta FTP cho hv03)



Hình 2.22: **FTP User Isolation**.

- Sau đó cấp quyền truy xuất cho **user**, sau cùng ta chọn **Finish**.
- Dùng lệnh:

<cmd_prompt>iisftp.vbs /SetADProp <username> FTPRoot <Local_dir>

<cmd_prompt>iisftp.vbs /SetADProp <user_name> FTPDir <sub_FTPRoot>

- Ví dụ:

iisftp.vbs /SetADProp hv03 FTPRoot c:\ftproot

iisftp.vbs /SetADProp hv03 FTPDir \hv03

- Trong đó \hv03 là thư mục con của c:\ftproot.

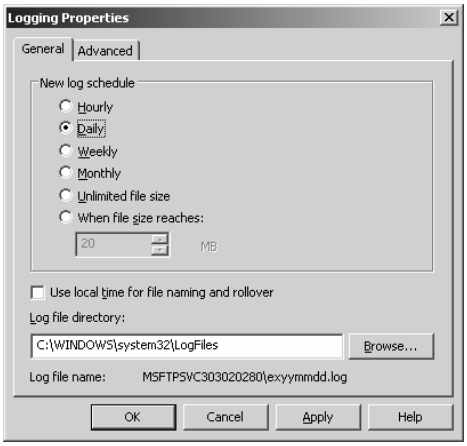
III.2.8 Theo dõi và cấu hình nhật ký cho FTP.

Mặc định **FTP** lưu lại một số sự kiện như: Địa chỉ của **FTP Client** truy xuất vào **FTP Server**, thời gian truy xuất của máy trạm, trạng thái hoạt động của dịch vụ,… để hỗ trợ cho người quản trị có thể theo dõi quản lý hệ thống hiệu quả hơn.

- Tất cả các sự kiện này lưu trữ trong các file trong thư mục **%systemroot%\system32\LogFiles\MSFTPSVnnnnnnnn**, trong đó **nnnnnnnn** là số **ID** của **FTP Site**.
- Để hiệu chỉ lại thông tin ghi nhận nhật ký (**logging**) của dịch vụ ta chọn **properties** của **FTP Site** | Tab **FTP Site** | **Properties** (tham khảo hình 2.23).

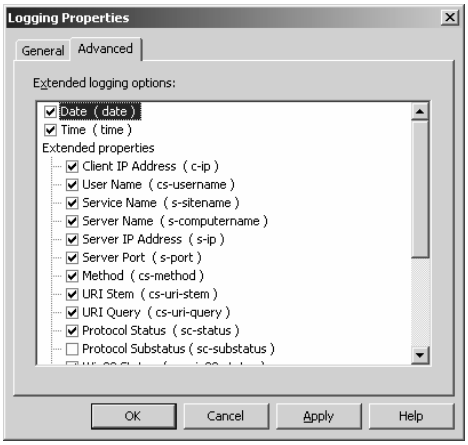
- **New log schedule:** Chỉ định ghi nhận theo lịch biểu, kích thước tập tin.

- **Log file directory:** Chỉ định thư lưu trữ **log file**.



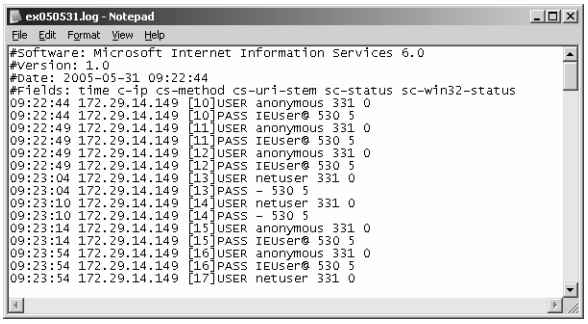
Hình 2.23: Thay đổi nhật ký.

- **Tab Advanced** để cho phép ta có thể chọn một số tùy chọn theo dõi khác như: **Username**, **service name**, **server name**, **server IP**…(Tham khảo hình 2.24)



Hình 2.24: Tùy chọn **logging**.

- Để xem thông tin nhật ký trên ta mở các tập tin trong thư mục **%systemroot%\system32\LogFiles\MSFTPSVCnnnnnnnn**, ví dụ ta xem tập tin nhật ký ex050531.log (dùng **notepad** để mở) (tham khảo hình 2.25).



Hình 2.25: Xem tập tin nhật ký.

III.2.9 Khởi động và tắt dịch vụ FTP.

Ta có thể dùng trình tiện ích **IIS** bằng cách bấm chuộc phải vào **FTP Site** chọn **Stop** để dùng dịch vụ và chọn **Start** để khởi động dịch vụ. Tuy nhiên ta có thể sử dụng dòng lệnh để khởi động và tắt dịch vụ **FTP**:

<command_prompt>net <stop/start> msftpsvc

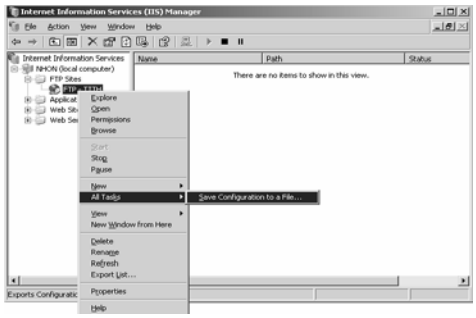
Hoặc có thể dùng lệnh **iisreset** để **restart** lại dịch vụ này:

< command_prompt >**iisreset**

III.2.10 Lưu trữ và phục hồi thông tin cấu hình.

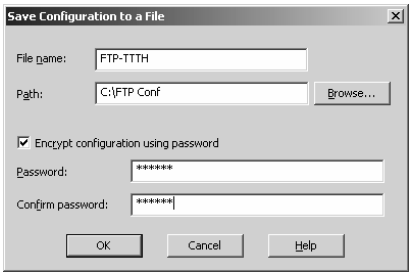
Sau khi ta cấu hình hoàn tất các thông tin cần thiết cho **FTP Site** ta có thể lưu trữ thông tin cấu hình này dưới dạng tập tin *.xml, sau đó ta có thể tạo mới hoặc phục hồi lại cấu hình cũ từ tập tin *.xml này.

- Lưu trữ thông tin cấu hình vào tập tin *xml ta bấm chuột phải vào **FTP Site** cần lưu thông tin cấu hình, chọn **All Task | Save Configuration to a File…**(Tham khảo hình 2.26)



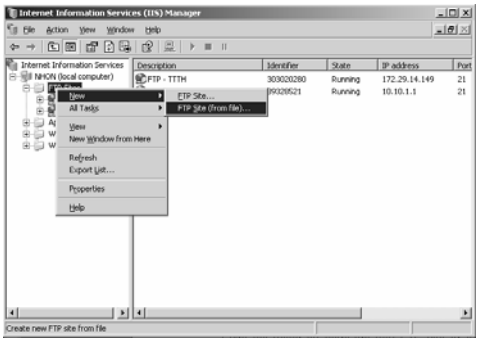
Hình 2.26: Lưu trữ thông tin cấu hình.

- Chỉ định tên tập tin và thư mục lưu trữ thông tin cho **FTP server**.
- **Encrypt configuration using password**: Sử dụng mật khẩu để mã hóa thông tin cấu hình (mặc định tùy chọn này không được chọn).



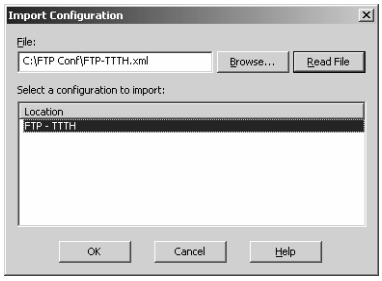
Hình 2.27: Chỉ định tên tập tin cấu hình.

- Phục hồi thông tin hoặc tạo mới **FTP site** từ tập tin cấu hình *.xml.



Hình 2.28

- Sau đó ta chọn nút **Browse**… để chọn tập tin cấu hình và chọn nút **Read File**, sau đó chọn tên mô tả trong hộp thoại **Location**, chọn **OK**.



Hình 2.29: **Import file** cấu hình.

- Sau đó chọn **OK** để đồng ý **import file** theo cách tạo mới **site** hay thay thế **site** hiện tại đã tồn tại.

Hình 2.30

Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học cho học viên có thể tổ chức, triển khai, quản trị một WebServer trên môi trường MS Windows, cụ thể là IIS 6.0	I. Giao thức HTTP. II. Nguyên tắc hoạt động của Web Server. III. Đặc điểm của IIS. IV. Cài đặt và cấu hình IIS 6.0.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

I. Giao thức HTTP.

HTTP là một giao thức cho phép **Web Browser** và **Web Server** có thể giao tiếp với nhau. **HTTP** bắt đầu là 1 giao thức đơn giản giống như với các giao thức chuẩn khác trên **Internet**, thông tin điều khiển được truyền dưới dạng văn bản thô thông qua kết nối **TCP**. Do đó, kết nối **HTTP** có thể thay thế bằng cách dùng lệnh **telnet** chuẩn.

Ví dụ:

> telnet www.extropia 80

GET /index.html HTTP/1.0

<- Có thể cần thêm ký tự xuống dòng

Để đáp ứng lệnh **HTTP GET** , **Web server** trả về cho **Client** trang "**index.html**" thông qua phiên làm việc **telnet** này, và sau đó đóng kết nối chỉ ra kết thúc tài liệu.

Thông tin gởi trả về dưới dạng:

<HTML>

<HEAD>

<TITLE>eXtropia Homepage</TITLE>

[...]

</HEAD>

</HTML>

Giao thức đơn giản yêu-cầu/đáp-ứng (**request/response**) này đã phát triển nhanh chóng và được định nghĩa lại thành một giao thức phức tạp (phiên bản hiện tại HTTP/1.1) . Một trong các thay đổi lớn nhất trong **HTTP/1.1** là nó hỗ trợ kết nối lâu dài (**persistent connection**).

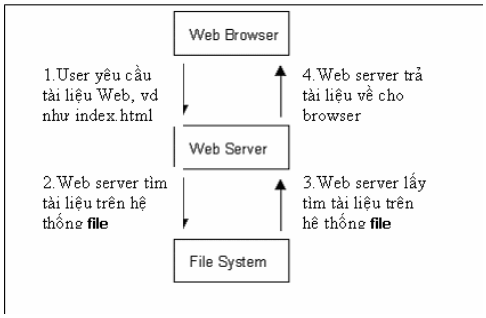
Trong **HTTP/1.0**, một kết nối phải được thiết lập đến **Server** cho mỗi đối tượng mà **Browser** muốn **download**. Nhiều trang Web có rất nhiều hình ảnh, ngoài việc tải trang **HTML** cơ bản, **Browser** phải lấy về một số lượng hình ảnh. Nhiều cái trong chúng thường là nhỏ hoặc chỉ đơn thuần là để trang trí cho phần còn lại của trang **HTML**.

II. Nguyên tắc hoạt động của Web Server.

Ban đầu **Web Server** chỉ phục vụ các tài liệu **HTML** và hình ảnh đơn giản. Tuy nhiên, đến thời điểm hiện tại nó có thể làm nhiều hơn thế.

Đầu tiên xét **Web Server** ở mức độ cơ bản, nó chỉ phục vụ các nội dung tĩnh. Nghĩa là khi **Web Server** nhận 1 yêu cầu từ **Web Browser**, nó sẽ ánh xạ đường dẫn này **URL** (ví dụ: http://www.hcmuns.edu.vn/index.html) thành một tập tin cục bộ trên máy **Web Server**.

Máy chủ sau đó sẽ nạp tập tin này từ đĩa và gởi tập tin đó qua mạng đến **Web Browser** của người dùng. **Web Browser** và **Web Server** sử dụng giao thức **HTTP** trong quá trình trao đổi dữ liệu.



Hình 3.1: Sơ đồ hoạt động của **Web Server**.

Trên cơ sở phục vụ những trang Web tĩnh đơn giản này, ngày nay chúng đã phát triển với nhiều thông tin phức tạp hơn được chuyển giữa **Web Server** và **Web Browser**, trong đó quan trọng nhất có lẽ là nội dung động (**dynamic content**).

II.1. Cơ chế nhận kết nối.

Với phiên bản đầu tiên, **Web Server** hoạt động theo mô hình sau:

- Tiếp nhận các yêu cầu từ **Web Browser**.
- Trích nội dung từ đĩa .
- Chạy các chương trình **CGI**.
- Truyền dữ liệu ngược lại cho **Client**.

Tuy nhiên, cách hoạt động của mô hình trên không hoàn toàn tương thích lẫn nhau. Ví dụ, một **Web Server** đơn giản phải theo các luật logic sau:

- Chấp nhận kết nối.
- Sinh ra các nội dung tĩnh hoặc động cho **Browser**.
- Đóng kết nối.
- Chấp nhận kết nối.
- Lập lại quá trình trên ...

Điều này sẽ chạy tốt đối với các **Web Sites** đơn giản, nhưng **Server** sẽ bắt đầu gặp phải vấn đề khi có nhiều người truy cập hoặc có quá nhiều trang Web động phải tốn thời gian để tính toán cho ra kết quả.

Ví dụ: Nếu một chương trình **CGI** tốn 30 giây để sinh ra nội dung, trong thời gian này **Web Server** có thể sẽ không phục vụ các trang khác nữa .

Do vậy, mặc dù mô hình này hoạt động được, nhưng nó vẫn cần phải thiết kế lại để phục vụ được nhiều người trong cùng 1 lúc. **Web Server** có xu hướng tận dụng ưu điểm của 2 phương pháp khác nhau để giải quyết vấn đề này là: đa tiểu trình (**multi-threading**) hoặc đa tiến trình (**multi-processing**) hoặc các hệ lai giữa **multi-processing** và **multi-threading**.

II.2. Web Client.

Là những chương trình duyệt Web ở phía người dùng, như **Internet Explorer**, **Netscape Communicator**.., để hiển thị những thông tin trang Web cho người dùng. **Web Client** sẽ gửi yêu cầu đến **Web Server**. Sau đó, đợi **Web Server** xử lý trả kết quả về cho **Web Client** hiển thị cho người

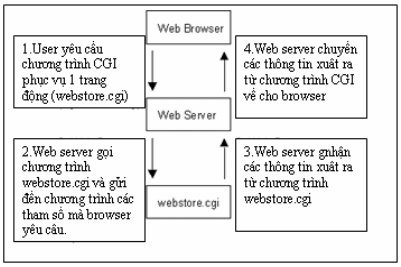
dùng. Tất cả mọi yêu cầu đều được xử lý bởi **Web Server**.

II.3. Web động.

Một trong các nội dung động (thường gọi tắt là Web động) cơ bản là các trang Web được tạo ra để đáp ứng các dữ liệu nhập vào của người dùng trực tiếp hay gián tiếp.

Cách cổ điển nhất và được dùng phổ biến nhất cho việc tạo nội dung động là sử dụng **Common Gateway Interface** (**CGI**). Cụ thể là **CGI** định nghĩa cách thức **Web Server** chạy một chương trình cục bộ, sau đó nhận kết quả và trả về cho **Web Browser** của người dùng đã gửi yêu cầu.

Web Browser thực sự không biết nội dung của thông tin là động, bởi vì **CGI** về cơ bản là một giao thức mở rộng của **Web Server**. Hình vẽ sau minh hoạ khi **Web Browser** yêu cầu một trang Web động phát sinh từ một chương trình **CGI**.



Hình 3.2: Mô hình Xử lý.

Một giao thức mở rộng nữa của **HTTP** là **HTTPS** cung cấp cơ chế bảo mật thông tin "nhạy cảm" khi chuyển chúng xuyên qua mạng.

III. Đặc điểm của IIS 6.0.

IIS 6.0 có sẵn trên tất cả các phiên của **Windows 2003**, **IIS** cung cấp một số đặc điểm mới giúp tăng tính năng tin cậy, tính năng quản lý, tính năng bảo mật, tính năng mở rộng và tương thích với hệ thống mới.

III.1. Các thành phần chính trong IIS.

Hai thành phần chính trong **IIS 6.0** là **kernel-mode processes** và **user-mode processes**, ta sẽ khảo sát một số thành phần sau:

- **HTTP.sys**: Là trình điều khiển thuộc loại **kernel-mode device** hỗ trợ chứng năng chuyển **HTTP request** đến tới các ứng dụng trên **user-mode**:
- Quản lý các kết nối **Transmission Control Protocol** (**TCP**).
- Định tuyến các **HTTP requests** đến đúng hàng đợi xử lý yêu cầu (**correct request queue**).
- Lưu giữ các **response** vào vùng nhớ (**Caching of responses in kernel mode**).
- Ghi nhận nhật ký cho dịch vụ **WWW** (**Performing all text-based logging for the WWW service**).
- Thực thi các chức năng về **Quality of Service** (**QoS**) bao gồm: connection limits, **connection time-outs**, **queue-length limits**, **bandwidth throttling**.
- **WWW Service Administration and Monitoring Component**: cung cấp cơ chế cấu hình dịch vụ **WWW** và quản lý **worker process**.
- **Worker process**: Là bộ xử lý các yêu cầu (**request**) cho ứng dụng **Web**, **worker process** có thể

xử lý các yêu cầu và gởi trả kết quả dưới dạng trang Web tĩnh, gọi các **ISAPI Extensions**, kích

hoạt các **CGI handler**, tập tin thực thi của **worker process** có tên là **W3wp.exe**. **Worker process** chạy trong **user-mode**.

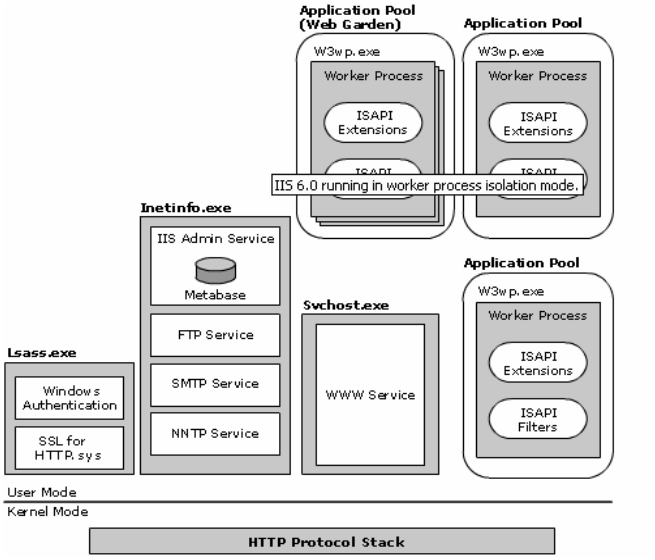
- **Inetinfo.exe** là một thành phần trong **user-mode**, nó có thể nạp (**host**) các dịch vụ trong **IIS 6.0**, các dịch vụ này bao gồm: **File Transfer Protocol service** (**FTP service**), **Simple Mail Transfer Protocol service** (**SMTP service**), **Network News Transfer Protocol service** (**NNTP service**), **IIS metabase**.

III.2. IIS Isolation mode.

Trong **IIS** có hai chế độ hoạt động tách biệt là ***worker process isolation mode*** *và* ***IIS 5.0 isolation mode***. Cả hai chế độ này đều dựa vào đối tượng **HTTP Listener**, tuy nhiên nguyên tắc hoạt động bên trong của hai chế độ này hoạt về cơ bản là khác nhau.

III.3. Chế độ Worker process isolation.

- Trong chế độ này mọi thành phần chính trong dịch vụ **Web** được tách thành các tiến trình xử lý riêng biệt (gọi là các **Worker process**) để bảo vệ sự tác động của các ứng dụng khác trong **IIS**, đây là chế độ cung cấp tính năng bảo mật ứng dụng rất cao vì hệ thống nhận diện mỗi ứng dụng chạy trên **Worker process** được xem là một **network service** trong khi đó các ứng dụng chạy trên **IIS 5.0** được xem là **LocalSystem** và nó có thể truy xuất và thay đổi hầu hết các tài nguyên được cung cấp trên hệ thống nội bộ.
- Sử dụng **worker process isolation** mode cho phép tích hợp thêm các tính năng mới như : **application pooling**, **recycling** và **health detection**, các tính năng này không được hỗ trợ trên **IIS 5.0**.
- Mô hình xử lý của **Worker process Isolation mode**:



Hình 3.3: Kiến trúc của **IIS 6.0** chạy trên chế độ **Worker Process Isolation**.

Trong hình 3.3, ta thấy các đoạn mã xử lý cho từng ứng dụng đặc biệt như **ASP**, **ASP.NET** được nạp vào bộ xử lý tiến trình (**Worker process**) bởi vì các bộ xử lý định thời(**run-time engine**) của ngôn ngữ lập trình này được thực thi như một Internet server **API** (**ISAPI**)

Các bước minh họa cho một yêu cầu xử lý trong **worker process**:

Yêu cầu của **Client** được chuyển đến đối tượng **HTTP Listener** (**HTTP.sys**)

HTTP.sys xác định yêu cầu có hợp lệ không?. Nếu yêu cầu không hợp lệ **HTTP.sys** sẽ gởi đoạn mã báo lỗi về cho **Client**.

Nếu yêu cầu hợp lệ **HTTP.sys** sẽ kiểm tra xem **response** của **request** này có trong **kernel-mode cache** không, nếu có thì nó sẽ đọc **response** này và gởi về cho **Client**.

Nếu **response** không có trong **cache** thì **HTTP.sys** xác định **request queue** phù hợp và đặt **request** vào trong **request queue**.

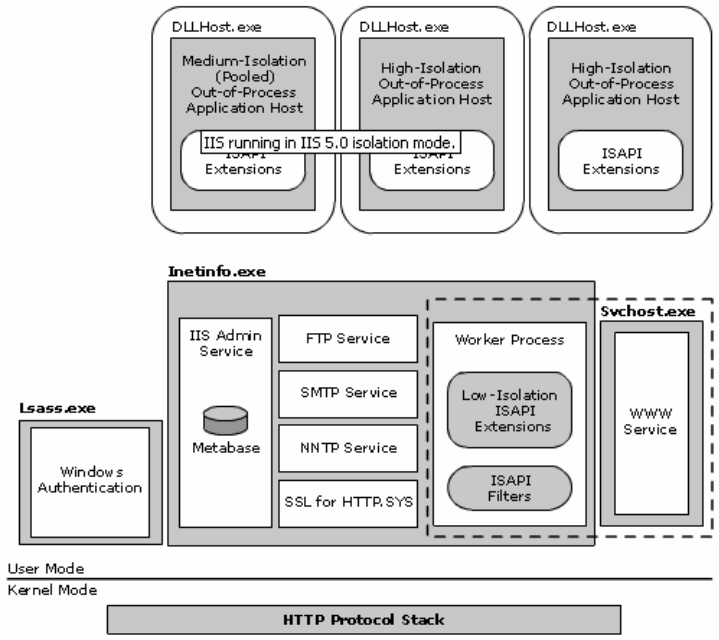
Nếu hàng đợi (**request queue**) không được cung cấp một **worker processes** thì **HTTP.sys** báo hiệu cho **WWW service** khởi tạo **worker processes** cho hành đợi (**request queue**).

Sau đó **worker process** xử lý các **request** và gởi trả kết quả về cho **HTTP.sys**.

HTTP.sys gởi kết quả về cho **Client** và **log** lại các yêu cầu này.

III.3.1 IIS 5.0 Isolation Mode.

IIS 5.0 Isolation mode đảm bảo tính tương thích cho ứng dụng được phát triển từ phiên bản **IIS 5.0**.



Hình 3.4: **IIS** chạy trên **IIS 5.0 Isolation mode**.

III.3.2 So sánh các chức năng trong IIS 6.0 mode.

Bảng mô tả vai trò của **IIS 6.0** khi chạy trong **IIS 5.0 isolation mode** và **worker process isolation mode**.

Các chức năng của IIS	IIS 5.0 Isolation Mode Host/Component	Worker Process Isolation Mode Host/Component
Worker process management		Svchost.exe (WWW service)

Worker process		W3wp.exe (Worker process)
Running in-process ISAPI extensions	Inetinfo.exe	W3wp.exe
Running out-of-process ISAPI extensions	DLLHost.exe	N/A (all of ISAPI extensions are in-process)
Running ISAPI filters	Inetinfo.exe	W3wp.exe
HTTP.sys configuration	Svchost.exe/WWW service	Svchost.exe/WWW service
HTTP protocol support	Windows kernel/HTTP.sys	Windows kernel/HTTP.sys
IIS metabase	Inetinfo.exe	Inetinfo.exe
FTP	Inetinfo.exe	Inetinfo.exe
NNTP	Inetinfo.exe	Inetinfo.exe
SMTP	Inetinfo.exe	Inetinfo.exe

Các Isolation mode mặc định:

Loại cài đặt	Isolation mode
Cài đặt mới IIS 6.0	Worker process isolation mode
Nâng cấp từ các phiên bản trước lên IIS 6.0	Vẫn giữ nguyên Isolation mode cũ.
Nâng cấp từ IIS 5.0	IIS 5.0 isolation mode
Nâng cấp từ IIS 4.0	IIS 5.0 isolation mode

III.4. Nâng cao tính năng bảo mật.

- **IIS 6.0** không được cài đặt mặc định trên **Windows 2003**, người quản trị phải cài đặt IIS và các dịch vụ liên quan tới **IIS**.
- **IIS 6.0** được cài trong **secure mode** do đó mặc định ban đầu khi cài đặt xong **IIS** chỉ cung cấp một số tính năng cơ bản nhất, các tính năng khác như **Active Server Pages** (**ASP**), **ASP.NET**, **WebDAV publishing**, **FrontPage Server Extensions** người quản trị phải kích hoạt khi cần thiết.
- Hỗ trợ nhiều tính năng chứng thực:
- **Anonymous authentication** cho phép mọi người có thể truy xuất mà không cần yêu cầu **username** và **password**.

- **Basic authentication:** Yêu cầu người dùng khi truy xuất tài nguyên phải cung cấp **username** và mật khẩu thông tin này được **Client** cung cấp và gởi đến **Server** khi **Client** truy xuất tài nguyên. **Username** và **password** không được mã hóa khi qua mạng.
- **Digest authentication:** Hoạt động giống như phương thức **Basic authentication**, nhưng **username** và mật khẩu trước khi gởi đến **Server** thì nó phải được mã hóa và sau đó **Client** gởi thông tin này dưới một giá trị của băm (***hash value***). **Digest authentication** chỉ sử dụng trên **Windows domain controller**.
- **Advanced Digest authentication:** Phương thức này giống như **Digest authentication** nhưng tính năng bảo mật cao hơn. **Advanced Digest** dùng **MD5 hash** thông tin nhận diện cho mỗi **Client** và lưu trữ trong **Windows Server 2003 domain controller**.
- **Integrated Windows authentication:** Phương thức này sử dụng kỹ thuật băm để xác nhận thông tin của **users** mà không cần phải yêu cầu gởi mật khẩu qua mạng.
- **Certificates:** Sử dụng thẻ chứng thực điện tử để thiết lập kết nối **Secure Sockets Layer** (**SSL**).
- **.NET Passport Authentication**: là một dịch vụ chứng thực người dùng cho phép người dùng tạo **sign-in name** và **password** để người dùng có thể truy xuất vào các dịch vụ và ứng dụng **Web** trên nền **.NET**.
- IIS sử dụng **account** (**network service**) có quyền ưu tiên thấp để tăng tính năng bảo mật cho hệ thống.
- Nhận dạng các phần mở rộng của file qua đó **IIS** chỉ chấp nhận một số định dạng mở rộng của một số tập tin, người quản trị phải chỉ định cho **IIS** các định dạng mới khi cần thiết.

III.5. Hỗ trợ ứng dụng và các công cụ quản trị.

IIS 6.0 có hỗ trợ nhiều ứng dụng mới như **Application Pool**, **ASP.NET**.

- **Application Pool**: là một nhóm các ứng dụng cùng chia sẻ một **worker process** (**W3wp.exe**).
- **worker process** (**W3wp.exe**) cho mỗi **pool** được phân cách với **worker process** (**W3wp.exe**) trong **pool** khác.
- Một ứng dụng nào đó trong một **pool** bị lỗi (**fail**) thì nó không ảnh hưởng tới ứng dụng đang chạy trong **pool** khác.
- Thông qua **Application Pool** giúp ta có thể hiệu chỉnh cơ chế tái sử dụng vùng nhớ ảo, tái sử dụng **worker process**, hiệu chỉnh **performance** (về **request queue**, **CPU**), **health**, **Identity** cho **application pool**.
- **ASP.NET:** là một **Web Application platform** cung cấp các dịch vụ cần thiết để xây dựng và phân phối ứng dụng **Web** và dịch vụ **XML Web**.

IIS 6.0 cung cấp một số công cụ cần thiết để hỗ trợ và quản lý **Web** như:

- **IIS Manager**: Hỗ trợ quản lý và cấu hình **IIS 6.0**
- **Remote Administration** (**HTML**) T**o**ol: Cho phép người quản trị sử dụng **Web Browser** để quản trị **Web** từ xa.
- **Command –line administration scipts**: Cung cấp các **scipts** hỗ trợ cho công tác quản trị **Web**, các tập tin này lưu trữ trong thư mục **%systemroot%\System32**.

IV. Cài đặt và cấu hình IIS 6.0.

IV.1. Cài đặt IIS 6.0 Web Service.

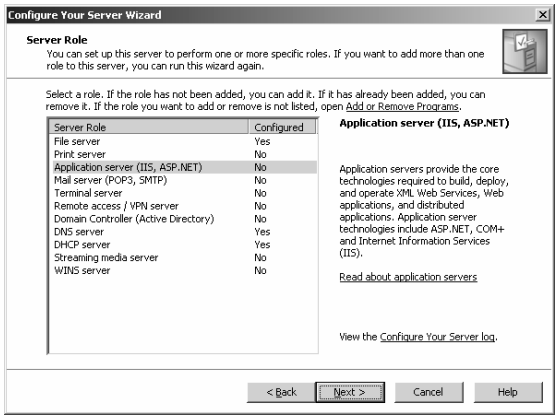
IIS 6.0 không được cài đặt mặc định trong **Windows 2003 server**, để cài đặt **IIS 6.0** ta thực hiện các bước như sau:

Chọn **Start** | **Programs** | **Administrative Tools** | **Manage Your Server**.

Hình 3.5: **Manage Your Server Roles**.

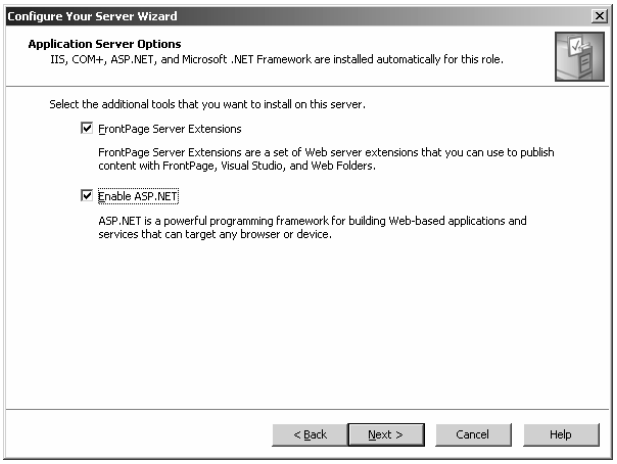
Từ hình 3.6 ta chọn biểu tượng **Add or remove a role**, chọn **Next** trong hợp thoại **Preliminitary Steps**

Chọn **Application server** (IIS, **ASP.NET**) trong hộp thoại **server role**, sau đó chọn **Next**.



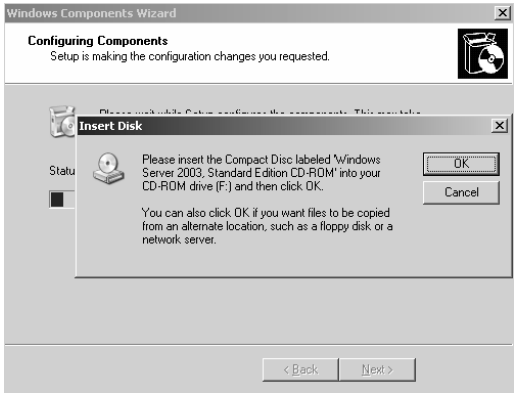
Hình 3.6: Chọn loại **Server**.

Chọn hai mục cài đặt **FrontPage Server Extentions** và **Enable ASP.NET**, sau đó chọn **Next**, chọn **Next** trong hộp thoại tiếp theo.



Hình 3.7: lựa chọn tùy chọn cho **Server**.

Sau đó hệ thống sẽ tìm kiếm **I386 source** để cài đặt **IIS**, nếu không tìm được xuất hiện yêu cầu chỉ định đường dẫn chứa bộ nguồn **I386**, sau đó ta chọn **Ok** trong hộp thoại Hình 3.8.

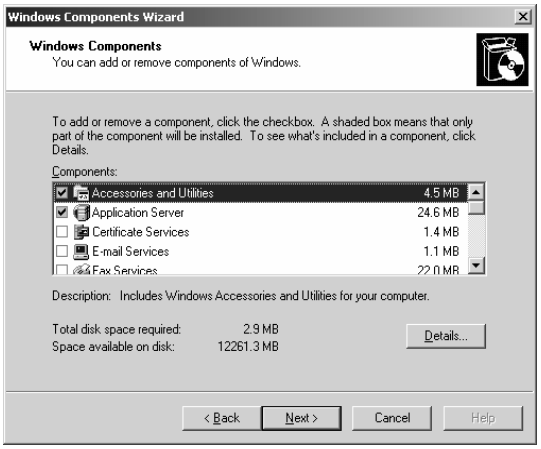


Hình 3.8: Chỉ định **I386 source**.

Chọn **Finish** để hoàn tất quá trình.

Tuy nhiên ta cũng có thể cài đặt **IIS 6.0** trong **Add or Remove Programs** trong **Control Panel** bằng cách thực hiện một số bước điển hình sau:

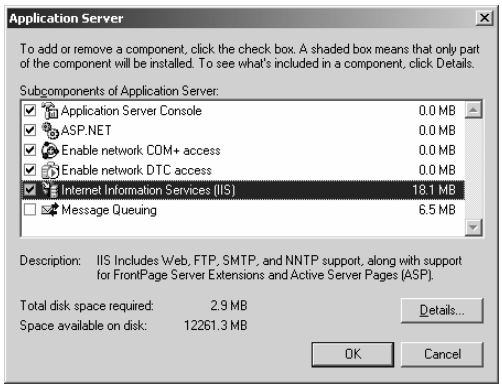
Mở cửa sổ **Control Panel** | **Add or Remove Programs** | **Add/Remove Windows Components**.



Hình 3.9: Chọn **Application Server**.

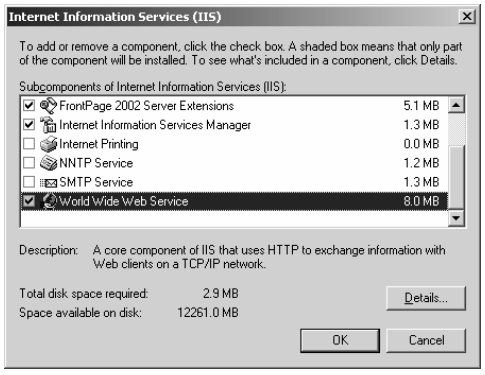
Chọn **Application Server**, sau đó chọn nút **Details**…

Chọn **Internet Information Services**, sau đó chọn nút **Details**…



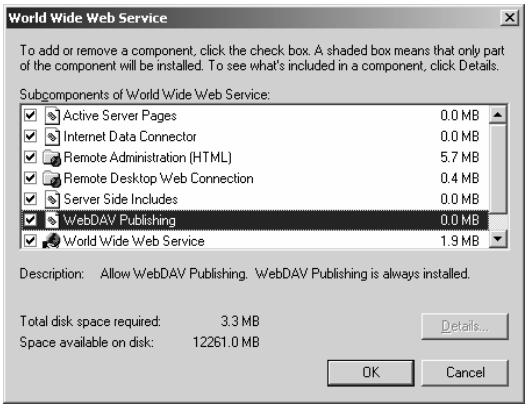
Hình 3.10: Chọn **IIS subcomponents**.

Chọn mục **World Wide Web service**, sau đó chọn nút **Details**…



Hình 3.11: Chọn **WWW service**.

Sau đó ta chọn tất cả các **Subcomponents** trong **Web Service**.



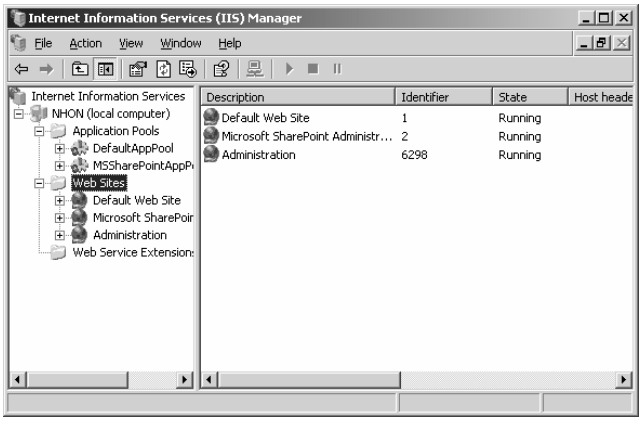
Hình 3.12: Chọn các thành phần trong **WWW service**.

IV.2. Cấu hình IIS 6.0 Web service.

Sau khi ta cài đặt hoàn tất, ta chọn **Administrative Tools** | **Information Service (IIS) Manager**, sau đó chọn tên **Server** (**local computer**)

Trong hộp thoại **IIS Manager** có xuất hiện 3 thư mục:

- **Application Pools**: Chứa các ứng dụng sử dụng **worker process** xử lý các yêu cầu của **HTTP request**.
- **Web Sites**: Chứa danh sách các **Web Site** đã được tạo trên **IIS**.
- **Web Service Extensions**: Chứa danh sách các **Web Services** để cho phép hay không cho phép **Web Server** có thể thực thi được một số ứng dụng Web như: **ASP**, **ASP.NET**, **CGI**, **WebDAV**,…



Hình 3.13: **IIS Manager**.

Trong thư mục **Web Sites** ta có ba **Web Site** thành viên bao gồm:

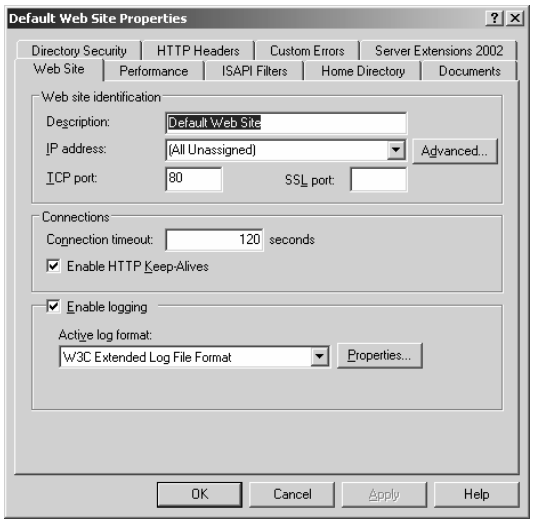
- **Default Web Site**: **Web Site** mặc định được hệ thống tạo sẵn.
- **Microsoft SharePoint Administration**: Đây là **Web Site** được tạo cho **FrontPage Server Extensions 2002 Server Administration**
- **Administration**: **Web Site** hỗ trợ một số thao tác quản trị hệ thống qua **Web**.

Khi ta cấu hình **Web Site** thì ta không nên sử dụng **Default Web Site** để tổ chức mà chỉ dựa **Web Site**

này để tham khảo một số thuộc tính cần thiết do hệ thống cung cấp để cấu hình **Web Site** mới của mình.

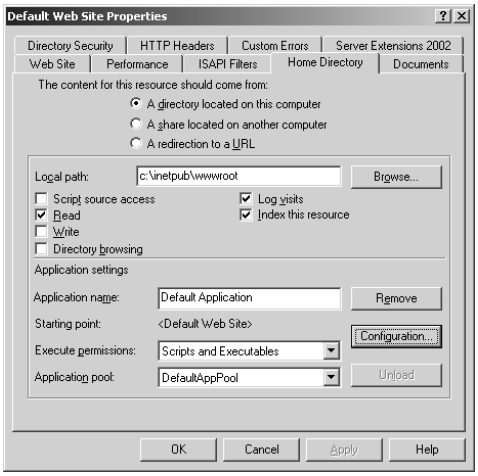
IV.2.1 Một số thuộc tính cơ bản.

Trước khi cấu hình **Web Site** mới trên **Web Server** ta cần tham khảo một số thông tin cấu hình do hệ thống gán sẵn cho **Default Web Site**. Để tham khảo thông tin cấu hình này ta nhấp chuột phải vào **Default Web Site** chọn **Properties**.



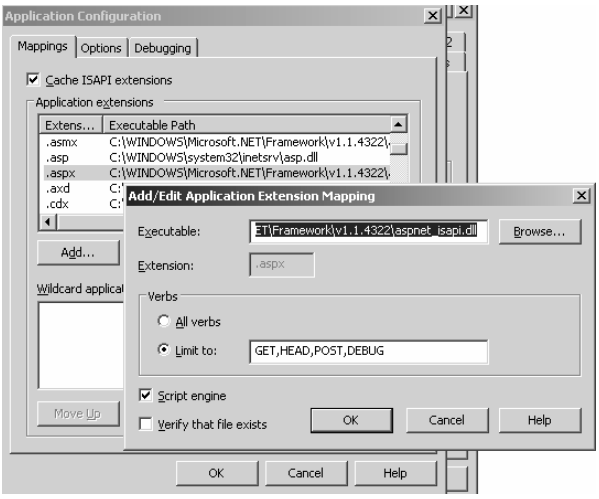
Hình 3.14: Thuộc tính **Web Site**.

- Tab **Web Site**: mô tả một số thông tin chung về dịch vụ Web như:
- **TCP port**: chỉ định cổng hoạt động cho dịch vụ **Web**, mặc định giá trị này là 80.
- **SSL Port**: Chỉ định port cho **https**, mặc định **https** hoạt động trên **port 443**. **https** cung cấp một số tính năng bảo mật cho ứng dụng **Web** cao hơn **http**.
- **Connection timeout** : Chỉ định thời gian duy trì một **http session**.
- Cho phép sử dụng **HTTP Keep-Alives**.
- Cho phép ghi nhận nhật ký (**Enable logging**)
- **Performance Tab**: cho phép đặt giới hạn băng thông, giới hạn **connection** cho **Web site**.
- **Home Directory Tab**: Cho phép ta thay đổi **Home Directory** cho **Web Site**, giới hạn quyền truy xuất, đặt một số quyền hạn thực thi **script** cho ứng dụng **Web** (như ta đặt các thông số: **Application name**, **Execute permission**, **Application pool**)



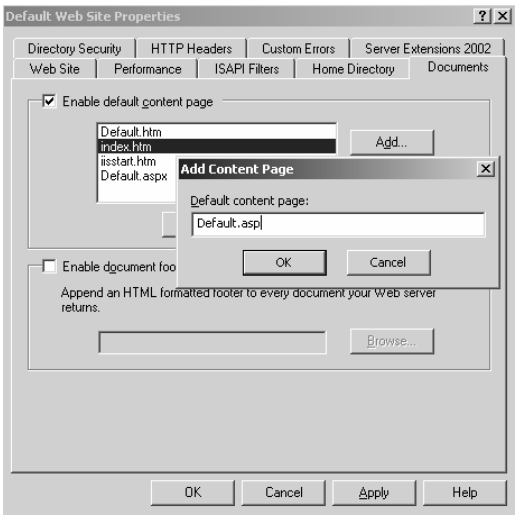
Hình 3.15: **Home Directory Tab**.

- Từ Hình 3.15 ta chọn nút **Configuration…** để có thể cấu hình các **extensions** về **.asp**, **.aspx**, **.asa**, … cho **Web Application** (tham khảo Hình 3.16)



Hình 3.16: Cấu hình **Script** cho **Web Application**.

- **Documents Tab**: Để thêm hoặc thay đổi trang **Web** mặc định cho **Web Site** (tham khảo hình 3.17).



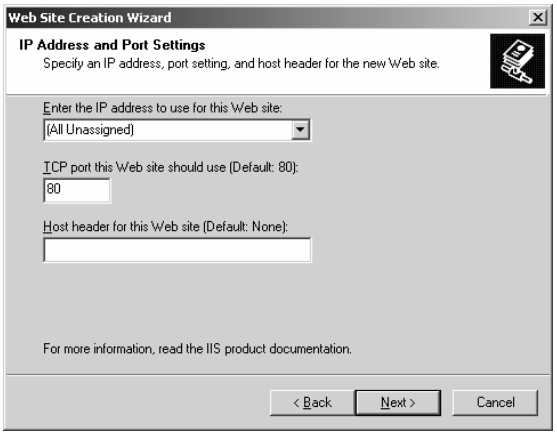
Hình 3.17: Chỉ định trang Web mặc định cho **Web Site**.

- **Directory Security Tab**: Đặt một số phương thức bảo mật cho **IIS** (tham khảo chi tiết trong mục "bảo mật cho dịch vụ Web")

IV.2.2 Tạo mới một Web site.

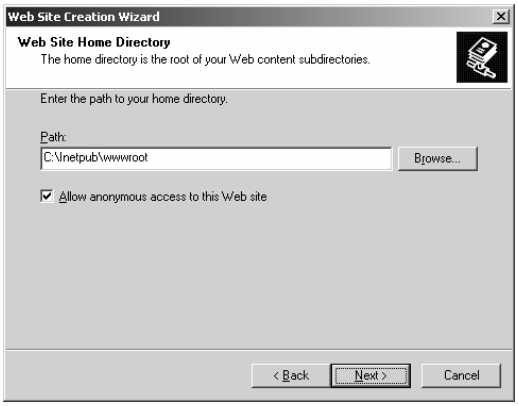
IIS cung cấp hai phương thức tạo mới **Web Site**:

- Tạo **Web Site** thông qua **Creation Wizard của IIS manager**.
- Tạo **Web Site** thông qua lệnh **iisweb.vbs**.
- Tạo **Web Site** thông qua "**Web Site Creation Wizard**" của **IIS manager**.
- Nhấp chuột phải vào thư mục **Web Sites** | **New | Web Site** | **Next**.
- Ta cung cấp tên **Web Site** trong hộp thoại **Description** | **Next**.
- Chỉ định các thông số về (Tham khảo Hình 3.18):
- **"Enter the IP address to use for this Web site"**: Chỉ định địa chỉ sử dụng cho **Web Site**, nếu ta chỉ định "**All Unassigned**" có nghĩa là **HTTP** được hoạt động trên tất cả các địa chỉ của **Server**.
- **"TCP port this Web site should use"**: Chỉ định cổng hoạt động cho dịch vụ.
- **"Host Header for this Web site (Default:None)"**: Thông số này để nhận diện tên **Web Site** khi ta muốn tạo nhiều **Web Site** cùng sử dụng chung một địa chỉ **IP** thì ta thường dùng thông số này để mô tả tên các **Web Site** đó, do đó khi ta chỉ tổ chức một **Web Site** tương ứng với 1 địa chỉ **IP** thì ta có thể không cần sử dụng thông số này.



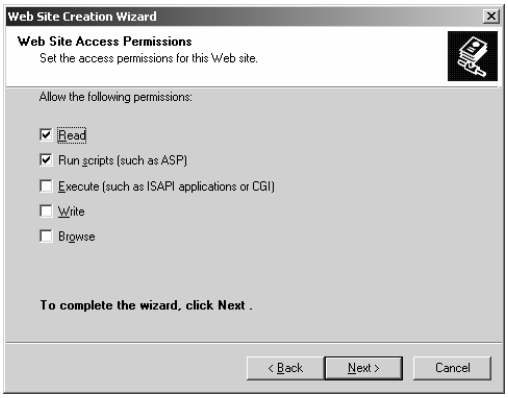
Hình 3.18: Chỉ định **IP Address** và **Port**.

- Trong hộp thoại "**Web Site Home Directory**" để chỉ định thư mục **home** của **Web Site** (thư mục lưu trữ nội dung của **Web Site)** và chỉ định **Anonymous** có được quyền truy xuất **Web Site** hay không (tham khảo Hình 3.19)



Hình 3.19: Chỉ định **Home Directory** cho **Web**.

- Chỉ định quyền hạn truy xuất cho **Web Site** (tham khảo Hình 3.20):
- **Read**: Quyền được truy xuất nội dung thư mục.
- **Run scripts** (**such as ASP**): Quyền được thực thi các trang **ASP**.
- **Execute** (**such as ISAPI Application for CGI**): Quyền được thực thi các ứng dụng **ISAPI**.
- **Write**: Quyền ghi và cập nhật dữ liệu của **Web Site**.
- **Browse**: Quyền liệt kê nội dung thư mục (khi không tìm được trang chủ mặc định)



Hình 3.20: Thiết lập quyền hạn truy xuất.

- Chọn **Finish** để hoàn tất quá trình.
- Tạo **Web Site** thông qua lệnh **iisweb.vbs**

Cú pháp lệnh:

iisweb.vbs /create <Home Directory> "Site Description" /i <IP Address> /b <Port>.

Các bước thực hiện:

- Nhấp chuột vào **Start** | **Run** | **cmd**.
- Từ dấu nhắc lệnh (**command prompt**) nhập vào lệnh: iisweb.vbs /create *c:\inetpub\wwwroot\newdirectory* "*MyWebSite*" /i *123.456.789* /b *80*.

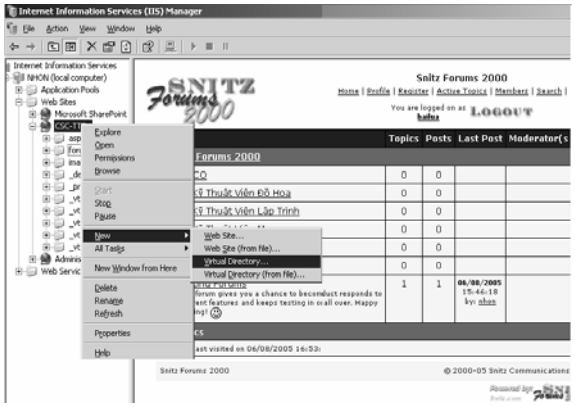
IV.2.3 Tạo Virtual Directory.

Thông thường để ta tạo thư mục ảo (**Virtual Directory** hay còn gọi là **Alias**) để ánh xạ một tài nguyên từ đường dẫn thư mục vật lý thành đường dẫn **URL**, thông qua đó ta có thể truy xuất tài nguyên này qua **Web Browser**.

Đường dẫn vật lý	Tên Alias	Địa chỉ URL
C:\Inetpub\wwwroot	Tên thư mục gốc (none)	http://SampleWebSite
\\Server2\SalesData	Customers	http://SampleWebSite/Customers
D:\Inetpub\wwwroot\Quotes	None	http://SampleWebSite/Quotes
D:\Marketing\PublicRel	Public	http://SampleWebSite/public

Các bước tạo **Virtual Directory**

Nhấp chuột phải vào tên **Web Site** cần tạo chọn **New**, chọn **Virtual Directory** (tham khảo Hình 3.21).



Hình 3.21: Tạo **Virtual Directory**.

Chọn **Next**, sau đó chỉ định tên **Alias** cần tạo (tham khảo Hình 3.22)

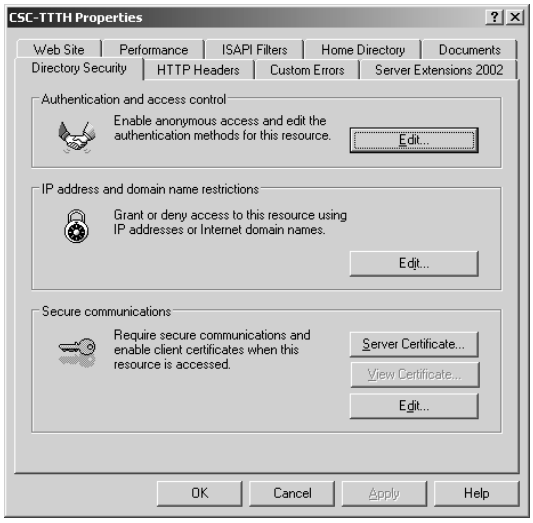
Hình 3.22: Chỉ định tên Alias

Chọn **Next** từ bước 2, sau đó chỉ định thư mục cục bộ hoặc đường dẫn mạng cần ánh xạ, Chỉ định quyền hạn truy xuất cho **Alias**, cuối cùng ta chọn **Finish** để hoàn tất quá trình.

IV.2.4 Cấu hình bảo mật cho Web Site.

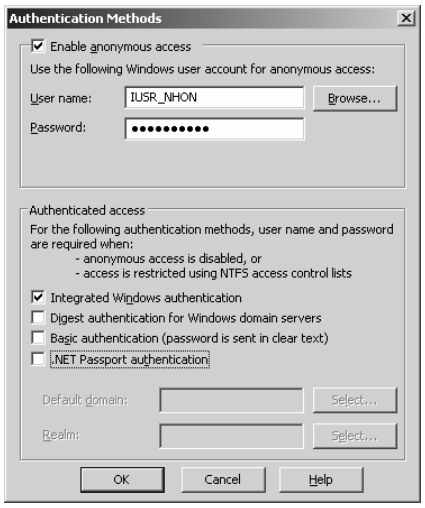
IIS cung cấp một số tính năng bảo mật cho **Web Site** như (tham khảo Hình 3.23):

- **Authentication And Access Control**: **IIS** cung cấp 6 phương thức chứng thực, kết hợp quyền truy cập **NTFS** để bảo vệ việc truy xuất tài nguyên trong hệ thống.
- **IP address and domain name restriction**: Cung cấp một số tính năng giới hạn **host** và **network** truy xuất vào **Web Site**.
- **Secure communication**: Cung cấp một số tính năng bảo mật trong giao tiếp giữa **Client** và **Server** bằng cách **Server** tạo ra các giấy chứng nhận cho **Client** (**Client Certificate**) và yêu cầu **Client** khi truy xuất tài nguyên vào **Server** thì phải gởi giấy chứng nhận để **Server** xác nhận yêu cầu có hợp lệ hay không.



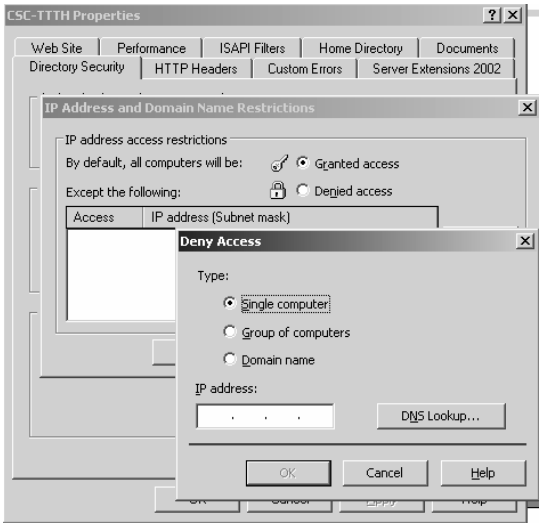
Hình 3.23: **Directory Security Tab**.

- Cấu hình **Authentication And Access Control:** từ Hình 3.23 ta chọn nút **Edit…**chọn các phương thức chứng thực cho phù hợp, mặc định hệ thống không yêu cầu chứng thực và cho mọi người sử dụng anonymous để truy xuất **Web Site**:



Hình 3.24: Chọn Phương thức chứng thực.

- Cấu hình **IP address and domain name restriction**: Từ hình 3.23 ta chọn nút **Edit**…



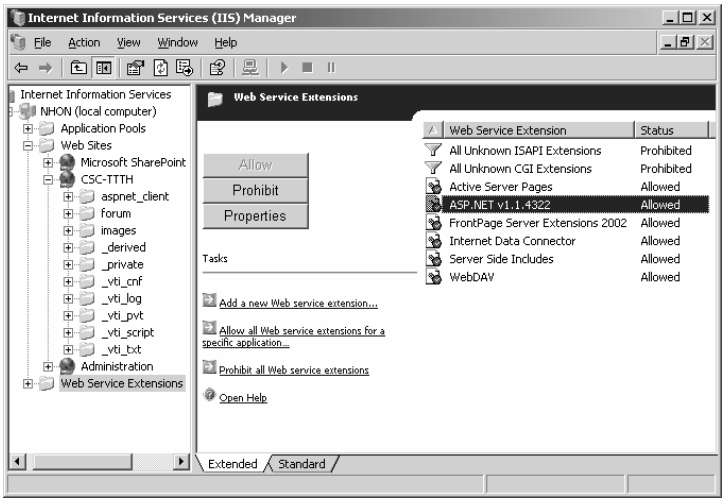
Hình 3.25: Giới hạn truy xuất cho **host**, **network** và **domain**.

- Cấu hình **Secure communication**: Từ hình 3.23 nút **Server Certificate**…để tạo giấy chứng nhận **Client**, nút **Edit** hiệu chỉnh các yêu cầu chứng nhận cho **Client** (tham khảo Hình 3.26).

Hình 3.26: Thay đổi thao tác chứng nhận.

IV.2.5 Cấu hình Web Service Extensions.

IIS Web Service Extensions cung cấp rất nhiều các dịch vụ mở rộng như: **ASP**, **ASP.NET**, **Frontpage Server Extensions 2002 WebDAV**, **Server Side Includes**, **CGI Extensions**, **ISAPI Extensions**. Thông qua **IIS Web Service Extensions** ta có thể cho phép hoặc cấm **Web Site** hỗ trợ các dịch vụ tương ứng (Nếu trên **Web Application** của ta có sử dụng các ứng dụng trên thì ta phải kích hoạt **Web Service** tương ứng)



Hình 3.27: Cấu hình **Web service extensions**.

IV.2.6 Cấu hình Web Hosting.

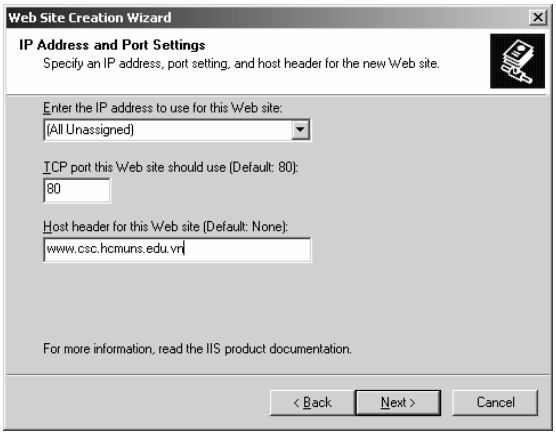
IIS cho phép ta tạo nhiều **Web Site** trên một **Web Server**, kỹ thuật này còn gọi là **Web Hosting**. Để nhận diện được từng **Web Site Server** phải dựa vào các thông số như **host header name, địa chỉ IP và số hiệu cổng Port**.

Tạo nhiều **Web Site** dựa vào **Host Header Names**:

Đây là phương thức tạo nhiều **Web Site** dựa vào tên **host** , có nghĩa rằng ta chỉ cần một địa chỉ **IP** để đại diện cho tất cả các **host name**.

Các bước tạo:

- Dùng **DNS** để tạo tên (**hostname**) cho **Web Site**.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Cung cấp **host name** (Ví dụ ta nhập tên: www.csc.hcmuns.edu.vn) cho **Web Site** cần tạo trong **Textbox Host Header Name** của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.28).



Hình 3.28: Tạo **Host Header Name**.

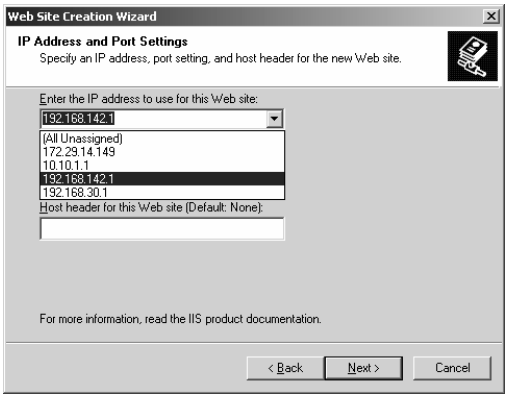
- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

Tạo nhiều **Web Site** dựa vào địa chỉ **IP**

Đối với phương thức này tương ứng một tên **Web Site** ta phải cung cấp một địa chỉ **IP**. Do đó nếu như ta tạo n **Web Site** thì ta phải tạo n địa chỉ, chính vì lẽ này nên phương thức này ít sử dụng hơn phương thức 1.

Các bước tạo:

- Ta phải thêm một hoặc nhiều địa chỉ **IP** cho card mạng.
- Dùng **DNS** tạo một **hostname** tương ứng với **IP** mới vừa tạo.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Chọn một địa chỉ **IP** cụ thể cho **Web Site** cần tạo trong tùy chọn "**Enter the IP address to use for this Web site**" của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.29).



Hình 3.29: Chọn địa chỉ **IP** cho **Web site**.

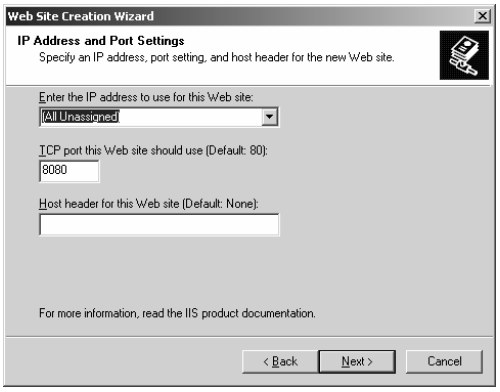
- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

Tạo nhiều **Web Site** dựa vào **Port**.

Mặc định **HTTP port** hoạt động trên **port 80** và **HTTPS** hoạt động trên **port 443**, thay vì mọi **Web Site** điều hoạt động trên cổng 80 hoặc 443 thì ta sẽ đổi **Web Site** hoạt động trên cổng (**port**) khác (ví dụ như 8080), vì thế ta chỉ cần dùng một địa chỉ **IP** để cung cấp cho tất cả các **Web Site**. Do đó khi ta truy xuất vào **Web Site** thì ta phải chỉ định cổng hoạt động cho dịch vụ (**http://www.csc.hcmuns.edu.vn:8080**).

Các cấu hình:

- Dùng **DNS** tạo một **hostname** tương ứng cho từng **Web Site** ánh xạ về cùng một địa chỉ **IP**.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Ta chỉ định thông số **Port** (ví dụ: **8080**) trong **Textbox** có tên "**TCP port for this Web site should use**" của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.30).

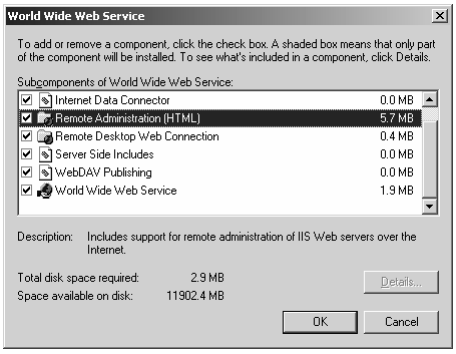


Hình 3.30: Chọn địa chỉ **IP** cho **Web Site**.

- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

IV.2.7 Cấu hình IIS qua mạng (Web Interface for Remote Administration).

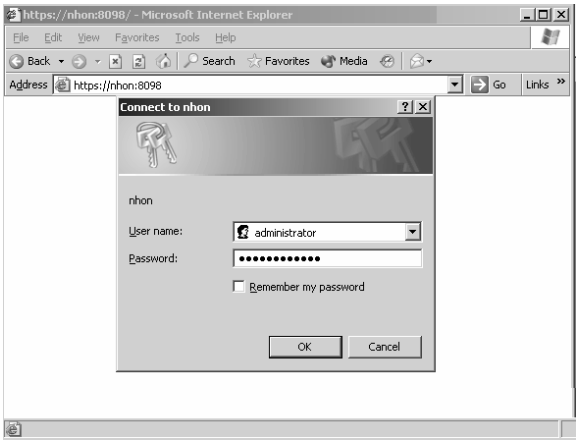
IIS cung cấp cơ chế quản trị dịch **Web** và quản trị một số tính năng cơ bản của hệ thống qua mạng, để sử dụng công cụ này ta phải cài thêm công cụ **Remote Administration (HTML)**



Hình 3.31: Cài đặt công cụ quản trị.

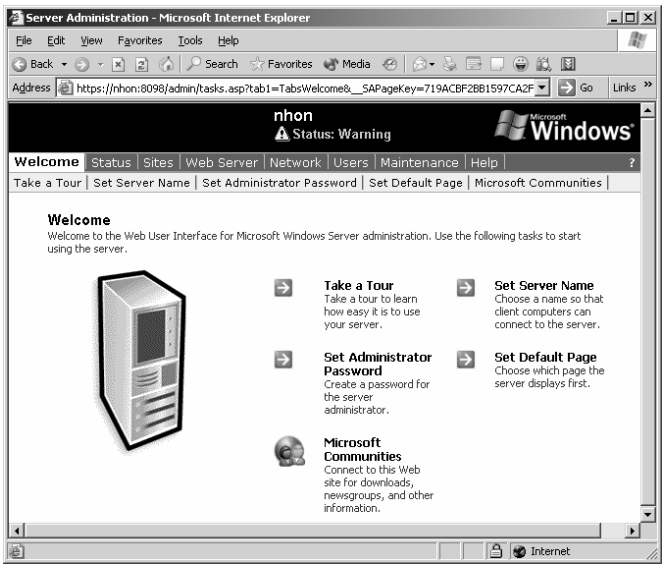
Truy cập vào **Administration Web Server** qua trình duyệt (**Web Browser**) thông qua địa chỉ **URL**: http://<Web Server>:8099 (tham khảo Hình 3.32), sau chỉ định **username**, **password** để truy xuất vào

Server.



Hình 3.32: Truy xuất vào **Administration Web Server**.

Sau khi đăng nhập thành công, giao diện **Server Administration** hiển thị (tham khảo hình 3.33):



Hình 3.33: Giao diện quản trị hệ thống qua **Web**.

Một số chức năng chính được cung cấp trong **Administration Server**.

Tên Tab	Chức năng
Welcome	Cho phép hiển thị lời chào, thay đổi mật khẩu của **administrator**, thay đổi tên máy,….
Status	Theo dõi trạng thái của hệ thống.
Sites	Quản lý các **Web Site** cấu hình.
Web Server	Thay đổi thông tin cấu hình cho **Web Service** và **FTP Service**.
Network	Thay đổi thông tin cấu hình mạng cho **Server**.

Users	Quản lý **user**.
Maintenance	Cung cấp một số thao tác để duy trì và sửa lỗi cho hệ thống.
Help	Cung cấp các trợ giúp về cấu hình.

IV.2.8 Quản lý Web site bằng dòng lệnh.

1. Tạo **Web Site**.

Ta dùng lệnh **iisweb.vbs** (**file scripte** này được lưu trữ trong thư mục *systemroot*\System32) để tạo một **Web** site mới trên máy nội bộ hoặc trên máy khác là **Windows 2003 member server** chạy **IIS 6.0**.

Cú pháp lệnh:

Iisweb.vbs /create Path SiteName [/b Port] [/I IPAddress] [/d HostHeader] [/dontstart] [/s Computer] [/u [Domain\]User [/p password]]

Danh sách tham số:

Tên tham số	Ý nghĩa
Path	Chỉ định vị trí đường dẫn ổ đĩa lưu trữ nội dung Web site.
SiteName	Mô tả tên **Web** site.
/b Port	Chỉ định **TCP Port** cho **Web Site**.
/I IPAddress	Chỉ định địa chỉ ip cho **Web Site**.
/d HostHeader	Chỉ định hostheader name cho **Web Site**.
/dontstart	Chỉ định cho **Web Site** không khởi tạo tự động khi tạo.
/s Computer	Chỉ định tên máy hoặc địa chỉ **IP** trên máy ở xa (sử dụng trong trường hợp tạo mới một **Web Site** trên máy tính ở xa)
/u [Domain\]User	Chạy script lệnh với **username** được chỉ định, **account** này phải là thành viên của nhóm **Administrators**, mặc định chay **script** với **username** hiện hành.
/p password	Chỉ định mật khẩu cho **account** chỉ định trong tham số /u

Ví dụ:

```
iisweb /create C:\Rome "My Vacations" /d www.reskit.com /dontstart
```

Hoặc dùng lệnh:

```
iisweb /create C:\New Initiatives\Marketing\HTMFiles "Marketing" /i 172.30.163.244 /s SVR01
/u Admin6 /p A76QVJ32#
```

2. Xóa **Web Site**.

Cú pháp lệnh:

iisweb /delete WebSite [WebSite...] [/s Computer [/u [Domain\]User/p Password]]

Ví dụ:

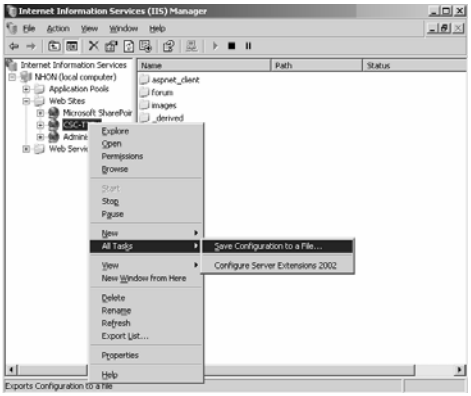
iisweb /delete "My First Novel"

IV.2.9 Sao lưu và phục hồi cấu hình Web Site.

IIS lưu trữ thông tin cấu hình theo định dạng **Extensible Markup Language** (**XML**) có tên **MetaBase.xml** và **MBSchema.xml**, các tập tin này thường lưu trữ trong thư mục *systemroot*\System32\Inetsrv. Do đó người quản trị có thao tác trực tiếp vào hai tập tin này để thay đổi thông tin cấu hình về IIS.

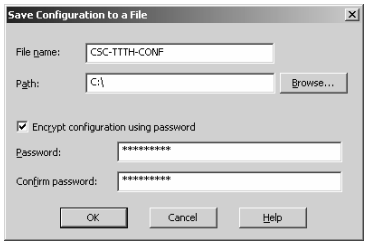
Lưu thông tin cấu hình

- Để sao lưu (**backup**) thông tin cấu hình cho **Web Site** ta nhấp chuột phải vào tên **Web Site** chọn **All Task**, chọn tiếp **Save Configuration to a file…**(tham khảo Hình 3.34)



Hình 3.34: sao lưu cấu hình Web site

- Sau đó ta chỉ định tập tin cấu hình, đường dẫn thư mục lưu trữ thông tin cấu hình, mật khẩu mã hóa cho tập tin cấu hình.

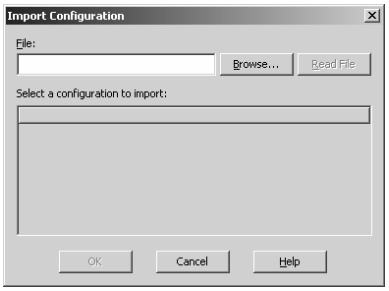


Hình 3.35: Sao lưu cấu hình **Web Site**.

Phục hồi cấu hình **Web Site** từ file cấu hình *.XML

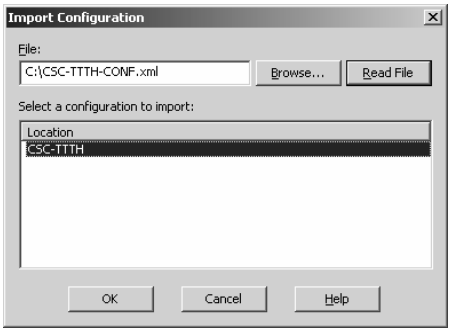
Để phục hồi thông tin cấu hình từ tập tin cấu hình *.xml ta thực hiện các thao thác sau:

- Nhấp chuột phải vào tên thư mục **Web Sites** chọn **New**, chọn **Web Site (from file)…** sau đó hộp thoại **Import configuration** xuất hiện (tham khảo Hình 3.36)



Hình 3.36: Phục hồi thông tin cấu hình.

- Chỉ định tập tin cấu hình từ nút Browse… sau đó nhấp chuột vào nút **Read File**, tập tin chỉ định được **Import** vào hộp thoại **Select a configuration to import**, cuối cùng chọn nút **OK** để hoàn tất quá trình (tham khảo Hình 3.37).



Hình 3.37: Phục hồi cấu hình cho Web Site.

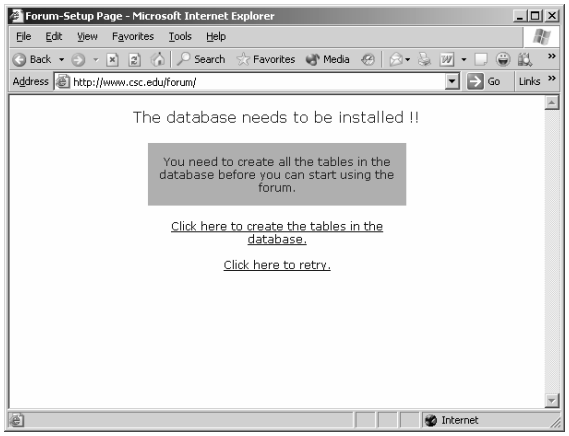
IV.2.10 Cấu hình Forum cho Web Site.

Trong phần này ta cấu hình một **Web** diễn đàn thảo luận **Snitz™ Forums 2000** được viết bằng ngôn ngữ **ASP** của nhóm tác giả "**Michael Anderson**, **Pierre Gorissen**, **Huw Reddick** and **Richard Kinser**", thông qua việc triển khai **forum** này giúp chúng ta phần nào hiểu được bản chất cơ bản của cơ chế cấu hình **Web** động (hỗ trợ kết nối cơ sở dữ liệu **MS Access**, **MS SQL Server**, **MySQL**) viết bằng ngôn ngữ **ASP**, **ASP.NET**, **PHP**,…Ta có thể **download forum** này từ URL: http://forum.snitz.com/.

Một số bước cơ bản để cấu hình **forum**:

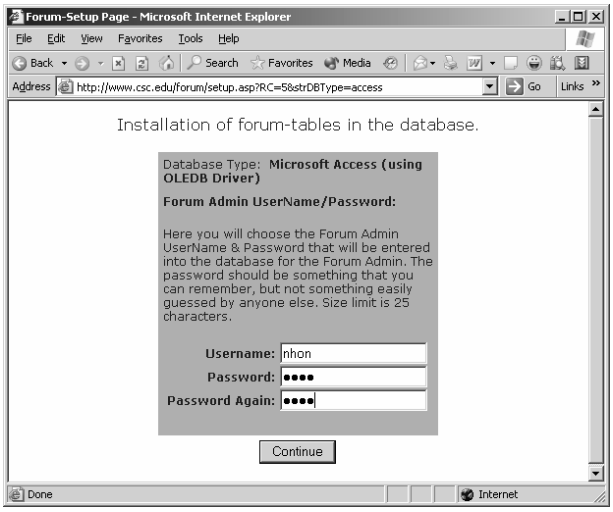
- Sau khi ta **download** tập tin **sf2k_v34_051.zip** (đối với phiên bản V3.4.051) hoàn tất ta giải nén và lưu trữ nội dung trong thư mục nào đó (Ví dụ C:\Inetpub\forum).
- Sau đó ta mở tập tin **config.asp** (dùng tiện ích **notepad**) để thay đổi một số thông tin cấu hình kết nối đến tập tin lưu trữ cơ sở dữ liệu **MS Access** có tên **snitz_forums_2000.mdb**
- strDBType = "access"
- strConnString="Provider=Microsoft.Jet.OLEDB.4.0;
- DataSource=" & Server.MapPath("snitz_forums_2000.mdb")
- Nếu thư mục lưu trữ nội dung của **forum** không phải là thư mục con của **WebRoot** thì ta phải tạo một **Virtual Directory** có tên **forum** để ánh xạ thư mục ổ đĩa (C:\Inetpub\forum) thành **URL Path** cho **Web Site**.

- Nhấp chuột phải vào **Virtual Directory** có tên **forum** chọn **Permissions** để cấp quyền cho mọi người được quyền **NTFS** là **Full** trên thư mục này.
- Sau đó ta vào **Internet Explorer** để truy xuất vào **forum** và cấu hình thêm một số thông tin mới (tham khảo Hình 3.38)



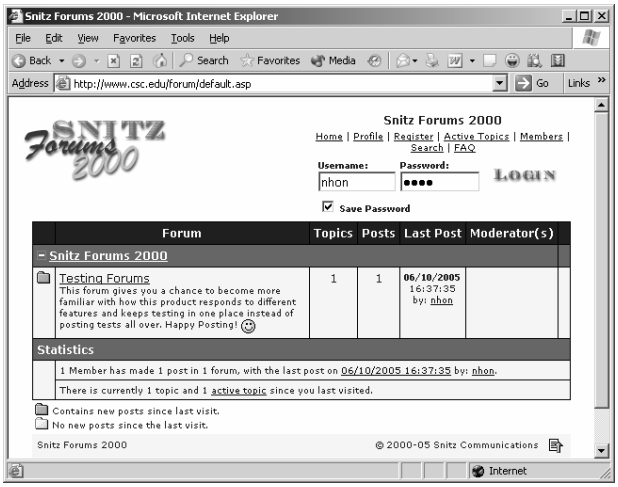
Hình 3.38: Tạo **table** cho **database**.

- Tạo **Admin Account** cho **forum**.



Hình 3.39: Tạo **Admin account** cho **forum**.

- Đăng nhập bằng **user** quản trị và tổ chức **forum**.



Hình 3.40: Đăng nhập **forum**.

Tóm tắt

Lý thuyết 8 tiết - Thực hành 16 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này giúp cho học viên có thể tổ chức, cài đặt, quản trị một hệ thống Mail Server phục vụ việc trao đổi thư điện tử trong hệ thống mạng nội bộ và mạng Internet.	I. Các giao thức được sử dụng trong hệ thống Mail. II. Giới thiệu về hệ thống mail. III. Một số khái niệm. IV. Mối liên hệ giữa DNS và Mail Server. V. Giới thiệu các chương trình Mail Server. VI. Cài đặt Exchange 2003 Server. VII. Cấu hình Microsoft Exchange 2003. VIII. Một số tiện ích cần thiết của Exchange Server.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

I. Các giao thức được sử dụng trong hệ thống Mail.

Hệ thống Mail được xây dựng dựa trên một số giao thức sau: **Simple Mail Transfer Protocol** (**SMTP**), **Post Office Protocol** (**POP**), **Multipurpose Internet Mail Extensions** (**MIME**) và **Interactive Mail Access Protocol** (**IMAP**) được định trong **RFC 1176** là một giao thức quan trọng được thiết kế để thay thế **POP**, nó cung cấp nhiều cơ chế tìm kiếm văn bản, phân tích **message** từ xa mà ta không tìm thấy trong **POP**..

I.1. SMTP(Simple Mail Transfer Protocol).

SMTP là giao thức tin cậy chịu trách nhiệm phân phát Mail, nó chuyển Mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển Mail trong hệ thống mạng nội bộ. Giao thức **SMTP** được định nghĩa trong **RFC 821**, **SMTP** là một dịch vụ tin cậy, hướng kết nối(**connection-oriented**) được cung cấp bởi giao thức **TCP**(**Transmission Control Protocol**), nó sử dụng số hiệu cổng (**well-known port**) 25. Sau đây là danh sách các tập lệnh trong giao thức **SMTP**.

Lệnh	Cú pháp	chức năng
Hello	HELO <sending-host>	Lệnh nhận diện SMTP.
From	MAIL FROM:<from-address>	Địa chỉ người gởi.
Recipient	RCPT TO:<to-address>	Địa chỉ người nhận.
Data	DATA	Bắt đầu gởi thông điệp.
Reset	RSET	Huỷ bỏ thông điệp.
Verify	VRFY <string>	Kiểm tra **username**.
Expand	EXPN <string>	Mở rộng danh sách Mail.
Help	HELP [string]	Yêu cầu giúp đỡ.
Quit	QUIT	Kết thúc phiên giao dịch **SMTP**.

Để sử dụng các lệnh **SMTP** ta dùng lệnh telnet theo port 25 trên hệ thống ở xa sau đó gởi Mail thông qua cơ chế dòng lệnh. Kỹ thuật này thỉnh thoảng cũng được sử dụng để kiểm tra hệ thống **SMTP Server**, nhưng điều chính yếu ở đây là chúng ta sử dụng **SMTP** để minh hoạ làm cách nào Mail được gởi qua các hệ thống khác nhau. Trong ví dụ sau minh hoạ quá trình gởi Mail thông qua cơ chế dòng lệnh **SMTP**.

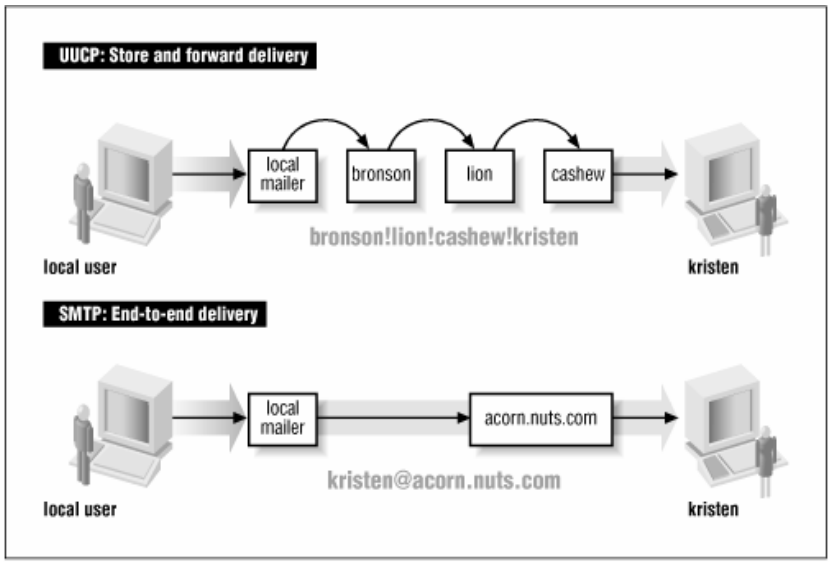
Hình 4.1: SMTP Session

Ngoài ra còn có một số lệnh khác như: **SEND**, **SOML**, **SAML**, và **TURN** được định trong **RFC 821** là những câu lệnh tuỳ chọn và không được sử dụng thường xuyên.

Lệnh **HELP** in ra tóm tắt các lệnh được thực thi. Ví dụ ta dùng lệnh **HELP RSET** chỉ định các thông tin được yêu cầu khi sử dụng lệnh **RSET**, Lệnh **VRFY** và **EXPN** thì hữu dụng hơn nhưng nó thường bị khoá vì lý do an ninh mạng bởi vì nó cung cấp cho người dùng chiếm dụng băng thông mạng. Ví dụ lênh **EXPN** <**admin**> yêu cầu liệt kê ra danh sách địa chỉ email nằm trong nhóm **Mail Admin**. Lệnh **VRFY** để lấy các thông tin cá nhân của một tài khoản nào đó, ví dụ lệnh **VRFY** <mac>, mac là một tài khoản cục bộ. Trường hợp ta dùng lệnh **VRFY** <**jane**>, **jane** là một bí danh nằm trong tập tin **aliases** thì giá trị trả về là địa chỉ Email được tìm thấy trong tập tin **aliases** này.

SMTP là hệ thống phân phát mail trực tiếp từ đầu đến cuối(từ nơi bắt đầu phân phát cho đến trạm phân phát cuối cùng), điều này rất hiếm khi sử dụng. hầu hết hệ thống mail sử dụng giao thức store and forward như **UUCP** và X.400, hai giao thức này di chuyển Mail đi qua mỗi hop, nó lưu trữ thông điệp tại mỗi hop và sau đó chuyển tới hệ thống tiếp theo, thông điệp đươc chuyển tiếp cho tới khi nó tới hệ thống phân phát cuối cùng.

Trong hình sau minh hoạ cả hai kỹ thuật store and forward và phân phát trực tiếp tới hệ thống Mail. Địa chỉ **UUCP** chỉ định đường đi mà Mail đi qua để tới người nhận, trong khi đó địa chỉ mail **SMTP** ngụ ý là hệ thống phân phát sau cùng.



Hình 4.2: Sơ đồ phân phối thư.

Phân phát trực tiếp(**Direct delivery**) cho phép **SMTP** phân phát mail mà không dự vào host trung gian nào. Nếu như **SMTP** phân phát bị lỗi thì hệ thống cục bộ sẽ thông báo cho người gởi hay nó đưa mail vào hàng đợi mail để phân phát sau. Bất lợi của việc phân phát trực tiếp(**direct delivery**) là nó yêu cầu hai hệ thống cung cấp đầu đủ các thông tin điều khiển mail, một số hệ thống không thể điều khiển Mail như **PC**, các hệ thống **mobile** như **laptops**, những hệ thống này thường tắt máy vào cuối ngày hay thường xuyên không trực tuyến (**mail offline**). Để điều khiển những trường hợp này cần phải có hệ thống **DNS** được sử dụng để chuyển thông điệp tới máy chủ mail thay cho hệ thống phân phát mail trực tiếp. Mail sau đó được chuyển từ **Server** tới máy trạm khi máy trạm kết nối mạng trở lại, giao thức mạng **POP** cho phép thực hiện chức năng này.

I.2. Post Office Protocol.

POP là giao thức cung cấp cơ chế truy cập và lưu trữ hộp thư cho người dùng.

Có hai phiên bản của **POP** được sử dụng rộng rãi là **POP2**, **POP3**. **POP2** được định nghĩa trong **RFC 937**, **POP3** được định nghĩa trong **RFC 1725**. **POP2** sử dụng 109 và **POP3** sử dụng **Port 110**. Các câu lệnh trong hai giao thức này không giống nhau nhưng chúng cùng thực hiện chức năng cơ bản là kiểm tra tên đăng nhập và **password** của **user** và chuyển Mail của người dùng từ **Server** tới hệ thống đọc Mail cục bột của **user**.

Trong khi đó tập lệnh của **POP3** hoàn toàn khác với tập lệnh của **POP2**.

Lệnh	Chức năng
USER username	Cho biết thông tin về **username** cần nhận Mail.
PASS password	Password của username cần nhận Mail.
STAT	Hiển thị số thông điệp chưa được đọc tính bằng bytes.
RETR n	Nhận thông điệp thứ n.
DELE n	Xoá thông điệp thứ n.
LAST	Hiển thị thông tin **message** cuối cùng.
LIST [n]	Hiển thị kích thước của thông điệp thứ n.
RSET	Không xoá tất cả thông điệp, và quay lại thông điệp đầu tiên.
TOP n	In ra các **HEADER** và dòng thứ n của thông điệp.
NOOP	Không làm gì.
QUIT	Kết thúc phiên giao dịch **POP3**.

Mặc dù các câu lệnh của **POP3** và **POP2** khác nhau như chúng cùng thực hiện một chức năng, sau

đây là ví dụ về phiên giao dịch **POP3** :

Hình 4.3: **POP3 Session**.

I.3. Internet Message Access Protocol.

Là giao thức hỗ trợ việc lưu trữ và truy xuất hộp thư của người dùng, thông qua **IMAP** người dùng có thể sử dụng **IMAP Client** để truy cập hộp thư từ mạng nội bộ hoặc mạng **Internet** trên một hoặc nhiều máy khác nhau.

Một số đặc điểm chính của **IMAP**:

- Tương thích đầy đủ với chuẩn **MIME**.
- Cho phép truy cập và quản lý message từ một hay nhiều máy khác nhau.
- Hỗ trợ các chế độ truy cập "**online**", "**offline**".
- Hỗ trợ truy xuất mail đồng thời cho nhiều máy và chia sẽ **mailbox**.
- **Client** không cần quan tâm về định dạng file lưu trữ trên **Server**.

I.4. MIME.

MIME (**Multipurpose Internet Mail Extensions**) cung cấp cách thức kết hợp nhiều loại dữ liệu khác nhau vào trong một thông điệp duy nhất có thể được gởi qua Internet dùng **Email** hay **Newgroup**. Thông tin được chuyển đổi theo cách này trông giống như những khối ký tự ngẫu nhiên. Những thông điệp sử dụng chuẩn **MIME** có thể chứa hình ảnh, âm thanh và bất kỳ những loại thông tin nào khác có thể lưu trữ được trên máy tính. Hầu hết những chương trình xử lý thư điện tử sẽ tự động giải mã những thông báo này và cho phép bạn lưu trữ dữ liệu chứa trong chúng vào đĩa cứng. Nhiều chương trình giải mã **MIME** khác nhau có thể được tìm thấy trên **NET**.

I.5. X.400.

X.400 là giao thức được **ITU-T** và **ISO** định nghĩa và đã được ứng dụng rộng rải ở Châu Âu và Canada, **X.400** cung cấp tính năng điều khiển và phân phối E-mail, **X.400** sử dụng định dạng nhị phân do đó nó không cần mã hóa nội dung khi truyền dữ liệu trên mạng.

Một số đặc điểm của giống nhau giữa **X.400** và **SMTP**.

- Cả hai đều là giao thức tin cậy (cung cấp tính năng thông báo khi gởi và nhận message).
- Cung cấp nhiều tính năng bảo mật.
- Lập lịch biểu phân phối Mail.

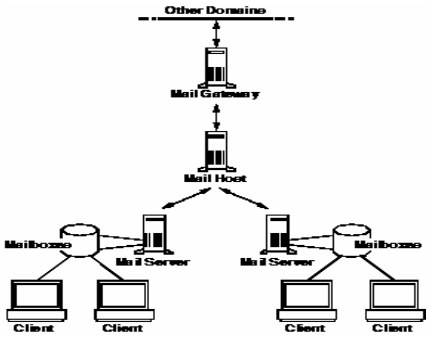
- Thiết lập độ ưu tiên cho Mail.

- **SMTP** có một số chức năng mà trên **X.400** không hỗ trợ.
- Kiểm tra địa chỉ người nhận trước khi phân phối **message** còn X.400 thì ngược lại.
- Kiểm tra kích thước của message trước khi gởi nó.
- Có khả năng chèn thêm bất kỳ loại dữ liệu nào vào **header** của **message**.
- Khả năng tương thích tốt với chuẩn **MIME**.

II. Giới thiệu về hệ thống mail.

Một hệ thống Mail yêu cầu phải có ít nhất hai thành phần, nó có thể định vị trên hai hệ thống khác nhau hoặc trên cùng một hệ thống, **Mail Server** và **Mail Client**. Ngoài ra, nó còn có những thành phần khác như **Mail Host**, **Mail Gateway**.

Sơ đồ về một hệ thống Email đầy đủa các thành phần:



Hình 4.4: Hệ thống Mail.

II.1. Mail gateway.

Một mail **gateway** là máy kết nối giữa các mạng dùng các giao thức truyền thông khác nhau hoặc kết nối các mạng khác nhau dùng chung giao thức. Ví dụ một **mail gateway** có thể kết nối một mạng **TCP/IP** với một mạng chạy bộ giao thức **Systems Network Architecture** (**SNA**).

Một mail gateway đơn giản nhất dùng để kết nối 2 mạng dùng chung giao thức hoặc mailer. Khi đó mail gateway chuyển mail giữa domain nội bộ và các domain bên ngoài.

II.2. Mail Host.

Một **mail host** là máy giữ vai trò máy chủ Mail chính trong hệ thống mạng. Nó dùng như thành phần trung gian để chuyển Mail giữa các vị trí không kết nối trực tiếp được với nhau.

Mail host phân giải địa chỉ người nhận để chuyển giữa các **Mail server** hoặc chuyển đến **Mail gateway**.

Một ví dụ về **Mail host** là máy trong mạng cục bộ **LAN** có **modem** được thiết lập liên kết **PPP** hoặc **UUCP** dùng đường dây thoại. **Mail host** cũng có thể là máy chủ đóng vai trò **router** giữa mạng nội bộ và mạng **Internet**.

II.3. Mail Server.

Mail Server chứa **mailbox** của người dùng. **Mail Server** nhận mail từ mail **Client** gửi đến và đưa vào

hàng đợi để gửi đến **Mail Host**.

Mail Server nhận mail từ **Mail Host** gửi đến và đưa vào **mailbox** của người dùng.

Người dùng sử dụng **NFS** (**Network File System**) để **mount** thư mục chứa **mailbox** trên **Mail Server** để đọc. Nếu **NFS** không được hỗ trợ thì người dùng phải **login** vào **Mail Server** để nhận thư.

Trong trường hợp **Mail Client** hỗ trợ **POP/IMAP** và trên **Mail Server** cũng hỗ trợ **POP/IMAP** thì người dùng có thể đọc thư bằng **POP/IMAP**.

II.4. Mail Client.

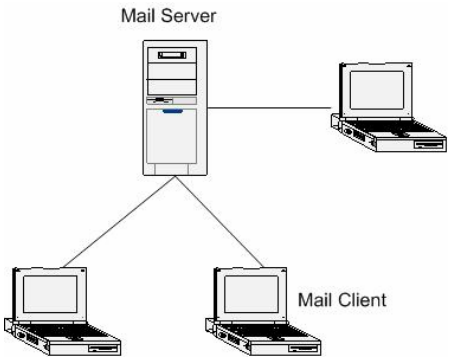
Là những chương trình hỗ trợ chức năng đọc và soạn thảo thư, **Mail Client** tích hợp hai giao thức **SMTP** và **POP**, **SMTP** hỗ trợ tính năng chuyển thư từ **Client** đến **Mail Server**, **POP** hỗ trợ nhận thư từ **Mail Server** về **Mail Client**. Ngoài giao thức việc tích hợp giao thức **POP Mail Client** còn tích hợp giao thức **IMAP**, **HTTP** để hỗ trợ chức năng nhận thư cho **Mail Client**.

Các chương trình **Mail Client** thường sử dụng như: **Microsoft Outlook Express**, **Microsoft Office Outlook**, **Eudora**,…

II.5. Một số sơ đồ hệ thống mail thường dùng.

II.5.1 Hệ thống mail cục bộ.

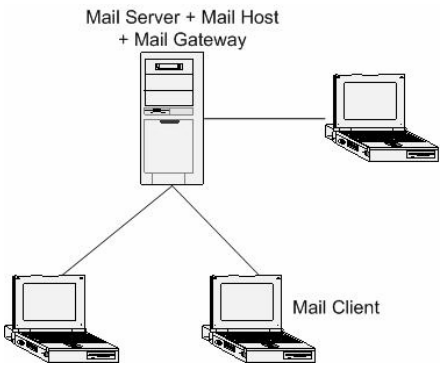
Cấu hình hệ thống Mail đơn giản gồm một hoặc nhiều trạm làm việc kết nối vào một **Mail Server**. Tất cả Mail đều chuyển cục bộ.



Hình 4.5: Hệ thống Mail cụ bộ.

II.5.2 Hệ thống mail cục bộ có kết nối ra ngoài.

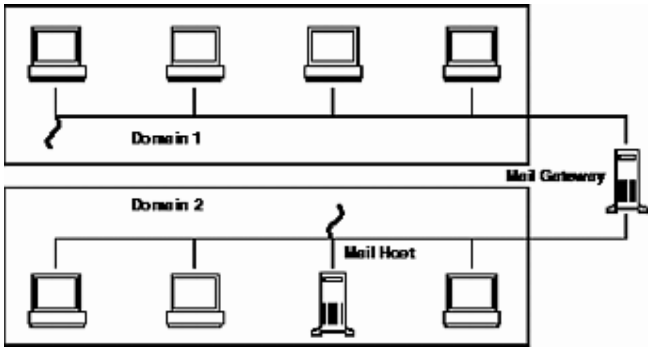
Hệ thống Mail trong một mạng nhỏ gồm một **Mail Server**, một **Mail Host** và một **Mail Gateway** kết nối với hệ thống bên ngoài. Không cần **DNS Server**.



Hình 4.6: Hệ thống Mail có kết nối ra ngoài.

II.5.3 Hệ thống hai domain và một gateway.

Cấu hình dưới đây gồm 2 **domain** và một **Mail Gateway**. Trong cấu hình này **Mail Server**, **Mail Host**, và **Mail Gateway** (hoặc **gateways**) cho mỗi **domain** hoạt động như một hệ thống độc lập. Để quản trị và phân phối Mail cho 2 **domain** thì dịch vụ **DNS** buộc phải có.



Hình 4.7: hệ thống kết nối mail thông qua **Mail gateway**.

III. Một số khái niệm.

III.1. Mail User Agent (MUA).

MUA : là những chương trình mà người sử dụng dùng để đọc, soạn thảo và gửi Mail.

III.2. Mail Transfer Agent (MTA).

MTA : là chương trình chuyển thư giữa các máy **Mail Hub**. **Exchange** là một **Mail Transfer Agent** (**MTA**) dùng giao thức **SMTP** để đóng vai trò là một **SMTP Server** làm nhiệm vụ định tuyến trong việc phân thư . Nó nhận Mail từ những **Mail User Agent** (**MUA**) và những **MTA** khác, sau đó chuyển Mail đến đó đến các **MTA** trên máy khác hay **MTA** trên máy của mình. Để nó không đóng vai trò là một trạm phân thư đến cho người dùng, ta phải dùng một chương trình khác như **POP**, **IMAP** để thực hiện việc này.

III.3. Mailbox.

Mailbox là một tập tin lưu trữ tất cả các Mail của người dùng. Trên hệ thống **Unix**, khi ta thêm một tài khoản người dùng vào hệ thống đồng thời sẽ tạo ra một **mailbox** cho người dùng đó. Thông thường, tên của **mailbox** trùng với tên đăng nhập của người dùng. Khi có Mail gửi đến cho người dùng, chương trình xử lý Mail của **Server** cục bộ sẽ phân phối Mail này vào **mailbox** tương ứng.

Khi người dùng đăng nhập vào hệ thống và sử dụng **Mail Client** để nhận Mail (hoặc **telnet** trực tiếp vào **Mail Server** để nhận), **POP Server** sẽ vào thư mục chứa **mailbox** lấy Mail từ **mailbox** chuyển cho người dùng.

Thông thường, sau khi **Client** nhận Mail, các Mail trong **mailbox** sẽ bị xóa. Tuy nhiên, người dùng cũng có thể yêu cầu giữ lại Mail trên **mailbox**, điều này thực hiện nhờ vào một tùy chọn của **Mail Client**.

III.4. Hàng đợi mail (mail queue).

Các Mail gởi đi có thể được chuyển đi ngay khi gởi hoặc cũng có thể được chuyển vào hàng đợi. Có nhiều nguyên nhân khiến một Mail bị giữ lại trong hàng đợi :

- Khi mail đó tạm thời chưa thể chuyển đi được hoặc có một số địa chỉ trong danh sách người nhận chưa thể chuyển đến được vào thời điểm hiện tại.
- Một số tùy chọn cấu hình yêu cầu lưu trữ Mail vào hàng đợi.
- Khi số lượng tiến trình phân phối bị tắt nghẽn vượt quá giới hạn quy định.

III.5. Alias mail.

Một số vấn đề phức tạp thường gặp trong quá trình phân thư là :

- Phân phối đến cho cùng một người qua nhiều địa chỉ khác nhau.
- Phân phối đến nhiều người nhưng qua cùng một địa chỉ.
- Kết nối thư với một tập tin để lưu trữ hoặc dùng cho các mục đích khác nhau.
- Lọc thư thông qua các chương trình hay các script.

Để giải quyết các vấn đề trên ta phải sử dụng **Alias**. **Alias** là sự thay thế một địa chỉ người nhận bằng một hay nhiều địa chỉ khác, địa chỉ dùng thay thế có thể là một người nhận, một danh sách người nhận, một chương trình, một tập tin hay là sự kết hợp của những loại này.

IV. Mối liên hệ giữa DNS và Mail Server.

DNS và **Mail** là 2 dịch vụ có mối quan hệ mật thiết với nhau. Dịch vụ Mail dựa vào dịch vụ **DNS** để chuyển Mail từ mạng bên trong ra bên ngoài và ngược lại. Khi chuyển Mail, **Mail Server** nhờ **DNS** để tìm **MX record** để xác định máy chủ nào cần chuyển Mail đến.

Cú pháp record MX:

```
[Domain_name]  IN  MX  0  [Mail_Host]
```


Thông qua việc khai báo trên cho ta biết tương ứng với **domain_name** được ánh xạ trực tiếp vào **Mail Host** để chỉ định máy chủ nhận và xử lý Mail cho tên miền.

Ví dụ:

t3h.com. IN MX 0 mailserver.t3h.com.

V. Giới thiệu các chương trình Mail Server.

Hiện tại có rất nhiều chương trình **Mail Server**, tương ứng với từng môi trường thì chỉ có một số chương trình được sử dụng thông dụng, ví dụ trên môi trường Windows:

- **Microsoft Exchange Server**: Là chương trình **Mail Server** rất thông dụng được **Microsoft** phát triển để cung cấp cho các doanh nghiệp tổ chức hệ thống thư điện tử **E-mail** cho người dùng.
- **Mdaemon**: Là chương trình **Mail Server** do công ty **Alt-N Technologies**, phát triển để hỗ trợ cho các doanh nghiệp tổ chức hệ thống thư tính điện tử (**E-mail**) cho người dùng.

VI. Cài đặt Exchange 2003 Server.

VI.1. Một số phiên bản chính của Exchange.

- Exchange Server 5.5
- Hoạt động trên hệ điều hành Windows NT 4 Server, Windows 2000 Server có sử dụng service pack.
- Không cần cài đặt Active Directory nhưng có thể nhân bảng dữ liệu đến Active Directory sử dụng Active Directory Connector (ADC).
- Exchange 2000 Server
- Windows 2000 Server (kèm theo Service pack 1 hoặc cao hơn)
- Có thể cài đặt trên member server hoặc domain controller.
- Exchange Server 2003
- Windows 2000 Server (yêu cầu SP3, SP4)
- Windows 2003Server
- Có thể cài đặt trên member server hoặc domain controller.

VI.2. Yêu cầu cài đặt.

Khi cài đặt **Microsoft Exchange 2003** ta cần tham khảo bảng yêu cầu về phần cứng:

Thành phần	Yêu cầu đề nghị
Bộ xử lý (CPU)	Pentium III 500 (Exchange Server 2003, Standard Edition) Pentium III 733 (Exchange Server 2003, Enterprise Edition)
Hệ điều hành (OS)	Windows 2003
Bộ nhớ (Memory)	512MB
không gian đĩa (Disk space)	200MB trên ổ đĩa hệ thống, 500MB trên ổ đĩa cài đặt Exchange.

Hệ thống tập tin (File System)	Tất cả các partition có liên qua đến Exchange phải được định dạng là NTFS.

Ngoài yêu cầu về phần cứng ta cần phải cài đặt thêm các dịch vụ hệ thống như:

- Microsoft .NET Framework.
- Microsoft ASP.NET.
- World Wide Web service.
- Simple Mail Transfer Protocol (SMTP) service.
- Network News Transfer Protocol (NNTP) service.

VI.3. Kiểm tra Active directory.

Để tăng tốc quá trình cài đặt **Exchange Server** cũng như để tránh một số lỗi không cần thiết ta cần cập nhật các thông tin về **Forest** và **Domain** trong **Active Directory** thông qua hai tiện ích **ForestPrep** và **DomainPrep**. **Active Directory** lưu trữ dữ liệu trong ba phân vùng.

- **Schema partition** (phân vùng lưu trữ loại **object** và thuộc tính của **object** được lưu trữ trong **Active Directory**)
- **Configuration partition**: Phân vùng lưu trữ thông tin cấu hình.
- **Domain partition**: Lưu trữ các đối tượng trong domain (**Domain Object**) như **Users**, **Groups**,….
- **ForestPrep** cập nhật thông tin trong **schema partitions**, **configuration partitions** của **Active Directory**.
- **DomainPrep** cập nhật thông tin trong domain partition:

Để chạy **ForestPrep** bạn phải đăng nhập vào hệ thống bằng tài khoản là thành viên của nhóm **Schema Admins** và **Enterprise**. Chạy **DomainPrep** bạn phải đăng nhập vào hệ thống bằng tài khoản là thành viên của nhóm **Domain Admins group** mới có quyền chạy **DomainPrep**.

Các bước chạy **ForestPrep**:

Từ **Run command line** ta truy cập vào thư mục **\setup\i386** trên đĩa **CDROM Exchange Server 2003** thực thi lệnh "**D:\setup\i386\setup.exe**" **/ForestPrep**.

khi hộp thoại "**Microsoft Exchange Installation Wizard**" xuất hiện ta chọn **Next** để tiếp tục.

Tham khảo một số thông tin **Licenses Agreement** và chọn "**I Agree**", chọn **Next** để tiếp tục.

Chọn **Next** để tiếp tục quá trình cho tới khi hộp thoại **Finish** xuất hiện báo hiệu hoàn tất quá trình.

Các bước chạy **DomainPrep** (tương tự như các bước của **ForestPrep** nhưng ta thay đổi tùy chọn trong bước đầu tiên là **/DomainPrep**)

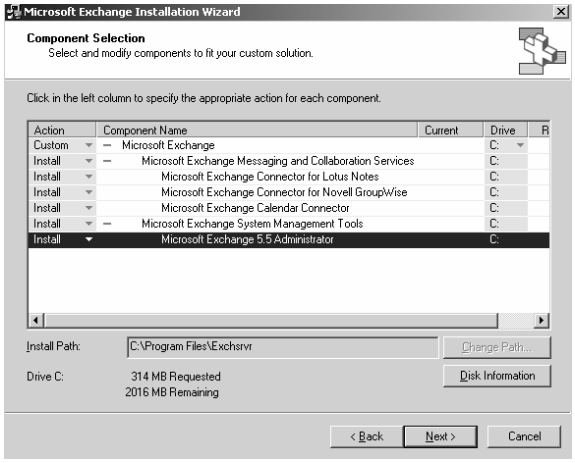
VI.4. Cài đặt Microsoft Exchange 2003 Server.

Các bước cài đặt:

Từ **Run command line** ta truy cập vào thư mục **\setup\i386** trên đĩa **CDROM Exchange Server 2003** thực thi lệnh **D:\setup\i386\setup.exe**

Chọn tùy chọn **I Agree** trong hộp thoại **Licence Agreement**, Chọn **Next**.

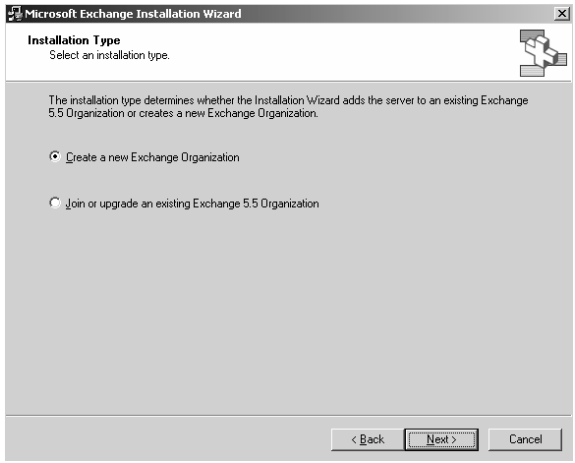
Lựa chọn các thành phần cần cài đặt trong hộp thoại **"Component Seclection"**, chọn **Next**.



Hình 4.8: Lựa chọn các thành phần cài đặt cho **Exchange**.

Chọn loại cài đặt trong hộp thoại "**Installation Type**"

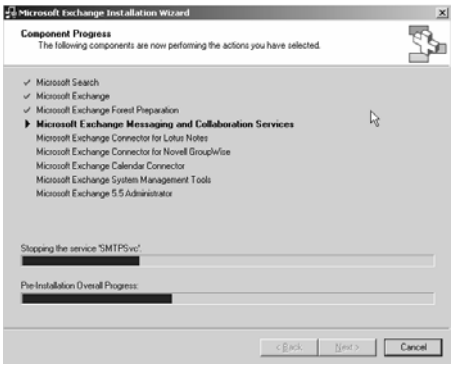
- Ta chỉ được chọn một trong hai tùy chọn sau:
- **Create a new Exchange Organization**: Tạo tổ chức (**Organization**) mới hoàn toàn.
- **Join or upgrade an existing Exchange 5.5 Organization** : khi ta muốn gia nhập vào nhóm **Exchange 5.5 Organization** hoặc khi ta muốn nâng cấp phiên bản **Exchange 5.5** thành **Exchange 2003**.



Hình 4.9: Chọn loại cài đặt.

Sau khi ta chọn "**Create a new Exchange Organization**" ở bước 4, ta phải chỉ định **Organization Name** trong hộp thoại **Organization Name**, chọn **Next** để tiếp tục.

Hộp thoại **Installation Summary** xuất hiện, tiếp tục chọn **Next** để bắt đầu tiến trình cài đặt.



Hình 4.10: Tiến trình cài đặt **Exchange**.

VII. Cấu hình Microsoft Exchange 2003.

VII.1. Khởi động các dịch vụ trong Exchange 2003.

Một số dịch vụ liên quan tới **Exchange 2003 Server**:

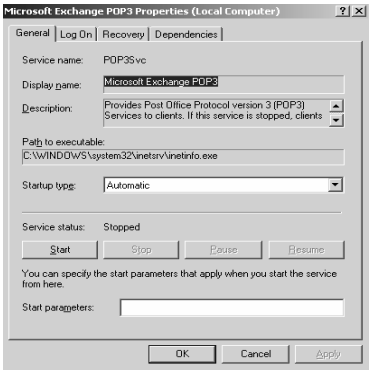
Tên dịch vụ	Ý nghĩa
Microsoft Exchange Event	Quản lý và theo dõi sự kiện cho **Exchange**.
Microsoft Exchange IMAP4	Cung cấp dịch vụ **Internet Message Access Protocol 4** (**IMAP4**) cho Client.
Microsoft Exchange Information Store	Quản lý các thông tin lưu trữ cho **Exchange** như: **Mailbox** và **Public Folder**.
Microsoft Exchange Management	Cung cấp cơ chế quản lý **Exchange** bằng cách sử dụng **Windows Management Instrumentation** (**WMI**).
Microsoft Exchange MTA Stacks	Cung cấp dịch vụ **Microsoft Exchange X.400 services** được sử dụng để kết nối với **Exchange 5.5 Server** thông qua **Connector**.
Microsoft Exchange POP3	Cung cấp dịch vụ **POP3** cho **Client** hỗ trợ nhận thư cho từng **Client**.
Microsoft Exchange Routing Engine	Cung cấp kiến trúc và thông tin định tuyến cho **Exchange 2003 Server**.
Microsoft Exchange Site Replication Service	Cho phép **Exchange 2003** có thể tương tích và đồng bộ dữ liệu với **Exchange 5.5**.

Microsoft Exchange System Attendant	Cung cấp cơ chế quan sát duy trì và tìm kiếm một số dịch vụ trong **Active Directory** (**monitoring Services**, **connectors**, **defragmenting Exchange store**, **forwarding Active Directory**, **lookups global catalog**

server).

Hoạt động của hệ thống **Exchange** phụ thuộc vào một số dịch vụ được tô đậm trong bảng trên. Các bước kích hoạt dịch vụ:

Chọn **Start | Programs | Administrative Tools | Services**, sau đó nhấp đôi vào dịch vụ cần kích hoạt, sau đó chọn **Startup type: Automatic**, chọn nút **Apply,** cuối cùng nhấp vào nút **Start** để khởi động dịch vụ.



Hình 4.11: khởi động dịch vụ **Microsoft Exchange POP3**.

VII.2. Quản lý tài khoản mail.

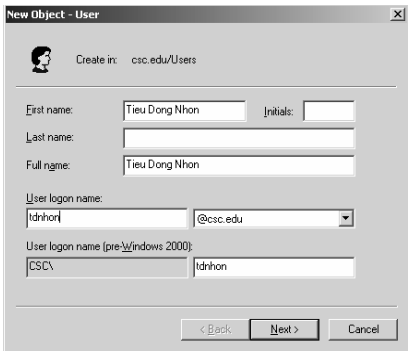
VII.2.1 Tạo tài khoản mail.

Mail Exchange sử dụng **Account** của hệ thống làm **Account Mail**, để tạo **Account Mail** ta thực hiện các bước sau:

Chọn **Start** | **Programs** | **Microsoft Exchange** | **Active Directory Users and Computers**.

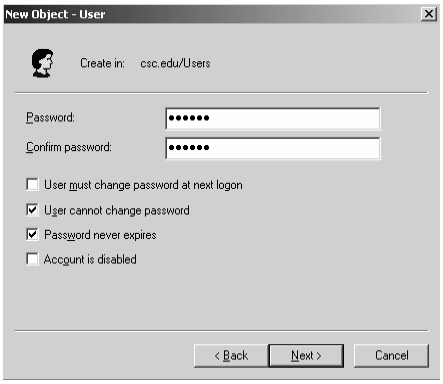
Chọn tên **Domain**, nhấp chuột phải vào đối tượng **Users**, chọn **New**, tiếp tục chọn **User**.

- Cung cấp các thông tin **First name**, **Initials**, **Last name** cho người dùng.
- Tên đăng đăng nhập của người dùng (**Users logon name**:)



Hình 4.12: Tạo người dùng.

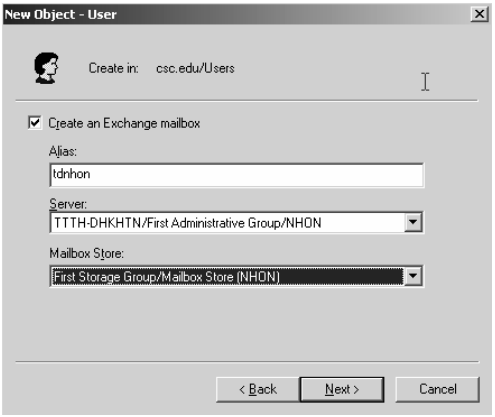
Cung cấp thông tin mật khẩu cho tài khoản.



Hình 4.13: Đặt mật khẩu cho người dùng.

Chọn **Next** để tiếp tục

- Chọn **Create an Exchange mailbox**.
- Tạo **Alias mail** cho người dùng trong **Exchange** trong **Textbox Alias:**



Hình 4.14: Tạo **mailbox** cho người dùng.

Chọn **Next** và **Finish** để hoàn tất.

VII.2.2 Truy cập thuộc tính của tài khoản mail.

Thông qua việc tìm hiểu thuộc tính của từng tài khoản Mail ta có thể di chuyển hoặc xóa **mailbox**, cấp nhận hạn ngạch **mailbox**, hiệu chỉnh một số thông tin cấu hình về một số tùy chọn mà Exchange gán cho tài khoản.

Một số **Tab** thuộc tính của tài khoản Mail:

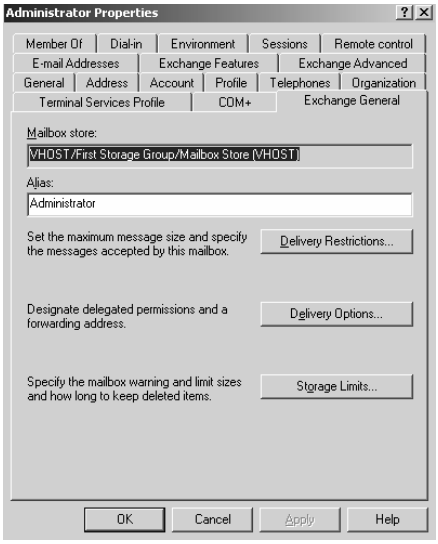
Tên Tab thuộc tính	Ý nghĩa
Exchange General	Chứa các thuộc tính **mailbox Alias**, vị trí lưu trữ **mailbox**, một số tùy chọn về giới hạn phân phối thư, giới hạn kích thước lưu trữ **mailbox**,…
Email Addresses	Chứa danh sách các địa chỉ mail của tài khoản được cung cấp bởi giao thức **SMTP** và các **connector** khác.

Exchange Features	Cung cấp một số tùy chọn để người quản trị có thể chỉ định một số

	phương thức truy cập Mail cho tài khoản như: **Outlook web access**, **POP3**, **IMAP4**, **Outlook mobie access**,….
Exchange Advanced	Hiệu chỉnh một số thuộc tính, quyền hạn về **mailbox**.

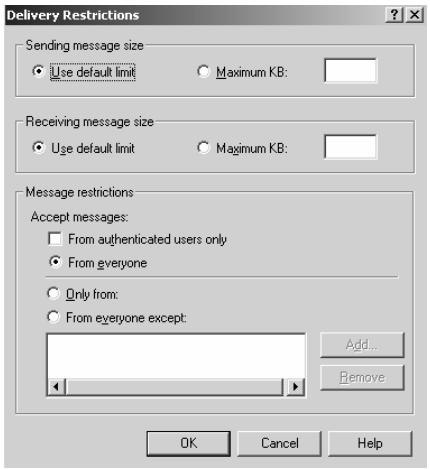
Exchange general Tab

Cho phép hiệu chỉnh thuộc tính **mailbox Alias**, trí lưu trữ **mailbox**, một số tùy chọn về giới hạn phân phối thư, giới hạn kích thước lưu trữ **mailbox**,…



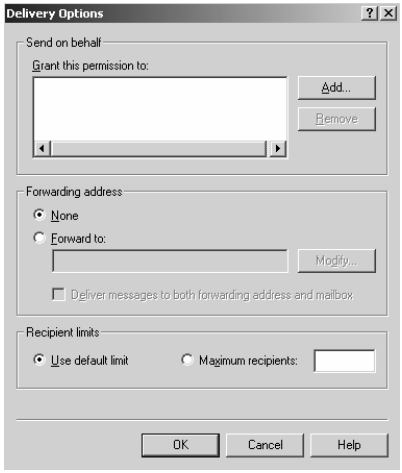
Hình 4.15: thay đổi thông tin Mail cho người dùng.

- Đặt giới hạn về phân phối thư cho người dùng bao gồm:
- Định nghĩa kích thước của thông điệp gởi(**send message size**)
- Định nghĩa kích thước của thông điệp nhận (**receiving message size**)
- Mặc định không giới hạn nhận thư cho tài khoản (**accept message size**)



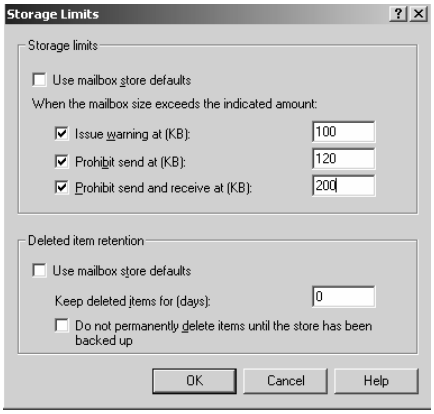
Hình 4.16: Giới hạn phân phối thư.

- Chỉ định cơ chế ủy quyền và chuyển Mail cho tài khoản.
- **Send on behalf:** chọn người dùng cần ủy quyền (nhấp chuột vào nút **Add**, chọn tên người dùng)
- **Forwarding address:** Chỉ định địa chỉ cần **forward**.
- **Recipient limits:** Chỉ định số lượng người nhận cho tài khoản.



Hình 4.17: Các tùy chọn trong phân phát thư.

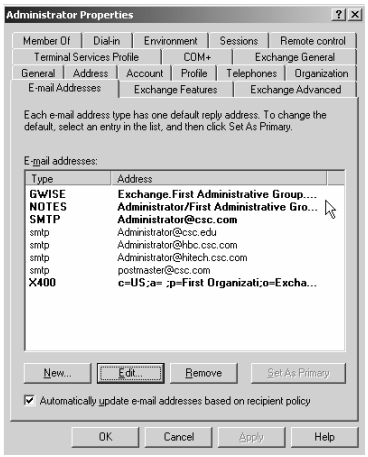
- Đặt giới hạn về kích thước của **mailbox**.
- **Storage limits**: Chỉ định một số thông tin cần thiết các thao tác cần thiết hỗ trợ giới hạn lưu trữ **mailbox** của người dùng.
- **Delete item retention**: Đặt một số tùy chọn giúp duy trì hoặc xóa **mailbox** của tài khoản.



Hình 4.18: Các tùy chọn giới hạn lưu trữ thư.

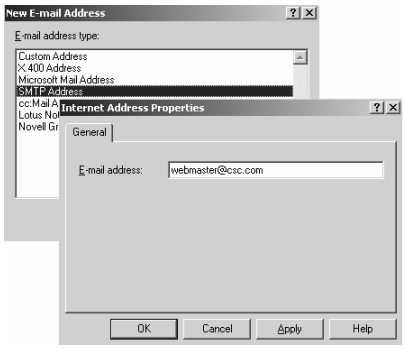
E-mail addresses Tab

Chứa danh sách các địa chỉ Mail của tài khoản được cung cấp bởi giao thức **SMTP** và các **connector** khác, thông qua tab này giúp ta có thể tạo **alias mail** cho tài khoản.



Hình 4.19: **E-mail addresses Tab**.

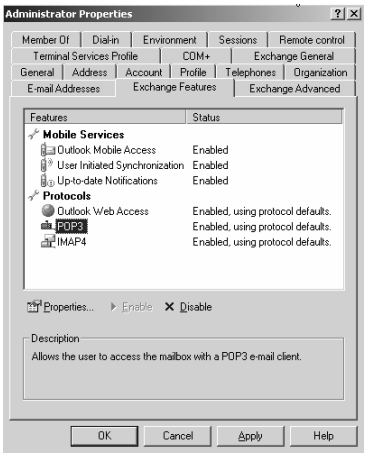
Để tạo **Alias mail** cho tài khoản ta chọn nút **New** từ **E-mail Addresses Tab**.



Hình 4.20: **E-mail addresses Tab**.

Exchange Features Tab

Cung cấp một số tùy chọn để người quản trị có thể chỉ định một số phương thức truy cập Mail cho tài khoản như: **Outlook Web Access**, **POP3**, **IMAP4**, **Outlook Mobie Access**,….(tham khảo Hình 4.20)

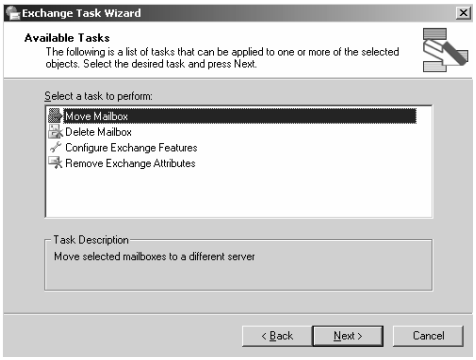


Hình 4.21: **Exchange Features Tab**.

VII.2.3 Một số tác vụ về tài khoản.

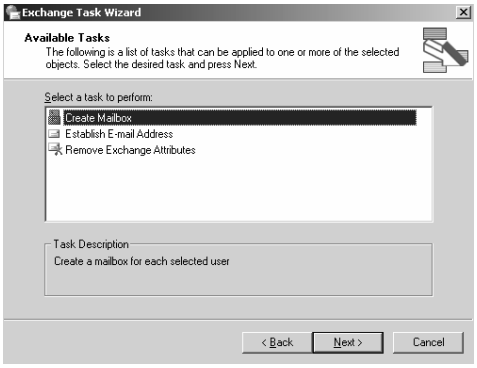
Thông qua tác vụ **Exchange Task** ta có thể xóa **mailbox**, di chuyển Mail, xóa thuộc tính Mail, cấu hình một số phương thức truy xuất Mail cho tài khoản.

Để thực thi các tác vụ về tài khoản ta nhấp chuột phải vào tên tài khoản, chọn **Exchange tasks**… xuất hiện màn hình **Welcome Exchange tasks wizard**, chọn **Next**.



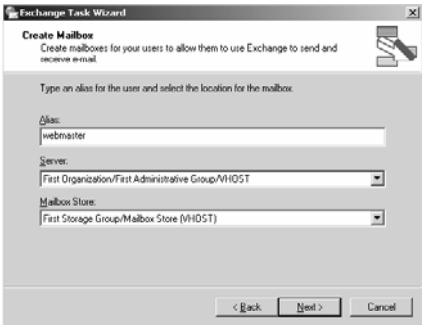
Hình 4.22: Di chuyển **mailbox**.

- Sau khi ta loại bỏ hoặc xóa địa chỉ Mail của **account** ta có thể dùng **Exchange task** để tạo Mail cho tài khoản.
- Để tạo Mail cho tài khoản ta chọn tác vụ **Create Mailbox**, chọn **Next**.



Hình 4.23: Tạo **mailbox** cho tài khoản.

- Tạo **mailbox** cho tài khoản với **mailbox alias** là **webmaster**.



Hình 4.24: Tạo **mailbox** cho tài khoản.

- Chọn **Finish** để hoàn tất quá trình.

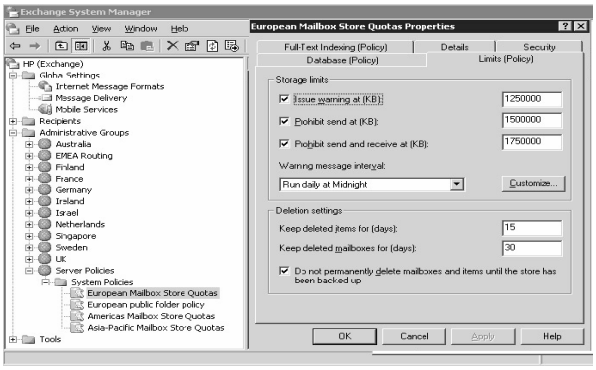
VII.3. Administrative và routing group.

VII.3.1 Administrative group.

Là một nhóm đối tượng của **Exchange** cùng chia sẻ chung một số quyền hạn nhất định nào đó. Thông qua Administrative group cung cấp quyền sử dụng **public folder**, đặt một số chính sách lưu trữ, quản lý các **mailbox server** trong cùng **site**,…

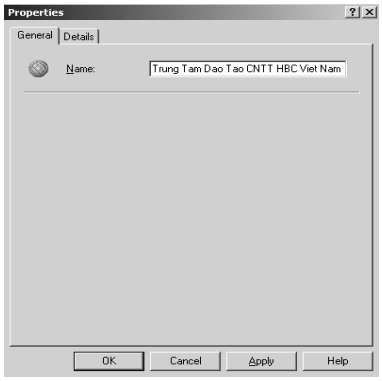
Administrative group chứa các nhóm:

- **Routing group:** Là nhóm chứa các **connector** hỗ trợ tính năng định tuyến thông điệp giữa các **Exchange server**.
- **System policy** : Chỉ định các chính sách về hộp thư (**mailbox**), thư mục dùng chung (**public folder**).
- **Public folder :** Thư mục dùng chung cho mọi người dùng.



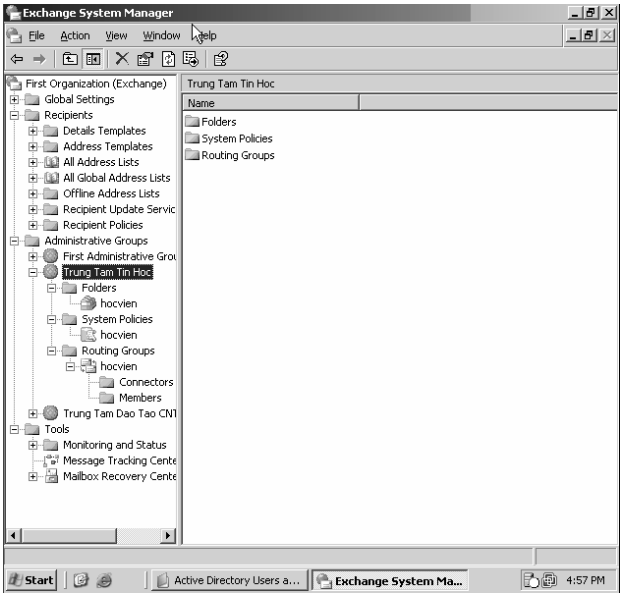
Hình 4.25: Chỉ định hạn ngạch cho **mailbox**.

Ta có thể sử dụng **Administrative group** để tạo nhóm quản lý cho công ty hoặc cơ qua có nhiều chi nhánh nhằm đơn giản hóa thao tác quản lý trong tổ chức hoặc trong **Active Directory**, để tạo **administrative group** ta nhấp chuột phải vào thư mục **Administrative Groups** chọn **New**, chọn **Administrative group**…



Hình 4.26: Tạo **Administrative group**.

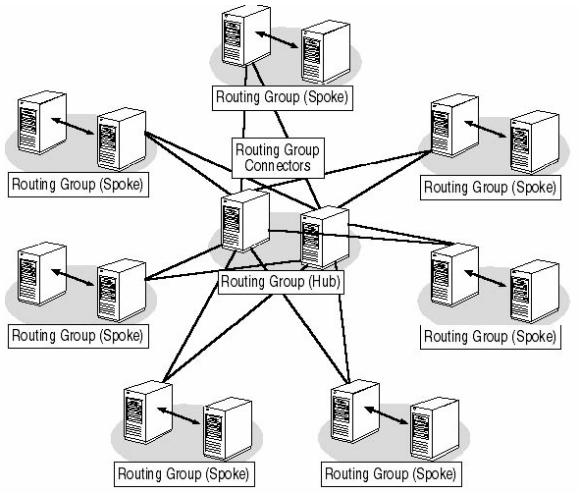
Sau khi ta tạo xong ta cần tạo các group như: **s folder**, **security group**, **routing group**, sau đó tạo các **object** cần thiết khác,….



Hình 4.27: Một số đối tượng trong **Administrative group**.

VII.3.2 Routing group.

Routing group là một nhóm các **Exchange Server** có kết nối **point to point** với nhau tạo nên một kiến trúc truyền thông điệp (**message topology**) để chỉ định phương thức chuyển thư giữa các **Exchange Server** và chuyển thư ra các tổ chức bên ngoài khi có yêu cầu.

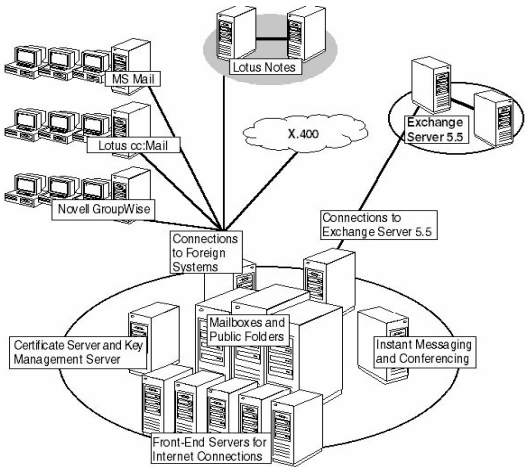


Hình 4.28: Kiến trúc của **Routing Group**.

- **Administrative group** quản lý các đối tượng (**objects**) bao gồm **server**, **routing group**, **system policy**, **public folder**.
- **Routing group** quản lý **routing topology** hỗ trợ tính năng định tuyến thông điệp đi đến **Exchange Server** khác.
- **Routing group** là thành phần con trong **administrative group** và nó luôn luôn được tạo bên trong **administrative group**.
- Trong một tổ chức, một **administrative group** có thể chưa tất cả **routing group**, các

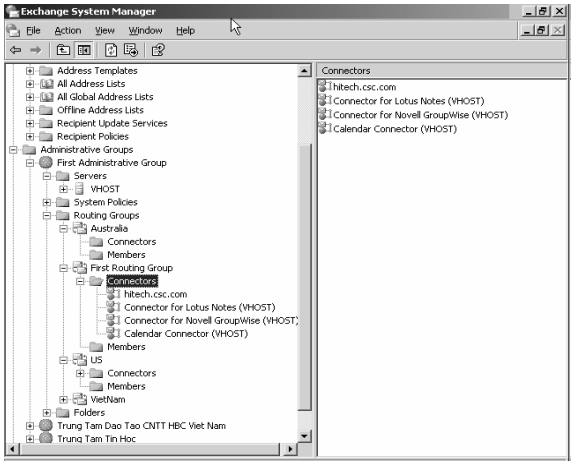
administrative group khác được sử dụng để quản lý hoạt động của **Server**.

- **Routing group** sử dụng các **connector** để kết nối các **Exchange Server** lại với nhau tạo nên một kiến trúc định tuyến thông điệp (**routing topology**), các **connector** này bao gồm: **SMTP connector**, **X.400 connector**.



Hình 4.29: Kết nối các **Mail Server** thông qua **conectors**.

- Các yếu tố cần quan tâm khi tạo **routing group**:
- Đảm bảo tính ổn định trong kết nối mạng.
- Băng thông cần thiết cho việc thiết lập kết nối **on-demain** giữa các **Server**.
- Cần để lập lịch kết nối giữa các **Server**.
- Cần để điều khiển việc truyền **message** có kích thước lớn (>=10MB).
- Cần giới hạn kết nối cho từng **user**.



Hình 4.30: **Routing group** và các **Connector**.

Các bước để tạo **connector** kết nối **point to point** tới **Exchange Server** khác.

Nhấp chuột phải vào **Connectors**, chọn **Properties**, chọn tiếp **SMTP connector** hoặc **X.400 connector**

Chỉnh định một số thông số sau:

- **Name:** Chỉ định tên **connector**.

- Tùy chọn **"Use DNS to route to each address space on this connector":** cho phép ta sử dụng **DNS** để định tuyến các Mail gởi ra ngoài thông qua **SMTP connector**.
- Tùy chọn "**Forward all mail through this connector to the following smart host"** cho phép chỉ định máy chủ **mail gateway** để phân phối thư ra ngoài cho Mail nội bộ, nếu ta chỉ định địa chỉ IP thì phải chỉ định theo cú pháp [192.168.114.201], **giá trị này sẽ override lên địa chỉ smart host được chỉ định trong Delivery tab của SMTP virtual server properties**.
- **Local bridgeheads:** Chỉ định **SMTP virtual server** từ các **routing group**.
- Tùy chọn "**Do not allow public folder referrals**" không cho chuyển **public folder** qua **connector**.

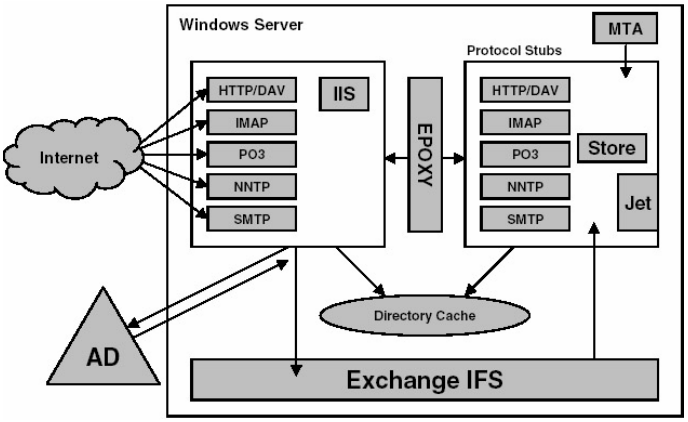
Hình 4.31: Tạo **conector** cho **routing group**.

VII.4. Microsoft Outlook Web Access.

Outlook Web Access (**OWA**) cung cấp cho người dùng sử dụng mail qua trình duyệt **Web**. **OWA** hỗ trợ **e-mail**, **calendar**, **contact management**, **server-side rules**, **spell checking**, **junk mail processing**,…

VII.4.1 Kiến trúc của OWA.

- Một số thành phần của **OWA** và các phương thức giao tiếp giữa **Browser** và **Exchange**.
- **Web Browser** gởi yêu cầu **HTTP request** hoặc **HTTPS request** đến **Server** thông qua **URL** (ví dụ: http://server/exchange).
- **HTTP request** sẽ được chuyển đến **IIS server** được chỉ định trong địa chỉ **URL**. **IIS Server** sẽ chuyển yêu cầu đến bộ xử lý **davex.dll** sẽ nhận và xử lý các **incoming request** cho **Exchange Application** được đăng ký trên **IIS**, tiếp theo **davex.dll** dịch các **request** và liên hệ với bộ lưu trữ dữ liệu (**Store**) thông qua kênh giao tiếp (**interprocess communication channel**) **epoxy** đến **HTTP epoxy stub**. Vì bộ giao tiếp trong (**interprocess communication**) sử dụng bộ nhớ chung (**share memory**) nên **epoxy** chỉ có thể hoạt động khi cả hai **IIS** và **Store processes** hoạt động trên cùng một máy. Mỗi giao thức có riêng một **epoxy stub** chạy trong **Store process**. **HTTP epoxy stub** lấy dữ liệu cần thiết từ bộ lưu trữ **Store** (**exoledb.dll**).
- **OWA** có thể sử dụng **ExIFS** nếu như nó muốn truy xuất thông tin từ file dữ liệu (**streaming file**). **ExIFS** có thể gởi dữ liệu trực tiếp đến **Browser**.
- **OWA** gởi dữ liệu theo định dạng **HTML** về cho **Web Browser** qua giao thức **HTTP**.



Hình 4.32: Kiến trúc của **OWA**.

VII.4.2 Thư mục lưu trữ và Virtual Directory của OWA.

Danh sách các thư mục của **OWA** được lưu trữ tại **Program Files\ Exchsrvr\Exchweb**

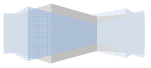
Tên thư mục	Chức năng
Exchsrvr\Bin	Chứa các tập tin thực thi bên **sever-side** và các **DLL** để định các **default** template cho **HTML form**.
Exchsrvr\Exchweb\Bin	**Exwform.dll-handles** hiệu chỉnh định dạng xử lý.
Exchsrvr\Exchweb\Controls	Lưu trữ các tập tin có định dạng .css (**cascading style sheets**), **html file**, **client Jscript libraries**. Ví dụ: **OWA** sử dụng **calendarprint.css** để xem **calendar**.
Exchsrvr\Exchweb\Img	OWA image files.
Exchsrvr\exchweb\help	Chứa các tập tin trợ giúp của **OWA**.
Exchsrvr\exchweb\views	Chứa các **XSL style sheet files** được sử dụng để xây dựng **OWA folder views**.

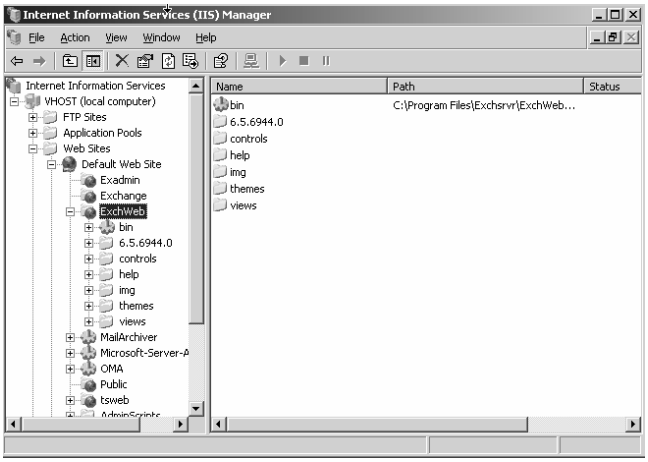
VII.4.3 Quản trị OWA.

Exchange Application tự động được thêm vào to the **IIS default Web site** hỗ trợ **OWA** để hỗ trợ **Web mail** cho người dùng (tham khảo Hình 4.29).

- Một số **Virtual Directory** của **Exchange Server**:
- **Exchange**: Là **Virtual Directory** để cho phép **Browser** truy xuất đến **mailboxe** của người dùng.
- **Exadmin**: là thư mục gốc lưu trữ các **ASP file** hỗ trợ cơ chế quản lý quá trình hoạt động của **Exchange Server**.
- **Public**: là thư mục gốc để cho phép **Browser** truy xuất tới **public folder**.
- **Exchweb**: lưu trữ đoạn mã của **Exchange application**.

- **OMA** và **Microsoft-Server-Active-Sync** hỗ trợ cho **Exchange Mobile Services**.





Hình 4.33: **Exchange Web**.

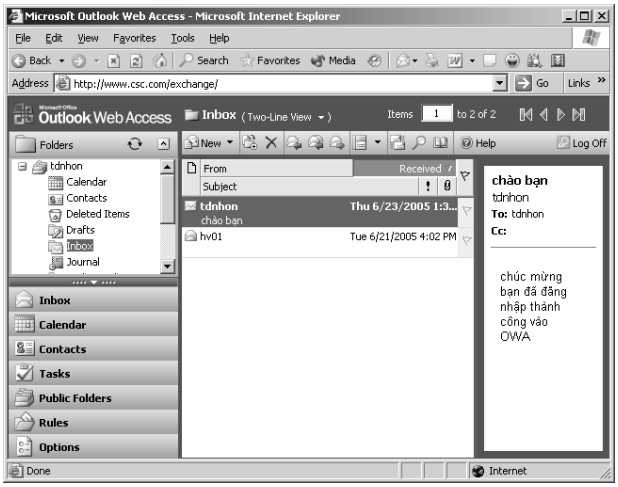
VII.4.4 Sử dụng OWA.

Để sử dụng **OWA** ta phải truy xuất vào đường dẫn **URL**: http://IIS-Server/exchange.

Nhập **Username** và mật khẩu đăng nhập cho **mailbox**.

Hình 4.34: Đăng nhập vào **OWA**.

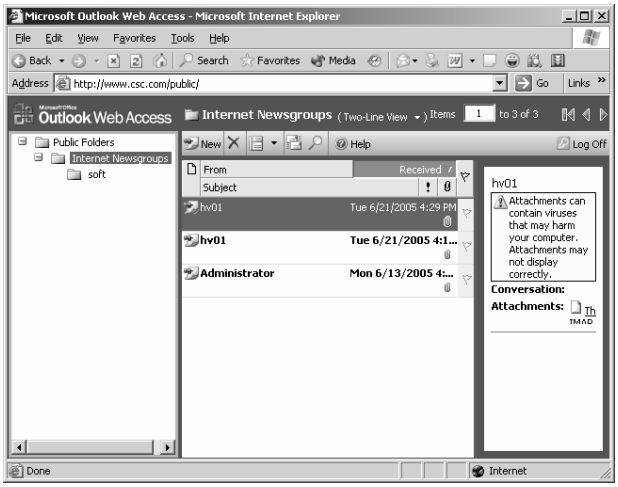
Chọn **OK** sau đó sẽ hiểu thị giao diện **Web** của **OWA**.



Hình 4.35: Giao diện sử dụng **OWA** cho **mailbox**.

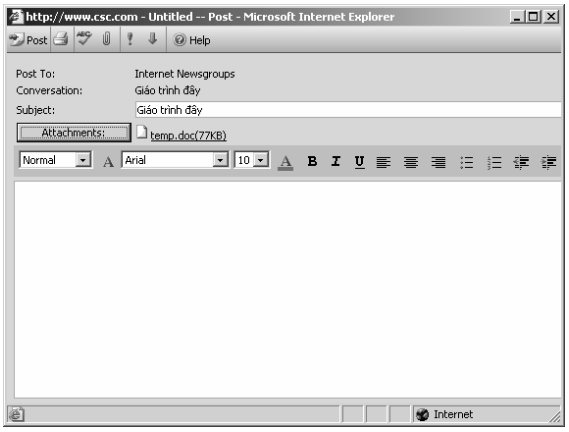
Truy cập **Public folders** của **OWA**: từ giao diện **OWA** của **mailbox** ta chọn thư mục **Public Folders**

- **Public Folders** chứa danh sách các tài nguyên dùng chung cho phép mọi người dùng có thể truy cập và sử dụng.
- Thông qua **Public Folder** này cho phép các **user** cũng có thể chia sẻ tài nguyên của mình bằng cách gởi dữ liệu qua phương thức **post**.



Hình 4.36: Truy cập **Public Folders**.

Post một **E-mail** vào **Public Folders**: Từ giao diện **Public Folders** ta chọn biểu tượng **New**, sau đó ta nhập chủ đề cần **Post**, chọn nút **Attachments** để thêm tài nguyên đính kèm, tiếp theo ta nhấp chuột vào biểu tượng **Post**.



Hình 4.37: **Post** tài nguyên vào **Public Folders**.

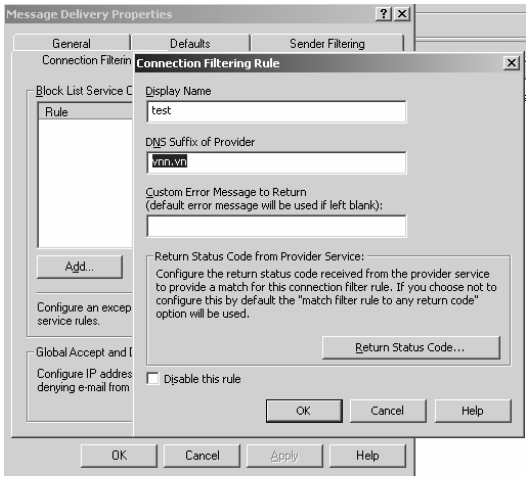
VII.5. Thiết lập một số luật phân phối message.

VII.5.1 Thiết lập bộ lọc thư.

Mục đích của việc thiết lập bộ lọc thư là giới hạn việc gởi nhận thư một số người dùng và kết nối. để thiết lập bộ lọc nhấp đôi chuột vào thư mục **Global settings**, sau đó nhấp chuột phải vào **Message Delivery**,

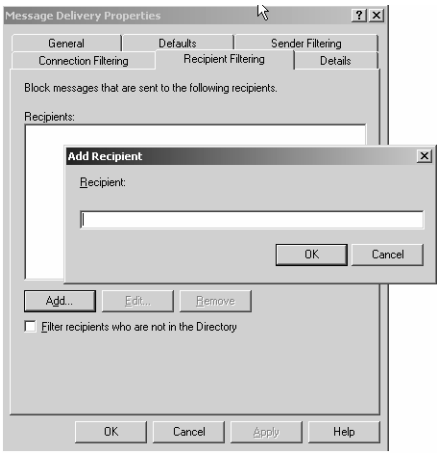
Hình 4.38: **Message delivery**.

- **Connection Filtering**:
- Ngăn một số kết nối dịch vụ dựa vào tên miền của nhà cung cấp dịch vụ (tham khảo hình 4.37).
- Cho phép hoặc cấm **host** truy xuất vào **Mail Server** thông qua tùy chọn **Global Accept and Deny List Configuration**.



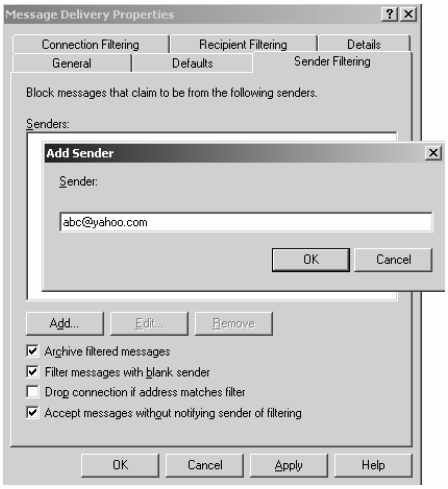
Hình 4.39: Thiết lậpluật cho **connection**.

- **Recipient Filtering**: Cấm một số người dùng gởi vào một đia chỉ nào đó được mô tả trong **textbox Recipients**(tham khảo Hình 4.38)



Hình 4.40: Giới hạn địa chỉ người nhận.

- **Sender Filtering**: Cấm một số người dùng gởi tới địa chỉ mail nào đó được mô tả trong **textbox Senders**.
- **Archive filrered messages**: Lưu trữ các **filter message**.
- **Filter messages with blank sender**: Lọc **message** mà không chứa địa chỉ người gởi.
- **Drop connection if address matches filter**: Hủy kết nối khi **message** thỏa bộ lọc.
- **Accept messages without notifying sender of filtering**: Lọc **message** mà không cần thông báo đến người gởi.

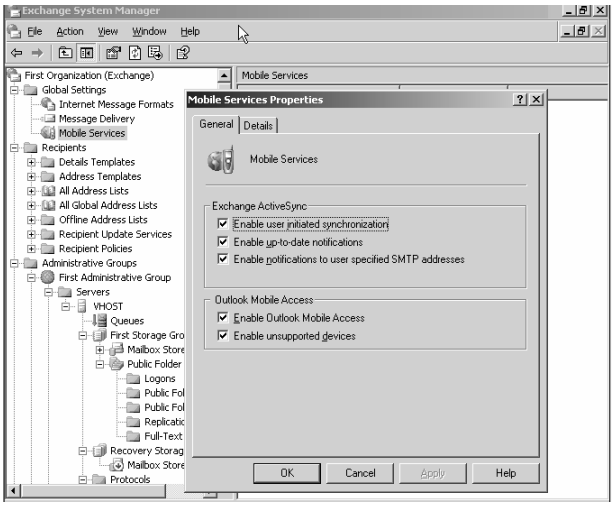


Hình 4.41: Giới hạn người gởi.

VII.5.2 Sử dụng mail thông qua điện thoại di động.

Exchange tích hợp **Mobie services** để cho phép người dùng có thể dùng phương tiện di động để **check mail** (tham khảo Hình 4.40)

- **Exchange ActiveAsync**: Cho phép một số cơ chế đồng bộ khi sử dụng thiết bị **mobie** để truy xuất **Exchange server**.
- **Outlook Mobie Access**: Cho phép thiết bị di động truy cập mail thông qua **Web** sử dụng **Outlook Mobie Access** (**OMA**), các thiết bị di động có thể truy xuất Mail thông qua địa chỉ http://mailhost/OMA.

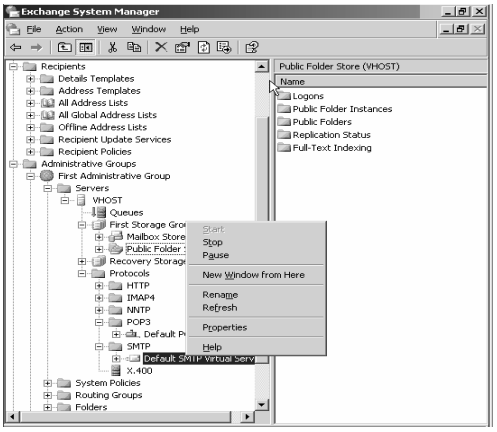


Hình 4.42: **Mobie services**.

VII.5.3 Relay mail.

Relay mail là kỹ thuật chấp nhận xử lý Mail cho một **host/subnet/domain** nào đó gởi Mail vào **SMTP Virtual Server** nội bộ, sở dĩ **SMTP Virtual Serv**er định nghĩa **relay mail** để phòng chống những **sparm mail** không cần thiết từ bên ngoài gởi đến **Mail Server** nội bộ. một số bước cấu hình **relay mail**.

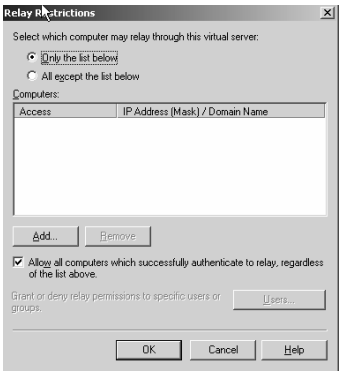
Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.



Hình 4.43: Cấu hình relay mail cho SMTP Server.

Chọn **Access Tab**, chọn tiếp nút **Relay**… xuất hiện hộp thoại **Relay Restrictions**, một số tùy chọn của hộp thoại.

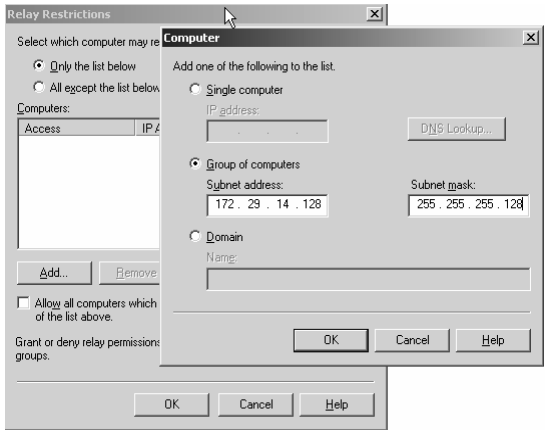
- **Only the list below:** Chỉ cho phép **relay** cho các **host**, **subnet**, **domain** được mô tả trong **textbox Computers**.
- **All accept the list below:** Cho phép **relay** cho tất cả các **host** khác ngoại trừ các **host**. **Subnet**, **domain**.



Hình 4.44: Chỉ định **relay mai**.

Ta sẽ chọn tùy chọn **"Only the list below"**, sau đó chỉ định các **host/subnet/domain** cho phép **relay**.

- **Single computer:** Relay cho host.
- **Group of computers**: Relay cho subnet.
- **Domain:** Relay cho domain.



Hình 4.45: Chỉ định **Relay** cho **subnet** nội bộ.

Chọn nút **OK** để hoàn tất quá trình

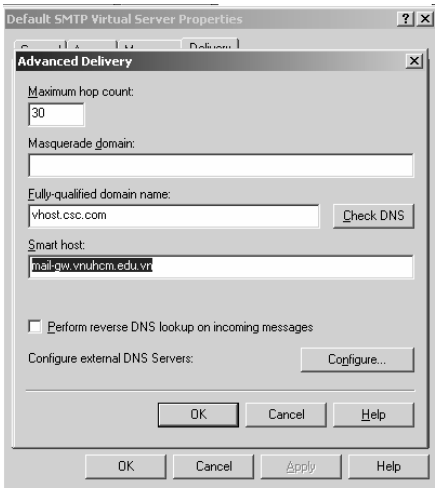
VII.5.4 Chỉ định smart host.

Khi **SMTP Server** nhận thư nó sẽ kiểm tra xem địa chỉ của người nhận là địa chỉ thuộc **domain** trong hay **domain** ngoài, nếu địa chỉ người nhận nằm ngoài **domain** nội bộ thì **SMTP** sẽ phân phối đến **smart host** hoặc chuyển thư trực tiếp đến **Mail Server** quản lý Mail của người nhận dựa vào **MX record** thông qua **DNS Server**. Ta lưu ý rằng trong **Exchange Server** có cung cấp cơ chế chuyển Mail ra ngoài qua **connectors** trong **routing group**, nếu cả hai thông tin **connector** và **smart host** được cấu hình thì **Mail Server** sẽ ưu tiên chuyển Mail đến **connector** xử lý. Đôi khi thao tác chỉ định smart host cho mail cũng có thể được gọi thao tác chỉ định **Mail Gateway**.

Các bước chỉ định **smart host**:

Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.

Chọn **Delivery Tab**, sau đó chọn nút **Advanced…** xuất hiện hộp thoại **Advanced Delivery**.



Hình 4.46: Chỉ định **smart host** cho **Mail Server**.

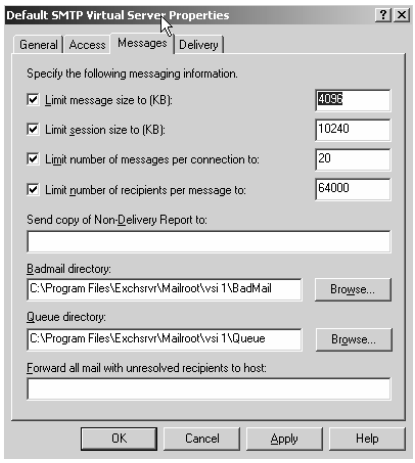
Ta chỉ định địa chỉ **Smart host** cho **Mail Server** trong **textbox smart host**, sau đó chọn nút **OK** để hoàn tất quá trình.

VII.5.5 Định kích thước của message.

Mặc định **SMTP** không giới hạn kích thước của **message** khi gởi ra ngoài, việc giới hạn kích thước của mỗi **message** giúp cho **Mail Server** không quá tải khi xử lý, cũng như quá tải trong quá trình phân phối. Để chỉ định kích thước tối đa được phép gởi ra ngoài mạng ta thực hiện các thao tác sau:

Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.

Chọn **Message Tab**, sau đó ta **Check** vào mục chọn **"Limit message size to (KB):"** để chỉ định kích thước của **message**.



Hình 4.47: Giới hạn kích thước của **sending message**.

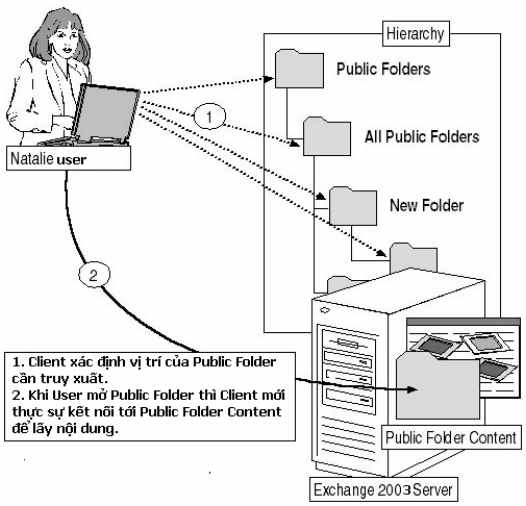
Chọn nút **OK** để hoàn tất quá trình.

VII.6. Public Folder.

Public folders là thư mục chứa các thông tin dùng chung. Thông tin này thường là các **E-mail** có chứa các **multimedia clips**, **text documents**, **spreadsheets**... Người dùng có thể sử dụng chương trình **Outlook 2000**, **Internet mail clients**, **newsreaders**, và **Web browsers**, để truy xuất **Public Folder** này.

VII.6.1 Các thành phần trong Public Folders.

Public Folder cung cấp hai thành phần chính: **Public folder hierarchy** và **public folder content** (Tham khảo hình 4.43). **Public folder hierarchy** lưu trữ các **Folder** theo dạng cây thư mục. **Public Folder Content** lưu trữ nội dung của thư mục bao gồm **messages**, **attachment**, **contact object**, **document**.



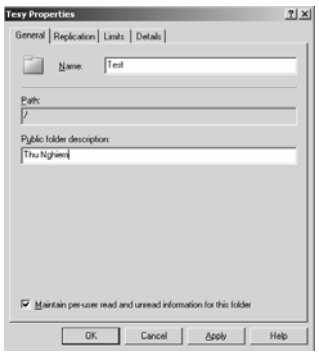
Hình 4.48: Các thành phần của **Public Folder**.

Người dùng có thể sử dụng địa chỉ **URL** http://mail_host/Public để truy xuất vào **Public Folder**, mặc định hệ thống có cung cấp sẵn thư mục **Internet Newsgroups** trong **Public Folder**. Mọi người dùng có thể gởi (Post) thông tin của mình lên **Public Folder**.

VII.6.2 Quản lý Public Folder.

Tạo mới **Public Folder** :

- Chọn **Folders** từ **Exchange System Manager**, Nhấp chuột phải vào thư mục **Public Folders** chọn **New**, chọn **Public Folder**…
- Chỉ định **Folder Name** và **Public Folder description**.



Hình 4.49: Tạo **Public Folder**.

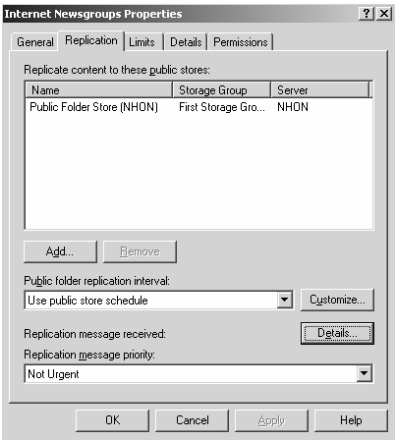
Quản lý thuộc tính của **Public Folder**

Thông qua việc quản lý thuộc tính của **Public Folder** ta có thể chỉ định giới hạn lưu trữ, đồng bộ dữ liệu (**replicate**), cung cấp quyền truy xuất cho người dùng truy xuất **Public Folder**,…Để truy xuất thuộc tính của **Public Folder** ta nhấp chuột phải vào tên thư mục chọn **Properties**.

- **General Tab**: Mô tả thông tin chung về **Public Folder**.
- **Replication Tab:** Chỉ định một số thông tin giúp **Public Folder** nhân bản dữ liệu lưu trữ trong một số **storage group**.

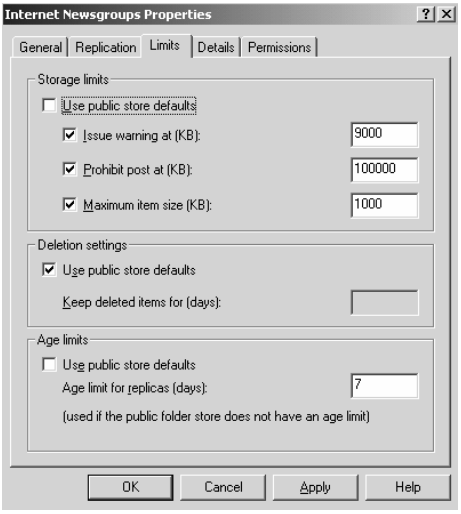
- **Replication content to these Public stores**: Chỉ định bộ lưu trữ cho **Public Folder**.

- **Public Folder Replication Interval**: Chỉ định lịch biểu nhân bản cho **Public Folder**, mặc định **Public Folder** được lưu trữ tại **First Storage Group** của Mail Server
- **Replication Message Priority:** Chỉ định độ ưu tiên cho quá trình nhân bản.



Hình 4.50: **Replication Public Folder**.

- **Limits Tab:** Chỉ định giới hạn dung lượng lưu trữ cho **Public Folder**:
- **Use public store defaults:** Định kích thước mặc định do hệ thống chỉ định.
- **Issue Warning at(KB):** Định kích thước cảnh báo.
- **Prohibit post at(KB):** không được phép **post** lên **Public Folder** khi kích thước đạt ngưỡng chỉ định,
- **Maximum item size(KB):** Kích thước của một **item** khi **post**.
- **Delete setting:** Chỉ định thời hạn xóa dung lượng trong **Public Folder**.
- **Age limit:** Chỉ định thời hạn **replication** dữ liệu trong **Public Folder**.

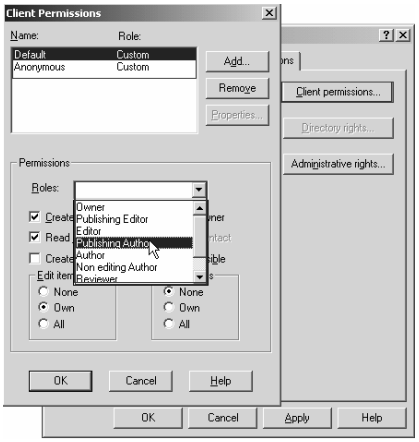


Hình 4.51: Giới hạn dung lượng lưu trữ cho **Public Folder**.

- **Details Tab:** Chỉ định một số mô tả khi cần thiết.
- **Permission Tab:** Chỉ định quyền hạn cho người dùng truy xuất vào **Public Folder** và quyền hạn

của người quản lý **Public Folder**. (Tham khảo Hình 4.47)

- **Client Permission:** Chỉ định người dùng được quyền truy xuất vào **Public Folder**, các người dùng này được chỉ định quyền hạn cụ thể trong mục chọn **Roles,** mặc định **Public Folder** cho phép mọi người truy xuất thông qua **Username** của mình hoặc thông qua **Anonymous user**.
- **Administrator Right:** Chỉ định quyền hạn của người quản lý **Public Folder.**
-



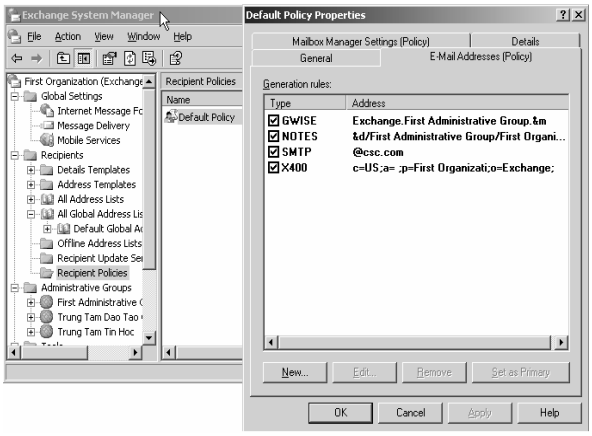
Hình 4.52: Thay đổi thuộc tính của **Public Folder**.

VII.7. Một số thao tác quản lý Exchange server.

VII.7.1 Lập chính sách nhận thư.

Recipient policies là tập hợp các chính sách và luật áp đặt trên tất cả các **mailbox** của người dùng bao gồm gởi thông báo đến người dùng khi xử lý thư, đặt các luật di chuyển và xóa thư của người dùng…

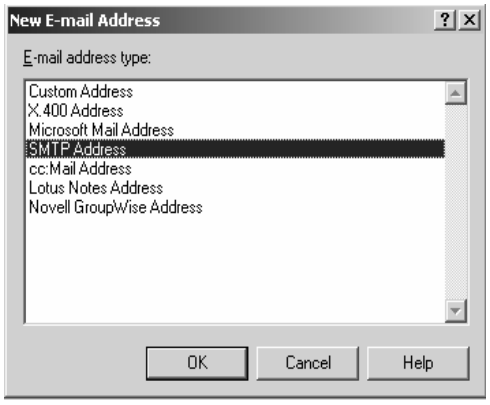
- Một số chức năng chính trong **Recipient policies**:
- Đặt một số chính sách về xử lý trên **mailbox**.
- Chỉ định tên **domain** cho phép **SMTP virtual server** nhận và xử lý thư thông qua **SMTP E-mail**.
- Để thay đổi một số chính sách nhận thư ta nhấp đôi chuột vào **default policy** trong thư mục **recipient policies** (tham khảo hình 3.30)
- Trong **E-mail Addresses** (**policy**) chứa một số luật được hệ thống tạo sẵn như dạng "**SMTP @csc.com**" để chỉ định **SMTP** chấp nhận xử lý **incoming mail** cho miền csc.com.
- Nút **New** để chỉ định các luật mới cần thêm vào **Generation rules.**



Hình 4.53: E-mail Addresses (policy) Tab.

Các bước tạo một **SMTP E-mail**:

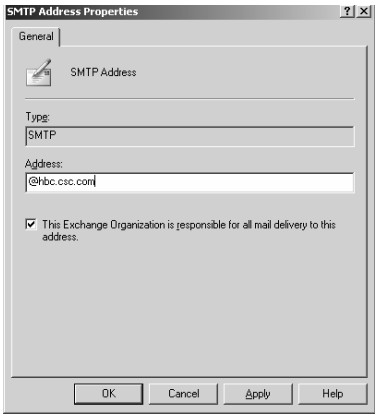
Từ Hình 4.28 ta chọn New để tạo **SMTP E-mail**.



Hình 4.54: Tạo **E-mail** cho **SMTP**.

Chọn **Ok** để tiếp tục.

- Chỉ định địa chỉ mail @domain_name để cho phép **SMTP** nhận và xử lý Mail cho **domain** này.
- Chọn nút **Apply** và chọn **OK** để hoàn tất quá trình tạo **SMTP E-mail address**.



Hình 4.55: Tạo **E-mail** cho **SMTP**.

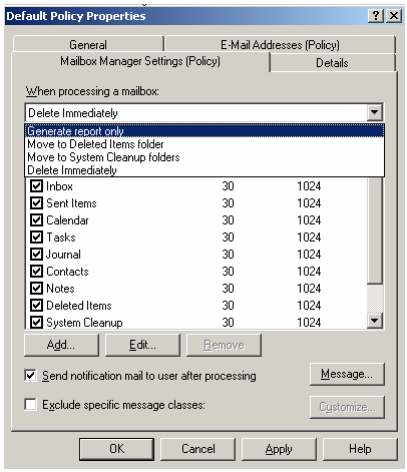
Chọn mục luật có dòng mô tả “SMTP @hbc.csc.com”.

Hình 4.56: Tạo **E-mail** cho **SMTP**.

Nhấp chuột phải vào **Default Policy** chọn **Apply this policy now…** để áp đặt luật vào hệ thống.

Thiết lập luật quản lý **mailbox**: để thiết lập luật quản lý **mailbox** ta nhấp đôi chuột vào **default policy** chọn **Mailbox manager settings (policy) Tab**

- **When processing a mailbox**: Cho phép ta chọn chế độ xử lý khi **mailbox** của người dùng khi nó đạt giới hạn lưu trữ trong thời hạn mặc định là 30 ngày, với dung lượng mặc định là 1M thì sẽ:
- **Generation report only**: Gởi thông báo cho người dùng với thông điệp được chỉ định trong nút **Message**.
- **Move to Deleted Items folder**: Tự động chuyển thư đến thư mục **Deleted**.
- **Move to System Cleanup folders**: Tự động chuyển thư đến thư mục **System Cleanup**.
- **Delete Immediately**: Xóa ngay lập tức.



Hình 4.57: Đặt luật quản lý **mailbox**.

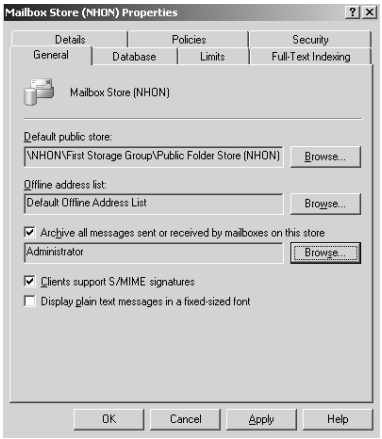
VII.7.2 Quản lý Storage group.

Storage group còn gọi là bộ lưu trữ thông tin, nó lưu trữ **mailbox** và **Public Folder** của hệ thống:

Mailbox Stores cho phép quản lý theo dõi bộ lưu trữ **mailbox** của hệ thống.

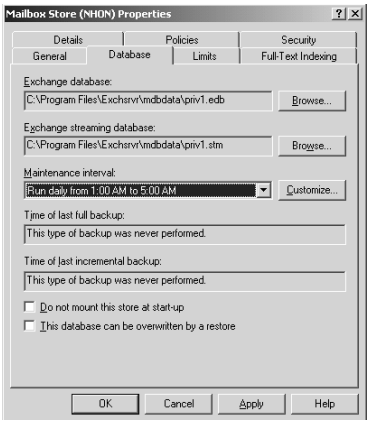
Public Folder Stores cho phép quản lý và theo dõi bộ lưu trữ **Public Folder**.

- Một số thuộc tính chính của **Mailbox Store**.
- **General Tab**.
- **Default public store:** Thư mục lưu trữ **public store**.
- **Default Offline Address list: maibox** được xem như **Offline address**.
- **Archive all message sent or received by mailbox on this store:** Chỉ định phương thức ghi nhận thư gởi ra hoặc gởi vào bằng cách chép bản sao của các thư này cho **administrator**.



Hình 4.58: **Mailbox Store**.

- **Database Tab:** Chỉ định thư mục tập tin lưu trữ **mailbox** của người dùng (tham khảo hình 4.33).

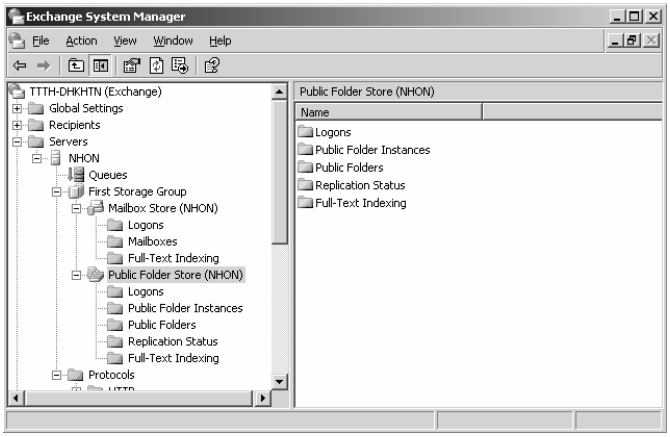


Hình 4.59: **Mailbox Database**.

- **Public Folder Stores**.

Cung cấp một số thao tác theo dõi, quản lý **public folder** của hệ thống cũng như một số dữ liệu do người dùng tạo ra, trạng thái nhân bản của **public folder**,…

- **Logons:** Hiển thị một số người dùng đang sử dụng **public folder**.
- **Public Folder Instances:** Chứa các **public folder** đang sử dụng.
- **Public Folders:** Chứa tất cả các **public folder** có sẵn trong hệ thống.
- **Replication Status:** Chứa trạng thái nhân bản của **public folder**.



Hình 4.60: **Public Folder Store**.

VIII. Một số tiện ích cần thiết của Exchange Server.

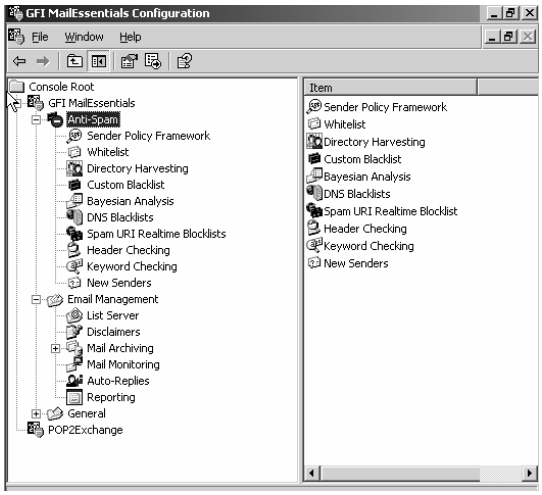
VIII.1. GFI MailEssentials.

GFI MailEssentials được tổ chức **GFI Software Ltd**. phát phát triển nhằm tích hợp thêm một số công cụ hỗ trợ công tác quản trị **Mail Server**.

- Một số đặc điểm của **GFI MailEssentials**:
- **Anti spam:** Cung cấp một số cơ chế chống **sparm mail**.
- **Company-wide disclaimer/footer text:** Được sử dụng để thêm một số thông tin chuẩn (**standard**

corporate message) cho **outgoing mail**.

- **Mail archiving to a database:** cho phép nhận tất cả các **inbound** và **outbound Internet mail** để ta có thể theo dõi hoặc **backup** tất cả các **E-mail** này.
- **Reporting:** Cho phép ta có thể thống kê hiện trạng sử dụng Mail của hệ thống
- **Personalized server-based auto replies with tracking number**: Cung cấp kỹ thuật tự động **reply message**.
- **POP3 downloader:** Một số **Mail Servers** như **Exchange Server** và **Lotus Notes**, không thể **download mail** từ **POP3 mailboxes**. **GFI MailEssentials** cung cấp tiện ích này để có thể chuyển Mail và phân phối Mail từ **POP3 mailboxes** tới **mailbox server** nội bộ.
- **Mail monitoring:** cung cấp một số cơ chế giúp theo dõi và giám sát hệ thống.

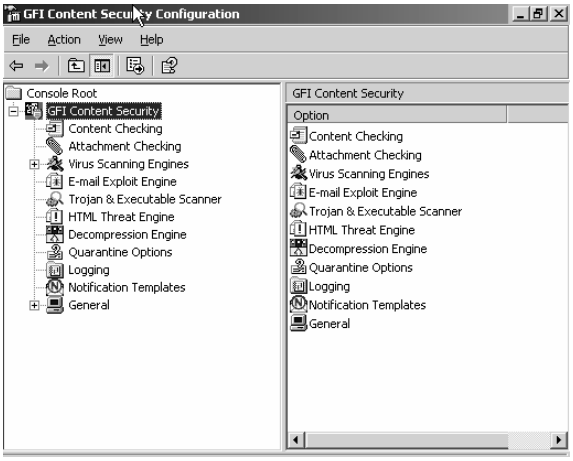


Hình 4.61: GFI MailEssentials.

VIII.2. GFI MailSecurity.

GFI MailEssentials được tổ chức **GFI Software Ltd.** phát phát triển, **GFI MailEssentials** tích hợp một số công cụ bảo mật như: **Content checking**, **Attachment Checking**, **Virus Scanning Engine**, **Trojan and Executables Scanner**,….**GFI MailSecurity** có thể được cài đặt trong hai mode: **the Exchange 2000 VS API mode** hoặc **SMTP gateway mode**. **Exchange 2000 VS API** được cài đặt và tích hợp chung với **Exchange Server 2000**. **SMTP gateway mode** thường được cài đặt trong mạng ngoại vi (**perimeter of the network**) dùng làm **mail gateway** cho các **mail host** khác.

- Một số đặc điểm chính của **GFI MailSecurity**:
- Kiểm tra và lọc nội dung thư (**Email Content checking/filtering**)
- Cung cấp bộ phân tích nội dung thư (**Email exploit detection engine**)
- Tự động loại bỏ các **HTML Scripts** (**Automatic removal of HTML scripts**)
- Tự động cô lập các **virus macros** trong các tài liệu về **Microsoft Word**.
- Cung cấp nhiều cơ chế **scanning virus** cho hệ thống (**Virus checking using multiple virus engines**)
- Trojan **Executable scanner**.



Hình 4.62: **GFI MailSecurity**.

Tóm tắt

Lý thuyết 8 tiết - Thực hành 16 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này giúp cho học viên có thể tổ chức và triển khai một Proxy Server phục vụ chia sẻ và quản lý kết nối Internet của các máy trạm, đồng thời học viên cũng có thể xây dựng một hệ thống Firewall để bảo vệ hệ thống mạng cục bộ của mình.	I. Firewall II. Giới thiệu ISA 2004 III. Đặt điểm của ISA 2004. IV. Cài đặt ISA 2004. V. Cấu hình ISA Server	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

I. Firewall.

Internet là một hệ thống mở, đó là điểm mạnh và cũng là điểm yếu của nó. Chính điểm yếu này làm giảm khả năng bảo mật thông tin nội bộ của hệ thống. Nếu chỉ là mạng **LAN** thì không có vấn đề gì, nhưng khi đã kết nối **Internet** thì phát sinh những vấn đề hết sức quan trọng trong việc quản lý các tài nguyên quý giá - nguồn thông tin - như chế độ bảo vệ chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng các nguồn thông tin mà họ được cấp quyền, và phương pháp chống rò rỉ thông tin trên các mạng truyền dữ liệu công cộng (**Public Data Communication Network**).

I.1. Giới thiệu về Firewall.

Thuật ngữ **firewall** có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, **firewall** là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép, bảo vệ các nguồn tài nguyên cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cụ thể hơn, có thể hiểu **firewall** là một cơ chế bảo vệ giữa mạng tin tưởng (**trusted network**), ví dụ mạng **intranet** nội bộ, với các mạng không tin tưởng mà thông thường là **Internet**. Về mặt vật lý, firewall bao gồm một hoặc nhiều hệ thống máy chủ kết nối với bộ định tuyến (**Router**) hoặc có chức năng **Router**. Về mặt chức năng, **firewall** có nhiệm vụ:

- Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại đều phải thực hiện thông qua **firewall**.
- Chỉ có những trao đổi được cho phép bởi hệ thống mạng nội bộ (**trusted network**) mới được quyền lưu thông qua **firewall**.
- Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ bao gồm :

Quản lý xác thực (**Authentication**): có chức năng ngăn cản truy cập trái phép vào hệ thống mạng nội bộ. Mỗi người sử dụng muốn truy cập hợp lệ phải có một tài khoản (**account**) bao gồm một tên người dùng (**username**) và mật khẩu (**password**).

Quản lý cấp quyền (**Authorization**): cho phép xác định quyền sử dụng tài nguyên cũng như các nguồn thông tin trên mạng theo từng người, từng nhóm người sử dụng.

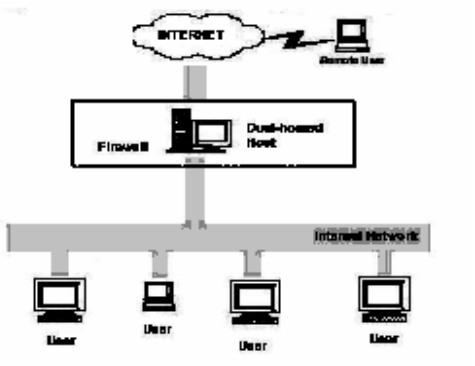
Quản lý kiểm toán (**Accounting Management**): cho phép ghi nhận tất cả các sự kiện xảy ra liên quan đến việc truy cập và sử dụng nguồn tài nguyên trên mạng theo từng thời điểm (ngày/giờ) và thời gian truy cập đối với vùng tài nguyên nào đã được sử dụng hoặc thay đổi bổ sung …

I.2. Kiến Trúc Của Firewall.

I.2.1 Kiến trúc Dual-homed host.

Firewall kiến trúc kiểu ***Dual-homed host*** được xây dựng dựa trên máy tính **dual-homed host**. Một máy tính được gọi là **dual-homed host** nếu nó có ít nhất hai **network interfaces**, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là **Router** mềm. Kiến trúc **dual-homed host** rất đơn giản. **Dual-homed host** ở giữa, một bên được kết nối với **Internet** và bên còn lại nối với mạng nội bộ (**LAN**).

Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (**proxy**) chúng hoặc cho phép **users** đăng nhập trực tiếp vào **dual-homed host**. Mọi giao tiếp từ một **host** trong mạng nội bộ và **host** bên ngoài đều bị cấm, **dual-homed host** là nơi giao tiếp duy nhất.



Hình 5.1: Kiến trúc **Dual-Home Host**.

I.2.2 Kiến trúc Screened Host.

Screened Host có cấu trúc ngược lại với cấu trúc **Dual-homed host**. Kiến trúc này cung cấp các dịch vụ từ một **host** bên trong mạng nội bộ, dùng một **Router** tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp ***Packet Filtering***.

Bastion host được đặt bên trong mạng nội bộ. **Packet Filtering** được cài trên **Router**. Theo cách này, **Bastion host** là hệ thống duy nhất trong mạng nội bộ mà những **host** trên **Internet** có thể kết nối tới. Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong **Bastion host**) mới được cho phép kết nối. Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới host này. Vì thế **Bastion host** là host cần phải được duy trì ở chế độ bảo mật cao.

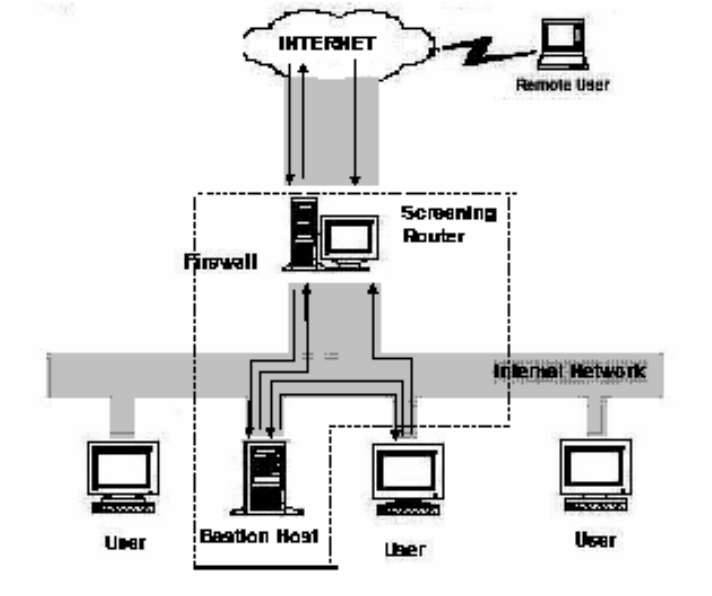
Packet filtering cũng cho phép **bastion host** có thể mở kết nối ra bên ngoài. Cấu hình của **packet filtering** trên **screening router** như sau:

- Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ cố định.
- Không cho phép tất cả các kết nối từ các **host** bên trong (cấm những **host** này sử dụng dịch **proxy** thông qua **bastion host**).
- Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau.
- Một số dịch vụ được phép đi vào trực tiếp qua **packet filtering**.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua **proxy**.

Bởi vì kiến trúc này cho phép các **packet** đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc **Dual-homed host**, vì thế nó được thiết kế để không một **packet** nào có thể tới được mạng bên trong. Tuy nhiên trên thực tế thì kiến trúc **dual-homed host** đôi khi cũng có lỗi mà cho phép các **packet** thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này. Hơn nữa, kiến trúc **dual-homed host** thì dễ dàng bảo vệ **Router** (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các **host** bên trong mạng.

Xét về toàn diện thì kiến trúc ***Screened host*** cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc ***Dual-homed host***.

So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc ***Screened subnet*** thì kiến trúc **Screened host** có một số bất lợi. Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập ***Bastion Host*** thì không có cách nào để ngăn tách giữa ***Bastion Host*** và các **host** còn lại bên trong mạng nội bộ. **Router** cũng có một số điểm yếu là nếu **Router** bị tổn thương, toàn bộ mạng sẽ bị tấn công. Vì lý do này mà **Sceened *subnet*** trở thành kiến trúc phổ biến nhất.



Hình 5.2: Mô hình Screened host.

I.2.3 Sreened Subnet.

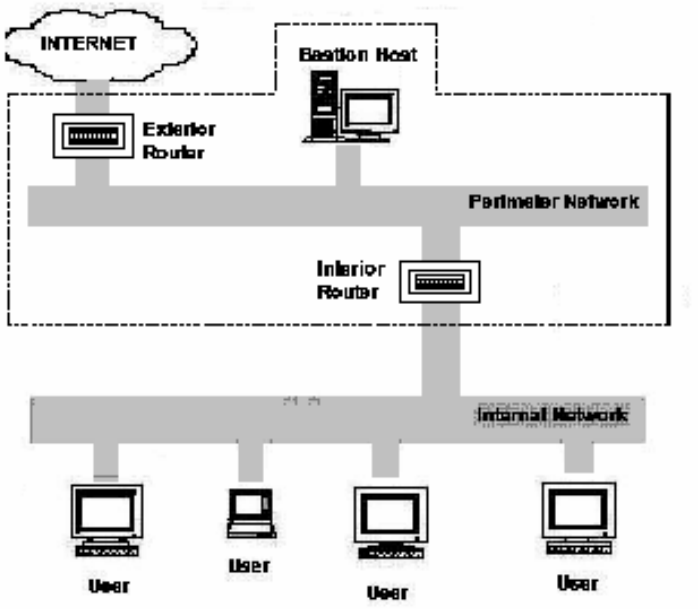
Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn *cho **bastion host***, tách **bastion host** khỏi các **host** khác, phần nào tránh lây lan một khi **bastion host** bị tổn thương, người ta đưa ra kiến trúc **firewall** có tên là **Sreened Subnet**.

Kiến trúc **Screened *subnet*** dẫn xuất từ kiến trúc **screened host** bằng cách thêm vào phần an toàn: mạng ngoại vi (**perimeter network**) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách **bastion host** ra khỏi các host thông thường khác. Kiểu **screened subnet** đơn giản bao gồm hai **screened router**:

Router ngoài (**External router** còn gọi là **access router**): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (**bastion host**, **interior router**). Nó cho phép hầu hết những gì **outbound** từ mạng ngoại vi. Một số qui tắc **packet filtering** đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ **bastion host** và **interior router** vì **bastion host** còn là **host** được cài đặt an toàn ở mức cao. Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai **Router**.

Interior Router (còn gọi là **choke router**): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc **packet filtering** của toàn bộ **firewall**. Các dịch vụ mà **interior router** cho phép giữa **bastion host** và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau. Giới hạn dịch vụ giữa **bastion host** và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi **bastion host** bị tổn thương và thoả hiệp với bên ngoài. Chẳng hạn nên giới hạn các dịch vụ được phép giữa **bastion host** và mạng nội bộ như **SMTP** khi có **Email** từ bên ngoài vào, có lẽ chỉ giới hạn

kết nối **SMTP** giữa **bastion host** và **Email Server** bên trong.



Hình 5.3: Mô hình Screened Subnet.

I.3. Các loại firewall và cách hoạt động.

I.3.1 Packet filtering (Bộ lọc gói tin).

Loại **firewall** này thực hiện việc kiểm tra số nhận dạng địa chỉ của các **packet** để từ đó cấp phép cho chúng lưu thông hay ngăn chặn . Các thông số có thể lọc được của một **packet** như:

- Địa chỉ IP nơi xuất phát (**source IP address**).
- Địa chỉ IP nơi nhận (**destination IP address**).
- Cổng TCP nơi xuất phát (**source TCP port**).
- Cổng TCP nơi nhận (**destination TCP port**).

Loại **Firewall** này cho phép kiểm soát được kết nối vào máy chủ, khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, nó còn kiểm soát hiệu suất sử dụng những dịch vụ đang hoạt động trên hệ thống mạng nội bộ thông qua các cổng **TCP** tương ứng.

I.3.2 Application gateway.

Đây là loại **firewall** được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ dựa trên những giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên mô hình **Proxy Service**. Trong mô hình này phải tồn tại một hay nhiều máy tính đóng vai trò **Proxy Server**. Một ứng dụng trong mạng nội bộ yêu cầu một đối tượng nào đó trên Internet, **Proxy Server** sẽ nhận yêu cầu này và chuyển đến **Server** trên **Internet**. Khi **Server** trên **Internet** trả lời, **Proxy Server** sẽ nhận và chuyển ngược lại cho ứng dụng đã gửi yêu cầu. Cơ chế lọc của **packet filtering** kết hợp với cơ chế "đại diện" của **application gateway** cung cấp một khả năng an toàn và uyển chuyển hơn, đặc biệt khi kiểm soát các truy cập từ bên ngoài.

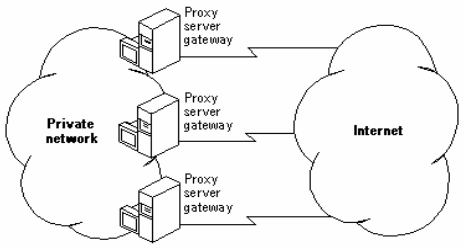
Ví dụ: Một hệ thống mạng có chức năng **packet filtering** ngăn chặn các kết nối bằng **TELNET** vào hệ

thống ngoại trừ một máy duy nhất - **TELNET application gateway** là được phép. Một người muốn kết nối vào hệ thống bằng **TELNET** phải qua các bước sau:

- Thực hiện **telnet** vào máy chủ bên trong cần truy cập.
- **Gateway** kiểm tra địa chỉ **IP** nơi xuất phát của người truy cập để cho phép hoặc từ chối.
- Người truy cập phải vượt qua hệ thống kiểm tra xác thực.
- **Proxy Service** tạo một kết nối **Telnet** giữa **gateway** và máy chủ cần truy nhập.
- **Proxy Ser**vice liên kết lưu thông giữa người truy cập và máy chủ trong mạng nội bộ.

Cơ chế bộ lọc **packet** kết hợp với cơ chế **proxy** có nhược điểm là hiện nay các ứng dụng đang phát triển rất nhanh, do đó nếu các **proxy** không đáp ứng kịp cho các ứng dụng, nguy cơ mất an toàn sẽ tăng lên.

Thông thường những phần mềm **Proxy Server** hoạt động như một **gateway** nối giữa hai mạng, mạng bên trong và mạng bên ngoài.

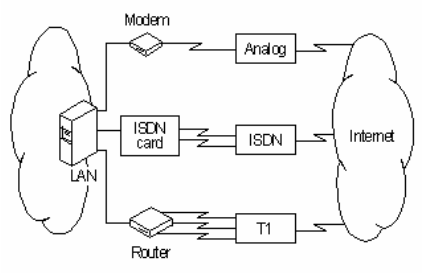


Hình 5.4: Mô hình hoạt động của **Proxy**.

Đường kết nối giữa **Proxy Server** và **Internet** thông qua nhà cung cấp dịch vụ **Internet** (**Internet Service Provider - ISP**) có thể chọn một trong các cách sau:

- Dùng **Modem analog**: sử dụng giao thức **SLIP/PPP** để kết nối vào **ISP** và truy cập **Internet**. Dùng **dial-up** thì tốc độ bị giới hạn, thường là 28.8 Kbps - 36.6 Kbps. Hiện nay đã có **Modem analog** tốc độ 56 Kbps nhưng chưa được thử nghiệm nhiều. Phương pháp dùng **dial-up** qua **Modem analog** thích hợp cho các tổ chức nhỏ, chỉ có nhu cầu sử dụng dịch vụ **Web** và **E-Mail**.
- Dùng đường **ISDN**: Dịch vụ **ISDN** (**Integrated Services Digital Network**) đã khá phổ biến ở một số nước tiên tiến. Dịch vụ này dùng tín hiệu số trên đường truyền nên không cần **Modem analog**, cho phép truyền cả tiếng nói và dữ liệu trên một đôi dây. Các kênh thuê bao **ISDN** (đường truyền dẫn thông tin giữa người sử dụng và mạng) có thể đạt tốc độ từ 64 Kbps đến 138,24 Mbps. Dịch vụ **ISDN** thích hợp cho các công ty vừa và lớn, yêu cầu băng thông lớn mà việc dùng **Modem analog** không đáp ứng được.

Phần cứng dùng để kết nối tùy thuộc vào việc nối kết trực tiếp **Proxy Server** với **Internet** hoặc thông qua một **Router**. Dùng **dial-up** đòi hỏi phải có **Modem analog**, dùng **ISDN** phải có bộ phối ghép **ISDN** cài trên **Server**.



Hình 5.5: Mô hình kết nối mạng **Internet**.

Việc chọn lựa cách kết nối và một **ISP** thích hợp tùy thuộc vào yêu cầu cụ thể của công ty, ví dụ như số người cần truy cập **Internet**, các dịch vụ và ứng dụng nào được sử dụng, các đường kết nối và cách tính cước mà **ISP** có thể cung cấp.

II. Giới Thiệu ISA 2004.

Microsoft Internet Security and Acceleration Sever (**ISA Server**) là phần mềm **share internet** của hãng phần mềm **Microsoft**, là bản nâng cấp từ phần mềm **MS ISA 2000 Server**. Có thể nói đây là một phần mềm **share internet** khá hiệu quả, ổn định, dễ cấu hình, thiết lập tường lửa (**firewall**) tốt, nhiều tính năng cho phép bạn cấu hình sao cho tương thích với mạng **LAN** của bạn. Tốc độ nhanh nhờ chế độ **cache** thông minh, với tính năng lưu **Cache** trên đĩa giúp bạn truy xuất thông tin nhanh hơn, và tính năng **Schedule Cache** (Lập lịch cho tự động **download** thông tin trên các **WebServer** lưu vào **Cache** và máy con chỉ cần lấy thông tin trên các **Webserver** đó bằng mạng **LAN**)

III. Đặc Điểm Của ISA 2004.

Các đặc điểm của **Microsoft ISA 2004**:

- Cung cấp tính năng **Multi-networking**: Kỹ thuật thiết lập các chính sách truy cập dựa trên địa chỉ mạng, thiết lập **firewall** để lọc thông tin dựa trên từng địa chỉ mạng con,…
- **Unique per-network policies**: Đặc điểm **Multi-networking** được cung cấp trong **ISA Server** cho phép bảo vệ hệ thống mạng nội bộ bằng cách giới hạn truy xuất của các **Client** bên ngoài **internet**, bằng cách tạo ra một vùng mạng ngoại vi **perimeter network** (được xem là vùng **DMZ**, **demilitarized zone**, hoặc **screened subnet**), chỉ cho phép **Client** bên ngoài truy xuất vào các **Server** trên mạng ngoại vi, không cho phép **Client** bên ngoài truy xuất trực tiếp vào mạng nội bộ.
- **Stateful inspection of all traffic**: Cho phép giám sát tất cả các lưu lượng mạng.
- **NAT and route network relationships**: Cung cấp kỹ thuật **NAT** và định tuyến dữ liệu cho mạng con.
- **Network templates**: Cung cấp các mô hình mẫu (network templates) về một số kiến trúc mạng, kèm theo một số luật cần thiết cho network templates tương ứng.
- Cung cấp một số đặc điểm mới để thiết lập mạng riêng ảo (**VPN network**) và truy cập từ xa cho doanh nghiệp như giám sát, ghi nhận **log**, quản lý **session** cho từng **VPN Server**, thiết lập **access policy** cho từng **VPN Client**, cung cấp tính năng tương thích với **VPN** trên các hệ thống khác.
- Cung cấp một số kỹ thuật bảo mật (**security**) và thiết lập **Firewall** cho hệ thống như **Authentication**, **Publish Server**, giới hạn một số **traffic**.
- Cung cấp một số kỹ thuật **cache** thông minh (**Web cache**) để làm tăng tốc độ truy xuất mạng,

giảm tải cho đường truyền, **Web proxy** để chia sẻ truy xuất **Web**.

- Cung cấp một số tính năng quản lý hiệu quả như: giám sát lưu lượng, **reporting** qua **Web**, **export** và **import** cấu hình từ **XML configuration file**, quản lý lỗi hệ thống thông qua kỹ thuật gởi thông báo qua **E-mail**,..
- **Application Layer Filtering** (**ALF**): là một trong những điểm mạnh của **ISA Server 2004**, không giống như **packet filtering firewall** truyền thống, **ISA 2004** có thể thao tác sâu hơn như có thể lọc được các thông tin trong tầng ứng dụng. Một số đặc điểm nổi bậc của **ALF**:
- Cho phép thiết lập bộ lọc **HTTP inbound** và **outbound HTTP**.
- Chặn được các cả các loại tập tin thực thi chạy trên nền **Windows** như .pif, .com,…
- Có thể giới hạn **HTTP download**.
- Có thể giới hạn truy xuất **Web** cho tất cả các **Client** dựa trên nội dung truy cập.
- Có thể điều kiển truy xuất **HTTP** dựa trên chữ ký (**signature**).
- Điều khiển một số phương thức truy xuất của **HTTP**.

IV. Cài Đặt ISA 2004.

IV.1. Yêu cầu cài đặt.

Thành phần	Yêu cầu đề nghị
Bộ xử lý (CPU)	**Intel** hoặc **AMD 500Mhz** trở lên.
Hệ điều hành (OS)	**Windows 2003** hoặc **Windows 2000** (**Service pack 4**).
Bộ nhớ (Memory)	256 (MB) hoặc 512 MB cho hệ thống không sử dụng **Web caching**, **1GB** cho **Web-caching ISA firewalls**.
không gian đĩa (Disk space)	ổ đĩa cài đặt **ISA** thuộc loại **NTFS file system**, ít nhất còn 150 MB dành cho **ISA**.
NIC	Ít nhất phải có một card mạng (khuyến cáo phải có 2 NIC)

IV.2. Quá trình cài đặt ISA 2004.

IV.2.1 Cài đặt ISA trên máy chủ 1 card mạng.

Khi ta cài đặt **ISA** trên máy **Server** chỉ có một card mạng (còn gọi là **Unihomed ISA Firewall**), chỉ hỗ trợ **HTTP**, **HTTPS**, **HTTP-tunneled** (**Web proxied**) **FTP**. **ISA** không hỗ trợ một số chức năng:

- SecureNAT client.
- Firewall Client.
- Server Publishing Rule.
- Remote Access VPN.
- Site-to-Site VPN.
- Multi-networking.
- Application-layer inspection (trừ giao thức HTTP)

Các bước cài đặt **ISA firewall** trên máy chủ chỉ có một **NIC**:

Chạy tập tin isaautorun.exe từ **CDROM ISA 2004** hoặc từ **ISA 2004 source**.

Nhấp chuột vào "**Install ISA Server 2004**" trong hộp thoại "**Microsoft Internet Security and Acceleration Server 2004**".

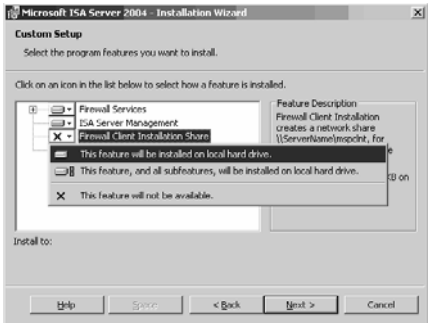
Nhấp chuột vào nút **Next** trên hộp thoại "**Welcome to the Installation Wizard for Microsoft ISA Server 2004**" để tiếp tục cài đặt.

Chọn tùy chọn **Select** "**I accept**" trong hộp thoại " **License Agreement**", chọn **Next**.

Nhập một số thông tin về tên **username** và tên tổ chức sử dụng phần mềm trong **User Name** và **Organization** textboxe. Nhập **serial number** trong **Product Serial Number textbox**. Nhấp **Next** để tiếp tục .

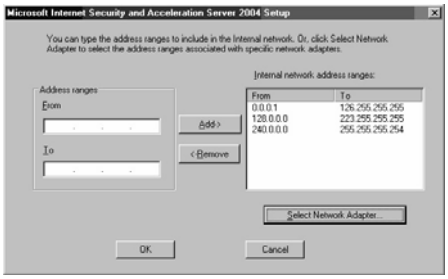
Chọn loại cài đặt (**Installation type**) trong hộp "**Setup Type"**, chọn tùy chọn **Custom,** chọn **Next.**.

trong hộp thoại "**Custom Setup"** mặc định hệ thống đã chọn **Firewall Services**, **Advanced Logging**, và **ISA Server Management**. Trên **Unihomed ISA firewall** chỉ hỗ trợ **Web Proxy Client** nên ta có thể không chọn tùy chọn **Firewall client Installation share** tuy nhiên ta có thể chọn nó để các **Client** có thể sử dụng phần mềm này để hỗ trợ truy xuất **Web** qua **Web Proxy**. Chọn **Next** để tiếp tục.



Hình 5.6: Chọn Firewall Client Installation Share.

Chỉ định **address range** cho cho **Internet network** trong hộp thoại "**Internal Network"**, sau đó chọn nút **Add**. Trong nút **Select Network Adapter, chọn Internal ISA NIC.**



Hình 5.7: Mô tả **Internal Network Range**.

Sau khi mô tả xong "**Internet Network address ranges**", chọn **Next** trong hộp thoại "**Firewall Client Connection Settings**".

Sau đó chương trình sẽ tiến hành cài đặt vào hệ thống, chọn nút **Finish** để hoàn tất quá trình.

IV.2.2 Cài đặt ISA trên máy chủ có nhiều card mạng.

ISA Firewall thường được triển khai trên **dual-homed host** (máy chủ có hai **Ethernet cards**) hoặc **multi-homed host** (máy chủ có nhiều card mạng) điều này có nghĩa **ISA server** có thể thực thi đầy đủ các tính năng của nó như **ISA Firewall**, **SecureNAT**, **Server Publishing Rule**, **VPN**,…

Các bước cài đặt **ISA firewall software** trên **multihomed host**:

Chạy tập tin isaautorun.exe từ **CDROM ISA 2004** hoặc từ **ISA 2004 source**.

Nhấp chuột vào "**Install ISA Server 2004**" trong hộp thoại "**Microsoft Internet Security and Acceleration Server 2004**".

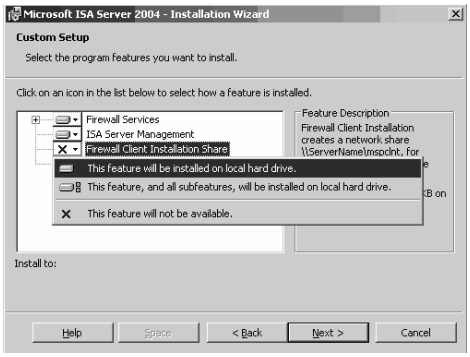
Nhấp chuột vào nút **Next** trên hộp thoại "**Welcome to the Installation Wizard for Microsoft ISA Server 2004**" để tiếp tục cài đặt.

Chọn tùy chọn **Select** "**I accept**" trong hộp thoại " **License Agreement**", chọn **Next**.

Nhập một số thông tin về tên **username** và tên tổ chức sử dụng phần mềm trong **User Name** và **Organization textboxe**. Nhập **serial number** trong **Product Serial Number textbox**. Nhấp **Next** để tiếp tục .

Chọn loại cài đặt (**Installation type**) trong hộp "**Setup Type"**, chọn tùy chọn **Custom,** chọn **Next.**

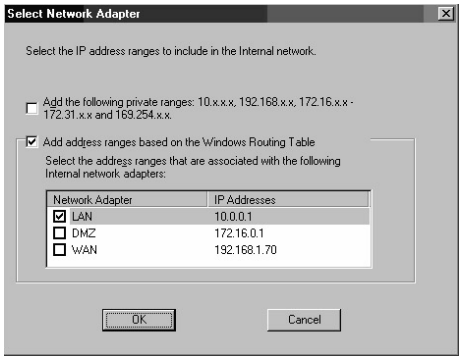
Trong hộp thoại "**Custom Setup**" mặc định hệ thống đã chọn **Firewall Services**, **Advanced Logging**, và **ISA Server Management**. Ta chọn tùy chọn **Firewall client Installation share** . Chọn **Next** để tiếp tục.



Hình 5.8: Chọn **Firewall Client Installation Share**.

Ta có hai cách Định nghĩa **internet network addresses** trong hộp thoại **Internal Network setup.** Cách thứ nhất ta mô tả dãy địa chỉ nội bộ (**Internal Network range**) từ **From** và **To text boxes**. Cách thứ hai ta cấu hình **default Internal Network** bằng cách chọn nút "**Select Network Adapter"** Sau đó ta nhấp chuột vào dấu chọn "**Select Network Adapter"** kết nối vào mạng nội bộ.

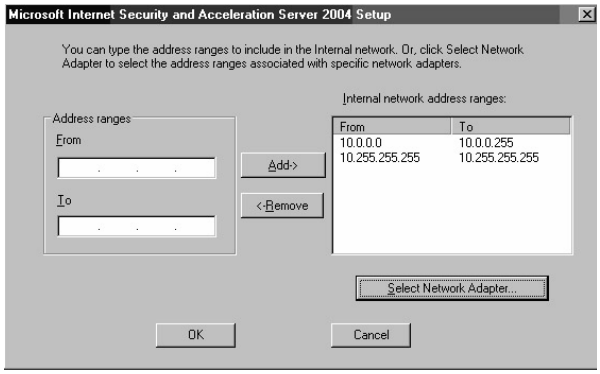
Trong hộp thoại **Configure Internal Network,** loại bỏ dấu check trong tùy chọn tên **Add the following private ranges**. Sau đó check vào mục chọn **Network Adapter**, chọn **OK**.



Hình 5.9: Chọn Network Adapter.

Xuất hiện thông báo cho biết **Internal network** được định nghĩa dựa vào **Windows routing table**.

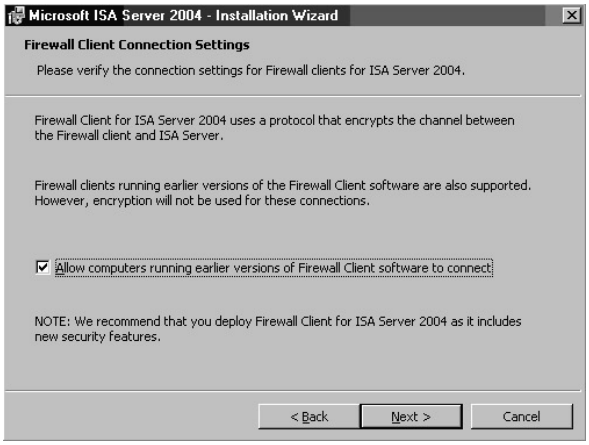
Chọn **OK** trong hộp thoại **Internal network address ranges**.



Hình 5.10: **Internal Network Address Ranges**.

Chọn **Next** trong hộp thoại "**Internal Network**" để tiếp tục quá trình cài đặt.

Chọn dấu check "**Allow computers running earlier versions of Firewall Client software to connect**" nếu ta muốn **ISA** hỗ trợ những phiên bản **Firewall client** trước, chọn **Next**.



Hình 5.11: Tùy chọn tương thích với **ISA Client**.

Xuất hiện hộp thoại **Services** để cảnh báo **ISA Firewall** sẽ stop một sốdịch vụ **SNMP** và **IIS Admin Service** trong quá cài đặt. **ISA Firewall** cũng sẽ vô hiệu hóa (**disable**) **Connection Firewall** (**ICF**) / **Internet Connection Sharing** (**ICF**), và **IP Network Address Translation** (**RRAS NAT service**) **services**.

Chọn **Finish** để hoàn tất quá trình cài đặt.

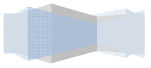
V. Cấu hình ISA Server.

V.1. Một số thông tin cấu hình mặc định.

- Tóm tắt một số thông tin cấu hình mặc định:
- **System Policies** cung cấp sẵn một số luật để cho phép truy cập vào/ra **ISA firewall**. Tất cả các **traffic** còn lại đều bị cấm.
- Cho phép định tuyến giữa VPN/**VPN-Q Networks** và **Internal Network**.
- Cho phép **NAT** giữa **Internal Network** và **External Network**.
- Chỉ cho phép **Administrator** có thể thay đổi chính sách bảo mật cho **ISA firewall**.

Đặc điểm	Cấu hình mặc định (Post-installation Settings)
User permissions	Cấp quyền cho **user** có quyền cấu hình **firewall policy** (chỉ có thành viên của **Administrators group** trên máy tính nội bộ có thể cấu hình **firewall policy**).
Network settings	Các **Network Rules** được tạo sau khi cài đặt: **Local Host Access**: Định nghĩa đường đi (**route**) giữa **Local Host network** và tất cả các mạng khác. **Internet Access**: Định nghĩa **Network Address Translation** (**NAT**). **VPN Clients to Internal Network** dùng để định nghĩa đường đi **VPN Clients Network** và **Internal Network**.
Firewall policy	Cung cấp một **Access Rule** mặc định tên là **Default Rule** để cấm tất cả các traffic giữa các mạng.
System policy	**ISA firewall** sử dụng **system policy** để bảo mật hệ thống. một số **system policy rule** chỉ cho phép truy xuất một số **service** cần thiết.
Web chaining	Cung cấp một luật mặc định có tên **Default Rule** để chỉ định rằng tất cả các request của **Web Proxy Client** được nhận trực tiếp từ **Internet**, hoặc có thể nhận từ **Proxy Server** khác.
Caching	Mặc định ban đầu **cache size** có giá trị 0 có nghĩa rằng cơ chế cache sẽ bị vô hiệu hóa. Ta cần định nghĩa một cache drive để cho phép sử dụng **Web caching**.
Alerts	Hầu hết cơ chế cảnh báo được cho phép để theo dõi và gián sát sự kiện.

Client configuration	**Web Proxy Client** tự động tìm kiếm **ISA Firewall** và sau đó nó sẽ cấu hình



V.2. Một số chính sách mặc định của hệ thống

Order/Comments	Name	Action	Protocol	from/Listener	To	Condition
1. Chỉ sử dụng khi ISA Firewall là thành viên của Domain	Allow access to Directory services purposes	Allow	LDAP ;LDAP (UDP) LDAP GC (global catalog) LDAPS ;LDAPS GC (Global Catalog)	Local Host	Internal	All Users
2. Cho phép quản lý ISA Firewall từ xa thông qua công cụ MMC	Allow remote management from selected computers using MMC	Allow	NetBIOS datagram NetBIOS Name Service NetBIOS	Remote Management Computers	Local Host	All Users
3. Cho phép quản lý ISA Firewall thông qua Terminal Services Protocol	Allow remote management from selected computers using Terminal Server Name	Allow	RDP (Terminal Services) Protocols	Remote Management Computers From/Listener	Local Host	All Users Continued Condition
4. Cho phép login tới một số server sử dụng giao thức NetBIOS	Allow remote logging to trusted servers using NETBIOS	Allow	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Local Host	Internal	All Users
5. Cho phép RADIUS authentication từ ISA đến một số trusted RADIUS servers	Allow RADIUS authentication from ISA Server to trusted RADIUS servers	Allow	RADIUS RADIUS Accounting	Local Host	Internal	All Users

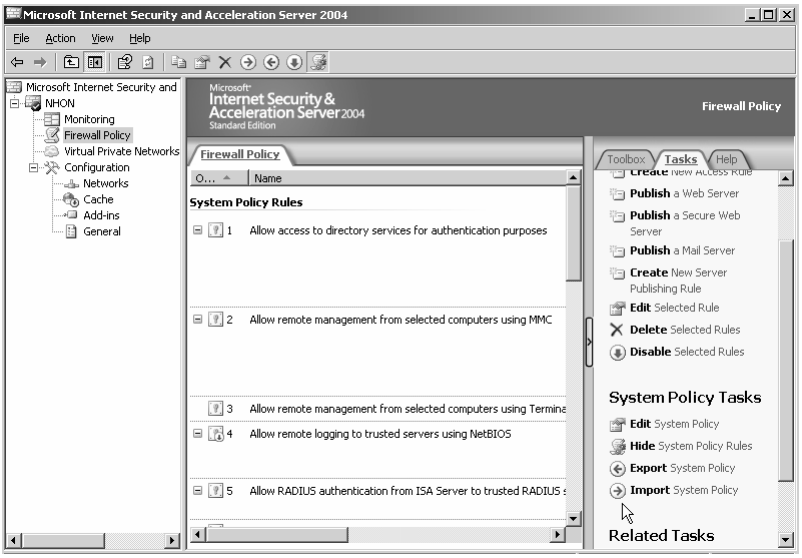
Order/Comments	Name	Action	Protocol	from/Listener	To	Condition	Order/Comments
6. Cho phép chứng thực kerberos từ ISA Server tới trusted server	Allow Kerberos authentication from ISA Server to trusted servers	Allow	Kerberos-Sec (TCP) Kerberos-Sec (UDP)	Local Host	Internal	All Users	11. Cho phép ISA Server gởi ICMP request tới một số server
7. Cho phép sử dụng DNS từ ISA tới một số DNS Server	Allow DNS from ISA Server to selected servers	Allow	DNS	Local Host	All Networks (and Local Host)	All Users	12. Cho phép tất cả các VPN Client bên ngoài kết nối vào ISA Server
8. Cho phép DHCP Request từ ISA gởi đến tất cả các mạng	Allow DHCP requests from ISA Server to all networks Name	Allow	DHCP(request) Protocols	Local Host From/Listener	Anywhere To	All Users Continued Condition	13. Cho phép DHCP Request từ ISA gởi đến tất cả các mạng
9. Chấp nhận DHCP replies từ DHCP Server tới ISA Server	Allow DHCP replies from DHCP servers to ISA Server	Allow	DHCP (reply)	Internal	Local Host	All Users	14. Cho phép ISA thiết lập kết nối VPN (site to site) đến VPN Server khác
10. Cho phép một số máy được quyền gởi ICMP request đến ISA Server	Allow ICMP (PING) requests from selected computers to ISA Server	Allow	Ping	Remote Management Computers	Local Host	All Users	15. Cho phép sử dụng CIFS để truy xuất share file từ ISA đến các server khác

Name	Action	Protocol	from/Listener	To	Condition	Order/Comments	Name	Action
Allow ICMP requests from ISA Server to selected servers	Allow	ICMP Information Request ICMP Timestamp	Local Host	All Networks (and Local Host Network)	All Users	16. Cho phép login từ xa bằng SQL qua ISA server	Allow remote SQL logging from ISA servers	Allow
All VPN client traffic to ISA Server	Allow	PPTP	External	Local Host	All Users	17. Cho phép truy xuất HTTP/HTTPS từ ISA đến một số site chỉ định	Allow HTTP/HTTPS requests from ISA Server to specified sites Name	Allow
Allow VPN site-to-site traffic to ISA Server Name	Allow	NONE	External IPSec Remote Gateways From/Listener	Local Host To	All Users Continued Condition	18. Cho phép HTTP/HTTPS từ ISA đến một số server khác	Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers	Allow
Allow VPN site-to-site traffic from ISA Server	Allow	NONE	Local Host	External IPSec Remote Gateways	All Users	19. Cho phép một số máy được truy xuất Firewall Client installation share trên ISA Server	Allow access from trusted computers to the Firewall Client installation share on ISA Server	Allow
CIFS (Common Internet File System) from ISA Server to trusted	Allow	Microsoft CIFS (TCP) Microsoft CIFS (UDP)	Local Host	Internal	All Users	20. Cho phép quan sát thông suất của ISA Server từ xa	Allow remote performance monitoring of ISA Server from trusted servers	Allow

Protocol	from/Listener	To	Condition	Order/Comments	Name	Action	Protocol	from/Listener
Microsoft SQL (TCP) Microsoft SQL (UDP)	Local Host	Internal	All Users	21. Cho phép sử dụng NetBIOS từ ISA Server đến một số Server chỉ định sẵn	Allow NetBIOS from ISA Server to trusted servers Name	Allow	NetBIOS Datagram NetBIOS Name Service NetBIOS Sessions Protocols	Local Host From/Listener
HTTP HTTPS Protocols	HTTP HTTPS Protocols	System Policy Allowed Sites To	All Users Continued Condition	21. Cho phép sử dụng RPC từ ISA truy xuất đến một số server khác	Allow RPC from ISA Server to trusted servers	Allow	RPC (all interfaces)	Local Host
HTTP HTTPS	Local Host	All Networks (and Local Host Network)	All Users	23. Cho phép truy xuất HTTP/HTTPS từ ISA Server tới một số Microsoft error reporting site	Allow HTTP/HTTPS from ISA Server to specified	Allow	HTTP HTTPS	Local Host
(TCP) Microsoft CIFS (UDP) NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Internal	Local Host	All Users	24. Cho phép chứng thực SecurID từ ISA đến một số server	authentication from ISA Server to trusted servers	Allow	SecurID	Local Host
NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Remote Management Computers	Local Host	All Users	25. Cho phép giám sát từ xa thông qua giao thức Microsoft Operations	Allow remote monitoring from ISA Server to		Microsoft Operations Manager Agent	Local Host

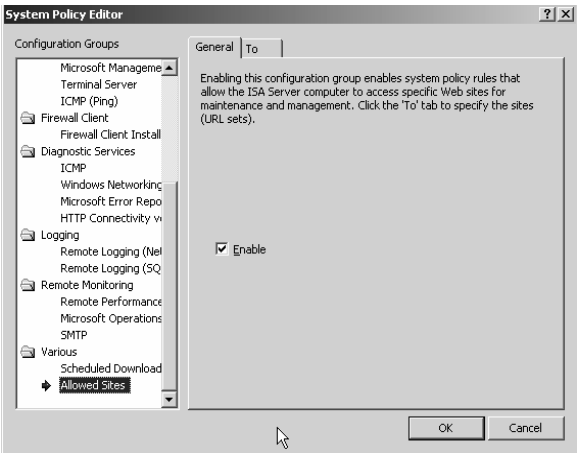
To	Condition	Order/Comments	Name	Action	Protocol	from/Listener	To	Condition
Internal To	All Users Continued Condition	26. Cho phép HTTP traffic từ ISA Server tới một số network hỗ trợ dịch vụ chứng thực download CRL	Traffic from ISA Server to all networks (for CRL downloads) Name	Allow + Action	HTTP Protocols	Local Host From/Listener	All Networks (and Local Host) To	All Users Continued Condition
Internal	All Users	27. Cho phép sử dụng NTP (giao thức đồng bộ thời gian trên Windows NT 2k, XP) từ ISA tới một	Allow NTP from ISA Server to trusted NTP servers	Allow	NTP (UDP)	Local Host	Internal	All Users
Microsoft Error Reporting sites	All Users	28. Cho phép traffic SMTP từ ISA Server tới một số Server	Allow SMTP from Allow ISA Server to trusted servers		SMTP	Local Host	Internal	All Users
Internal	All Users	29. Cho phép một số máy sử dụng Content Download Jobs.	ISA Server to selected computers for Content Download Jobs	Allow	HTTP	Local Host	All Networks (and Local Host)	System and Network Service
Internal	All Users	30. Cho phép một số máy khác sử dụng MMC điều khiển ISA	Allow Microsoft communication to selected computers	Allow	All Outbound traffic	Local Host	Remote Management Computers	All Users

Ta có thể xem các chính sách mặc định của hệ thống **ISA Firewall** (**system policy rule)** bằng cách chọn **Filewall Policy** từ hộp thoại **ISA Management**, sau đó chọn item **Show system policy rule** trên cột **System policy**.



Hình 5.12: **System policy Rules**.

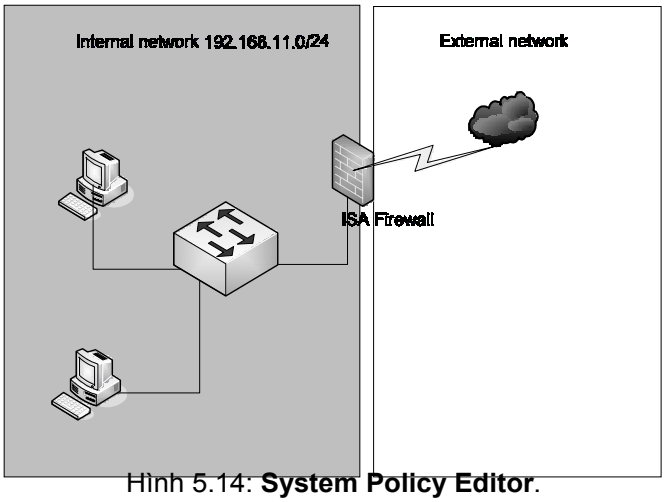
Ta cũng có thể hiệu chỉnh từng **system policy** bằng cách nhấp đôi chuột vào **system policy item**.



Hình 5.13: System Policy Editor.

V.3. Cấu hình Web proxy cho ISA.

Trong phần này ta sẽ khảo sát nhanh các bước làm sao để cấu hình **ISA Firewall** cung cấp dịch vụ **Web Proxy** để chia sẻ kết nối **Internet** cho mạng nội bộ.

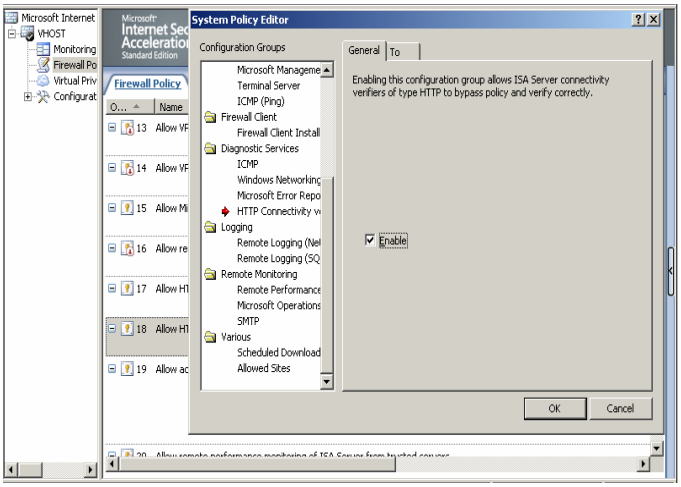


Hình 5.14: **System Policy Editor**.

- Mặc định **ISA Firewall** cho phép tất cả mạng nội bộ chỉ có thể truy xuất **Internet Web** thông qua giao thức **HTTP/HTTPS** tới một số **site** được chỉ định sẵn trong **Domain Name Sets** được mô tả dưới tên là "**system policy allow sites"** bao gồm:
- *.windows.com
- *.windowsupdate.com
- *.microsoft.com

Do đó khi ta muốn cấu hình cho mạng nội bộ có thể truy xuất đến bất kỳ một **Internet Web** nào bên ngoài thì ta phải hiệu chỉnh lại thông tin trong **System Policy Allowed Sites** hoặc hiệu chỉ lại **System Policy Rule** có tên

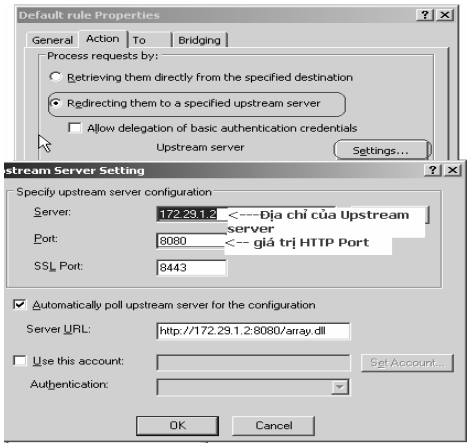
  + Hiệu chỉnh **System Policy Allowed Sites** bằng cách Chọn **Firewall Policy** trong ISA **Management Console**, sau đó chọn cột **Toolbox**, chọn **Domain Name Sets**, nhấp đôi vào item **System Policy Allowed Sites** để mô tả một số site cần thiết cho phép mạng nội bộ truy xuất theo cú pháp *.domain_name.
- Nếu ta muốn cho mạng nội bộ truy xuất bất kỳ **Internet Website** nào thì ta phải **Enable** luật 18 có tên "**Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers**" (tham khảo Hình 5.15)**,** sau đó ta chọn nút **Apply** trong **Firewall Policy** pannel để áp đặt sự thay đổi vào hệ thống.



Hình 5.15: Mô tả **System Policy Sites**.

Chú ý:

- Nếu **ISA Firewall** kết nối trực tiếp **Internet** thì ta chỉ cần cấu hình một số thông số trên, ngược lại nếu **ISA Firewall** còn phải thông qua một hệ thống **ISA Firewall** hoặc **Proxy** khác thì ta cần phải mô tả thêm tham số **Uptream Server** để chuyển yêu cầu truy xuất lên **Proxy** cha để nhờ **Proxy** cha lấy thông tin từ **Internet Web Server**.
  + Để cấu hình **Uptream Server** cho **ISA Server** nội bộ ta chọn **Configuration panel** từ **ISA Management Console**, sau đó chọn item **Network** , chọn **Web Chaining Tab**, Nhấp đôi vào **Rule Set** có tên **Last default rule**, chọn **Action Tab**, chọn tùy chọn **Redirecting them to specified upstream server**, chọn tiếp nút **Settings…**Chỉ định địa chỉ của **upstream server**.

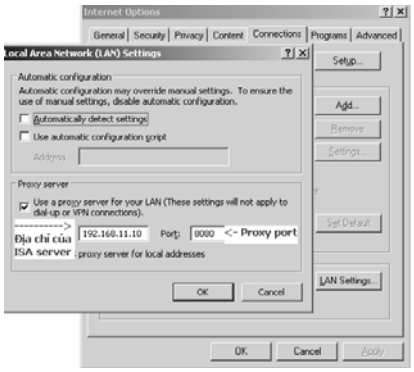


Hình 5.16: Chỉ định **Upstream server**.

  + Ta cần chỉ định **DNS Server** cho **ISA Server** để khi **ISA** có thể phân giải **Internet Site** khi có yêu cầu, ta có thể sử dụng **DNS Server** nội bộ hoặc **Internet DNS Server**, tuy nhiên ta cần lưu ý rằng phải cấu hình **ISA Firewall** để cho phép **DNS request** và **DNS reply**.
- Để cho phép **Client** có thể sử dụng **Web Proxy** ta cấu hình **Proxy Server** có địa chỉ là địa chỉ của Internal interface của **ISA Firewall** trong trình duyệt **Web** cho từng **Client**, hoặc ta cài **ISA Client**

Share trên từng **Client** để **Client** đóng vai trò lài **ISA Firewall Client**.

- Chỉ định địa chỉ của **Web Proxy** trong **textbox Address.**
- Chỉ **Web Proxy Port** trong Textbox **Port** là **8080.**



Hình 5.16: Chỉ định **Client** sử dụng **Proxy Server**.

V.4. Tạo Và Sử Dụng Firewall Access Policy.

- **Access Policy** của **ISA Firewall** bao gồm các tính năng như: **Web Publishing Rules**, **Server Publishing Rules** và **Access Rules**.
  - + **Web Publishing Rules** và **Server Publishing Rules** được sử dụng để cho phép **inbound access**.
    - o **Access rules dùng để điều khiển outbound access.**
- **ISA Firewall** kiểm tra **Access Rules** trong **Access Policy** theo cơ chế **top down** (Lưu ý rằng **System Policy** được kiểm tra trước **Access Policy** do **user** định nghĩa), nếu **packet** phù hợp với một luật nào đó thì **ISA Firewall** thì **ISA Firewall** sẽ thực thi **action** (**permit/deny**) tùy theo luật, sau đó **ISA Firewall** sẽ bỏ qua tất cả các luật còn lại. Nếu **packet** không phù hợp với bất kỳ **System Access Policy** và **User-Defined Policy** thì **ISA Firewall deny packet** này.
- Một số tham số mà **Access Rule** sẽ kiểm tra trong **connection request**:
  - + **Protocol**: Giao thức sử dụng.
  - + **From**: Địa chỉ nguồn.
  - + **Schedule**: Thời gian thực thi luật.
  - + **To**: Địa chỉ đích.
  - + **Users**: Người dùng truy xuất.
  - + **Content type**: Loại nội dung cho **HTTP connection**.

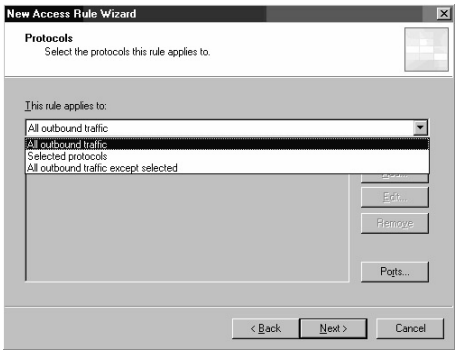
V.4.1 Tạo một Access Rule.

Access Rules trên **ISA Firewall** luôn luôn áp đặt luật theo hướng ra (**outbound**). Ngược lại, **Web Publishing Rules**, **Server Publishing Rules** áp đặt theo hướng vào (**inbound**). **Access Rules** điều khiển truy xuất từ **source** tới **destination** sử dụng **outbound protocol**. Một số bước tạo **Access Rule**:

3. Kích hoạt **Microsoft Internet Security and Acceleration Server 2004 management console**, mở rộng **server name**, nhấp chuột vào **Firewall Policy panel**, chọn **Tasks tab** trong **Task Pane**, nhấp chuột vào liên kết **Create New Access Rule**.

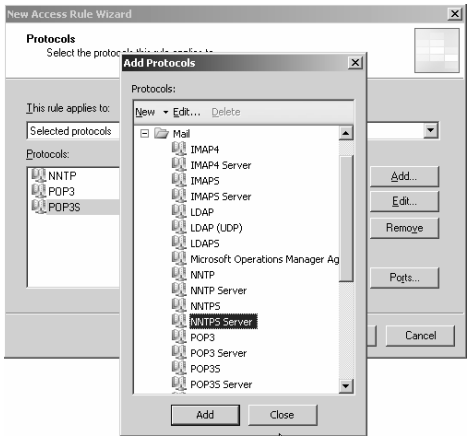
4. Hiển thị hộp thoại **"Welcome to the New Access Rule Wizard"**. Điền vào tên **Access Rule name**, nhấp chuột vào nút **Next** để tiếp tục.
5. Hiển thị hộp thoại **Rule Action** có hai tùy chọn: **Allow** hoặc **Deny**. Tùy chọn **Deny** được đặt mặc định, tùy vào loại Rule ta cần mô tả mà chọn **Allow** hoặc **Deny** cho phù hợp, chọn **Next** để tiếp tục.
6. Hiển thị hộp thoại "**Protocols"** (tham khảo Hình 5.17). Ta sẽ chọn giao thức (protocol) để cho phép/cấm **outbound traffic** từ **source** đến **destination**. Ta có thể chọn ba tùy chọn trong danh sách **This rule applies to.**

- **All outbound traffic**: Để cho phép tất cả các protocols **outbound**. Tầm ảnh hưởng của tùy chọn này phụ thuộc vào loại **Client** (**client type**) sử dụng để truy xuất luật. đối với **Firewall clients**, thì tùy chọn này cho phép tất cả các **Protocol** ra ngoài (**outbound**), bao gồm cả **secondary protocols** đã được định nghĩa hoặc chưa được định trong **ISA firewall**. Tuy nhiên đối với **SecureNAT client** kết nối **ISA Firewall** thì **outbound access** chỉ cho phép các protocol mà đã được định nghĩa trong **Protocols list** của **ISA firewall**, nếu **SecureNAT client** không thể truy xuất tài nguyên nào đó bên ngoài bằng một **protocol** nào đó thì ta phải mô tả **protocol** vào **Protocol Panel** được cung cấp trên **ISA firewall** để nó có thể hỗ trợ kết nối cho **SecureNAT client**.
- **Selected protocols**: Tùy chọn này cho phép ta có thể lựa chọn từng **protocols** để áp đặt vào luật (**rule**). Ta có thể lựa chọn một số **protocol** có sẵn trong hộp thoại hoặc có thể tạo mới một **Protocol Definition**.
- **All outbound traffic except selected**: Tùy chọn này cho phép tất cả các **protocol** cho luật mà không được định nghĩa trong hộp thoại.



Hình 5.17: Lựa chọn **protocol** để mô tả cho **Rule**.

Nếu ta chọn tùy chọn **Selected Protocols** ta sẽ chọn danh sách các **protocol** cần mô tả cho luật (tham khảo hình 5.18).



Hình 5.18: Lựa chọn **protocol** để mô tả cho **Rule**.

1. Hiển thị hộp thoại **Access Rule Sources**, chọn địa chỉ nguồn (**source location**) để áp đặt vào luật bằng cách chọn nút **Add**, hiển thị hộp thoại **Add Network Entities**, sau đó ta có thể chọn địa chỉ nguồn từ hộp thoại này (tham khảo hình), chọn **Next** để thực hiện bước tiếp theo.

Hình 5.19: Chọn địa chỉ nguồn.

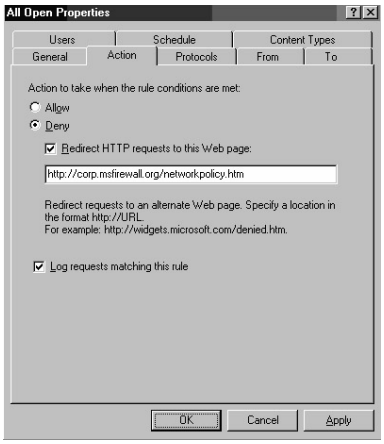
2. Hiển thị hộp thoại **Access Rule Destinations** cho phép chọn địa chỉ đích (**destination**) cho luật bằng cách chọn nút **Add** sau đó xuất hiện hộp thoại **Add Network Entities**, trong hộp thoại này cho phép ta chọn địa chỉ đích (**Destination**) được mô tả sẵn trong hộp thoại hoặc có thể định nghĩa một **destination** mới, thông thường ta chọn **External network** cho **destination rule**, sau khi hoàn tất quá trình ta chọn nút **Next** để tiếp tục.
3. Hiển thị hộp thoại **User Sets** cho phép ta lựa chọn **User** truy xuất cho **access Rule**. Mặc định luật sẽ áp đặt cho tất cả user (**All Users)**, ta có thể hiệu chỉnh thông số này bằng cách chọn **Edit** hoặc thêm **user** mới vào **rule** thông qua nút **Add**, chọn **Next** để tiếp tục
4. Chọn **Finish** để hoàn tất.

V.4.2 Thay đổi thuộc tính của Access Rule.

Trong hộp thoại thuộc tính của **Access Rule** chứa đầy đủ các thuộc tính cần thiết để thiết lập luật, có một số thuộc tính chỉ có thể cấu hình trong hộp thoại này mà không thể cấu hình trong quá trình tạo **Access Rule**, thông thường ta truy xuất hộp thoại thuộc tính của luật khi ta muốn kiểm tra hoặc thay đổi các điều kiện đã đặt trước đó. Để truy xuất thuộc tính của **Access Rule** ta nhấp đôi chuột vào tên luật trong **Firewall Policy Panel**.

Một số Tab thuộc tính của Access Rule:

- **General tab:** Cho phép ta có thể thay đổi tên **Access rule**, **Enable/Disable Access rule**.
- **Action tab:** Cung cấp một số tùy chọn để hiệu chỉnh luật như (Tham khảo hình 5.20):
- **Allow:** Tùy chọn cho phép các kết nối phù hợp (**matching**) với các điều kiện được mô tả trong **Access rule** đi qua **ISA firewall**.
- **Deny:** Tùy chọn cấm các kết nối phù hợp (**matching**) với các điều kiện được mô tả trong **Access rule** đi qua **ISA firewall**.
- **Redirect HTTP requests to this Web page**: Tùy chọn được cấu hình để chuyển hướng **HTTP requests** (phù hợp với điều kiện của **Access rule**) tới một **Web page** khác.
- **Log requests matching this rule** Cho phép ghi nhận lại tất cả các **request** phù hợp với **Access Rule**.



Hình 5.20: Thuộc tính của **Access Rule**.

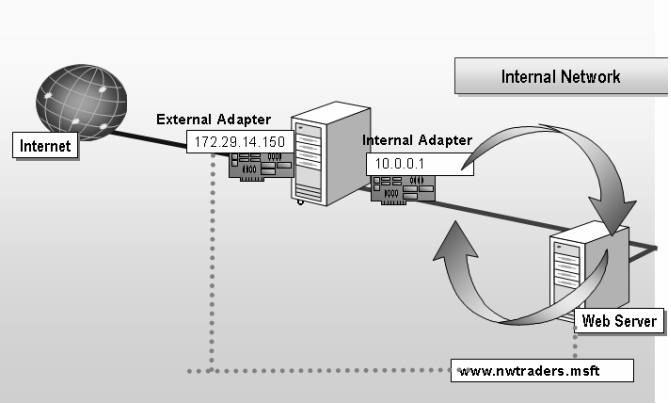
- **Protocols tab:** Cung cấp các tùy chọn để cho phép ta hiệu chỉnh giao thức (**protocol**) cho **Access rule**.
- **From tab:** Cung cấp các tùy chọn để hiệu chỉnh địa chỉ nguồn cho **Access rule**.
- **To tab:** Cung cấp các tùy chọn để hiệu chỉnh địa chỉ đích cho **Access rule**.
- **Users tab:** Cung cấp các tùy chọn để hiệu chỉnh thông tin **User** trong **Access rule**.
- **Schedule tab:** Hiệu chỉnh thời gian áp đặt (**apply**) luật.
- **Content Types tab:** Cho phép hiệu chỉnh **Content Type** chỉ áp đặt **HTTP connection**.

V.5. Publishing Network Services.

V.5.1 Web Publishing and Server Publishing.

Publishing services là một kỹ thuật dùng để công bố (**publishing**) dịch vụ nội bộ ra ngoài mạng Internet thông qua **ISA Firewall**. Thông qua **ISA Firewall** ta có thể publish các dịch vụ **SMTP**, **NNTP**, **POP3**, **IMAP4**, **Web**, **OWA**, **NNTP**, **Terminal Services**,,,.

- **Web publishing:** Dùng để **publish** các **Web Site** và dịch vụ **Web**. **Web Publishing** đôi khi được gọi là **'reverse proxy'** trong đó **ISA Firewall** đóng vai trò là **Web Proxy** nhận các Web request từ bên ngoài sau đó nó sẽ chuyển yêu cầu đó vào **Web Site** hoặc **Web Services** nội bộ xử lý (tham khảo hình 5.21), Một số đặc điểm của **Web Publishing**:
- Cung cấp cơ chế truy xuất ủy quyền **Web Site** thông qua **ISA firewall**.
- Chuyển hướng theo đường dẫn truy xuất **Web Site** (**Path redirection**)
- **Reverse Caching of published Web Site**.
- Cho phép **publish** nhiều **Web Site** thông qua một địa chỉ **IP**.
- Có khả năng thay đổi (**re-write**) **URLs** bằng cách sử dụng **Link Translator** của **ISA firewall**.
- Thiết lập cơ chế bảo mật và hỗ trợ chứng thực truy xuất cho **Web Site** (**SecurID authentication**, **RADIUS authentication**, **Basic Authentication**)
- Cung cấp cơ chế chuyển theo **Port** và **Protocol**.



Hình 5.21: Mô hình **Web Publishing**.

- **Server publishing:** Tương tự như **Web Publishing**, **Server publishing** cung cấp một số cơ chế công bố (**publishing**) các **Server** thông qua **ISA Firewall**.

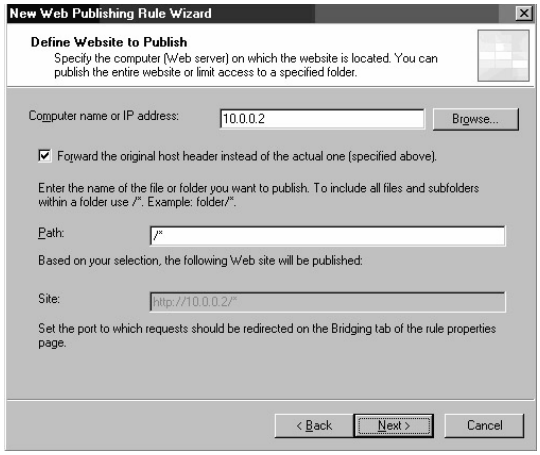
V.5.2 Publish Web server.

Để **publish** một **Web Services** ta thực hiện các bước sau:

1. kích hoạt màn hình "**Microsoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Publish a Web Server**", hiển thị hộp thoại "**Welcome to the New Web Publishing Rule Wizard**" yêu cầu nhập tên **Web publishing rule**, chọn **Next** để tiếp tục.
3. Chọn tùy chọn **Allow** trong hộp thoại "**Select Rule Action**", chọn **Next**.
4. Cung cấp một số thông tin về **Web Site** cần được **publish** trong hộp thoại **"Define Website to Publish"** (tham khảo hình 5.22):

- **"Computer name or IP address"**: chỉ định địa chỉ của **Web Server** nội bộ.

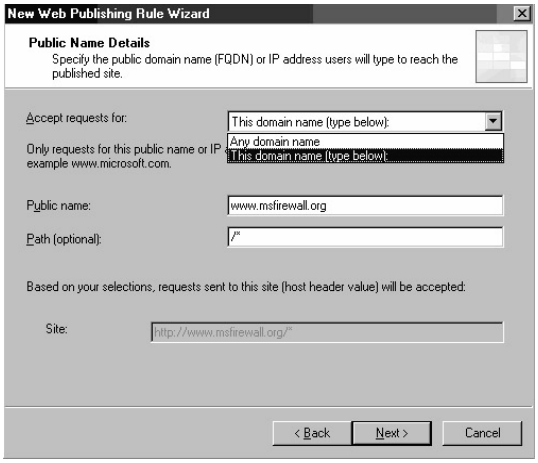
- **"Forward the original host header instead of the actual one (specified above)":** Chỉ định cơ chế chuyển yêu cầu vào **Web Server** nội bộ theo dạng **host header name**, tùy chọn này được sử dụng trong trường hợp ta muốn **publish Web hosting** cho một **Web Server**.
- **"Path"**: Chỉ định tên tập tin hoặc thư mục ta muốn truy xuất vào **Web Server** nội bộ.
- **"Site"**: Chỉ định tên **Web Site** được **publish**.



Hình 5.22: Chỉ định **Web Site** cần **Publish**.

1. Chỉ định một số thông tin về **FQDN** hoặc **IP addresses** được phép truy xuất tới **publish Web Site** thông qua **Web Publishing Rule** (tham khảo hình 5.23). Các tùy chọn cần thiết:

- **Accept requests for**: Chỉ định tên **publish** được **Web listener** chấp nhận.
- **Path** (**optional**): Chỉ định đường dẫn **Web Site** cho phép truy xuất
- **Site**: Tên **Web Site** được phép truy xuất **Web Site** nội bộ.



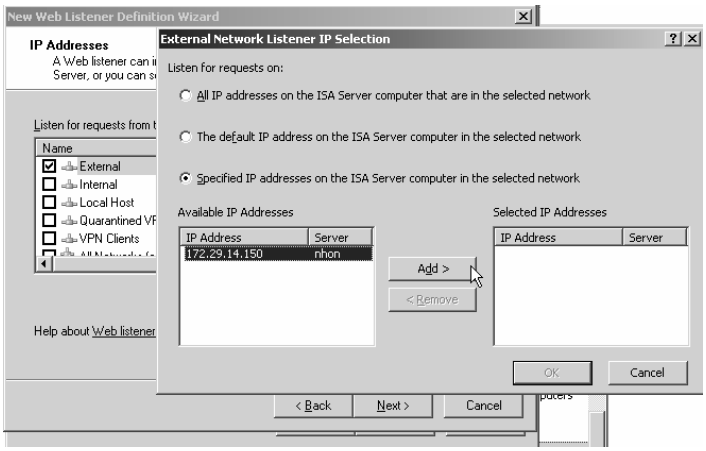
Hình 5.23: Chỉ định tên **domain** được truy xuất **publish site**.

2. Chọn **Web Listener** cho **Web Publishing Rule** (là một **Network Object** được sử dụng cho **Web Publishing Rule** để **listen** các kết nối đi vào **interface** (**incoming connection**) theo port được định nghĩa trước), ở bước này ta có thể lựa chọn **Web Listener** đã tạo trước đó hoặc ta có thể tạo mới **Web Listener**. Sau đây là một số bước tạo mới **Web Listener.**

- Từ hộp thoại "**Seclect Web Listener**" bằng cách nhấp chuột vào nút **New**…, cung cấp tên **Web**

Listener trong hộp thoại "**Welcome to the New Web Listener Wizard**", chọn **Next**.

- Chọn tên **Interface** cho phép chấp nhận kết nối **Incoming Web**, sau đó ta có thể chọn nút **Address** để chỉ định địa chỉ **IP** cụ thể trên **interface** đã lựa chọn, Chọn nút **Add>** (tham khảo hình 5.24), cuối cùng ta chọn nút **OK** để chấp nhận quá trình tạo mới **Web Listener**, chọn **Next** để tiếp tục.



Hình 5.24: Chọn địa chỉ chấp nhận **incoming web request**.

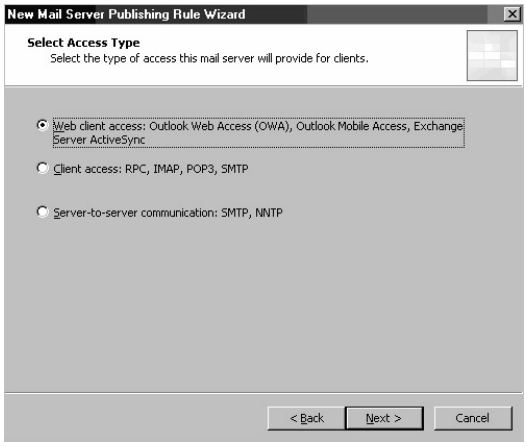
3. Chỉ định **HTTP port** và **SSL port** trong hộp thoại **Port Specification** cho phép **ISA Server** sử dụng để chấp nhận **incoming web requests**, chọn **Next**.
4. Chọn **Finish** để hoàn tất quá trình.

V.5.3 Publish Mail Server.

Các bước tiến hành publish Mail server:

1. Kích hoạt màn hình "**Microsoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Publish a Mail Server**", hiển thị hộp thoại "**Welcome to the New Mail Server Publishing Rule Wizar**d" yêu cầu nhập tên **Mail Server Publishing Rule**, chọn **Next** để tiếp tục.
3. Chọn các tùy chọn về loại truy xuất cho **Client** trong hộp thoại "**Select Client Type**" (Tham khảo hình 5.25).

- **Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync**: **Publish Web Mail Server** để cho phép **client** có thể truy xuất **E-Mail** qua **Web** thông qua **OWA**, **OMA**, **ESA**,..
- **Client access: RPC, IMAP, POP3, SMTP**: **Publish** các giao thức **IMAP**, **POP3**, **SMTP** cho **Mail Server**.
- **Server-to-server communication: SMTP, NNTP**: Cho phép **Server Mail** bên ngoài có thể giao tiếp với **Server Mail** nội bộ thông qua giao thức **SMTP**, **NNTP**.

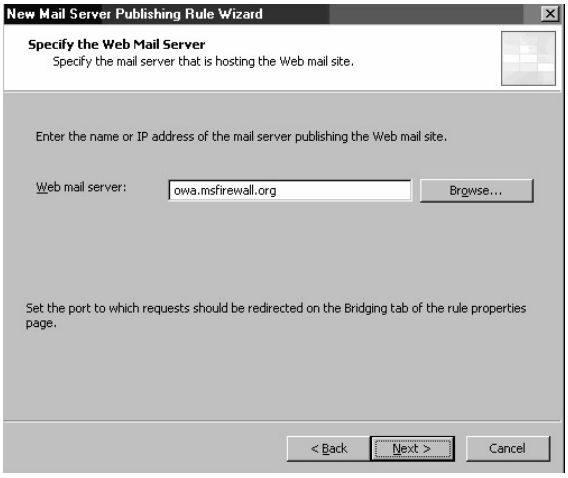


Hình 5.25: Chọn **Client Type**.

1. Ví dụ trong bước 3 ta chọn tùy chọn **Web Client Access**, chọn **Next**, sau đó xuất hiện hộp thoại "**Select Services**" cho phép ta chọn các dịch vụ **Exchange Web Services** bao gồm: **Outlook Web Access**, **Outlook Mobile Access**, **Exchange ActiveAsync** (tham khảo hình 5.26), chọn **Next** để tiếp tục.

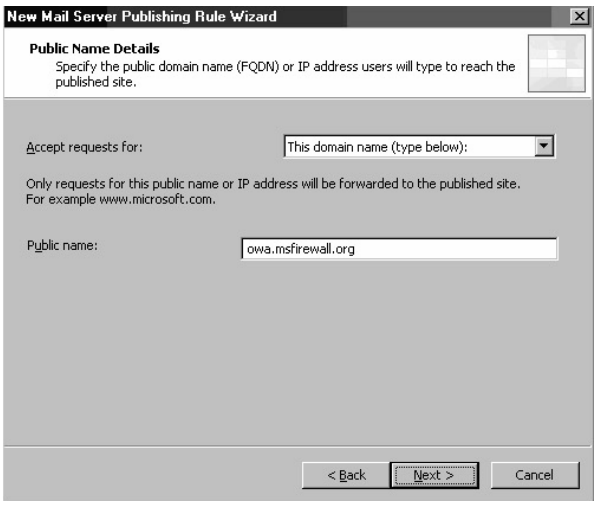
Hình 5.26: Chọn **Exchange Web Services**.

2. Chỉ định địa chỉ **Web Mail Server** trong hộp thoại "**Specify the Web Mail Server"**, chọn **Next.**



Hình 5.27: Chỉ định địa chỉ **Web Mail Server**.

3. Chỉ định **Publish Name** được **Web Listener** chấp nhận trong hộp thoại "**Public Name Details"**, chọn **Next.**



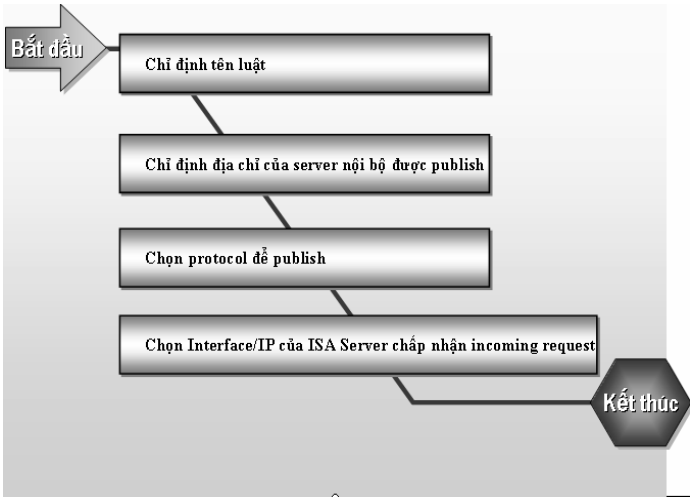
Hình 5.28: Chỉ định **Publish Name**.

4. Chọn **Finish** để hoàn tất quá trình.

V.5.4 Tạo luật để publish Server.

Tạo luật để **publish** một **Server** thực chất các thao tác cũng tương tự như ta **publish** một **Web** hoặc **Mail** chỉ có điều ta được phép lựa chọn **protocol** cần được **publish**, khi ta **publish** một **Server** ta cần chuẩn bị một số thông số sau:

- **Protocol** mà ta cần **publish** là **protocol** gì?
- Địa chỉ **IP** trên **ISA firewall** chấp nhận **incoming connection**.
- Địa chỉ **IP address** của **Publish Server** nội bộ (**Protected Network server**).



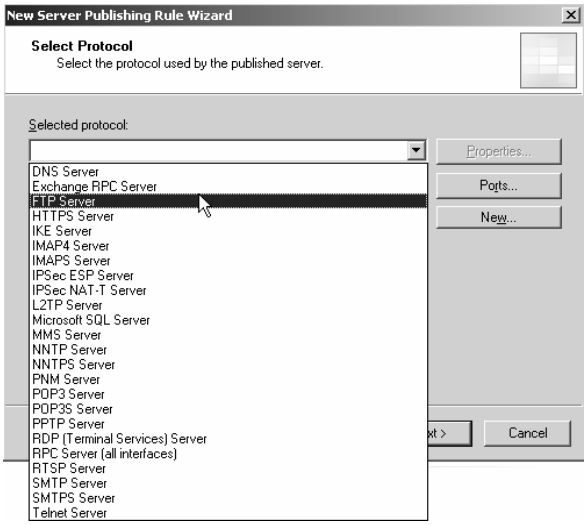
Hình 5.29: Mô hình tạo luật để **publish server**.

Các bước tạo một **Publish Server**:

1. Kích hoạt màn hình "M**icrosoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Create New Server Publishing Rule**", hiển thị hộp thoại "**Welcome to the New Server Publishing Rule Wizard**" yêu cầu nhập tên **Server Publishing** Rule, chọn **Next** để tiếp tục.
3. Chỉ định địa chỉ của server nội bộ cần để **publish**, chọn **Next** để tiếp tục.

Hình 5.30: Chỉ định địa chỉ của **Server** để **publish**.

4. Chọn **Protocol** cần để **Publish**, chọn **Next**.



Hình 5.31: Chọn **protocol**.

5. Chọn tên **Interface** cho phép chấp nhận kết nối **Incoming Web**, sau đó ta có thể chọn nút **Address** để chỉ định địa chỉ IP cụ thể trên **interface** đã lựa chọn, Chọn nút **Add>** (tham khảo hình 5.24), cuối cùng ta chọn nút **OK** để chấp nhận quá trình tạo mới **Web Listener**, chọn **Next** để tiếp tục.
6. Chọn **Finish** để hoàn tất quá trình.

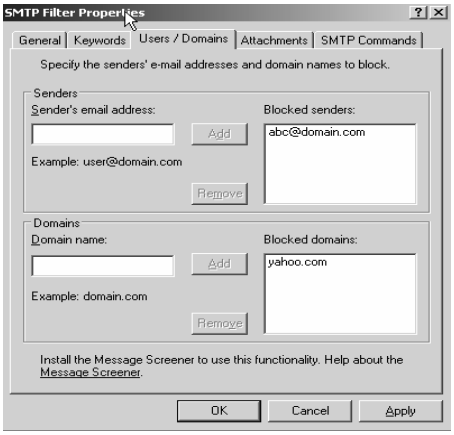
V.6. Kiểm tra trạng thái và bộ lọc ứng dụng.

ISA firewall có thể thực thi được hai chức năng quan trọng **stateful filtering** và **stateful application layer inspection**. **stateful filtering** kiểm tra và thiết lập bộ lọc tại tầng **network**, **transport**. **Stateful filtering** thường được gọi là bộ kiểm tra trạng thái **packet** (***stateful packet inspection***). Trái ngược với phương thức **packet filtering** dựa trên **hardware firewalls**, **ISA firewall** có thể kiểm tra thông tin tại tầng ứng dụng (**stateful application layer inspection**). **stateful application layer inspection** yêu cầu **Firewall** có thể kiểm tra đầy đủ thông tin trên tất cả các tầng giao tiếp bao gồm hầu hết các tầng qua trọng và **application layer** trong mô hình tham chiếu **OSI**.

V.6.1 Lập bộ lọc ứng dụng.

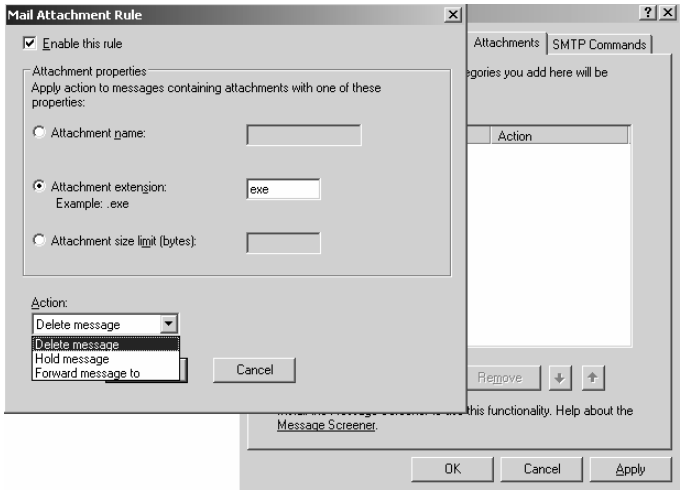
ISA firewall thiết lập bộ lọc ứng dụng (**Application filters**) với mục đích bảo vệ các **publish server** chống lại một số cơ chế tấn công bất hợp pháp từ bên ngoài mạng, để hiệu chỉnh bộ lọc ta chọn mục **Add-ins** trong **Configuration Panel**, sau đó ta nhấp đôi chuột vào tên bộ lọc cần hiệu chỉnh,…Một số các bộ lọc ứng dụng cần tham khảo như:

- **SMTP filter and Message Screener: SMTP filter** và **Message Screener** được sử dụng để bảo vệ **publish SMTP server** chống lại cơ chế tấn công làm tràn bộ nhớ (**buffer overflow attacks**), **SMTP Message Screener** bảo vệ mạng nội bộ ngăn một số **E-mail messages** không cần thiết.
- Dùng **SMTP filter** để ngăn chặn địa chỉ Mail hoặc **domain** truy xuất **Publish STMP Server** (tham khảo hình 5.32)



Hình 5.32: ngăn chặn **Users/domain** sử dụng **SMTP**.

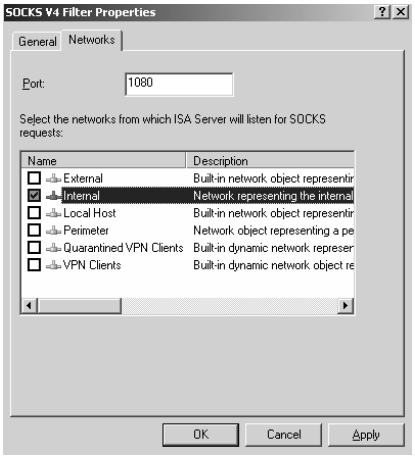
- Dùng **SMTP filte**r để ngăn chặn gởi file đính kèm (tham khảo hình 5.33), ta có thể xóa, lưu giữ **message**, chuyển **message** đối với file đính kèm có tên file giống với tên được mô tả trong **Attachment name:**, hoặc file đính kèm có phần mở rộng được mô tả trong **Textbox Attachment Extensions**, hoặc file đính kèm có kích thước lớn hơn hay bằng kích thước mô tả trong **textbox Attachment size limit (bytes):**,



Hình 5.33: ngăn chặn **Users/domain** sử dụng **SMTP**.

- **DNS filter:** Được sử dụng để bảo vệ **Publish DNS Server** để ngăn, chống lại một số cơ chế tấn công từ bên ngoài vào dịch vụ **DNS**.
- **POP Intrusion Detection filter:** Được sử dụng để bảo vệ **Publish POP Server** để ngăn, chống lại một số cơ chế tấn công từ bên ngoài vào dịch vụ **POP**.
- **SOCKS V4 filter:** được sử dụng để chấp nhận yêu cầu kết nối **SOCKS version 4**. **SOCKS v4 filter** mặc định không được kích hoạt. Thông thường hệ thống Windows không cần sử dụng SOCKS filter vì ta có thể cài đặt **Firewall client** trên các máy mà ta muốn chứng thực trong suốt (**transparently authenticate**) với **ISA firewall**. Ta có thể enable **SOCK v4 fileter** để cung cấp dịch vụ **SOCK** cho các **host** không thể cài đặt **Firewall clients** như **Linux** và **Mac hosts**. Để **enbale SOCK services** ta nhấp đôi chuột vào mục **SOCK V4 Filter**, sau đó chọn tùy chọn **Enable**

this filter, chọn **Networks Tab** để chọn **interface** trên **ISA Firewall** cho phép **listen** tại **port 1080.**



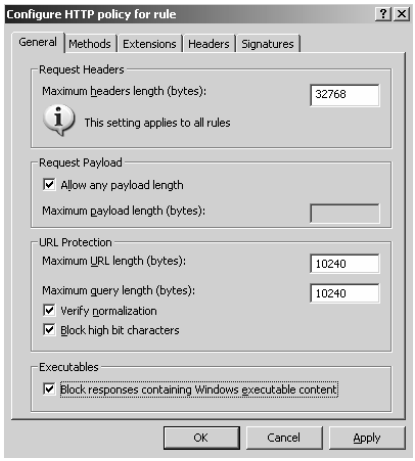
Hình 5.32: Kích hoạt **SOCK Service**.

V.6.2 Thiết lập bộ lọc Web.

ISA firewall Web filters được sử dụng để **ISA firewall** lọc các kết nối thông qua giao thức **HTTP**, **HTTPS**, and **FTP tunneled** (**Web proxied**).

HTTP Security filter: Là một trong những kỹ thuật chính yếu để thiết lập bộ lọc ứng dụng, **HTTP Security filter** cho phép **ISA firewall** thực hiện một số cơ chế kiểm tra thông tin ứng dụng (**application layer inspection**) dựa trên tất cả các **HTTP traffic** qua **ISA firewall** và chặn các kết nối không phù hợp với yêu cầu được mô tả trong **HTTP security**, để thay đổi **HTTP Security Filter** ta nhấp đôi chuột vào **Web Publishing Rule** | **Traffic Tab** | **Filtering** | **Configure HTTP**.

- **General Tab**: Quy định chiều dài tối đa của **HTTP Request Header**, **URL Length**, giới hạn thông tin trả về có chứa các code thực thi,..
- **Methods Tab**: Điều khiển các HTTP method như: **GET**, **PUT**, **POST**, **HEAD**, **SEARCH**, **CHECKOUT**,…
- **Extensions Tab**: Giới hạn **file extensions** trong các thông tin **request** của **user**, như ta có thể block các **user** truy xuất file có phần mở rộng là .exe, .com, .zip.
- **Headers Tab**: Giới hạn **HTTP header** trong các thông tin yêu cầu cũng như thông tin trả lời từ **Web client**.
- **Signatures Tab**: Cho phép điều khiển truy xuất dựa vào **HTTP signature**. Thông tin chữ ký (**signatures**) dựa vào chuỗi ký tự có trong **HTTP communication**.



Hình 5.32: Cấu hình **HTTP policy**.

ISA Server Link Translator: Link Translator là một trong những kỹ thuật được xây dựng sẵn trong **ISA firewall Web filter** để thực hiện biến đổi địa chỉ **URL** cho các kết nối của **user** bên ngoài truy xuất vào **Web publishing** nội bộ, **Link Translation dictionary** được tạo khi ta kích hoạt (**enable**) **link translation** cho **Web Publishing Rule**. Một số **Link Translator dictionary** mặc định:

- Bất kỳ sự kiện nào xảy ra trên **Web Site** được chỉ định trong **Tab To** của **Web Publishing** Rule được thay thế bằng một tên **Web Site** (hoặc địa chỉ **IP**). Ví dụ, nếu ta đặt một luật cho **Web Publishing** là chuyển tất cả các **incoming request** theo địa chỉ http://www.microsoft.com của **Client** truy xuất vào **ISA Server** thì sẽ chuyển tới **Web Server** nội bộ có tên là SERVER1 (có địa chỉ192.168.1.1), khi đó **ISA Server** sẽ thay thế tất cả các **response** của http://SERVER1 thành địa chỉ http://www.microsoft.com gởi trả lại cho **Client** bên ngoài.
- Nếu không chỉ định **port** mặc định trên **Web listener**, thì **port** đó sẽ được gởi trả lại cho **Client**. Ví dụ, nếu có chỉ định **port** mặc định trên **Web listener** thì thông số **port** sẽ được loại bỏ khi thay thế địa chỉ **URL** trong trang trả về (**response page**). Nếu **Web listener** lắng nghe (**listening**) trên port 88 của giao thức **TCP** thì thông tin trả về cho **Web Client** có chứa giá trị port 88 của giao thức **TCP**.
- Nếu **Client** sử dụng **HTTPS** gởi yêu cầu đến **ISA firewall** thì **firewall** sẽ thay thế **HTTP** thành **HTTPS** gởi trả về **Client**.
- Ví dụ: Giả sử **ISA firewall publish** một site trên máy có tên là SERVER1. **ISA firewall publish** site sử dụng tên chính (**public name**) là www.msfirewall.org/docs. **External Web client** gởi một **request** với thông tin "GET /docs HTTP/1.1Host: www.msfirewall.org" Khi **Internet Information Services** (**IIS**) **Server** nhận **request** thì nó sẽ tự động trả về mã số 302 **response** với **header** được mô tả là http://SERVER1/docs/, đây là tên nội bộ (**Internal Name**) **Web server**. **Link Translator** của **ISA firewall** sẽ thay đổi (**translates**) **header** trả lời (**response header**) với giá trị là http://www.msfirewall.org/docs/. Trong ví dụ trên thì một số thông tin (**entries**) sẽ tự động thêm vào **Link Translation dictionary**:

http://SERVER1 --> ***http://www.msfirewall.org***

http://SERVER1:80 --> ***http://www.msfirewall.org***

https://SERVER1 **-->** https://***www.msfirewall.org***

- Nếu **ISA firewall publish** một site sử dụng **Web listener** không phải trên **port** mặc định (**nondefault ports**) (ví dụ: 85 cho HTTP và 885 cho SSL),thì địa chỉ **URL** sẽ được thay đổi như sau theo các mục ánh xạ địa chỉ URL như sau:

http://SERVER1 **-->** http://www.msfirewall.org:85

http://SERVER1:80 **-->** http://www.msfirewall.org:85

https://SERVER1 **-->** https://www.msfirewall.org:885

https://SERVER1:443 **-->** https://www.msfirewall.org:885

V.6.3 Phát Hiện Và Ngăn Ngừa Tấn Công.

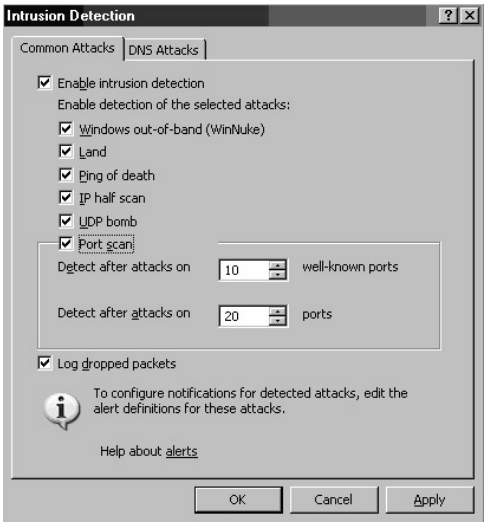
- Một số phương thức tấn công thông dụng:

Denial-of-Service Attacks: Là kiểu tấn công rất lợi hại, với kiểu tấn công này ,bạn chỉ cần 1 máy tính kết nối đến **internet** là đã có thể thực hiện việc tấn công đối phương. thực chất của **DoS** là **attacker** sẽ chiếm dụng 1 lượng lớn tài nguyên trên **Server** làm cho **Server** không thể nào đáp ứng yêu cầu của người dùng khác và **Server** có thể nhanh chóng bị ngừng hoạt động hay bị treo. **Attacker** làm tràn ngập hệ thống có thể là bằng tin nhắn, tiến trình, hay gửi những yêu cầu đến hệ thống mạng từ đó buộc hệ thống mạng sẽ sử dụng tất cả thời gian để khứ hồi tin nhắn và yêu cầu. nhiều lúc dẫn đến việc bị tràn bộ nhớ. Khi sự làm tràn ngập dữ liệu là cách đơn giản và thông thường nhất để phủ nhận dịch vụ thì 1 **attacker** không ngoan hơn sẽ có thể tắt dịch vụ, định hướng lại và thay thế theo chiều hướng có lợi cho **attacker.**

SYN Attack/LAND Attack: bằng cách lợi dụng cơ chế bắt tay đối với một số dịch vụ dựa trên chuẩn giao thức **TCP**, **Client** tấn công theo kiểu **SYN attack** bằng cách gởi một loạt **SYN packets** mà có địa chỉ nguồn giả, điều này **Client** có thể làm tràn ngập (**flooded**) hàng đợi **ACK** của gói **SYN/ACK** gởi cho **Client** từ **Server**, đến một lúc nào đó **Server** sẽ bị quá tải.

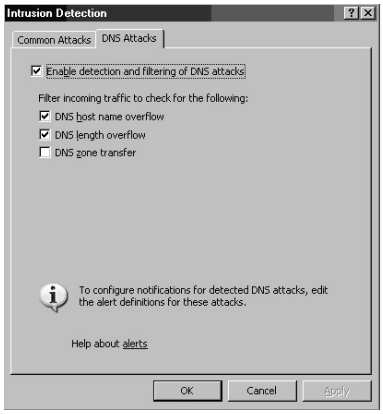
Ngoài ra còn có một số phương thức tấn công khác như: Ping of Death, **Teardrop**, **Ping Flood** (**ICMP Flood**), **SMURF Attack**, **UDP Bomb**, **UDP Snork Attack**, **WinNuke** (**Windows Out-of-Band Attack**), **Mail Bomb Attack**, **Scanning and Spoofing**, **Port Scan**.

Để cho phép **ISA Firewall** có thể **dectect** và ngăn một số phương thức tấn công trên ta truy xuất vào hộp thoại **Intrusion Detection** bằng cách mở giao diện "**Microsoft Internet Security and Acceleration Server 2004 management console**", chọn nút **Configuration**. Chọn nút **General,** sau đó ta nhấp chuột vào liên kết "**Enable Intrusion Detection and DNS Attack Detection"** (tham khảo hình 5.33)



Hình 5.33: Phát hiện một số cơ chế tấn công.

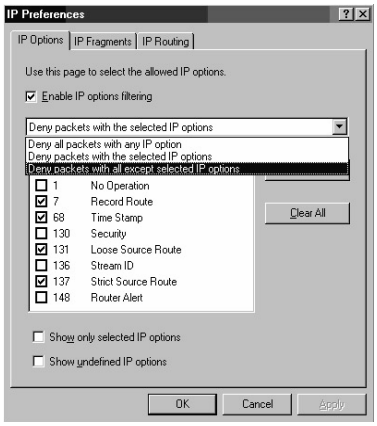
Chọn **DNS Attacks Tab** để hiệu chỉnh một số phương thức ngăn, ngừa tấn công theo dịch vụ **DNS** (tham khảo hình 5.34).



Hình 5.34: Phát hiện và ngăn tấn công DNS.

- **IP option filtering**.

Ta có thể thiết lập một số bộ lọc cho giao thức **IP** để chống lại một số cơ chế tấn công dựa vào một số tùy chọn của giao thức này. Để cấu hình ta chọn liên kết **Define IP preferences** trong nút **Configuration** (tham khảo hình 5.35).



Hình 5.35: IP option filtering.

V.7. Một số công cụ bảo mật.

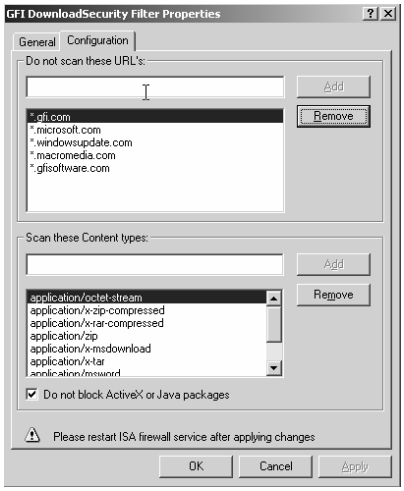
V.7.1 Download Security.

DownloadSecurity là một công cụ tích hợp với **ISA** được tổ chức **GFI Software LtdGFI** phát triển. **DownloadSecurity** được thiết kế để tăng cường khả năng kiểm soát và quản lý thông tin **download** từ **Internet**. Một số chức năng về **DownloadSecurity**:

- **Scan viruses** cho tất cả các tập tin được **download** từ **internet**.
- Tự động cập nhật **Anti-virus signature**.
- Tự động kiểm tra một số loại file nguy hiểm như *.exe, *.doc,…
- Cung cấp cơ chế cảnh báo an ninh cho người quản trị.
- Được tích hợp với **ISA Firewall**, dễ quản lý và cấu hình.
- Tính hiệu quả cao trong việc thực hiện một số chức năng như lọc nội dung, chống virus, kiểm soát truy xuất internet.
- Cung cấp cơ chế cảnh báo **user** hoặc trình duyệt chặn một số **ActiveX Control** và **Java applet** nguy hiểm.
- Phân tích các đoạn code thực thi nguy hiểm để chống **Trojans**.
- Cấu hình **ISA Web Filtering**.

Mặc định sau khi ta cài phần mềm **DownloadSecurity**, **DownloadSecurity** sẽ tự động được kích hoạt để hỗ trợ thiết lập bộ lọc **Web Filters**. Để hiệu chỉnh bộ lọc ta chọn **Configuration | Add-ins | Web Filters | GFI DownloadSecurity Filter | Configuration Tab** (tham khảo Hình 5.36).

- **Do not scan these URLs:** Chỉ định danh sách địa chỉ **URL** không cần kiểm tra nội dung và virus.
- **Scan these Content types:** Chỉ định loại nội dung cần kiểm tra bao gồm các đoạn code có thể thực thi, **Java applets**, **ActiveX Control**.

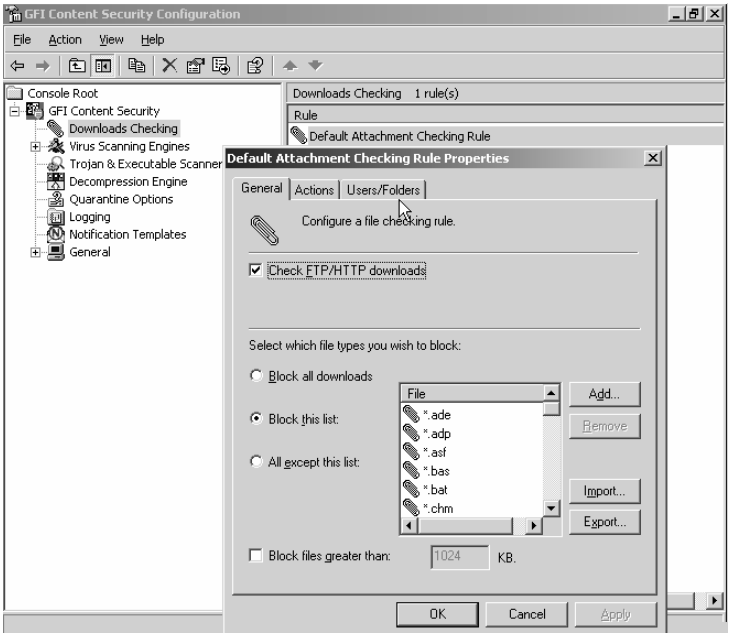


Hình 5.36: Download security Web Filter.

Thiết lập một số chính sách kiểm tra **download**.

Thiết lập chính sách kiểm tra **download** để giới hạn hoặc cô lập loại **file**, dung lượng **file download**,… để thay đổi luật **download** mặc định trong hệ thống bằng cách chọn **Start | Programs | GFI DownloadSecurity | DownloadSecurity Configuration | Download Checking**, Nhấp đôi chuột vào rule có tên **"Default Attachment Download Checking Rule"** (tham khảo hình 5.37)

- **General Tab:** Cho phép lựa chọn một số chế độ cấm **download**, cấm **download** các tập tin có dung lượng lớn hơn dung lượng định nghĩa.
- **Actions Tab:** Hiệu chỉnh các **Action** khi cấm như thông báo Mail, quản lý thông báo qua mail, ghi nhận nhật ký,…
- **Users/Folders Tab:** Chọn **User** hoặc thư mục cần thiết để thiết lập luật.

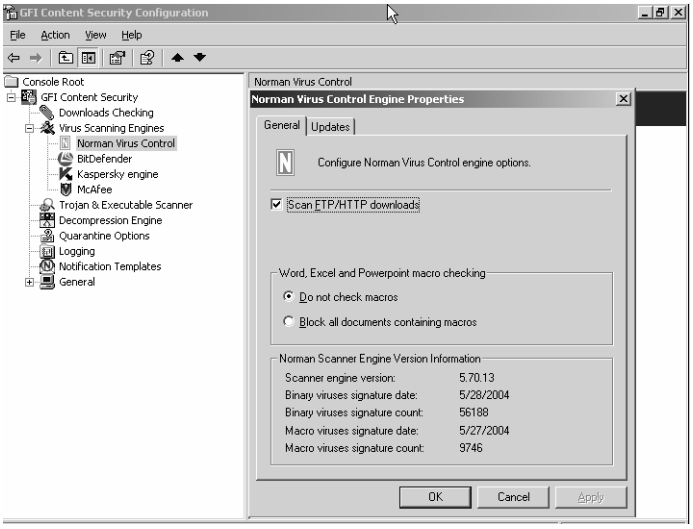


Hình 5.37: Thay đổi thuộc tính của **Download checking rule**.

Cấu hình kiểm tra **Virus**, chống **Trojans**.

DownloadSecurity tích hợp sẵn các chương trình kiểm tra và quét **virus** cho các **file download**, các chương trình này được cập nhận thường xuyên để có thể ngăn chặn sự tấn công của các loại **Virus** mới. Ngoài ra **DownloadSecurity** còn tích hợp một số scanners để **scan** và kiểm tra **Trojans**, đoạn mã thực thi nguy hiểm (**Executable**)

Để thay đổi hiệu chỉnh một số bộ kiểm tra **Virus** (**Virus Engine**) ta chọn **Start | Programs | GFI DownloadSecurity | DownloadSecurity Configuration | Virus Scanning Engines**, Nhấp đôi chuột vào một **engine** cụ thể (Tham khảo hình 5.38)



hình 5.38: Hiệu chỉnh thuộc tính của **Virus Control Engine**.

V.7.2 Surfcontrol Web Filter.

SurfControl Web Filter giúp nâng cao tính năng bảo mật, tối ưu hóa băng thông của hệ thống. **SurfControl Web Filter** thiết sẵn một group các đối tượng để cho phép ta quản lý và thiết lập luật để giới hạn truy xuất **Internet** dễ dàng hơn.

Một số công cụ hỗ trợ trong SurfControl Web Filter:

- **Monitor**: Cung cấp một số cách theo dõi và giám sát **traffic** của các **user** trong mạng, thông tin về giám sát hoạt động của **user** được lưu trong **SurfControl database**, chúng được hiển thị trong cửa sổ **the Monitor window**.
- **Real Time Monitor:** Giám sát và hiển thị **traffic** mạng theo thời gian thực.
- **Rules Administrator:** Cho phép ta có thể tạo luật để điều khiển truy xuất **internet**.
- **Scheduler:** Cho phép thiết lập lịch biểu để theo dõi sự kiện hệ thống.
- **Virtual Control Agent (VCA)**: Phân loại **Web site** theo nội dung truy xuất.
- **Report Central**: là công cụ mạng hỗ trợ tạo **report** để thống kê **traffic**.
- **Remote Administration:** Cho phép điều khiển từ xa **SurfControl Web Filter**.

Database của chương trình **SurfControl Web Filter** được lưu trên một hệ quản trị cơ sở dữ liệu, có thể là **MS SQL Se**rver, **msde2000**, do đó trước khi cài đặt **SurfControl Web Filter** ta cần phải cài đặt một trong hai hệ quản trị cơ sở dữ liệu trên.

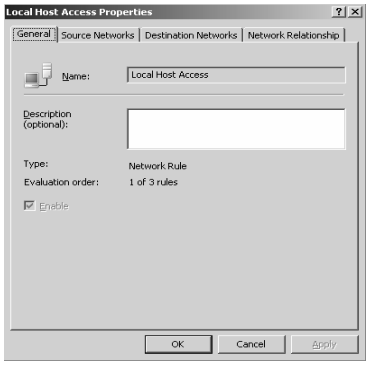
V.8. Thiết lập Network Rule.

Mặc định hệ thống tạo ra các **Network rule** để cho phép thiết lập một số cơ chế như định tuyến (**Route**) giữa hai mạng (tham khảo hình 5.39), thay đổi đĩa chỉ (**NAT**). Mặc định hệ thống tạo ra một số **Network rule** sau:

- **Local Host Access**: Định tuyến traffic localhost đến mạng nội bộ.
- **VPN Client to Internal Network**: Định tuyến từ **VPN Client** đến **Internal network**.
- **Internet Access**: **NAT Internal network** ra ngoài mạng **internet**.

V.8.1 Thay đổi thuộc tính của một Network Rule.

Để thay đổi thuộc tính của **Network Rule** ta nhấp đôi chuột vào tên luật trong **Network Rules tab** (tham khảo hình 5.39).

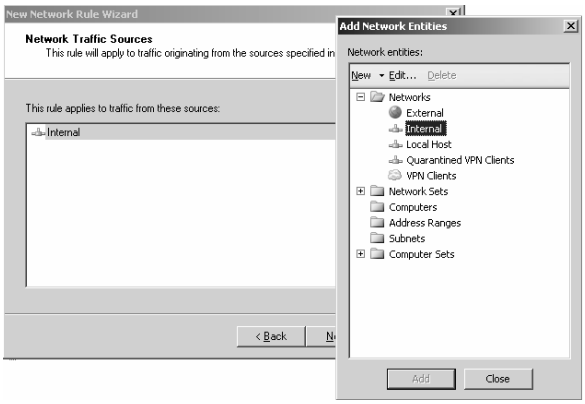


Hình 5.39: Thay đổi thuộc tính cho **Network Rule**.

V.8.2 Tạo Network Rule.

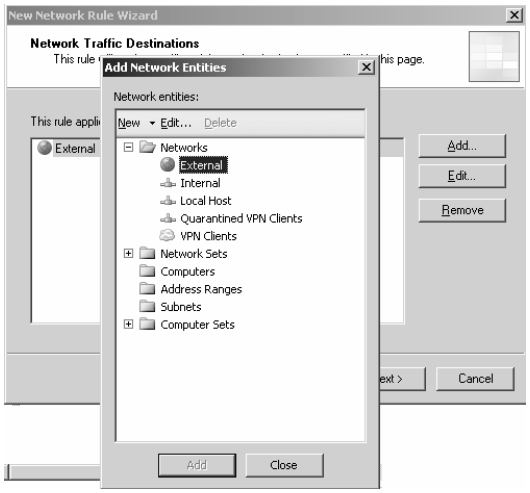
Để tạo **Network Rule** ta thực hiện các bước sau:

1. Chọn nút **Configuration**, chọn **Network**, chọn **Network Rules tab**, **Create a New Network Rule** trong **Task Panel**, chỉ định tên **Network Rule**, chọn **Next**.
2. Chỉ định địa chỉ nguồn trong hộp thoại **Network Traffic Source**.



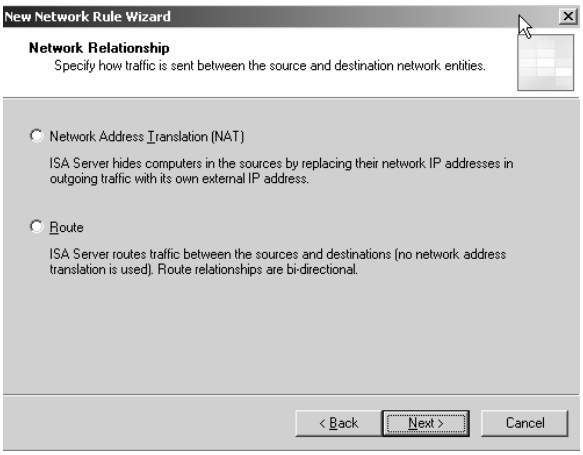
Hình 5.40: Chỉ định địa chỉ nguồn.

3. Chỉ định địa chỉ đích trong hộp thoại **Network Traffic Destination**.



Hình 5.41: Chỉ định địa chỉ đích cho **Network Rule**.

4. Chọn phương thức đặt **Network Rule** theo **NAT** (khi ta muốn **NAT** cho mạng nội bộ ra ngoài mạng **Internet**) hay **Route** (khi ta muốn định tuyến mạng nội bộ ra ngoài mạng khác)



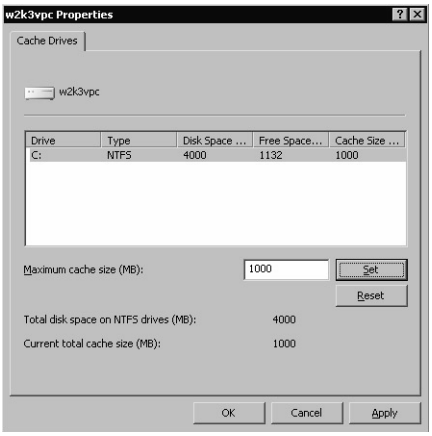
Hình 4.42: Chỉ định **Network Relationship**.

5. Chọn **Finish** để hoàn tất quá trình.

V.9. Thiết lập Cache, quản lý và theo dõi traffic.

V.9.1 Thiết lập Cache.

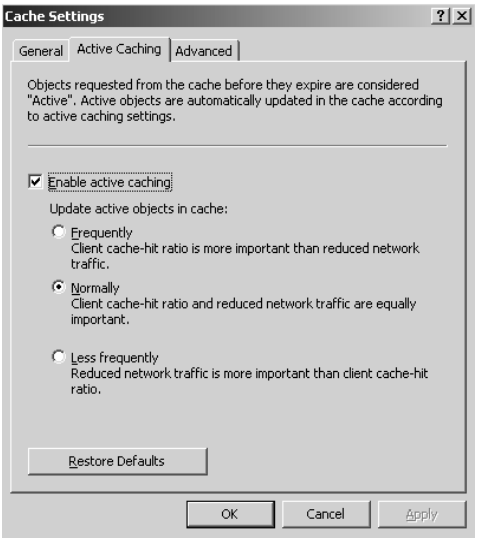
- Để cấu hình **Cache** ta chọn nút **Configuration -> Cache** của trình quản lý **ISA management**:
- Nhấp chuột phải vào nút **Cache** chọn **Define Cache Drives,** hoặc ta có thể nhấp chuột vào **Cache Rules** sau đó chọn **Define Cache Drives (enable caching)** từ **Tasks** panel**.**
- Trong hộp thoại **"Define Cache Drives"** chọn một ổ địa định dạng **NTFS** và chỉ định kích thước cache **Maximum cache size** , chọn nút **Set** (tham khảo hình 5.39).



Hình 5.43: Chỉ định dung lượng Cache.

V.9.2 Thay đổi tùy chọn về vùng Cache.

- Để cấu hình **Cache** ta chọn nút **Configuration -> Cache** của trình quản lý **ISA management**, nhấp chuột phải vào nút **Cache** chọn liên kết **Configure Cache Settings** từ **Tasks** panel, chọn **Active Caching** tab, chọn **Enable active caching** (tham khảo hình 5.40)**.**

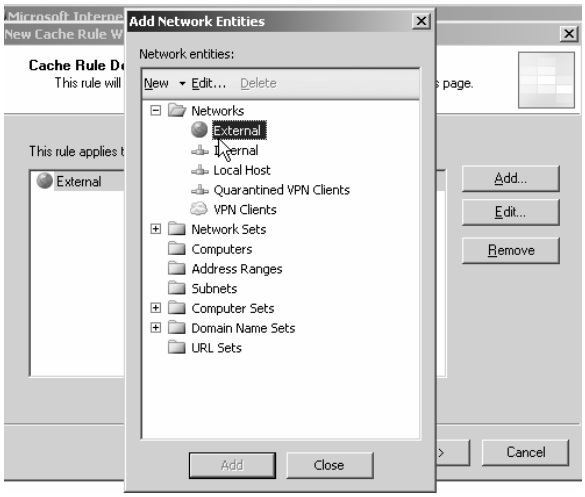


Hình 5.44: **Enable cache**.

V.9.3 Tạo Cache Rule.

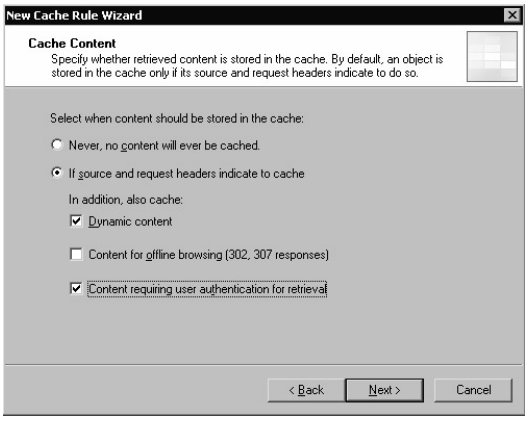
Tạo **Cache Rule** để cho phép ta có thể đặt một số luật quy định đối tượng (**Object**) cần **cache**, thời gian lưu trữ **cache**, kích thước của từng đối tượng **cache**, … Các bước tạo **cache rule** như sau:

1. Nhấp chuột phải vào nút **Cache**, chọn **New,** chọn **Cache Rule…**
2. Chỉ định tên **cache rule** trong hộp thoại **"Welcome to the New Cache Rule Wirzard**", chọn **Next**.
3. Chọn nút **Add** để chỉ **Distination** cho **Cache Rule** (tham khảo hình), chọn **Next**.



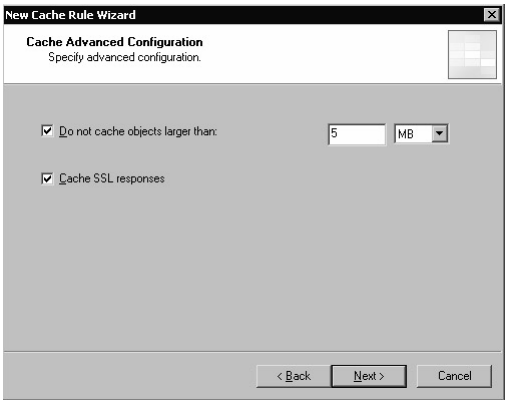
Hình 5.45: Destination cache.

4. Chỉ định loại **Object** nào được nhận cho một **request** cụ thể nào đó trong hộp thoại **Cache retrieval**. Một số tùy chọn cần lưu ý:
   + **"Only if a valid version of the object exists in the cache if no valid object exists, the request will be routed to the Web server"**: Cho phép nhận những **Object** hợp lệ (**Valid Object)** trong **cache** ngược lại tồn tại hoặc không tồn tại **Object** hợp lệ thì **request** sẽ được chuyển đến **Web Server** để nhận các **Object** cần thiết.
   + **"If any version of the object exists in the cache it will be returned from cache If no version exists route request server"** : Cho phép **request** có thể nhận **Valid Object** hoặc **Invalid Object** trong **cache**, nếu không có **Object** nào trong **cache** thì **Server** sẽ chuyển **request** tới **server**.
   + **"If any version of the object exists in cache if no exists the request will be dropped"** Nếu **request** yêu cầu một **Object** nào đó không tồn tại trong **cache** thì nó sẽ bị ngăn chặn (**Drop**)
5. Trong hộp thoại **Cache Content**, chỉ định nội dung cần lưu trong **cache**(tham khảo hình 5.41), chọn **Next**.



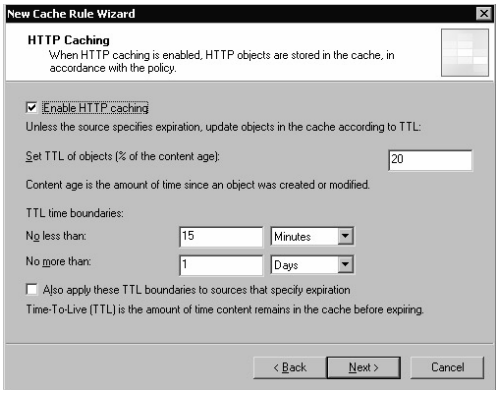
Hình 5.46: **cache content**.

6. Trong hộp thoại **Cache Advanced Configuration**, định giới hạn kích thước của các object cần được **cache** trong **textbox "Do not cache objects larger than"** (tham khảo hình 4.42), chọn **Next**.



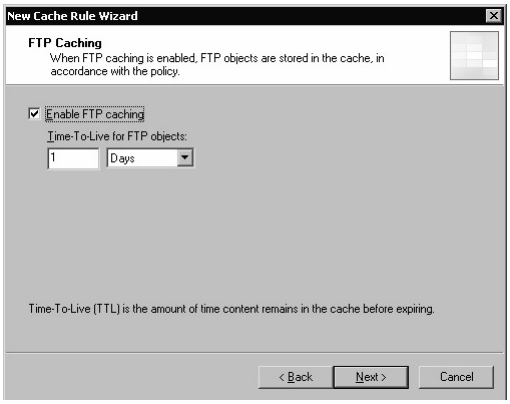
Hình 5.47: Giới hạn kích thước cho đối tượng **cache**.

7. Chỉ định thời gian lưu trữ **HTTP Object** trong **cache**, chọn **Next**.



Hình 5.48: Chỉ định **TTL** cho **HTTP Object**.

8. Chỉ định thời gian lưu trữ **FTP Object** trong **cache**, chọn **Next**.



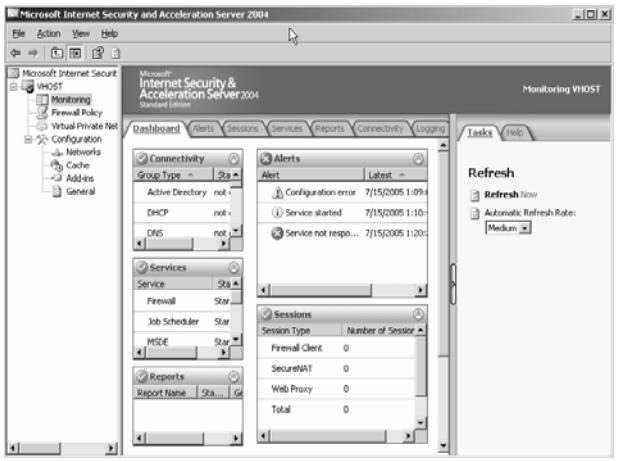
Hình 5.49: **TTL** của **HTTP Object**.

9. Chọn **Finish** để hoàn tất quá trình.

V.9.4 Quản lý và theo dõi traffic.

Một trong những chức năng qua trong của **Firewall** là khả năng giám sát (**monitoring**) và thống kê (**reporting**) sự kiện xảy ra trong hệ thống, nó giúp cho Người quản trị mạng (**Network administrator**) có thể theo dõi sự xâm nhập (**attempted intrusions**) và tấn công từ bên ngoài.

ISA Server 2004 bao gồm một số công cụ như: giám sát hoạt động của hệ thống (**monitor ISA Server activities**), tạo và cấu hình cơ chế cảnh báo, thống kê thông tin hệ thống, giám sát thông suất (**performance**) của **ISA Server**. Tất cả các công cụ này đề được đặt tại **Monitoring node** của trình quản lý **"ISA Server 2004 management console"** (tham khảo hình 5.44).



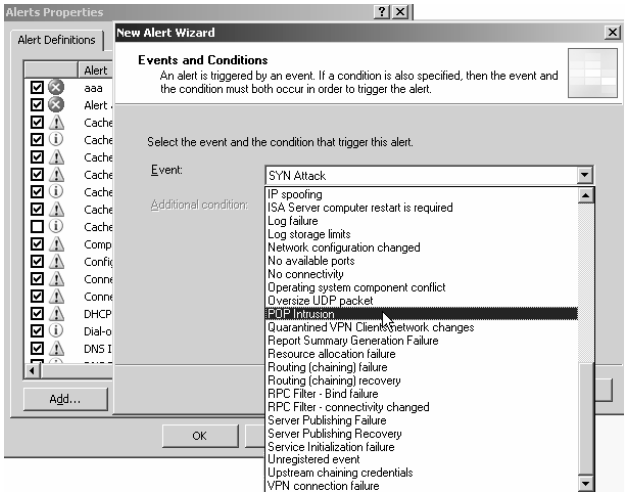
Hình 5.50: Dashboard theo dõi **log**.

Thiết lập một số cảnh báo (**alert**) cho hệ thống

+ Chọn **Tab Alerts**, chọn liên kết **Configure Alert Definitions** trên **Task** panel, chọn nút **Add** từ hộp thoại **Alert properties,** chỉ định tên **Alerts,** chọn **Next** (tham khảo hình 5.45).

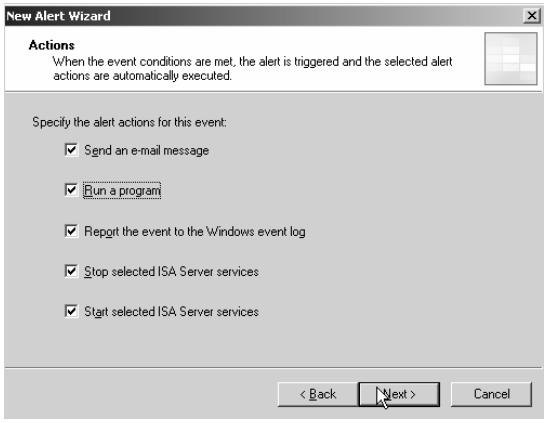
Hình 5.51: Lập cảnh báo cho hệ thống.

+ Chọn loại sự kiện để lập cảnh báo cho hệ thống, chọn **Next**.



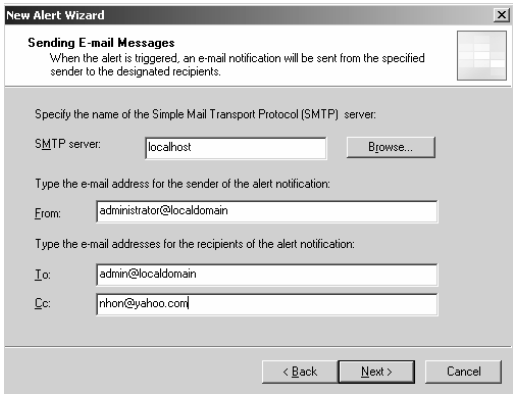
Hình 5.52: Chọn loại cảnh báo cho hệ thống.

+ Chỉ định loại cảnh báo (**Alert**) và mức độ kiểm soát (lỗi, cảnh báo, thông báo) trong hộp thoại **Category and Severity**, chọn **Next**.
+ Chỉ định các **action** để thực hiện cơ chế cảnh báo cho hệ thống, có thể cảnh báo qua Mail, chương trình, …(tham khảo hình 5.46)



Hình 5.53: Chọn cơ chế cảnh báo.

+ Chỉ định địa chỉ Email sẽ nhận cảnh báo của hệ thống, chọn **Next**.

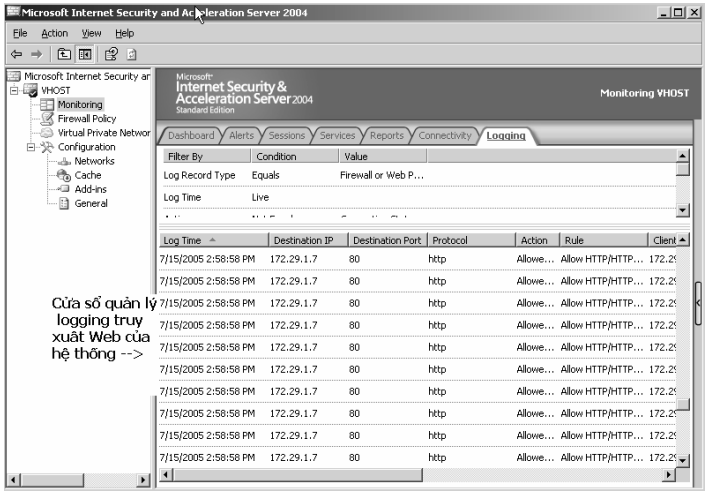


Hình 5.54: Chọn cơ chế cảnh báo.

+ Chọn dịch vụ sẽ bị **stop** khi **Alert** gặp sự cố, chọn **Next**.
+ Chọn **Finish để hoàn tất quá trình.**

Theo dõi thông tin truy xuất **Web** trong mạng nội bộ

Để theo dõi từng máy tình hoặc từng **host** trong mạng nội bộ truy xuất **internet** ta chọn **Logging Tab** từ màn hình chính của **Monitoring node** (tham khảo hình 5.47).



Hình 5.55: Theo dõi log truy xuất **Web**.

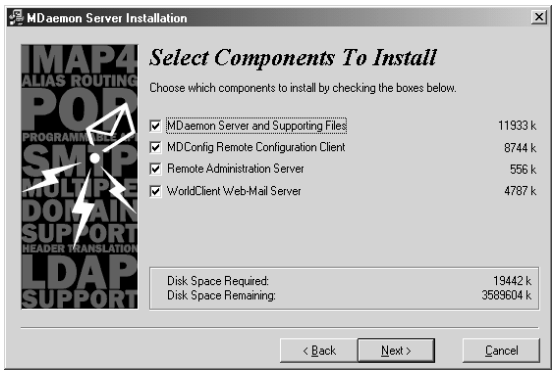
Tóm tắt

Lý thuyết 6 tiết - Thực hành 0 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này giúp cho học viên biết thêm một số phần mềm Mail Server và Proxy Server được sử dụng rộng rãi trên thị trường. Đồng thời học viên cũng có thể so sánh với các phần mềm đã học để có một lựa chọn chính xác khi triển khai trong một môi trường thực tế.	I. Phần mềm Mail Server - MDaemon II. Phần mềm Proxy Server - WinGate	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.	Dựa vào bài tập môn Dịch vụ mạng Windows 2003.

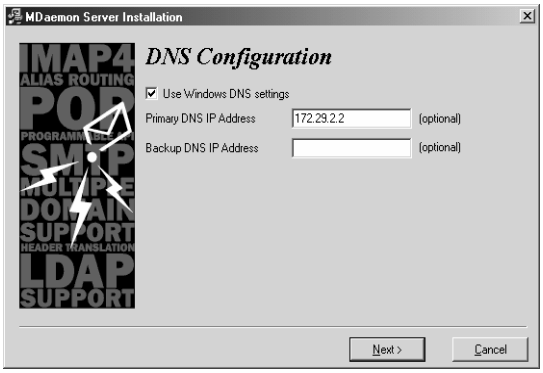
I. Cài Đặt Mdaemon.

1. Click vào tập tin cài đặt có tên **setup.exe** sau đó màn hình **License** sẽ hiện ra. Để tiếp tục, hãy nhấn nút **I Agree**.
2. Chọn thư mục để cài đặt, mặc định chương trình **MDaemon** sẽ cài vào ổ đĩa cài hệ điều hành. Ta có thể cài **Mdaemon** ở một vị trí khác bằng cách chọn nút **Browse**, chọn **Next** để tiếp tục việc cài đặt.
3. Nhập tên **user** và tên công ty, chọn **Next** để tiếp tục việc cài đặt.
4. Chọn các thành phần sẽ cài đặt
   - + **MDaemon server and supporting Files**: cài chương trình **Mdaemon Server**.
   - + **MDConfig Remote Configuration Client :** điều khiển những biến cấu hình **MDaemon** từ xa.
   - + **Remote Administration Server:** Quản trị **Mail Server** từ xa
   - + **WorldClient Web-Mail Server:** Cấu hình **Web-Mail Server** để cho phép những **Client** gửi/nhận mail ở bất kỳ nơi nào.



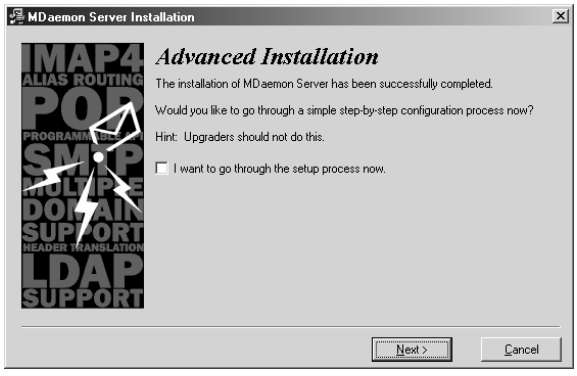
Hình 6.1: Chọn thành phần cài đặt.

5. Sau khi nhấn **Next**, trình **Setup MDaemon** sẽ sao chép các file vào thư mục đã chọn, tạo folder chương trình **MDaemon** và bước kế tiếp là cấu hình cho **MDaemon**.



Hình 6.2: Chỉ định **DNS Server**.

6. Cấu hình **DNS Server**: Trong quá trình cài đặt bạn không cần hoặc cần chỉ ra những **DNS Server** bằng cách chọn nút **Use Windows DNS Se**ttings. Sau đó, chỉ ra địa chỉ **IP** của **Primary DNS Server** và **Backup DNS Server**.
7. Nhập vào những thông tin của **user** để **MDaemon** tạo ta **account** trong quá trình setup.
   + **Full Name:** nhập vào tên đầy đủ của **account**. Ví dụ Tran Thanh Tri
   + **Mailbox:** địa chỉ Email của **account** (không bao gồm tên domain)
   + **Password:** nhập vào **password** cho **account** (Không có khoảng trắng)
   + **This account is the Postmaster:** chỉ định **account** này là **Postmaster alias**.
   + **This account has Administration level web access**: cho phép **account** này có quyền quản trị khi truy cập Mail qua **Web**.
   + Nhấn **Next để tiếp tục việc cài đặt.**
8. Chọn chế độ khởi động **MDaemon Server**: Nếu bạn muốn chương trình **MDaemon** khởi động khi máy tính bật lên thì chọn **Setup MDaemon as a system service**. Khi cấu hình ở chế độ này, bạn không cần **logon** vào **Server** để thao tác.
9. Tiếp theo là màn hình cho phép lựa chọn việc cấu hình theo hướng dẫn (**wizard**) hay không?

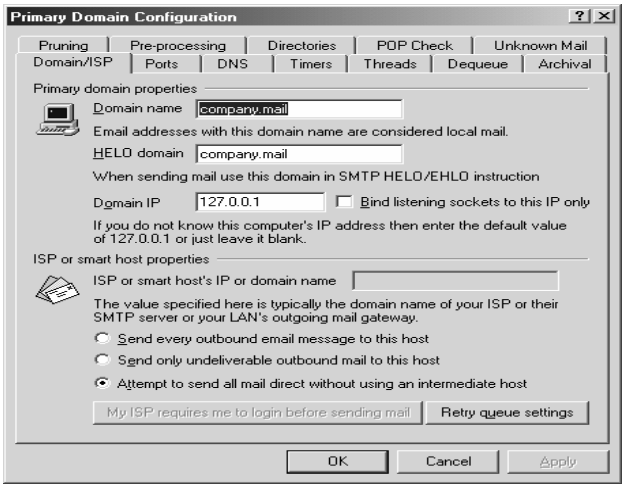


Hình 6.3 chọn chế độ **configure** qua **Wizard**.

II. Cấu hình Mail Server.

- Sau khi cài đặt chương trình **Mdaemon**, bước quan trọng kế tiếp là chúng ta phải cấu hình **Domain** của mình để người dùng trong **domain** có thể gửi/ nhận mail.

- Tất cả những thao tác cấu hình **domain** thông qua menu **Setup | Primary Domain.**



Hình 6.4: Cấu hình domain cho **Mail Server**.

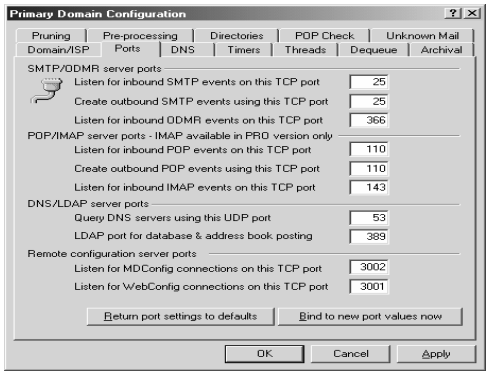
II.1. Cấu hình Domain/ISP.

Hộp thoại này lưu những thông tin về địa chỉ **IP** và **domain name**. Thêm vào đó, chúng ta sẽ chỉ ra mức độ mà **Mail Server** sẽ chuyển mail đến **ISP** hay **gateway**.

- **Domain Name:** Nhập vào tên **domain**. Tên **domain** này mặc định khi tạo **account** và nó được đăng ký trên **Internet**.
- **HELO domain:** Tên **domain** này sẽ được sử dụng trong câu lệnh **SMTP HELO/EHLO**.
- **Domain IP:** Địa chỉ **IP** của **Primary Domain**.
- **ISP or smart ...:** chỉ ra **ISP** của bạn hoặc tên của máy Mail hoặc địa chỉ **IP**. Thông thường, chúng ta chỉ ra địa chỉ IP của **SMTP Server ISP**.
- **Send every outbound ...:** tất cả những Mail gửi ra khỏi domain đều chuyển đến máy gateway. Máy **gateway** được chỉ ra trong ISP or smart...
- **Send only ...:** chỉ những Mail gửi ra ngoài mà không được chuyển đến đích sẽ được chuyển đến **Mail Gateway** chỉ ra trong **ISP or Smart**...
- **Attempt ...:** Gửi tất cả những **mail** ra ngoài đến một máy trung gian. Những **mail** không gửi được sẽ được gửi lại theo những cấu hình trong phần **Retry queue setting**.

II.2. Cấu hình Ports.

Chỉ ra những port mà chương trình **Mdaemon** giám sát. Và những **port** mà chúng ta cấp cho **SMTP**, **POP**, **IMAP** hay **UDP** để truy vấn **DNS**. Thông thường, chúng ta không thay đổi những thông số mặc định này.

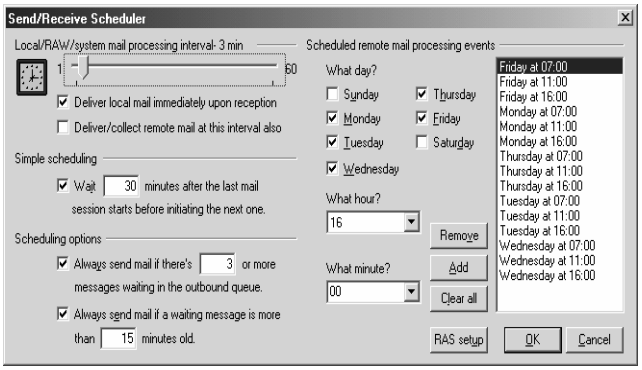


Hình 6.5: Chỉ định giá trị **Port**.

III. Cấu hình lịch kết nối và dịch vụ quay số.

III.1. Lập lịch kết nối.

- Click vào menu **Setup** | **Send/receive scheduling**



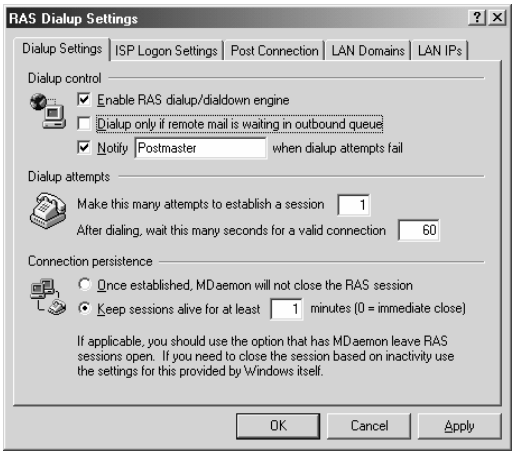
Hình 6.6: Lập lịch biểu kết nối quay số.

- **Local/RAW/system mail processing interval- 3 min**: thời gian nghỉ giữa các giao dịch xử lý Mail là 1 – 60 phút.
  + **Deliver/collect remote mail...:** nếu **checkbox** này được chọn thì thời gian phân phối/tập hợp mail sẽ dựa trên **Local/RAW/system mail**.... Ngược lại, nó sẽ hoạt động dựa trên lịch mà chúng ta lập.
  + **Deliver local mail... :** xử lý và phân phát ngay sau khi một giao dịch **SMTP** hoàn thành. Điều này có tác dụng phân phát Mail cục bộ ngay lập tức.
- **Simple scheduling:** thời gian nghỉ giữa lần giao dịch Mail cuối cùng được **start** trước khi khởi tạo một giao dịch mới.

+ **Scheduling options:** Hiệu chỉnh tùy chọn về lịch biểu.
+ **Always send mail if there's ...: Mdaemon** sẽ khởi tạo một giao dịch nếu trong hàng đợi ra ngoài có từ **xx messages** trở lên.
+ **Always send mail if a waiting...: Mdaemon** sẽ khởi tạo một giao dịch nếu có một **message** trong hàng đợi ra ngoài đợi đến số phút chỉ định.
+ **Scheduled remote mail ...:** lập lịch để **Mdaemon** xử lý Mail bao gồm ngày, giờ, phút.

III.2. Cấu hình Quay số.

- Click vào **Setup | Dialup/Dialdown**.



Hình 6.7: Cấu hình kết nối quay số.

- Dialup Settings.
- ISP Logon Settings.
- Post Connection.
- LAN Domains.
- LAN Ips.

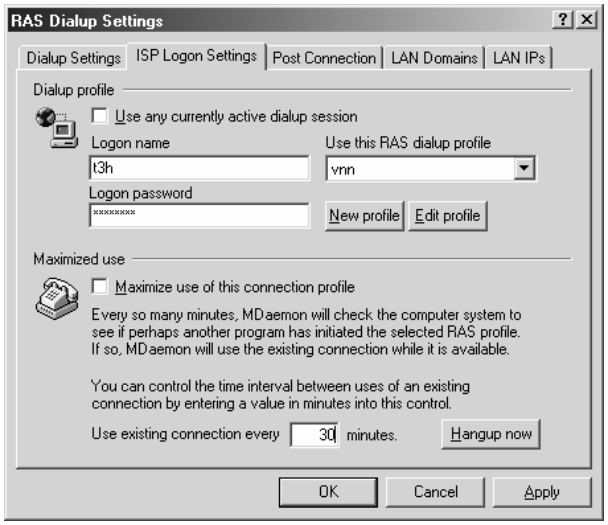
III.2.1 Dialup Settings.

- **Dialup control**:
  + **Enable RAS Dialup/Dialdown Engine**: Chọn tuỳ chọn này cho phép dùng dịch vụ **RAS** kết nối vào **ISP** để gửi và nhận thư.
  + **Dialup Only if Remote Mail is Waiting in Outbound Queue** Chọn tuỳ chọn này để **MDaemon** chỉ quay số kết nối khi có thư gửi ra (**outbound message**) trong hàng đợi chờ gửi. Tuỳ chọn này cho phép tiết kiệm thời gian quay số tuy nhiên nếu không quay số thì **MDaemon** sẽ không lấy được thư từ bên ngoài gửi vào.
  + **Notify Postmaster When Dialup Attempts Fail** Gửi thông báo đến **Postmaster** xử lý khi có lỗi không quay số được.
- **Dialup attempts**:

+ **Make This Many Attempts To Establish A Session:** Số lần thử quay số kết nối máy ở xa.
+ **After Dialing, Wait This Many Seconds For A Valid Connection**: Thời gian **MDaemon** chờ cho máy ở xa trả lời và hoàn thành kết nối **RAS**.

- **Connection persistance**:
  + **Once Established, MDaemon Will Not Close The RAS Session** Mặc định **MDaemon** sẽ đóng phiên kết nối **RAS** sau khi việc gửi nhận Mail với máy ở xa hoàn tất. Đánh dấu tuỳ chọn này cho phép phiên làm việc cho dù đã hoàn thành việc gửi nhận.
  + **Keep Sessions Alive For At Least XX Minutes** Thời gian giữ kết nối trước khi đóng.

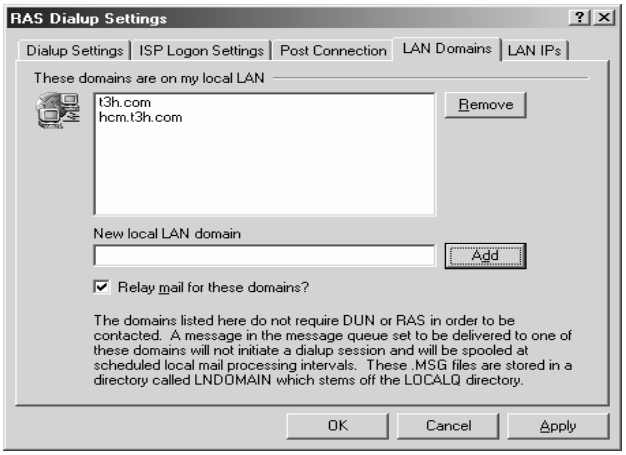
III.2.2 ISP Logon Settings.



Hình 6.8: Chỉ định **Account** kết nối quay số.

- **Logon Name:** Tên logon dùng để chuyển cho máy ở xa trong quá trình đăng nhập
- **Password:** Mật khẩu dùng để chuyển cho máy ở xa trong quá trình đăng nhập
- **Use This RAS Dialup Profile:** Tên **profile** đã tạo dùng cho kết nối từ xa trong cửa sổ **Dialup Networking**.
- **Maximize Use of this Connection Profile:** Cho phép **MDaemon** theo dõi **profile** được mô tả ở trên, trong trường hợp **profile** này đang dùng để kết nối thì **Mdaemon** sẽ dùng luôn kết nối này để gửi nhận Mail mà không theo lịch.
- **New Profile:** Tạo mới **profile Dialup Networking**.
- **Edit Profile:** Sửa **profile Dialup Networking**.
- **Hang-up Now:** Ngắt kết nối **RAS** với **ISP**. Nút này chỉ sáng lên khi đang có kết nối.

III.2.3 LAN Domains.



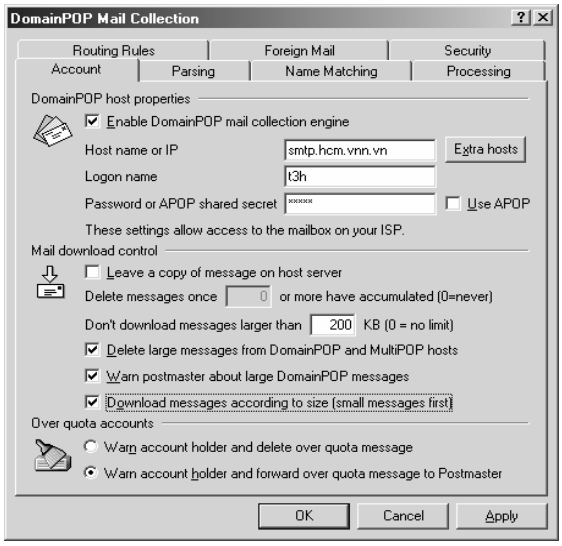
Hình 6.9: Chỉ định tên **domain** cho **Mail Server** quản lý.

- **These Domains Are On My Local LAN** Các domain liệt kê ở đây được **MDaemon** xem như domain cục bộ của mạng cục bộ **LAN**. Như vậy không cần phải quay số khi có thư gửi cho **domain** cục bộ.
- **New Local LAN Domain** Thêm 1 tên **domain LAN** cục bộ và nhấn nút **ADD**.
- **Relay Mail For These Domains** Nếu chọn tuỳ chọn này **MDaemon** sẽ chuyển tiếp mail cho các **domain** trên.

IV. Cấu hình DomainPOP Mail.

Cấu hình **DomainPOP** nhằm mục đích nhận mail từ **POP mailbox** từ **ISP** để phân phát lại cho người dùng trong **domain**.

- Từ menu **Setup** chọn **DomainPOP mail collection**...
- Chọn tab **Account** để khai báo những thông số.



Hình 6.10: Chỉ định **pop Mail Server**.

- **DomainPOP host properties**.

+ **Enable Domain Pop Mail Collection:** Chọn tuỳ chọn này cho phép **MDaemon** lấy thư từ hộp thư trên **POP server** của **ISP** về phân phát lại cho các **user** nội bộ.
+ **Host name or IP:** Tên **DNS** hoặc địa chỉ **IP** của máy chủ **POP** của **ISP**.
+ **Logon name/Password:** Tên **user** và mật khẩu dùng để lấy thư trên máy chủ **ISP**.

- **Mail download control**.
  + **Leave a copy of message on host server:** nếu chọn, **Mdaemon** sẽ không xóa những mail được tập hợp từ **ISP**.
  + **Don't download messages larger than [XX] KB (0 = no limit) :** không **download** những messages > xx KB.
  + **Delete large messages from DomainPOP and MultiPOP hosts: Mdaemon** sẽ xóa những message có kích thước vượt quá qui định bằng cách xóa chúng từ **DomainPOP** và không **download** về.
    - **Warn postmaster about large DomainPOP messages: gửi một thông báo đến Postmaster khi có một message lớn được phát hiện trong DomainPOP mailbox.**
  + **Download messages according to size (small messages first):** cho phép **Mdaemon download message** theo kích thước từ nhỏ nhất đến lớn nhất.
- **Over quota accounts**.
  + **Warn account holder and delete over quota message**: nếu chọn, **Mdaemon** sẽ gửi **message** đến cho **user** khi dung lượng đĩa của **user** vượt quá giới hạn cho phép. Những **message** sau đó sẽ bị hủy.
  + **Warn account holder and forward over quota message to Postmaster**: nếu chọn, **Mdaemon** sẽ gửi **message** đến cho **user** và **Postmaster** thông báo dung lượng đĩa của **user** vượt quá giới hạn cho phép.

V. WorldClient Server.

- **World Client** là một giải pháp của **webmail**, cho phép các máy trạm có thể sử dụng mail thông qua trình duyệt Web, các **user** có thể truy cập Mail của mình ất cứ nơi nào.
- Các tính năng lợi của **workclient server**: cho phép tìm kiếm thư, đọc thư từ trình duyệt Web, Client có thể giao tiếp bằng nhiều ngôn ngữ, hỗ trợ cơ chế lưu địa chỉ, có thể quản lý các thư mục(chứa danh sách các Mail được lưu trữ), gởi nhận **file attachment**…
- Ngoài ra **world client** còn cung cấp:
  + **Calendar and scheduling system**(lập lịch biểu cho hệ thống)
  + **ComAgent's Instant Messaging System**: cung cấp các thông báo(**sound**, **visual alert**) khi có thư mới.

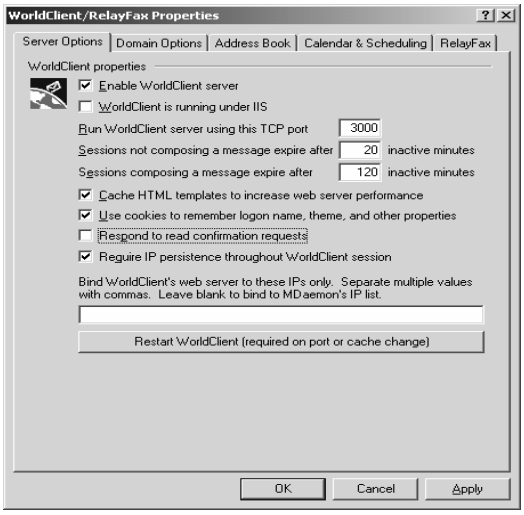
V.1. Cách Cấu Hình WorldClient server.

Khởi tạo **world client** ta chọn **Setup**->**WorldClient/RelayFax**… -> **Enable worldclient server**.

- **Login** vào **worldclient**:

+ Từ trình duyệt Web ta gõ địa chỉ http://<mailserver>:port. Thông thường **worldclient** mặc định được đặt **portnumber** là 3000.
+ Nhập vào **MDaemon account's user name and password**.
+ Chọn nút **Sign-in**.

- Thay đổi **WorldClient's Port**.
  + Chọn **Setup->WorldClient Server**…
  + Nhập vào **port number** trong hộp thoại "**Run WorldClient Server using this TCP Port**".
- Các thuộc tính của **worldclient**: Để xem các thuộc tính của **worldclient** ta thực hiện: Từ menu **setup** chọn **worldclient/relay fax**:
  + Server Options.
  + Domain Options.
  + Address Book.
  + Calendar & Scheduling.
  + RelayFax.



Hình 6.11: Thay đổi thuộc tính của **World Client**.

- **Server Options Tab**.

+ **Enable WorldClient server:** Nếu **checkbox** này được lựa chọn nghĩa là ta cho phép **workclient server** hoạt động ngược lại nếu ta không chọn tức là ta khoá **workclient server**(**disable**).
+ **WorldClient is running under IIS:** nếu tuỳ chọn này được chọn thì **WorldClient** được chạy dưới **Internet Information Server** (**IIS**) mà không chạy dưới **webserver** của **WorldClient**.
+ **Run WorldClient server using this TCP port**: Mặc định **WorldClient** sẽ lắng nghe kết nối từ **webbrowser** của **user** trên port**n**umber là 3000.
+ **Sessions not composing a message expire after xx inactive minutes:** định thời gian tồn tại cho một **session** khi một **user login** vào **worldclient** mà không gởi **message**.
+ **Sessions composing a message expire after xx inactive minutes:** định thời gian cho một **session** gởi thông điệp.
+ **Cache HTML templates to increase web server performance:** cho phép **worldclient** lưu trữ lại các mẫu **HTML** vào trong bộ nhớ để phục vụ cho các lần truy cập sau này của **browser**, điều này sẽ làm tăng thông suất của **server**.
+ **Use cookies to remember logon name, theme, and other properties:** cho phép sử dụng **cookies** để nhớ lại các thông tin của **user**(**logon name**, **theme** và những thông tin khác) tại máy tính cục bộ của người dùng.
+ **Respond to read confirmation requests**: tuỳ chọn này cho phép **worldclient** các thông điệp yêu cầu xác nhận thông tin.
+ **Require IP persistence throughout WorldClient session**: yêu cầu **session** của **user** phải sử dụng địa chỉ **IP** tĩnh khi **connect** tới **worldclient server**.
+ **Bind WorldClient's web server to these IPs only:** cho phép ta giới hạn **WorldClient server** lắng nghe trên các địa chỉ **IP** cụ thể nào. Chú ý rằng nếu ta chỉ định nhiều địa chỉ IP thì giữa chúng phải cách nhau bằng dấu phẩy. Nếu chúng ta không chỉ định địa chỉ IP nào thì mặc định **WorldClient** sẽ hoạt động trên các địa chỉ chỉ định cho miền **Primary** and **Secondary**.
+ **Restart WorldClient (required to recognize new TCP port):** cho phép khởi động lại **WorldClient server**. Chú ý: khi ta thay đổi cấu hình **Port** của **WorldClient** thì ta phải khởi động lại dịch vụ này.

V.2. Sử dụng WorldClient.

- **WorldClient** cho phép ta có thể sử dụng Mail bằng trình duyệt Web(còn gọi là **webmail**). để sử dụng Mail này ta truy cập vào địa chỉ http:// địa chỉ **IP** của **Server** hay địa chỉ **DNS** của **Server** kèm theo dấu ":" và số hiệu **Port**.
- Tuy nhiên ta có thể sử dụng cách truy cập thông thường vào địa chỉ **mailserver** mà không cần kèm theo số hiệu **Port** theo sau địa chỉ **URL**, để làm điều này ta phải hiệu chỉnh lại số hiệu **Port** cho phép **WorldClient** lắng nghe trên **Port 80**. Ví dụ http://www.nhon.com:3000

Hình 6.12: Truy cập **Web Mail**.

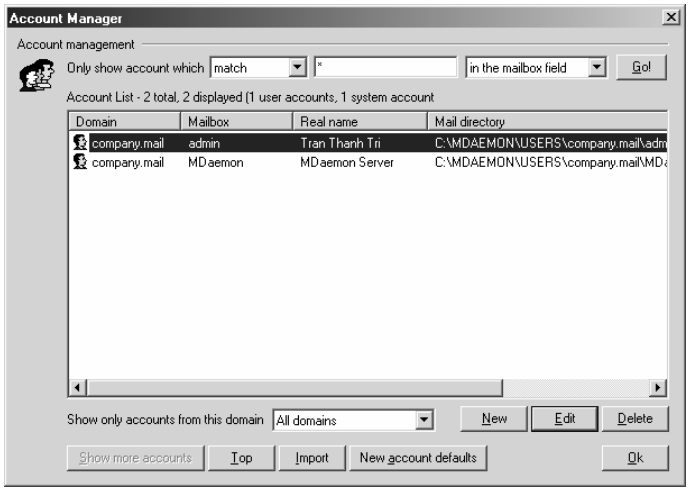
- Để **Logon** vào và sử dụng hệ thống ta phải được **Mail Server** cung cấp một **Account**. Sau khi nhập vào **Username** và **Password** chọn nút **Sign In**, lúc này màn hình sử dụng Mail được hiển thị.

Hình 6.13: Sử dụng **Web mail**.

VI. Quản trị người dùng.

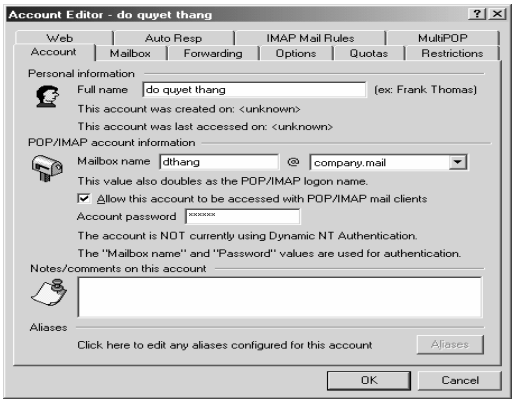
VI.1. Tạo và thay đổi thuộc tính người dùng.

- Tạo account bằng cách từ menu **Account** | **New account** hoặc **Account Manager**. **Account Manager** là một công cụ giúp quản lý những **account**.



Hình 6.14: Quản lý tài khỏan Mail.

- Khi tạo mới một **account** click vào nút **New**, chỉnh sửa hay hủy **account** thì chọn **account** sau đó click vào **Edit** hay **Delete**.



Hình 6.15: Tạo tài khoản Mail.

VI.1.1 Thông tin của Account.

- **Full name**: Họ tên đầy đủ. Các thông tin khác sẽ được phát sinh từ các macro. Có thể để nguyên hoặc sửa đổi nếu cần
- **Mailbox name**: tên hộp thư của **user**. Tên hộp thư này kết hợp với tên **domain** trong cấu hình **Setup\Primary Domain name** để tạo thành địa chỉ **E-mail** của **user** này theo dạng MailboxName@DomainName
- **Allow This Account To Be** : cho phép **user** truy cập hộp thư bằng các phần mềm **POP3 Client** như **Eudora** hoặc **Outlook Express**.
- **Account password**: mật khẩu cho **user** dùng khi truy cập bằng **POP3 client**.
- **Note/Comment**...:

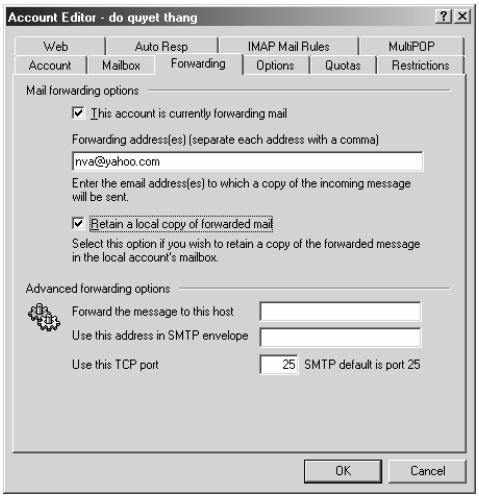
VI.1.2 Thông tin của Mailbox.

- **Message Directory** : đường dẫn thư mục **mailbox** chứa các thư nhận trên máy chủ chờ **user** kết nối vào và lấy thư về đọc

- **Storage Format** : định dạng tên file mail lưu trong thư mục **mailbox**. Mặc định là theo **RFC822**.

VI.1.3 Forwarding.

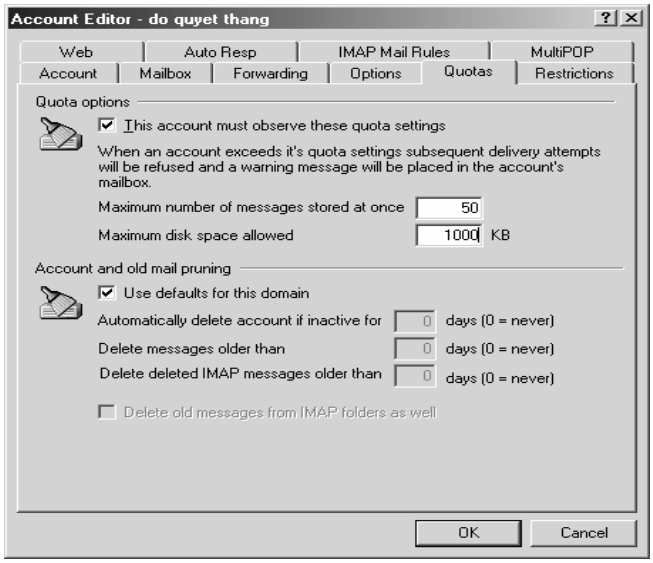
- Cho phép chuyển tiếp Mail nhận đến 1 địa chỉ khác



Hình 6.16: Chỉ định **forward mail**.

- **This Account is Currently Forwaring Mail** : **user** này cho phép chuyển Mail đến địa chỉ nhập vào bên dưới. Tính năng này dùng cho người đi công tác xa không có điều kiện truy cập hộp thư cục bộ, khi đó họ đăng ký 1 hộp thư khác và chuyển mail đến hộp thư mới.
- **Retain A Local Copy Of Forwarded mail** : giữ lại 1 bản sao của thư chuyển tiếp trong hộp thư cục bộ.
- **Advanced Forwarding Option**.
  - + **Forward The Message To This Host**: chuyển thư đến 1 máy chủ khác mô tả trong ô này.
  - + **Use This Address In SMTP Envelope**: địa chỉ Mail dùng trong cấu trúc của thư chuyển tiếp.
  - + **Use This TCP Port**: kết nối vào cổng nào trên máy chủ nhận thư chuyển tiếp.

VI.1.4 Thiết lập hạn ngạch cho mailbox.



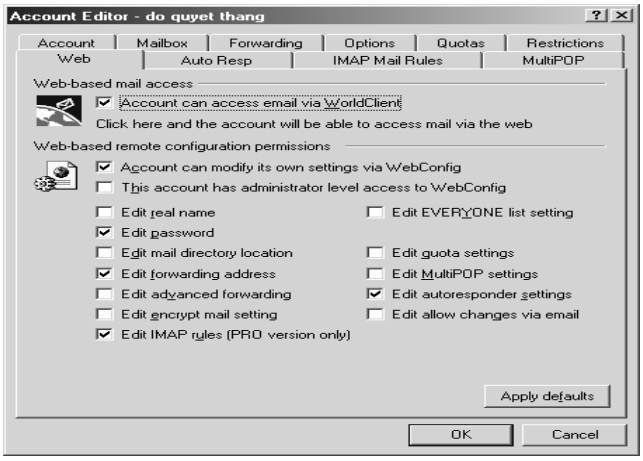
Hình 6.17: Giới hạn hạn nghạch đĩa.

- **This Account must Observe These Quota Settings** : **user** bị giới hạn số thư lưu trong hộp thư và giới hạn dung lương hộp thư.
  - + **Maximum Number Of Messages Stored At Once**: tổng số thư được lưu trong **mailbox**.
  - + **Maximum Disk Space Allowed**: dung lượng tối đa của **mailbox**. Khi **user** đạt tới 2 giới hạn trên thì thư gửi đến cho **user** này sẽ bị từ chối.

VI.1.5 Webmail cho tài khoản.

- **Account can access email**...: đánh dấu tuỳ chọn này cho phép **user** truy cập **mailbox** qua **Web**.
- **This Account can Config Itself Via Web** : cho phép **user** tự cấu hình qua **Web**.
- Chọn các tham số cấu hình mà **user** có thể thay đổi qua **Web**, ví dụ:

+ **Edit Real Name:** đổi tên.
+ **Edit POP logon:** đổi tên logon vào **POP server**.
+ **Edit POP password**: đổi mật khẩu **logon** vào **POP server**.



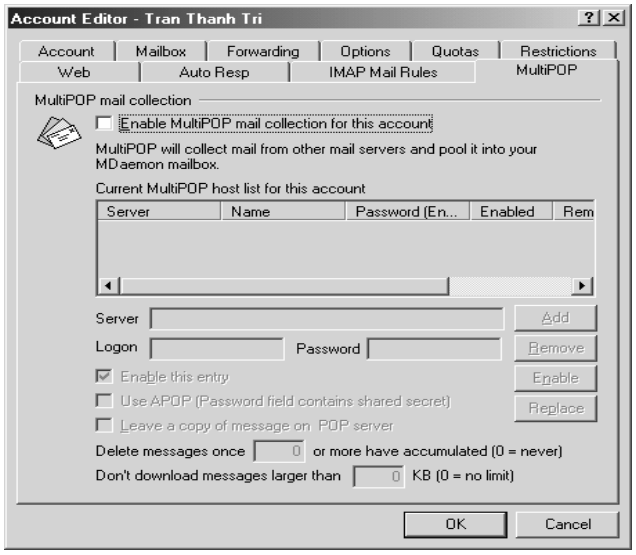
Hình 6.18: **Webmail** cho tài khoản.

VI.1.6 MultiPOP.

Cho phép **user** truy cập vào nhiều **mailbox** trên nhiều **POP Server**.

- **Enable MultiPOP Mail Collection For This Account :** đánh dấu tuỳ chọn này cho phép lấy thư từ nhiều **mailbox** trên các **POP Server** khác về đưa vào **mailbox** này của **user**. Với mỗi **Server**, nhập vào các tham số.

+ **Server** : địa chỉ **IP** hoặc tên **DNS** của **POP Server**.
+ **Logon :** tên **logon**.
+ **Pass** : mật khẩu.
+ Nhấn nút **Add** để đưa vào danh sách hoặc **Remove** để loại bỏ.
+ Nhấn nút **Enable** để cho phép truy cập vào **Server**.
+ Đánh dấu **Leave A Copy Of Message On POP Server**: để lại bản sao trên **POP Server** sau khi lấy Mail về.
+ **Don't download Messages Lager Than n KB**: không lấy các thư kích thước lớn hơn n KB.

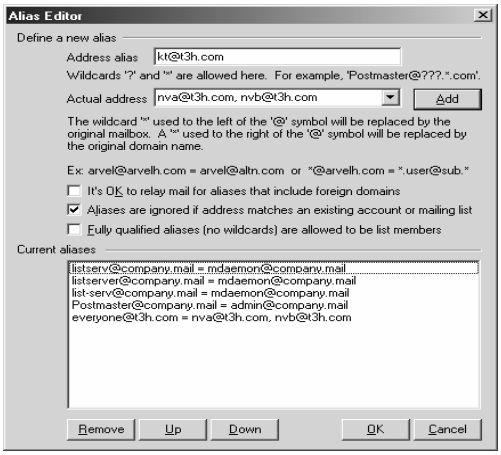


Hình 6.19: Hiệu chỉnh **MultiPOP Mail**.

VI.2. Tạo bí danh cho tài khoản.

- Chọn menu **Accounts** | **Address Aliases**.

+ **Address Alias :** tên bí danh.
+ **Actual address** : tên **user** mà bí danh này trỏ đến.
+ Nhấp chuột vào nút **Add** để tạo bí danh.
+ Nhấp chuột vào nút **Remove** để bỏ bí danh đáng chọn.

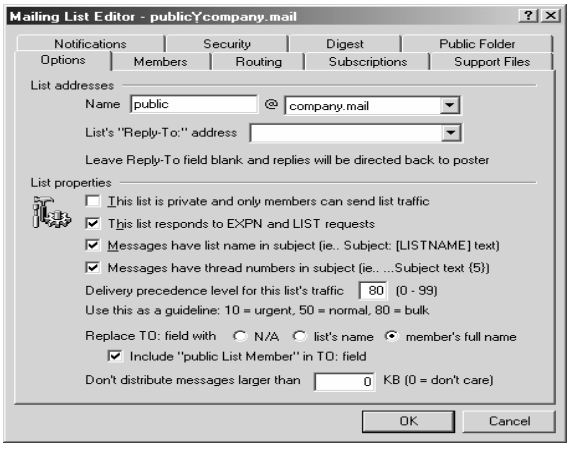


Hình 6.20: Tạo **Alias** cho tài khoản.

VI.3. Tạo Mailing List cho tài khoản.

Chọn menu **Lists** | **New List**.

- **Tab Options** :
  + Đặt tên cho **mailing list**.
  + **Name Of Mailing List**: tên danh sách thư tín. Tên này kết hợp với tên **domain** để trở thành địa chỉ **E-mail** của nhóm.
  + **List Reply To Address**: địa chỉ **E-mail** trả về của nhóm thư tín.



Hình 6.21: Tạo **group mail**.

- **Tab Members:** Cho phép thêm, hủy thành viên của nhóm thư tín, để thêm một thành viên ta thực hiện như sau: chọn tên **user** trong danh sách **New Member's E-mail Address** và nhấn nút **Add**.

Giới thiệu WinGate Proxy.

WinGate là 1 dịch vụ chạy trên máy tính đơn và cung cấp cho nhiều máy tính khác truy cập vào **Internet** . Nó làm được điều này bằng cách cho phép tất cả máy tính đó chia sẻ đồng thời một kết nối **Internet** . **WinGate** cung cấp 3 phương pháp để hỗ trợ việc chia sẽ một kết nối Internet (**Proxies** , **WinGate Internet Client** , **NAT-based General Purpose Internet Sharing**) , và cho phép ta tùy chỉnh **WinGate** lệ thuộc vào người dùng mạng .

WinGate cho phép kết nối toàn bộ mạng cục bộ vào **Internet** bằng 1 **Modem** đơn.

I. Cài đặt Wingate.

I.1. Yêu cầu phần cứng.

Để cài đặt chương trình **WinGate** , ta cần phải chuẩn bị các yêu cầu về phần cứng và phần mềm như sau :

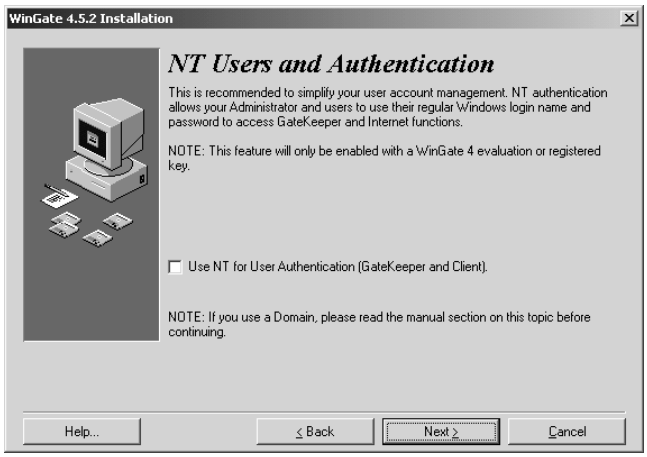
- **Windows 95** , **98** , **NT** (đối với các phiên bản từ 4.0 trở về sau) . Phiên bản **WinGate** từ 3.0.5 trở đi không thể chạy trên môi trường **Windows NT 3.5.1** .
- Nếu cài trên máy tính chạy hệ điều hành **Windows NT**, cần phải cài phiên bản **Service Pack 4** trở đi .
- Cần có 1 kết nối trực tiếp ra **Internet** .
- Cả hai loại máy **WinGate Server** và máy **Client** đều phải cài bộ nghi thức **TCP/IP**.
- Cài đặt **Winsock 2** đối với một số phiên bản của **Windows 95**.

I.2. Cài đặt Wingate proxy.

- Kiểm tra cấu hình phần cứng và phần mềm theo đúng yêu cầu.
- Từ thư mục của đĩa/thư-mục cài đặt , chạy tập tin **WinGate.exe**.
- Chọn nút **I Agree** để đồng ý các điều kiện của phần mềm đề ra.
- Xuất hiện cửa sổ yêu cầu chọn loại dịch vụ cần cài đặt , có 2 loại:
    + **Configure this Computer as a WinGate Internet Client** : cấu hình máy tính như là 1 máy **Client** (máy trạm).
    + **Configure this Computer as the WinGate Server** : cấu hình máy tính như là 1 máy **WinGate Server**.
    + Trong phần hướng dẫn này ta chọn vào nút cấu hình như là 1 máy **Server**. Sau đó nhấn nút **Continue**.
- Xuất hiện cửa sổ thông báo cài đặt **WinGate Server**, nhấn nút chọn **Next** để tiếp tục.
- Xuất hiện cửa sổ yêu cầu ta chọn loại cài đặt:

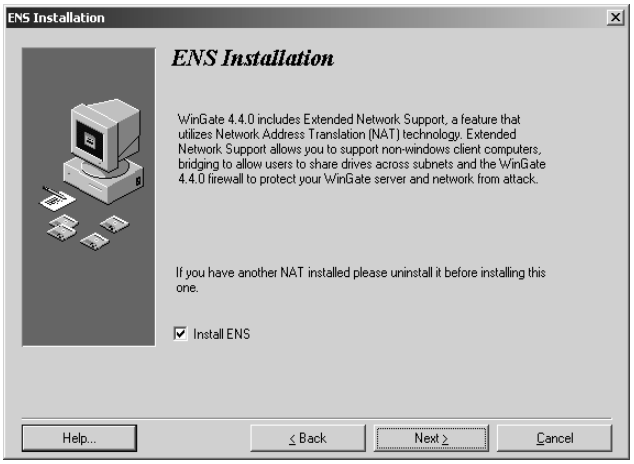
+ **Install WinGate (Enter your WinGate key below):** cài đặt WinGate , khi chọn nút này ta phải nhập vào **Lincense Name** và **Lincense Key** .
+ **Evaluate WinGate Home , Standard or Pro (Free 30 day trial):** cài đặt thử nghiệm **WinGate** trong vòng 30 ngày .
+ **Purchase WinGate now (Online):** Vào trang Web của **WinGate** để mua 1 **license** dùng để cài đặt sử dụng.

- Trong trường hợp này, chọn nút ở trên cùng (**Install WinGate**) , nhập vào **License Name** và **Lincense Key** và nhấn nút **Next** để tiếp tục .
- Màn hình kế tiếp đưa ra lựa chọn **Use NT for User Authentication** (**GateKeeper and Client**) . Nếu chọn lựa chọn này thì các tài khoản người dùng được tạo sẵn trong **Windows NT/2000** sẽ đồng bộ với các tài khoản tạo trong **WinGate** .
- Trong trường hợp này ta không cần chọn lựa chọn này , nhấn **Next** để tiếp tục .



Hình 6.22: **NT User and Authentication**.

- Trong bước cài đặt kế tiếp, màn hình cài đặt đưa ra 1 lựa chọn **Install ENS**. Nếu chọn lựa chọn này, quá trình cài đặt sẽ cài thêm vào **Extended Network Support** (**ENS**) hỗ trợ kĩ thuật **Network Address Translation** (**NAT**), **firewall** .



Hình 6.23: Chọn **ENS**.

- Nhấp chuột vào lựa chọn **Enable Auto Update** để tự động cập nhật phiên bản mới của **WinGate**. Chọn **Next** để tiếp tục.
- Màn hình cài đặt cho biết vị trí thư mục cài dịch vụ **WinGate** . nhấp chuột vào **Begin** để tiếp tục .
- Sau khi cài đặt xong dịch vụ , quá trình cài đặt hiển thị màn hình thông báo hoàn tất việc cài đặt. chọn **Finish**.
- Nhấp chuột vào nút **Ok** để khởi động lại máy tính .
- Sau khi cài đặt xong, ta sẽ thấy biểu tượng của **WinGate** được tạo ra tại thanh tác vụ.

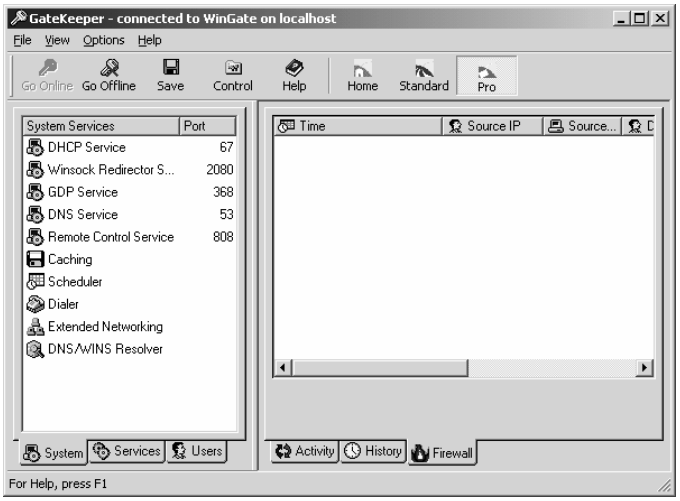
I.3. Khởi động/tạm ngưng WinGate.

- Khởi động **Wingate**: Chọn **Start | Programs | WinGate | Start WinGate Engine**.
- Tạm ngừng dịch vụ **WinGate** bằng cách nhấp chuột vào phải vào biểu tượng **WinGate** , chọn **Stop Engine**.

II. Cấu hình Wingate.

II.1. Khảo sát các thông tin chung.

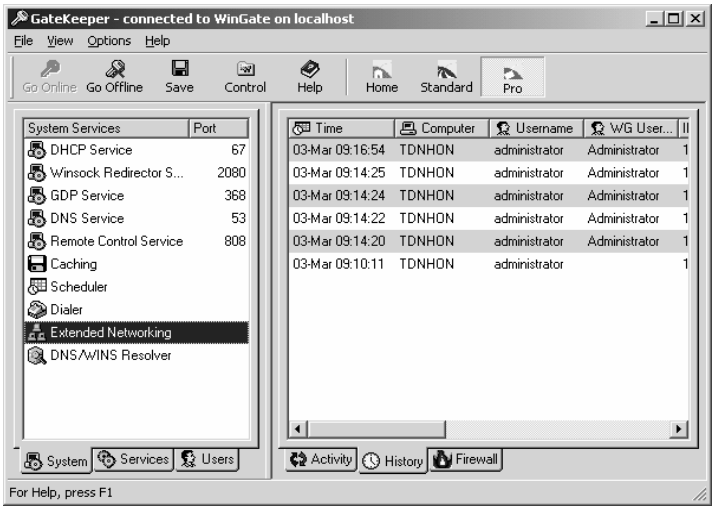
- **Use current Windows login:** Dùng lựa chọn này khi ta đang dùng định danh trên **NT Server** . Khi bật lựa chọn này cho phép ta tự động đăng nhập, **WinGate** sử dụng **username** và **password** của **NT Server** hiện hành.
- **Log on to local machine:** Đăng nhập vào máy cục bộ.
- **Use these details next time to login directly :** Các lần đăng nhập kế tiếp không đưa ra yêu cầu nhập **username** và **password** . Lưu ý là **GateKeeper** không lưu lại các **password**, do đó chỉ dùng lựa chọn này khi dùng lựa chọn **User current Windows login**.
- Sau khi khởi động chương trình **WinGate** lên, xuất hiện **GateKeeper**.



Hình 6.24: Giao diện **GateKeeper**.

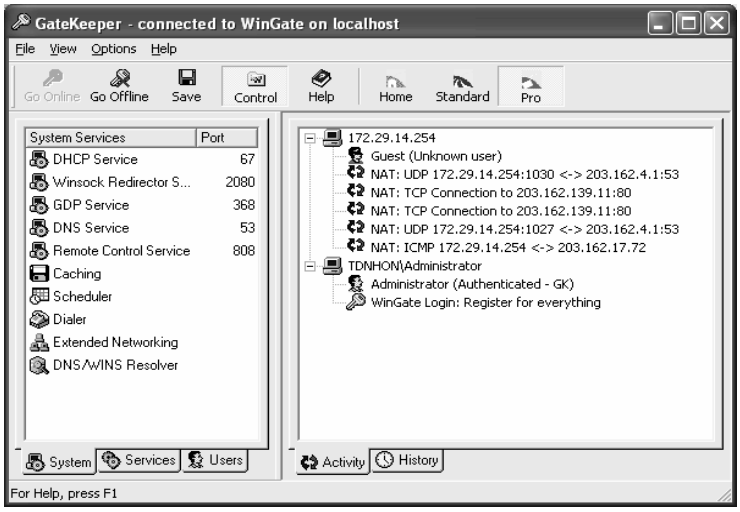
- **Activity Panel**.
  - + Hiển thị tất cả các phiên làm việc của người dùng và được cập nhật theo thời gian. Người quản trị có thể dùng màn hình này để quan sát và có thể xóa đi những phiên làm việc cụ thể nào đó.
  - + Có nhiều biểu tượng thể hiện các phiên làm việc trong màn hình **Activity**. Những biểu tượng này xuất hiện khi các phiên làm việc còn hoạt động, và biến mất khi các phiên làm việc hoàn tất.
  - + **Data sessions :** thể hiện thực thể của proxy hoặc dịch vụ đang dùng.
  - + **User sessions :** thể hiện người dùng nào đang sử dụng **WinGate** và đang mở phiên làm việc dữ liệu nào. Nếu một người dùng chưa được định danh, họ chỉ xuất hiện khi có một phiên làm việc dữ liệu đang hoạt động. Nếu một người dùng được định danh, họ sẽ xuất hiện với một biểu tượng chìa khóa, và ở màn hình **Activity** cho tới khi thoát ra.
  - + **Computer Session :** Có dạng biểu tượng máy tính, chỉ ra máy tính nào đang sử dụng **WinGate** .
  - + **Authenticated User:** Người dùng được định danh.
  - + **Assumed User:** Người dùng sử dụng **WinGate** từ 1 vị trí có thể nhận biết được, nhưng chưa đăng nhập vào **WinGate**.
  - + **Unknow User:** người dùng sử dụng **WinGate** từ 1 vị trí không nhận biết được, và chưa đăng nhập vào **WinGate**.
- History Panel.

Hiển thị thông tin về các lần truy cập sử dụng dịch vụ WinGate.



Hình 6.25: **Active Panel**.

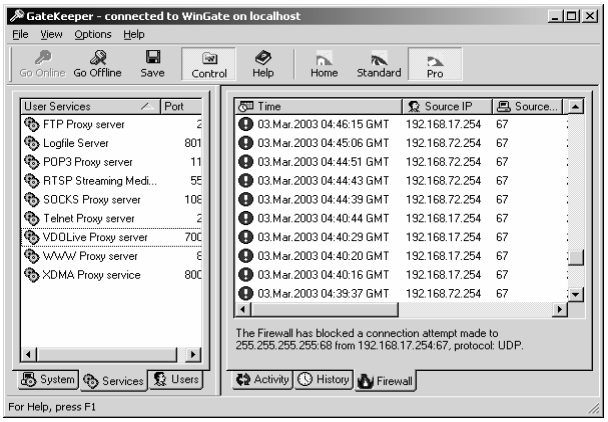
- Firewall Panel.
  + Hiển thông về connection của các máy trạm bị bộ lọc của **wingate** ngăn chặn.
- System Tab.
  + Trong tab này giúp chúng ta theo dõi và đặt cấu hình về **caching**, **dialer**, **ENS**, **Scheduler** … trong hệ thống **wingate**.



Hình 6.26: **System Tab**.

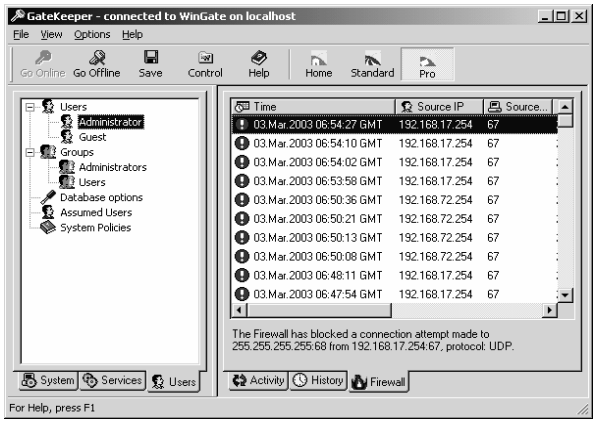
- **Service Tab**.

Cho phép **user** có thể cấu hình, **start** hoặc **stop** các **service**, thêm hoặc loại bỏ một dịch vụ.



Hình 6.27: **Services tab**.

- **Users Tab :** Cho phép ta quản lý, kiểm toán, tạo mới, ghi nhận các thông tin của các **wingate user**, giới hạn quyền truy cập các dịch vụ trong **wingate** cho các **user**, giới hạn các **user logon** vào **wingate** thông qua **wingate keeper**.



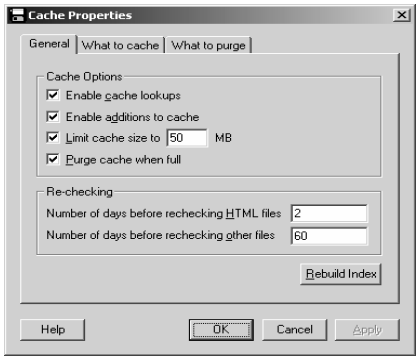
Hình 6.28: User tab.

III. Cấu Hình Các Dịch Vụ Hệ Thống.

III.1. Cấu hình Caching.

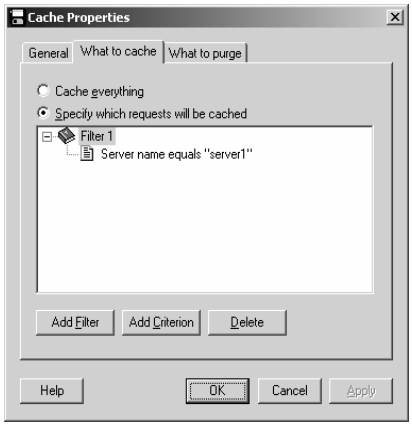
- **Caching** : Lưu trữ dữ liệu dùng chung tại 1 nơi mà nó có thể được truy xuất nhanh chóng và thuận tiện khi cần thiết. **WinGate** cung cấp việc **caching** các tài nguyên **Internet**, bao gồm : đồ họa, các tài liệu **HTML** hoặc các tập tin khác.
- Điều thuận lợi của **Caching** đó là nó chia sẽ cho tất cả các người dùng sử dụng dịch vụ **WWW Proxy Service**, giúp người dùng có thể truy cập thông tin nhanh chóng các **website** mà họ thường xuyên vào (do **website** được lưu trữ lại cho các lần truy cập sau).
- Từ cửa sổ **GateKeeper** : Chọn **tab System** – click đôi vào **Caching**. Cửa sổ **Caching Properties** hiện ra.
- Tab **General**.

+ **Enable cache lookups :** cho phép tìm kiếm trong **cache**.
+ **Enable additions to cache** : cho phép thêm thông tin vào **cache**.
+ **Limit cache size to ... MB :** giới hạn kích thước của **cache**.
+ **Purge cache when full :** xoá sạch thông tin được lưu khi **cache** đầy.
+ **Number of days before rechecking HTML files :** số lượng ngày trước khi kiểm tra lại các tập tin dạng **HTML**.
+ **Number of days before rechecking HTML files :** số lượng ngày trước khi kiểm tra lại các tập tin dạng khác.



Hình 6.28: Cấu hình **Cache**.

- **What to cache tab**.



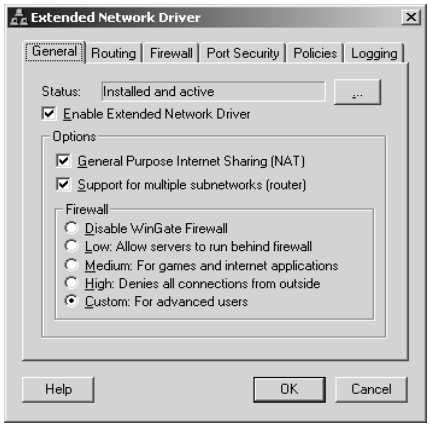
Hình 6.29: Thay đổi thuộc tính cho **Cache**.

+ **Cache everything** : lưu trữ mọi thông tin.
+ **Specify which request will be cached** : lưu lại những dữ liệu được chỉ định trong các bộ lọc phía dưới.
+ **Add Filters** : thêm vào một bộ lọc thông tin mới.
+ **Add Criterion** : thêm vào các tiêu chuẩn lọc thông tin cho bộ lọc.
+ **Delete** : xóa đi các thông tin theo qui định trong các bộ lọc phía dưới.

III.2. Extended Network Support (ENS):

ENS cung cấp các công cụ mới cho phép quản trị kết nối của **user** trong mạng **wingate**, cung cấp các cơ chế lọc packet thông qua **firewall**, hỗ trợ **NAT**, hỗ trợ **Multisubnetwork**.

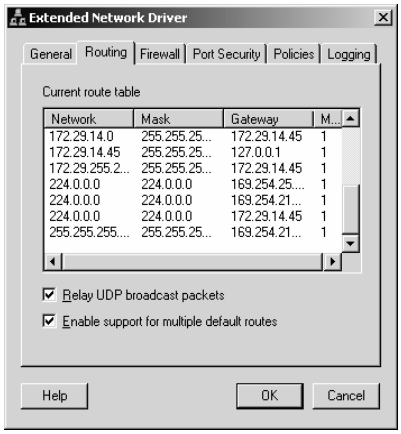
- **General tab**.



Hình 6.30: **General tab**.

+ **General Purpose Internet Sharing (NAT)**:Tuỳ chọn này là một công cụ dịch địa chỉ(**NAT**) cho phép bất kỳ một máy tính nào trong mạng nội bộ có thể truy cập trực tiếp **Internet** qua **wingate server** mà không cần phải thông qua **www proxy server**.
+ **Support for Multiple Subnetworks (router)**:Tuỳ chọn này cho phép chia sẻ các tài nguyên mạng(**drive**, **data**, **resource**…) giữa các máy tính trên các đường mạng khác nhau và chúng được liên thông với nhau thông qua một **Router** mềm có cài đặt **wingate**.
+ **Security Firewall Protection**: **Wingate** còn cung cấp một kỹ thuật lọc **packet**(**packet**-filtering), ở những phiên bản trước wingate chỉ được cung cấp ở mức độ **proxy firewall**, trong phiên bản mới này cung cấp chức năng **packet-filtering** mạnh hơn chức năng trước để chống sự tấn công trên mạng bao gồm : cấm dịch vụ (**denial of service** (**DOS**)), tấn công thông qua cơ chế **ping** (**ping of death**), quét **port** (**port scanners**), **Trojans** và nhiều cơ chế khác.

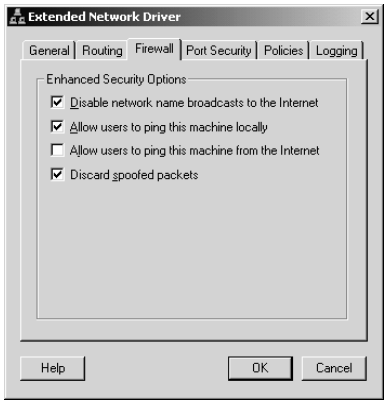
- **Routing Tab**.



Hình 6.31: Cấu hình **routing**.

+ Hiển thị bảng **routing table** hiện tại trên **Server** bao gồm các thông số về **network**, **gateway** và **subnetmask**, **metric**.
+ **Relay UDP broadcast Packets**: cho phép cơ chế tiếp nhận và chuyển tiếp **UDP packet** từ **subnet** này sang **subnet** khác.
+ **Enable support for multiple default routes**: Khi **connection** được tạo thì **default gateway** khác được chỉ định tới **Router**, và **default gateway** này được gán mức độ ưu tiên cao hơn **default gateway** thông thường, và thường xảy ra lỗi **routing** giữa hai **subnet**, vì **packet** được gởi từ **subnet** này sang **subnet** khác dự vào **gateway** có độ ưu tiên cao hơn do đó làm **packet** không tới đích được, khi tuỳ chọn này được lựa chọn thì chức năng **routing** trong **wingate** dự vào **gateway** được **Router** chỉ định ban đầu.

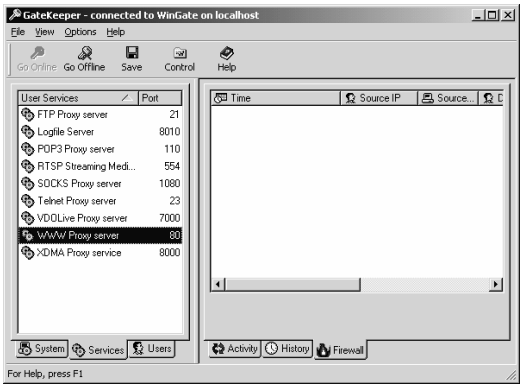
- **Firewall tab**.
  + **Extended Security Options:** Cung cấp các chức năng cơ sở về an ninh mật giúp ta có thể bảo vệ hệ thống chống lại một số phương pháp tấn công thông dụng.
  + **Advanced Packet-Filtering:** Các gói tin (**packets**) có thể được lọc (**filtered**) thông qua **protocol**, **interface**, **port** và có thể cho phép (**allowed**), không cho phép (**denied**) hay giới hạn (**redirected**) việc truy cập của các máy tính khác trong mạng đi qua **proxy** (ta có thể xem tab **Port Security** và **Policies**)
  + **Intrusion Logging**: Ghi nhận về các sự kiện về bất kỳ sự tấn công từ bên ngoài vào, hay các dấu hiệu của sự tấn công vào hệ thống(xem tab **Logging**).



Hình 6.32: Cấu hình **Firewall**.

III.3. Cấu hình các dịch vụ proxy.

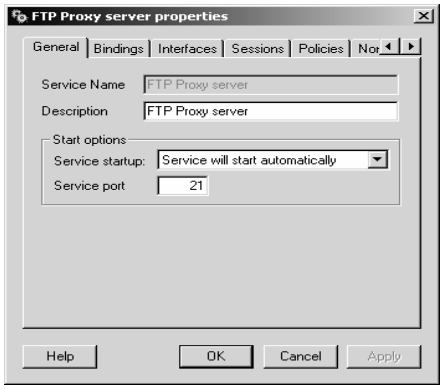
Wingate proxy cung cấp các dịch vụ **user** như: **ftp proxy server**, **Logfile Server**, **Pop3 Proxy server**, **RTSP Streaming Media**, **SockProxy server**, **Telnet Proxy server**, **VDOlive proxy server**, **WWW proxy server**, **XDMA Proxy service**, trong phần này ta sẽ thảo luận một số dịch vụ đặc trưng như: **www proxy server**, **sockproxy server**, **ftp proxy server**.



Hình 6.33: Cấu hình dịch vụ **proxy**.

III.3.1 Cấu hình FTP Proxy.

FTP Proxy Server cho phép sử dụng các trình ứng dụng **FTP Client** mà có hỗ trợ phương thức username@hostname qua firewall. Ví dụ: **WS_FTP**, **CuteFTP**.

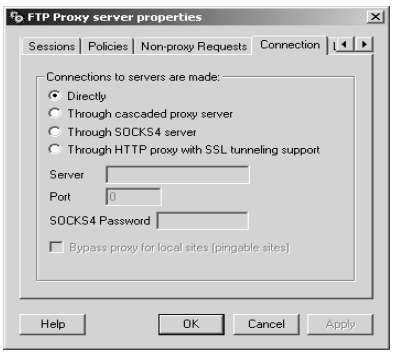


Hình 6.33: Cấu hình dịch vụ **FTP Proxy**.

Port 21 thường được sử dụng cho **FTP proxy server**. **FTP service** cho phép chúng ta có thể kết nối qua **firewall** khác.Trong phần **Connection** tab trong tuỳ chọn **cascaded proxy server** cho phép ta thực hiện điều này, các tab về **binding** và **interface**, **session**, **Policies**, **logging** chúng tôi đã khảo sát qua trên phần **DHCP Server**.

- **None-proxy Requests tab**.
  - + **FTP Proxy Service** có thể được cấu hình để phục vụ cho cả 2 loại yêu cầu: **proxy** (ủy quyền) và **non-proxy** (không ủy quyền). Các yêu cầu không ủy quyền thường xuất phát từ các người dùng bên ngoài **Internet** .
  - + Sau đây là các xử lý của dịch vụ đối với các yêu cầu không ủy quyền **Reject request** : loại bỏ yêu cầu.
  - + **Pipe request through to predetermined server** : chuyển yêu cầu sang một máy **Server** khác được xác định trước bởi các tham số phía dưới (**Server – Port**)
  - + **Redirect client to predetermined location** : chuyển hướng máy trạm sang vị trí khác trong **URL** .
  - + **Server Request** : phục vụ yêu cầu này dựa vào các thiết lập **Web Server** (ví dụ như thư mục gốc của **Server** , tên tập tin mặc định,..).
- **Connection tab**.

+ **Directly:** đây là **Option** mặc định được sử dụng khi **wingate server** được kết nối trực tiếp tới **internet**.
+ **Through cascaded proxy server**: sử dụng khi ta muốn **wingate proxy** truy cập qua **proxy** khác, trước khi nó truy cập **internet**.
+ **Through SOCKS4 server:** kết nối qua **SOCK4 Server** kèm theo **password**.
+ **Through HTTP proxy with SSL support:** tuỳ chọn này được sử dụng khi ta muốn **tunneling SSL** thông qua **http proxy**.



Hình 6.34: Connection tab.

III.3.2 Cấu Hình Dịch Vụ WWW Proxy.

Cung cấp việc truy cập **Internet** cho các máy trạm sử dụng nghi thức **HTTP**.

- Mở cửa sổ **GateKeeper**, chọn tab **Service**, double click vào biểu tượng **WWW Proxy Server**.

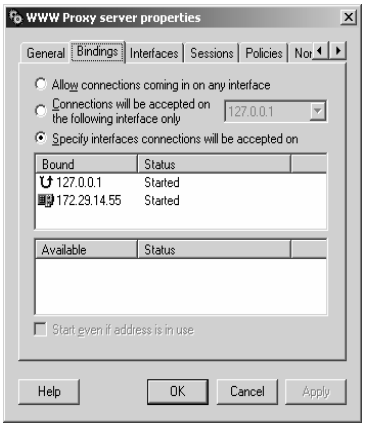
Hình 6.35: Cấu hình **WWW proxy**.

- **General tab**.
  + **Service Name:** Tên loại dịch vụ
  + **Description:** Dòng mô tả về dịch vụ.
  + **Service will start automatically**: dịch vụ tự động được khởi động.
  + **Manual start/stop:** Dịch vụ được khởi động hoặc ngừng bằng tay.
  + **Service is disabled:** Dịch vụ mặc định bị tắt đi.
  + **Service port:** Cổng cho phép máy trạm kết nối vào dịch vụ **proxy**.
  + **Use java client authentication as required by policies:** Cho phép kiểm tra định danh các máy trạm sử dụng trình duyệt có khả năng **Java**.

- **Bindings tab**.

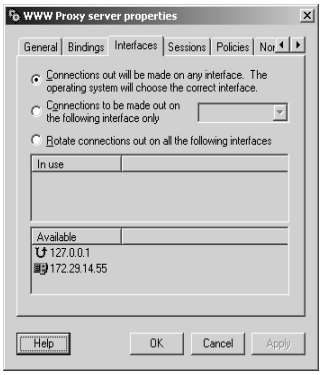
+ **Allow connections coming in on any interface**: cho phép các kết nối đến từ mọi **interface**.
+ **Connecitons will be accepted on the following interface only** : chỉ chấp nhận các kết nối đến từ **interface** được chỉ định.
+ **Specify interfaces connections will be accepted on** : chấp nhận các kết nối từ các **interface** mô tả phía dưới.

-



Hình 6.36: **Bindings tab**.

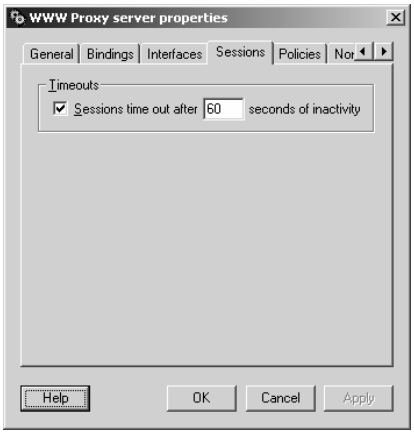
- **Interfaces tab**.
  + **Connections out will be made on any interface . The operating system will choose the correct interface**: sử dụng tất cả các **interface** để quay kết nối ra ngoài (**Internet**)
  + **Connections to be made out on the following interface only** : chỉ sử dụng **interface** được chỉ định để quay kết nối ra ngoài.
  + **Rotate connections out on all the following interfaces** : sử dụng luân phiên các **interface** được chỉ định phía dưới để quay số ra ngoài.



Hình 6.37: **Interface tab**.

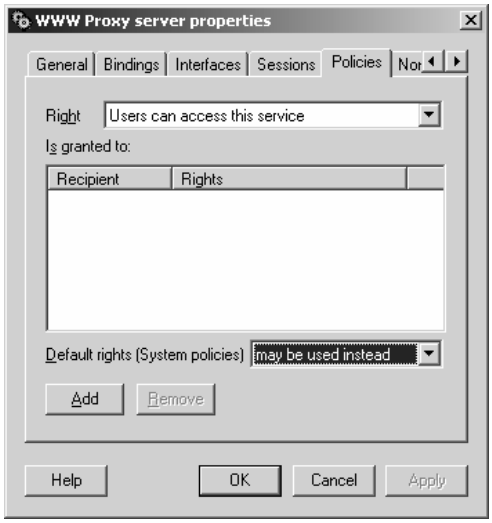
- **Sessions tab**.

+ **Sessions time out after ... seconds of inactivity** : thời gian hết hạn một phiên làm việc không còn hoạt động.



Hình 6.38: **Session tab**.

- **Polices tab**.
  + **Right:** một số quyền người dùng đối với dịch vụ này.
  + **User can access this service**: người dùng có khả năng truy cập vào dịch vụ này.
  + **User can modify this service:** người dùng có thể thay đổi cấu hình dịch vụ này.
  + **User can start/stop this service:** người dùng có thể khởi động hoặc ngừng dịch vụ này.
  + **Add:** thêm vào người dùng mới có quyền được chỉ định trong **Right**.



Hình 6.39: **Policies tab**.

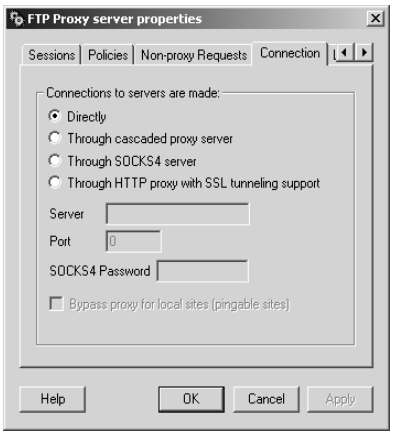
- **Non-proxy Requests tab**.

WWW Proxy Service có thể được cấu hình để phục vụ cho cả 2 loại yêu cầu: **proxy** (ủy quyền) và **non-proxy** (không ủy quyền). Các yêu cầu không ủy quyền thường xuất phát từ các người dùng bên ngoài **Internet** .

Sau đây là các xử lý của dịch vụ đối với các yêu cầu không ủy quyền.

+ **Reject request :** loại bỏ yêu cầu.
+ **Pipe request through to predetermined server** : chuyển yêu cầu sang một máy **Server** khác được xác định trước bởi các tham số phía dưới (**Server** – **Port**).
+ **Redirect client to predetermined location** : chuyển hướng máy trạm sang vị trí khác trong **URL**.
+ **Server Request** : phục vụ yêu cầu này dựa vào các thiết lập **Web Server** (ví dụ như thư mục gốc của **Server** , tên tập tin mặc định , ...).

- **Connection tab**.
  + **Directly:** đây là **Option** mặc định được sử dụng khi **wingate server** được kết nối trực tiếp tới **internet**.
  + **Through cascaded proxy server:** sử dụng khi ta muốn **wingate proxy** truy cập qua **proxy** khác, trước khi nó truy cập **internet**.
  + **Through SOCKS4 server:** kết nối qua **SOCK4 server** kèm theo **password**.



Hình 6.40: **Connection tab**.