

TRƯỜNG CAO ĐẲNG LÝ TỰ TRỌNG TP.HỒ CHÍ MINH

NỘI DUNG BÀI GIẢNG : THIẾT LẬP HỆ THỐNG MẠNG

KỸ THUẬT MẠNG LAN – WAN

I-KỸ THUẬT MẠNG LAN

I.1/Lịch sử:

Vào thời gian trước khi những máy tính cá nhân xuất hiện, một máy tính trung tâm chiếm trọn 1 căn phòng, người dùng truy nhập những thiết bị đầu cuối máy thông qua cáp truyền dữ liệu tốc độ thấp. Những Mạng SNA của IBM (cấu trúc mạng hệ thống) được tập trung vào những thiết bị đầu cuối liên kết hay những máy tính lớn khác tại những chỗ từ xa qua những đường dây cáp thuê bao. Từ đây nó là những mạng được kết nối trên diện rộng. Những mạng cục bộ LAN (Local Network Area) đầu tiên đã được tạo ra vào cuối những năm 1970 và thường tạo ra những mối liên kết cao tốc giữa vài máy tính trung tâm lớn tại một chỗ. Nhiều hệ thống cạnh tranh được tạo ra vào thời gian này Ethernet và ARCNET được biết đến nhiều nhất.

Sự phát triển vượt bậc của CP/M – Và sau đó những máy tính cá nhân chạy trên nền DOS có nghĩa rằng có hàng trăm máy tính đã có thể hoạt động đơn lẻ và độc lập với máy tính trung tâm. Sự hấp dẫn ban đầu của mạng máy tính là việc có thể chia sẻ ổ đĩa và những máy in laser, mà là cả hai thứ này rất đắt lúc đó. Có nhiều người hào hứng với khái niệm mới và trong vài năm, từ khoảng 1983 về phía trước, những học giả công nghiệp tin học đều đặn khai báo năm tới sẽ là năm của mạng LAN.

Trên thực tế, nhận định đó bị lung lay mạnh bởi sự tăng nhanh của các loại lớp vật lý khác nhau và những thủ tục thi hành mạng không tương thích, và sự bối rối về việc làm thế nào để chia sẻ tài nguyên tốt nhất. Điển hình, mỗi nhà cung cấp có một kiểu card mạng riêng của họ, dây cáp, giao thức kết nối, hệ điều hành mạng riêng của họ. Và một giải pháp quan trọng xuất hiện với cái tên NetWare Novell, giải pháp của họ hỗ trợ 40 kiểu card mạng khác nhau, và một hệ điều hành phức tạp hơn so với hầu hết các đối thủ của nó. Phần mềm mạng thống trị các máy tính cá nhân được nối với nhau (LAN) của các doanh nghiệp từ những năm đầu 1983 – khi nó được giới thiệu – cho đến giữa những năm 1990 khi Microsoft giới thiệu hệ điều hành mạng tân tiến Windows NT advanced server và Windows cho nhóm làm việc (Windows for working group).

Những đối thủ của phần mềm mạng, chỉ có Banyan Vines có những kỹ thuật mạnh để cạnh tranh nhưng Banyan chẳng bao giờ có một vị thế an toàn. Microsoft và 3Com làm việc cùng nhau tạo ra một hệ điều hành mạng đơn giản, tiền thân 3+Share của 3Com và LAN Manager của Microsoft cũng như LAN Server của IBM. Không một ai trong số trên đặc biệt thành công.

Trong cùng thời gian với máy tính trạm lớn frame, những trạm làm việc UNIX từ những nhà cung cấp như Sun Microsystems, Hewlett-Packard, Silicon Graphics, Intergraph, NeXT và Apollo sử dụng giao thức TCP/IP. Dù phân đoạn đoạn thị trường cho trạm làm việc chạy trên UNIX đã và đang sụt giảm nhưng những công nghệ được phát triển bởi họ tiếp tục có ảnh hưởng trên Internet và trong cả hai Hệ điều hành Linux Mac OS X của Apple và giao thức TCP/IP gần như hoàn toàn thay thế IPX, AppleTalk, NetBEUI và những giao thức khác được dùng trong buổi đầu mạng LAN được sinh ra. Bài này còn sơ khai.

I.2/Kỹ thuật mạng LAN

Mặc dầu ngày nay mạng Ethernet chuyển đổi là giao thức thông dụng nhất dùng trong tầng liên kết dữ liệu và IP là giao thức thông dụng nhất trong tầng Network, rất nhiều sự lựa chọn khác nhau đã và đang được sử dụng, và một vài trong số đó trở nên phổ biến trong những lĩnh vực thích hợp. Mạng LAN nhỏ hơn gồm có một hoặc vài liên kết chuyển mạch tới những mạng khác – thường với một liên kết tới một bộ định tuyến, modem cáp, hay DSL modem cho truy nhập Internet.

Những mạng LAN lớn hơn được mô tả bởi người dùng với những đường dẫn dư thừa và chuyển đổi sử dụng giao thức giải thuật cây để ngăn chặn vòng lặp, khả năng của chúng để điều khiển các loại giao thông khác nhau thông qua chất lượng dịch vụ (QoS), và cô lập giao thông qua VLANs. Mạng LAN lớn hơn cũng bao gồm nhiều và đa dạng các thiết bị như bộ chuyển đổi, tường lửa, bộ định tuyến, bộ cân bằng tải, cảm biến và hơn thế nữa.

LAN có thể có liên kết với những mạng cục bộ khác thông qua đường thuê bao, dịch vụ thuê bao, hoặc bằng "đường hầm" thông qua mạng Internet sử dụng công nghệ VPN. Tùy thuộc vào cách tạo ra và bảo đảm các liên kết, và độ rộng địa lý của mạng, hệ các mạng LAN này có thể trở thành Mạng liên kết chủ (MAN) hoặc Mạng liên kết diện rộng (WAN), hoặc một phần của Mạng toàn cầu.

I.3/Các thiết bị cần thiết

Máy chủ (Server)

– Là một máy tính có CPU tốc độ cao, RAM và ổ đĩa lớn, thường liên kết với các thiết bị ngoại vi khác như máy in (printer, máy quét (scanner), ...).

Máy trạm (Workstation)

Máy trạm đôi khi còn gọi là máy khách (client). Các máy khách kết nối với máy chủ và có thể liên lạc với nhau thông qua máy chủ.

Nguồn tham khảo : www.wikilek.org

II/Kỹ thuật mạng WAN

WAN (wide area network), còn gọi là "mạng diện rộng", dùng trong vùng địa lý lớn thường cho quốc gia hay cả lục địa, phạm vi vài trăm cho đến vài ngàn km. Chúng bao gồm tập hợp các máy nhằm chạy các chương trình cho người dùng. Các máy này thường gọi là máy lưu trữ(host) hay còn có tên là máy chủ, máy đầu cuối (end system). Các máy chính được nối nhau bởi các mạng truyền thông con (communication subnet) hay gọn hơn là mạng con (subnet). Nhiệm vụ của mạng con là chuyển tải các thông điệp (message) từ máy chủ này sang máy chủ khác.

Mạng con thường có hai thành phần chính:

Các đường dây vận chuyển còn gọi là mạch (circuit), kênh (channel), hay đường trung chuyển (trunk).

Các thiết bị nối chuyển. Đây là loại máy tính chuyên biệt hoá dùng để nối hai hay nhiều đường trung chuyển nhằm di chuyển các dữ liệu giữa các máy. Khi dữ liệu đến trong các đường vô, thiết bị nối chuyển này phải chọn (theo thuật toán đã định) một đường dây ra để gửi dữ liệu đó đi. Tên gọi của thiết bị này là nút chuyển gói (packet switching node) hay hệ thống trung chuyển (intermediate system). Máy tính dùng cho việc nối chuyển gọi là "bộ chọn đường" hay "bộ định tuyến" (router).

Hầu hết các WAN bao gồm nhiều đường cáp hay là đường dây điện thoại, mỗi đường dây như vậy nối với một cặp bộ định tuyến. Nếu hai bộ định tuyến không nối chung đường dây thì chúng sẽ liên lạc nhau bằng cách gián tiếp qua nhiều bộ định tuyến trung gian khác. Khi bộ định tuyến nhận được một gói dữ liệu thì nó sẽ chứa gói này cho đến khi đường dây ra cần cho gói đó được trống thì nó sẽ chuyển gói đó đi. Trường hợp này ta gọi là nguyên lý mạng con điểm nối điểm, hay nguyên lý mạng con lưu trữ và chuyển tiếp (store-and-forward), hay nguyên lý mạng con nối chuyển gói.

Có nhiều kiểu cấu hình cho WAN dùng nguyên lý điểm tới điểm như là dạng sao, dạng vòng, dạng cây, dạng hoàn chỉnh, dạng giao vòng, hay bất định.

Bài 4 Quản trị Email Server, Web Server, FTP Server

I/Quản trị Mail server

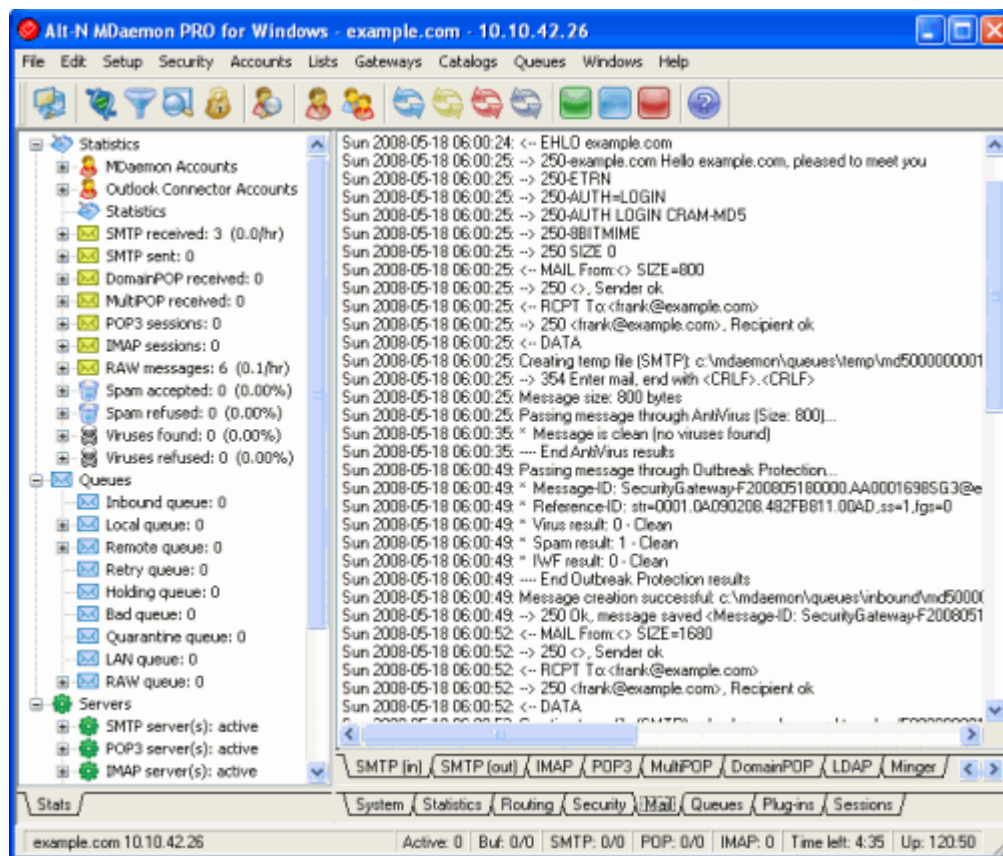
1/Giới thiệu

Là Hệ thống dịch vụ ứng dụng E-mail Chuyên biệt dành cho Doanh nghiệp đáp ứng nhu cầu sử dụng Thư điện tử dùng riêng nguoidung@tenmienrieng.com.vn

- Hệ thống đảm bảo các tính năng cơ bản của dịch vụ mail như gửi, nhận thư qua các giao thức chuẩn smtp, pop, web,...
- Cung cấp dịch vụ check thư qua IMAP, cho phép khách hàng nhận thư cùng lúc trên nhiều máy.
- Cung cấp dịch vụ backup hộp thư, đảm bảo dữ liệu được an toàn trong trường hợp có sự cố.
Dung lượng lưu trữ Email không giới hạn.
- Gửi, nhận file tối đa 20Mb.
- Chức năng antivirus, antispam thực hiện tự động.
- 1 gói (block) cho phép tạo nhiều hơn 1 tên miền riêng

2.Cài đặt Mdaemon

Quản Trị Mạng - MDaemon Mail Server: là 1 trong những giải pháp hệ thống mail server toàn diện nhất hiện nay dành cho các công ty, doanh nghiệp với quy mô khác nhau. MDaemon Mail Server hiện có 3 phiên bản: Standard, Pro và Free. Sau đây là một số điểm đáng chú ý của chương trình.



Màn hình hiển thị chính của MDAemon

Màn hình hiển thị chính của MDAemon (*Graphical User Interface - GUI*) đưa ra thông tin quan trọng về các nguồn tài nguyên, các giao dịch, số liệu thống kê, luồng dữ liệu đang trong trạng thái hoạt động (active) và các mail đang trong quá trình chờ đợi (queued) để được xử lý. Bên cạnh đó, còn có sự lựa chọn cho người dung chuyển đổi trạng thái activating/deactivating đối với các hệ thống máy chủ khác nhau có sử dụng MDAemon. Cửa sổ bên phải hiển thị đầy đủ thông tin về kết nối dữ liệu đầu vào và ra (incoming và outgoing) đang được thực hiện.

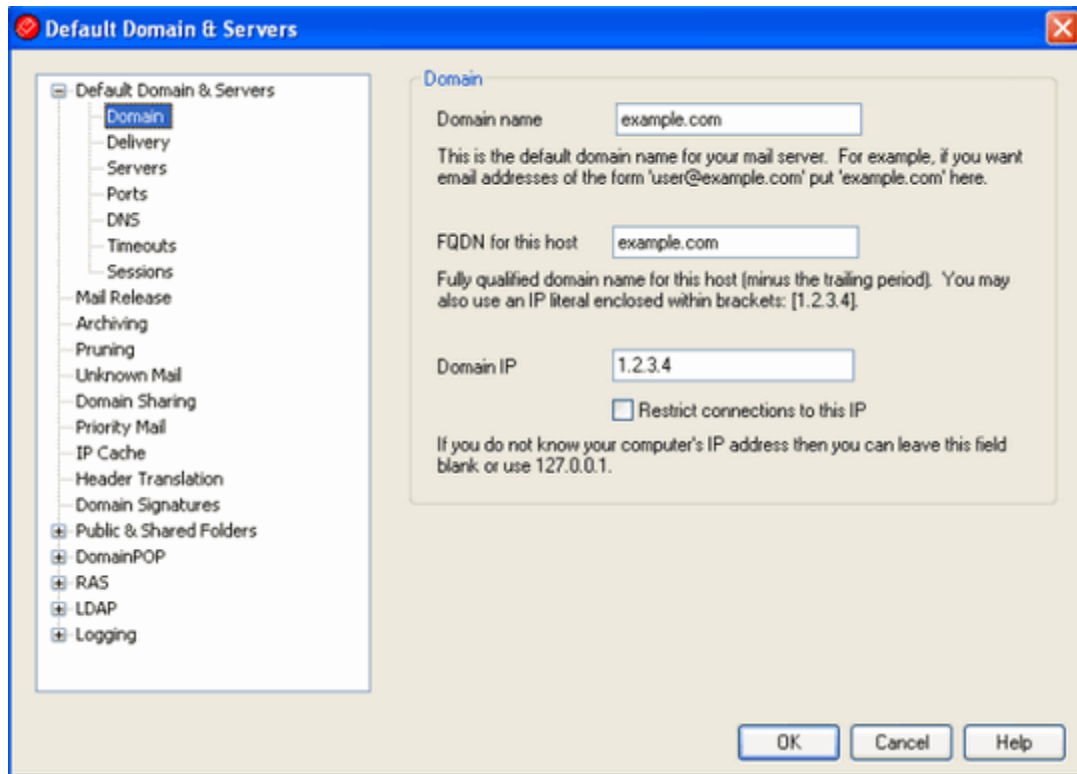
Setup Menu

Giá trị Domain/Servers mặc định:

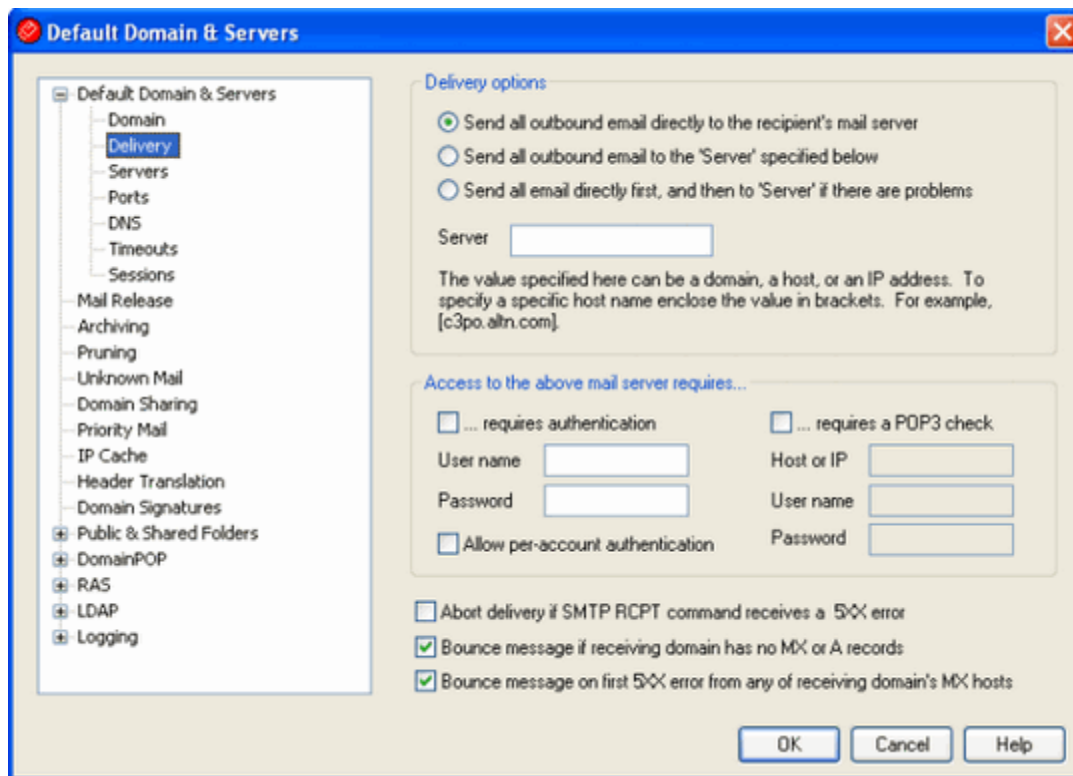
Giá trị mặc định của Domain/Servers có thể được thiết lập dễ dàng thông qua lựa chọn menu **Setup > Default Domain/Servers**, tùy theo từng domain và servers của người dùng mà có thể thiết lập thông số tùy chỉnh. Duy nhất chỉ có giá trị mặc định của Domain có thể điều chỉnh được, nhưng MDAemon có thể quản lý tất cả các con số, giá trị của các Extra Domain khác nhau (tính năng này chỉ có trong phiên bản MDAemon Pro), và lưu trữ thư điện tử đối với các hệ thống Domain Gateways.

Cửa sổ làm việc của Default Domain bao gồm các mục sau:

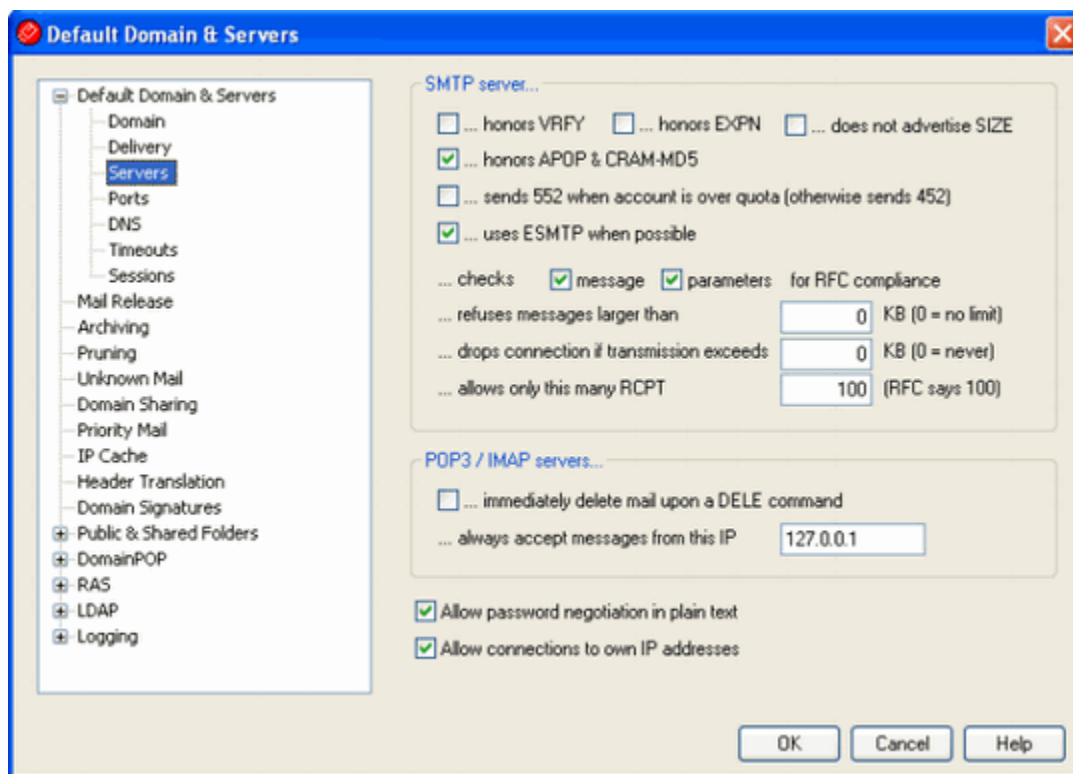
- *Domain*: cửa sổ này hiển thị tên mặc định của domain và địa chỉ IP



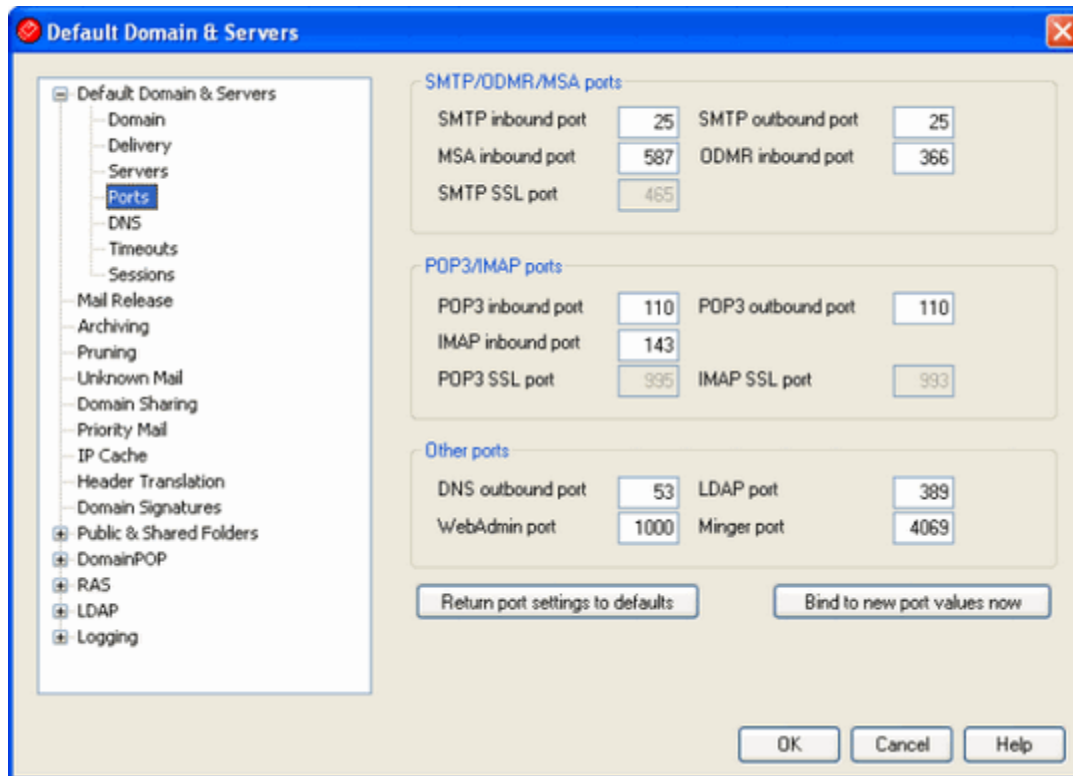
- *Delivery*: tại đây, người sử dụng sẽ khai báo giá trị dành cho MDAemon để quản lý quá trình chuyển phát, nhận mail tùy thuộc vào các yếu tố khác như ISP, gateway host, hoặc các server khác



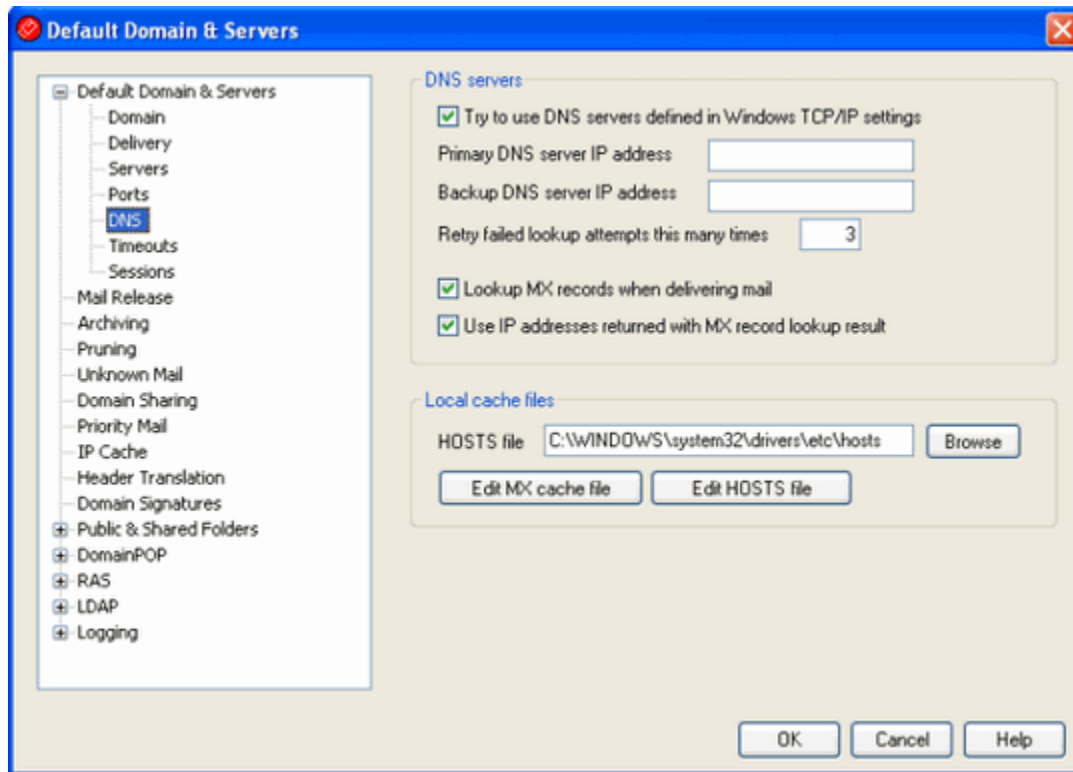
- *Servers*: với các sự lựa chọn để tùy chỉnh số lượng server, địa chỉ email. Ví dụ như việc thiết lập MDAemon sẽ làm việc với các giao thức SMTP server như VRFY, EXPN, APOP và CRAM-MD5... Hoặc bạn cũng có thể thiết lập số lượng tối đa dành cho email, số lượng lệnh thực hiện RCPT được cho phép trong SMTP...



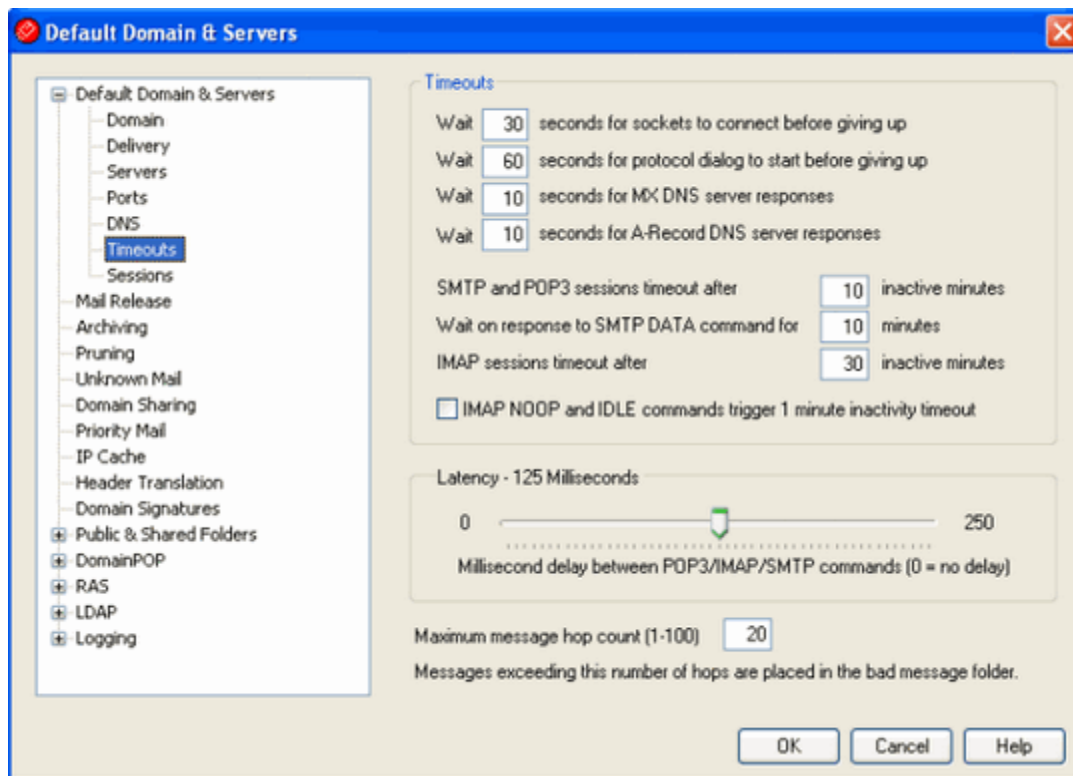
- *Ports*: chứa đựng giá trị hoặc số lượng các cổng (ports) mà MDAemon sẽ điều khiển và sử dụng dành cho các giao thức SMTP và POP trong quá trình gửi và nhận email. Hoặc bạn cũng có thể gán lại giá trị dành cho các cổng khác nhau mà MDAemon sẽ “lắng nghe” theo các sự kiện IMAP, còn cổng UDP dành cho việc truy vấn DNS servers. Trong hầu hết các trường hợp, giá trị mặc định của các cổng sẽ không cần phải thay đổi, tuy nhiên tùy vào từng server khác nhau mà người sử dụng sẽ có những thay đổi phù hợp.



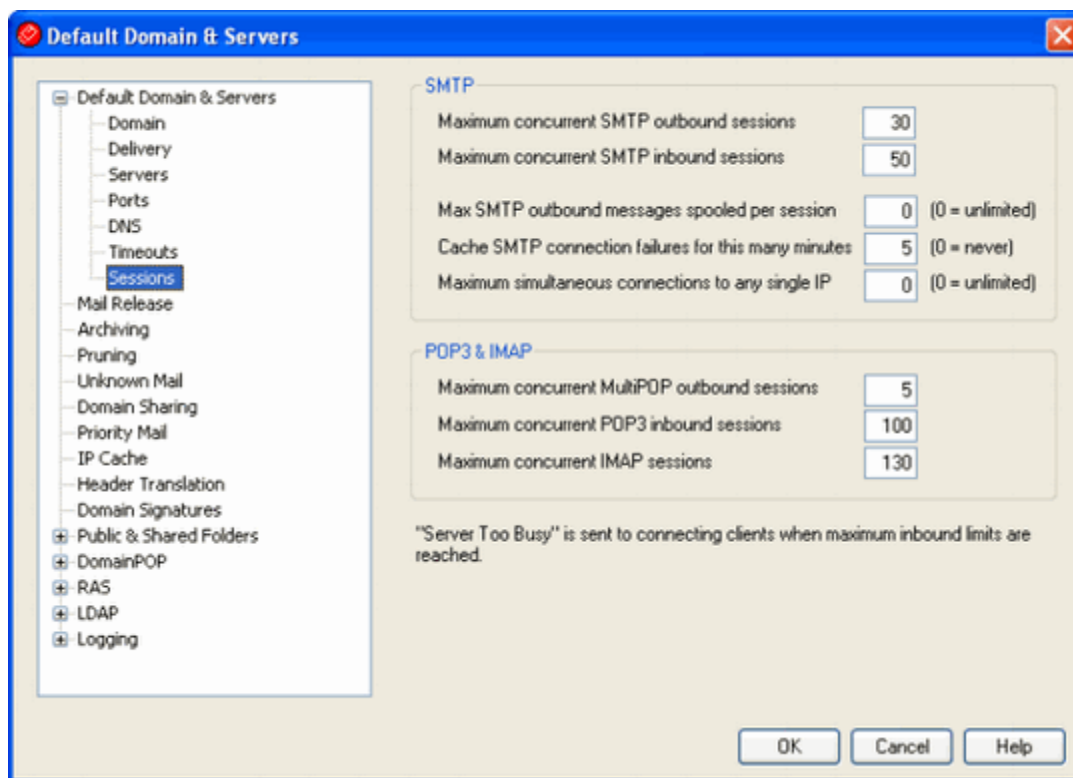
- *DNS*: cửa sổ này cho phép người dùng gán giá trị dành cho địa chỉ IP của DNS server chính và dự phòng. Bên cạnh đó, còn các sự lựa chọn khác dành cho việc điều khiển và lưu trữ các giá trị bản ghi MX.



- *Timeouts*: chứa đựng các giá trị giới hạn thời gian dành cho MDAemon chờ đợi trong khi kết nối đến host điều khiển, chờ giá trị phản hồi của các địa chỉ, DNS server... Bên cạnh đó, giá trị giới hạn “*Maximum message hop count*” được sử dụng trong các trường hợp bảo vệ các tin nhắn trong quá trình luân chuyển theo vòng lặp.



- *Sessions*: tại đây, người sử dụng sẽ thiết lập số lượng tối đa các luồng xử lý dữ liệu mà MDAemon sẽ dùng để gửi và nhận mail thông qua giao thức SMTP, POP, và IMAP, hoặc bạn cũng có thể thiết lập số lượng tin nhắn mà MDAemon dự định sẽ gửi và nhận email trong cùng 1 thời gian. Bên cạnh đó, bạn cũng có thể thiết lập số lượng tin nhắn thông qua giao thức outbound SMTP sẽ được đóng gói qua mỗi tiến trình.



II-Dịch vụ FTP

1-Giới thiệu

FTP (viết tắt của *File Transfer Protocol* dịch ra là "Giao thức truyền tập tin") thường được dùng để trao đổi tập tin qua mạng lưới truyền thông dùng giao thức **TCP/IP** (chẳng hạn như **Internet** - mạng ngoại bộ - hoặc **intranet** - mạng nội bộ). Hoạt động của FTP cần có hai máy tính, một **máy chủ** và một **máy khách**. **Máy chủ FTP**, dùng chạy phần mềm cung cấp dịch vụ FTP, gọi là trình chủ, lắng nghe yêu cầu về dịch vụ của các máy tính khác trên mạng lưới. **Máy khách** chạy phần mềm FTP dành cho người sử dụng dịch vụ, gọi là trình khách, thì khởi đầu một liên kết với máy chủ. Một khi hai máy đã liên kết với nhau, máy khách có thể xử lý một số thao tác về tập tin, như tải tập tin lên máy chủ, tải tập tin từ máy chủ xuống máy của mình, đổi tên của tập tin, hoặc xóa tập tin ở máy chủ v.v. Vì giao thức FTP là một giao thức chuẩn công khai, cho nên bất cứ một công ty **phần mềm** nào, hay một lập trình viên nào cũng có thể viết trình chủ FTP hoặc trình khách FTP. Hầu như bất cứ một nền tảng hệ điều hành máy tính nào cũng hỗ trợ giao thức FTP. Điều này cho phép tất cả các máy tính kết nối với một mạng lưới có nền TCP/IP, xử lý tập tin trên một máy tính khác trên cùng một mạng lưới với mình, bất kể máy tính ấy dùng **hệ điều hành** nào (nếu các máy tính ấy đều cho phép sự truy cập của các máy tính khác, dùng giao thức FTP). Hiện nay trên thị trường có rất nhiều các trình khách và trình chủ FTP, và phần đông các trình ứng dụng này cho phép người dùng được lấy tự do, không mất tiền.

1.1.Khái quát

FTP thường chạy trên hai [cổng](#), 20 và 21, và chỉ chạy riêng trên nền của [TCP](#). Trình chủ FTP lắng nghe các yêu cầu dịch vụ từ những kết nối vào máy của các trình khách FTP, trên cổng 21. Đường kết nối trên cổng 21 này tạo nên một dòng truyền điều khiển, cho phép các dòng lệnh được chuyển qua trình chủ FTP. Để truyền tải tập tin qua lại giữa hai máy, chúng ta cần phải có một kết nối khác. Tùy thuộc vào chế độ truyền tải được sử dụng, trình khách (ở chế độ năng động - *active mode*) hoặc trình chủ (ở chế độ bị động - *passive mode*) đều có thể lắng nghe yêu cầu kết nối đến từ đầu kia của mình. Trong trường hợp kết nối ở chế độ năng động, (trình chủ kết nối với trình khách để truyền tải dữ liệu), trình chủ phải trước tiên đóng kết vào cổng 20, trước khi liên lạc và kết nối với trình khách. Trong chế độ bị động, hạn chế này được giải tỏa, và việc đóng kết trước là một việc không cần phải làm.

Trong khi dữ liệu được truyền tải qua [dòng dữ liệu](#), dòng điều khiển đứng im. Tình trạng này gây ra một số vấn đề, đặc biệt khi số lượng dữ liệu đòi hỏi được truyền tải là một số lượng lớn, và đường truyền tải chạy thông qua những [bức tường lửa](#). Bức tường lửa là dụng cụ thường tự động ngắt các phiên giao dịch sau một thời gian dài im lặng. Tuy tập tin có thể được truyền tải qua hoàn thiện, song dòng điều khiển do bị bức tường lửa ngắt mạch truyền thông giữa quãng, gây ra báo lỗi.

1.2.Mục đích của giao thức FTP

Mục đích của giao thức FTP, như được phác thảo trong bản [RFC](#), là:

1. Khuyến khích việc dùng chung tập tin (như chương trình ứng dụng vi tính hoặc dữ liệu)
2. Khuyến khích việc sử dụng máy tính ở xa một cách gián tiếp / âm thầm (*implicit*).
3. Che đậy sự khác biệt về hệ thống lưu trữ tập tin giữa các [máy chủ](#), hầu cho người dùng không cần phải quan tâm đến những sự khác biệt riêng tư của chúng.
4. Truyền tải dữ liệu một cách đáng tin cậy và có hiệu quả cao.

1.3.Những phê bình về giao thức FTP

1. [Mật khẩu](#) và nội dung của tập tin được truyền qua đường cáp mạng ở dạng [văn bản thường](#) (*clear text*), vì vậy chúng có thể bị chặn và nội dung bị lộ ra cho những kẻ nghe trộm. Hiện nay, người ta đã có những cải tiến để khắc phục nhược điểm này.
2. Cần phải có nhiều kết nối TCP/IP: một dòng dành riêng cho việc điều khiển kết nối, một dòng riêng cho việc truyền tập tin lên, truyền tập tin xuống, hoặc liệt kê thư mục. Các phần mềm bức tường lửa cần phải được cài đặt thêm những logic mới, để có thể lường trước được những kết nối của FTP.
3. Việc thanh lọc giao thông FTP bên trình khách, khi nó hoạt động ở chế độ năng động, dùng bức tường lửa, là một việc khó làm, vì trình khách phải tùy ứng mở một [cổng](#) mới để tiếp nhận đòi hỏi kết nối khi nó xảy ra. Vấn đề này phần lớn được giải quyết bằng cách chuyển FTP sang dùng ở chế độ bị động.
4. Người ta có thể lạm dụng tính năng ủy quyền, được cài đặt sẵn trong giao thức, để sai khiến [máy chủ](#) gửi dữ liệu sang một cổng tùy chọn ở một máy tính thứ ba. Xin xem thêm về [FXP](#).

5. FTP là một giao thức có tính trì trệ rất cao (*high latency*). Sự trì trệ gây ra do việc, nó bắt buộc phải giải quyết một số lượng lớn các dòng lệnh khởi đầu một phiên truyền tải.
6. Phần nhận không có phương pháp để kiểm chứng tính toàn vẹn của dữ liệu được truyền sang. Nếu kết nối truyền tải bị ngắt giữa lưng chừng thì không có cách gì, trong giao thức, giúp cho phần nhận biết được rằng, tập tin nhận được là hoàn chỉnh hay còn vẫn còn thiếu sót. Sự hỗ trợ bên ngoài, như việc dùng kiểm tra tổng [MD5](#), hoặc dùng [kiểm đo dư tuần hoàn](#) (*cyclic redundancy checking*) là một việc cần thiết.

1.4. Những vấn đề về bảo an khi dùng FTP

FTP là một phương pháp truyền tập tin có truyền thống phi bảo an (không an toàn), vì theo như bản thiết kế gốc đặc tả của FTP, không có cách nào có thể truyền tải dữ liệu dưới hình thức mật mã hóa được. Ảnh hưởng này có nghĩa là, phần lớn các cài đặt của mạng lưới truyền thông, tên người dùng, mật khẩu, dòng lệnh FTP và tập tin được truyền tải, đều có thể bị người khác trên cùng một mạng lưới, "ngửi" hoặc quan sát, dùng phần mềm [phân tích giao thức](#) (*protocol analyzer*) (hoặc còn gọi là "dụng cụ ngửi dữ liệu", tiếng Anh là "sniffer"). Nên chú ý rằng đây là vấn đề thường thấy ở các giao thức của Internet được thiết kế trước khi [SSL](#) (*Secure Sockets Layer*) ra đời (tạm dịch là giao thức "tàng kết nối bảo mật"), như [HTTP](#), [SMTP](#) và [Telnet](#). Giải pháp thường thấy, đối với vấn đề này, là dùng [SFTP](#) (*Secure Shell File Transfer Protocol* - tạm dịch là "giao thức truyền tập tin dùng trình bao bảo mật"), một giao thức dựa trên nền của [SSH](#), hoặc trên [FTPS](#) (*FTP over SSL*). [SFTP](#) là FTP được cộng thêm chức năng mã hoá dữ liệu của [SSL](#) hoặc [TLS](#) (*Transport Layer Security* - tạm dịch là "Bảo mật tầng giao vận").

1.5. Các mã hồi âm của FTP

Xin xem thêm: [Danh sách toàn bộ các mã hồi âm của trình chủ FTP](#).

Mã hồi âm của trình chủ FTP chỉ định hiện trạng của trình, sau khi đã hoạt động, bằng giá trị của con số trong vị trí của nó. Nghĩa của những con số và vị trí có thể được lược giải như sau:

- 1xx: Hồi âm sơ bộ tích cực. Đề nghị thao tác đã bắt đầu khởi hành, song chương trình còn phải đợi một thông điệp hồi âm nữa, trước khi đề nghị thao tác được tiến hành.
- 2xx: Hồi âm hoàn thành tích cực. Đề nghị thao tác đã hoàn thành. Trình khách có thể tiếp tục gửi dòng lệnh mới sang.
- 3xx: Hồi âm trung gian tích cực. Dòng lệnh đã được thao tác và xử lý thành công, song trình chủ còn phải đợi một dòng lệnh khác nữa, trước khi toàn bộ đề nghị được giải quyết.
- 4xx: Hồi âm phủ quyết tạm thời. Dòng lệnh không được thao tác và xử lý, song trình khách có thể gửi yêu cầu sang một lần nữa, vì sự thất bại trong việc xử lý dòng lệnh đầu tiên chỉ là tạm thời.
- 5xx: Hồi âm phủ quyết toàn phần. Dòng lệnh không được xử lý, và trình khách không nên gửi lại yêu cầu ấy thêm một lần nào nữa.
- x0z: Sự thất bại xảy ra vì lỗi trong cú pháp.
- x1z: Thông điệp trả lời là hồi âm của một yêu cầu về tin tức.
- x2z: Thông điệp trả lời là hồi âm về tin tức liên quan đến liên kết (*connection*).

- x3z: Thông điệp trả lời là hồi âm liên quan đến trương mục và quyền hạn.
- x4z: Không rõ.
- x5z: Thông điệp trả lời là hồi âm liên quan đến hệ thống tập tin.

1.6.FTP nặc danh

Nhiều máy chủ chạy [trình chủ FTP](#) cho phép cái gọi là "FTP [nặc danh](#)". Bố trí này cho phép người dùng truy nhập vào máy chủ mà không cần có [trương mục](#). Tên người dùng của truy cập nặc danh thường là hai chữ 'nặc danh' hoặc một chữ 'ftp' mà thôi. Trương mục này không có mật khẩu. Tuy người dùng thường bị đòi hỏi phải kèm địa chỉ thư điện tử của mình vào, thay thế cho mật khẩu, hòng giúp phần mềm xác minh người dùng, song thủ tục xác minh thường là rất sơ sài và hầu như không có - tùy thuộc vào trình chủ FTP đang được dùng và sự cài đặt của nó. [Internet Gopher](#) đã được đề nghị trở thành một hình thức thay thế của FTP [nặc danh](#).

1.7.Dạng thức của dữ liệu

Có hai chế độ được dùng để truyền tải dữ liệu qua mạng lưới truyền thông:

1. Chế độ [ASCII](#)
2. Chế độ [Nhi phân](#)

Hai chế độ này khác nhau trong cách chúng gửi dữ liệu. Khi một tập tin được truyền dùng chế độ [ASCII](#), mỗi một chữ, mỗi con số, và mỗi ký tự đều được gửi trong dạng mã ASCII. Máy nhận tin lưu trữ chúng trong một tập tin văn bản thường, dưới dạng thức thích hợp (chẳng hạn, một máy dùng Unix sẽ lưu trữ nó trong dạng thức của Unix, một máy dùng Macintosh sẽ lưu trữ nó trong dạng thức của Mac). Vì thế, khi chế độ [ASCII](#) được dùng trong một cuộc truyền tải dữ liệu, phần mềm FTP sẽ tự cho rằng các dữ liệu được truyền gửi có dạng thức [văn bản thường](#) (*plain text*), và lưu trữ trên máy nhận theo dạng thức của máy. Chuyển đổi giữa các dạng thức [văn bản thường](#) bao gồm việc, thay thế mã kết dòng và mã kết tập tin, từ những mã tự được dùng ở máy nguồn, sang những mã tự được dùng ở máy đích, chẳng hạn một máy dùng hệ điều hành Windows, nhận một tập tin từ một máy dùng hệ điều hành Unix, máy dùng Windows sẽ thay thế những chữ xuống dòng ([carriage return](#)) bằng một cặp mã, bao gồm mã xuống dòng và mã thêm hàng ([carriage return and line feed pairs](#)). Tốc độ truyền tải tập tin dùng mã [ASCII](#) cũng nhanh hơn một chút, vì bit ở hàng cao nhất của mỗi byte của tập tin bị bỏ [\[1\]](#).

Gửi tập tin dùng chế độ nhị phân khác với cái trên. Máy gửi tập tin gửi từng bit một sang cho máy nhận. Máy nhận lưu trữ dòng bit, y như nó đã được gửi sang. Nếu dữ liệu không phải ở dạng thức văn bản thường, thì chúng ta phải truyền tải chúng ở chế độ nhị phân, nếu không, dữ liệu sẽ bị thoái hóa, không dùng được.

Theo như cài đặt sẵn, phần lớn các trình khách FTP dùng chế độ [ASCII](#) khi khởi công. Một số trình khách FTP xét nghiệm tên và nội dung của tập tin được gửi, để xác định chế độ cần phải dùng.

1.8.FTP và các trình duyệt

Đa số các [trình duyệt web](#) (web browser) gần đây và [trình quản lý tập tin](#) (file manager) có thể kết nối vào các máy chủ FTP, mặc dù chúng có thể còn thiếu sự hỗ trợ cho những mở rộng của giao thức, như [FTPS](#) chẳng hạn. Điều này cho phép người dùng thao tác các tập tin từ xa, thông qua kết nối FTP, dùng một giao diện quen thuộc, tương tự như giao diện trong máy của mình (ví dụ liệt kê danh sách của các tập tin của máy ở xa trông giống như phần liệt kê của máy mình, đồng thời các thao tác sao bản tập tin (copy), đổi tên, xóa, v.v.. được xử lý như là chúng ở trong máy mình vậy). Phương pháp làm là thông qua FTP [URL](#), dùng dạng thức ftp(s)://<địa chỉ của máy chủ FTP> (ví dụ: <ftp.gimp.org>). Tuy không cần thiết, song mật khẩu cũng có thể gửi kèm trong URL, ví dụ: ftp(s)://<tên người dùng>:<mật khẩu>@<địa chỉ của máy chủ FTP>:<số cổng>. Đa số các [trình duyệt web](#) đòi hỏi truyền tải FTP ở chế độ bị động, song không phải máy chủ FTP nào cũng thích ứng được. Một số [trình duyệt web](#)

2-Ứng dụng cài đặt dịch vụ FTP

Các bước thực hiện

1. Cài đặt Web Server (IIS)
2. Cấu hình và thiết lập bảo mật cho Server FTP
3. Cấu hình Firewall trên Server cho phép nhận kết nối đến qua giao thức FTP
4. Cấu hình Router cho phép kết nối đến thông qua cổng của giao thức FTP

• **Bước 1: Cài đặt WebServer IIS**

nhấp vào để xem hướng dẫn:

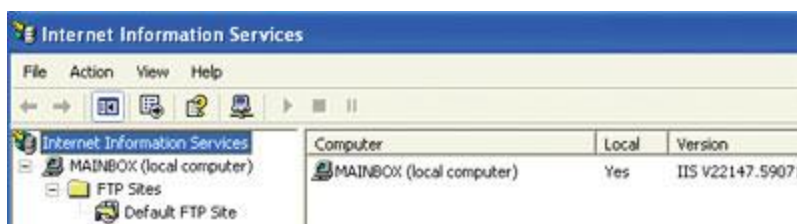
Bước 2: Cấu hình và thiết lập bảo mật cho Server FTP

Sau khi IIS đã được cài đặt thành công, một site FTP sẽ được tự động thiết lập trong thư mục C:\inetpub\ftproot. Thư mục này mặc định trống và hoàn toàn không được áp đặt bất cứ biện pháp bảo mật nào.

Bất cứ ai cũng có thể truy cập thông qua dòng lệnh ftp://(địa chỉ IP của bạn).

Để thay đổi một số tùy chọn, bạn thực hiện như sau:

Vào Start > Control Panel và chọn Switch to Classic View trong ô tùy chọn phía trên bên trái. Tiếp theo, bạn chọn Administrative Tools > Internet Information Services.

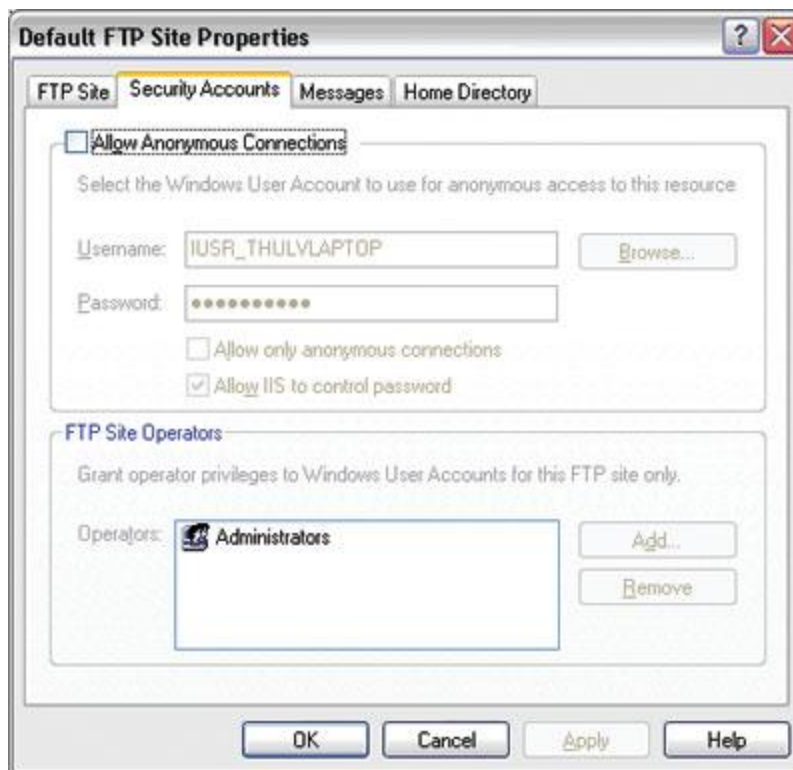


Từ cửa sổ này, bạn mở Local Computer > FTP Sites > Default FTP Site. Nhấn chuột phải vào đây và chọn Rename để đổi tên.

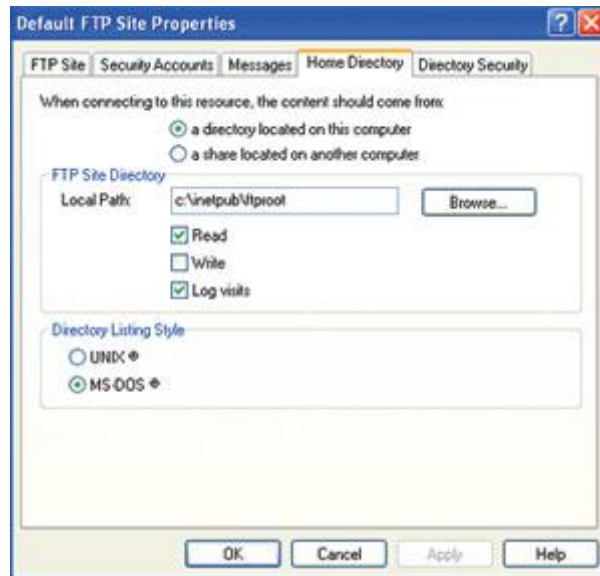


Nhấn chuột phải vào site rồi chọn Properties. Cửa sổ này là trung tâm điều khiển site FTP của bạn.

- Tab đầu tiên FTP Site cho phép bạn đổi tên site và thiết lập cổng truy cập (bạn có thể để mặc định 21). Ngoài ra còn có thông tin về các kết nối và báo cáo chi tiết (Log).
- Phần Connection có 2 mục. Hộp Limited To cho phép thiết lập số người dùng tối đa có thể truy cập vào site FTP trong cùng một thời điểm. Chú ý, với Windows XP Professional mặc định tối đa luôn là 10, dĩ nhiên bạn có thể thiết lập thấp hơn nếu muốn.
- Hộp thoại Connection TimeOut biểu thị thời gian cho phép người dùng kết nối trong trạng thái rồi trước khi bị máy chủ ngắt kết nối. Nhấn vào Current Sessions ở phía dưới, bạn sẽ xem được danh sách những người dùng đang kết nối và nếu muốn bạn có thể ngắt bất cứ kết nối nào.
- Tab Security Accounts sẽ xác lập những người dùng vô danh (Anonymous Users) có thể thực hiện truy cập vào site FTP hay không. Như đã đề cập ở trên, mặc định bất cứ ai cũng có thể truy cập mà không cần tài khoản do IIS sử dụng một tài khoản mặc định tích hợp. Tài khoản này có tên dạng IUSR_(tên máy tính) được tạo ra khi bạn cài đặt IIS. Nó cũng có chức năng kiểm soát truy cập những website và thành phần web khác mà máy tính bạn đang lưu giữ.



Việc để nguyên thiết lập mặc định sẽ cho phép bất cứ ai cũng có thể xem nội dung thông tin site FTP của bạn, tuy nhiên nếu vô hiệu hóa nó, bạn cũng sẽ phải đối mặt một số vấn đề (sẽ được đề cập trong phần sau của bài viết). Tạm thời bạn có thể để nguyên thiết lập mặc định. Trong phần cuối Messages, bạn có thể tạo một số thông báo mà người dùng truy cập vào site FTP sẽ nhận được khi thực hiện các tác vụ cơ bản. Tab thứ tư Home Directory cho phép bạn chỉ định thư mục gốc FTP trên ổ đĩa cứng nơi lưu thông tin sẽ hiển thị trên site FTP. Trong mục FTP Site Directory, bạn chỉ định thư mục muốn dùng và xác lập quyền truy cập đối với người dùng (cho phép đọc/ghi và thiết lập theo dõi nếu cần thiết). Sau khi chỉ định thư mục, bạn chỉ cần copy những dữ liệu muốn chia sẻ vào đó là xong.

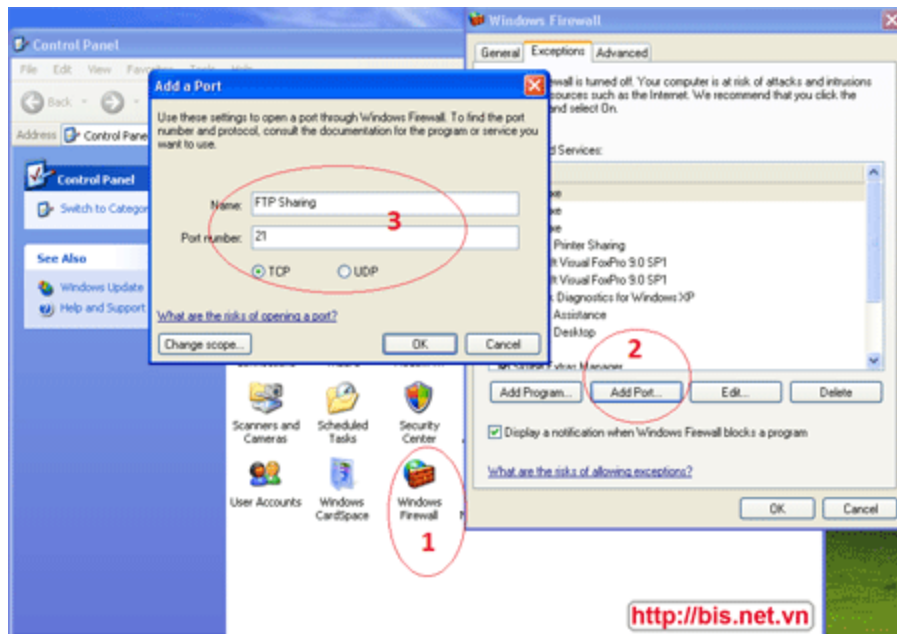


• **Bước 3: Cấu hình Firewall cho phép nhận kết nối đến qua giao thức FTP**

Mục đích của việc này là để mở cổng Firewall của Windows cho phép nhận kết nối từ bên ngoài qua cổng của giao thức FTP, mặc định là cổng 21

*** Trên WindowsXP**

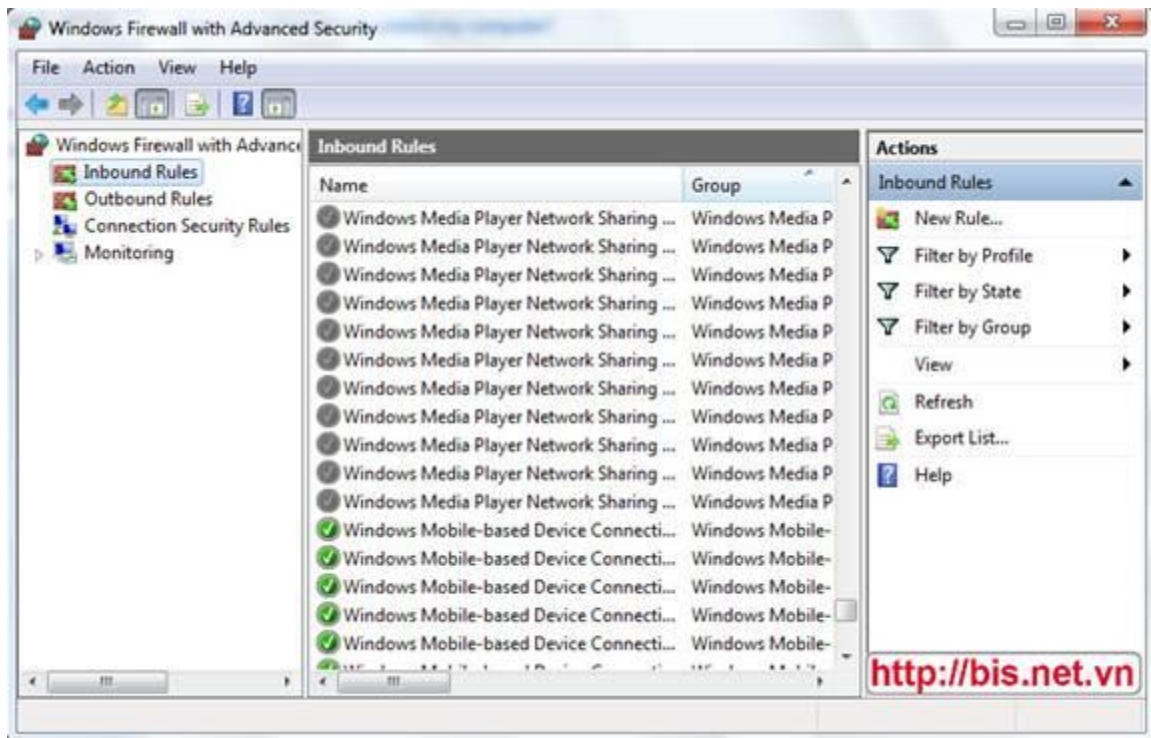
- Vào Control Panel -> Windows Firewall
- Trong Tab Exceptions, click vào nút Add Port để thêm cổng 21
- Hộp thoại Add Port hiện ra, trong mục Name gõ tên bất kỳ, Port Number gõ số 21, click chọn vào mục TCP (xem hình dưới)
- Nhấn OK
- Log Off hoặc Restart lại máy



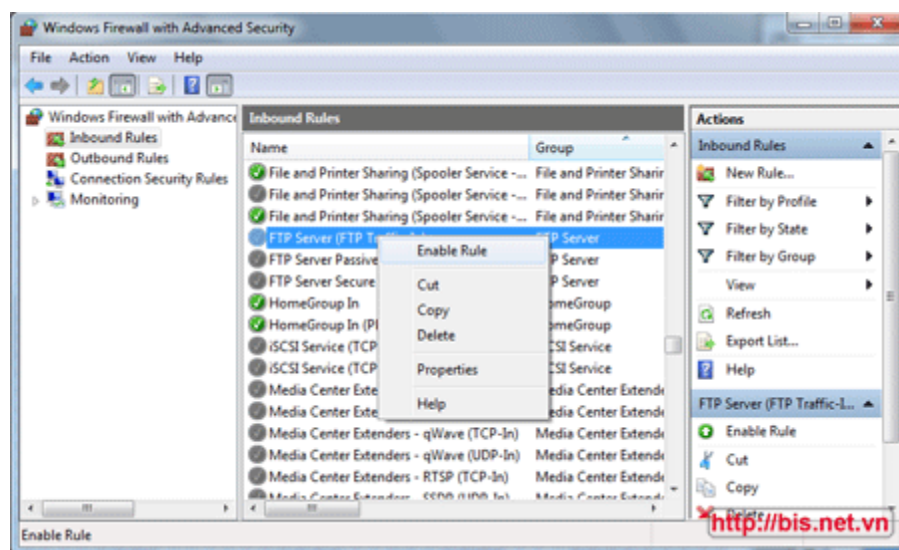
*** Trên Windows Vista, Windows 7:**

Vào Start -> Control Panel -> Windows Firewall -> Ở menu bên trái chọn Advanced settings

Menu bên trái, click vào mục Inbound Rules



Mặc định thì Windows đã có sẵn mục FTP Server, bạn tìm trong danh sách và Click chuột phải -> Properties, đánh chọn Enabled và Allow the connection như hình



Log Off hoặc Restart lại máy

• **Bước 4: Cấu hình Router cho phép kết nối qua Port 21**

Mục đích của việc này:

- Mở cổng của Router trên mạng của bạn để cho phép nhận kết nối từ bên ngoài mạng (từ Internet) qua cổng của giao thức FTP (Port 21).
- Chuyển hướng (Forward) kết nối về đến đúng máy mà bạn làm Server khi Router nhận được yêu cầu qua cổng 21. (Hãy nhớ rằng trong mạng LAN của bạn có thể có nhiều máy, và Router cần phải biết rằng bạn đang cài IIS trên máy nào)

Tùy loại Router mà bạn đang sử dụng, việc cấu hình có thể khác nhau đôi chút. Ở đây tôi đang thực hiện config trên một loại Router của Dlink. Các loại Router khác bạn có thể tự tìm hiểu thêm. Cách thiết lập trên các loại Router cơ bản là giống nhau, chỉ khác nhau về cách bố trí trên menu thôi.

Đầu tiên mở IE ra và gõ địa chỉ của Gateway -> Enter và đăng nhập vào quản trị Router

Ví dụ: Gateway của tôi là 192.168.1.1 thì tôi gõ vào Address của IE là <http://192.168.1.1> -> Enter

Hãy đọc hướng dẫn sử dụng kèm theo router của bạn để biết được địa chỉ gateway cũng như user và password đăng nhập vào quản trị.

Menu bên trái, chọn Advanced Setup -> NAT -> Virtual Servers

Click Add và thiết lập như trong hình -> Save

ADSL MODEM

Device Info
Quick Setup
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
Security
Quality of Service
Routing
DNS
DSL
Diagnostics
Management

<http://bis.net.vn>

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets. "Port End" cannot be changed. It is the same as "External Port End" normally and will be the same either one is modified.
Remaining number of entries that can be configured: 28

Server Name: Select One

Select a Service: Select One

Custom Server: FTP Sharing

Server IP Address: 192.168.1.2

Save/Apply

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
21	21	TCP	21	21
		TCP		
		TCP		
		TCP		

Hãy chú ý các mục mà tôi đánh dấu:

- Custom Server: Tên của thiết lập, do bạn tự đặt tùy ý
- Server IP Address: Đây là địa chỉ IP của máy mà bạn cài làm máy chủ. Ví dụ của tôi là 192.168.1.2. *Chú ý: Đây chính là IP của máy mà yêu cầu sẽ được Router chuyển đến. Do đó bạn nên khai báo IP tĩnh cho máy bạn cài làm máy chủ để khỏi phải vào mục này thiết lập lại mỗi khi restart máy. Xin nhớ rằng đây là IP của máy trong mạng LAN chứ không phải là IP đối với mạng Internet.*
- Port Start, Port End là số hiệu của cổng nhận yêu cầu, đều khai báo là 21. Ở đây sở dĩ có Port Start và Port End là vì Router cho phép bạn Forward trong cả một dải các cổng (từ cổng đến cổng). Đối với FTP thì chỉ cần Port 21 thôi. Một số loại router có mục Single Port Forwarding – cho phép bạn chỉ cần config một cổng thôi là đủ.
- Mục Protocol: Chọn phương thức kết nối là TCP.

Chú ý: Thường thì phần thiết lập này nằm trong mục NAT (Network Address Translation), hoặc có thể là Port Forwarding, ... tùy router. Để test kết quả thiết lập, bạn có thể dùng một chương trình quét cổng nào đó. Ở đây tôi xin bỏ qua việc hướng dẫn cách dò cổng.

Đến đây bạn đã hoàn thành việc cài máy chủ Web để xử lý giao dịch FTP qua cổng 21.

3-Dịch vụ Webserver

3.1.Giới thiệu

1. Web Server là gì?

Web Server (máy phục vụ Web): máy tính mà trên đó cài đặt phần mềm phục vụ Web, đôi khi người ta cũng gọi chính phần mềm đó là Web Server.

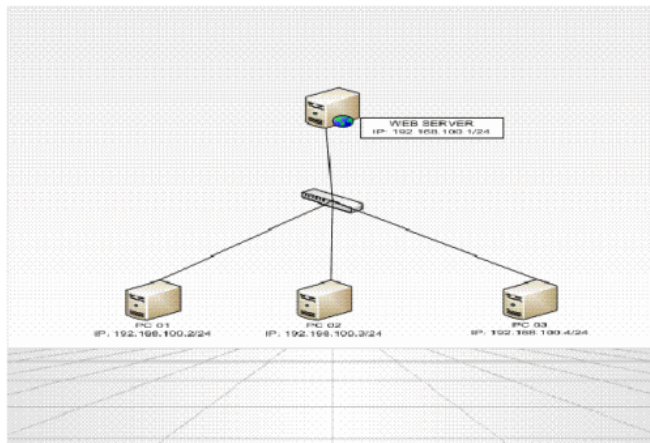


Web Server hay chính là máy chủ phục vụ web

Tất cả các Web Server đều hiểu và chạy được các file *.htm và *.html, tuy nhiên mỗi Web Server lại phục vụ một số kiểu file chuyên biệt chẳng hạn như IIS của Microsoft dành cho *.asp, *.aspx...; Apache dành cho *.php...; Sun Java System Web Server của SUN dành cho *.jsp...

3.2. Ứng dụng cài đặt

Mô hình lab



2. Yêu cầu

Cấu hình server 192.168.100.1 làm Web server

a) Cài đặt cơ bản

Cấu hình cho PC1

IP address: 192.168.100.2

Subnet mask: 255.255.255.0

Cấu hình cho PC2

IP address: 192.168.100.3

Subnet mask: 255.255.255.0

Cấu hình cho PC3

IP address: 192.168.100.4

Subnet mask: 255.255.255.0

Cấu hình cho Web Server

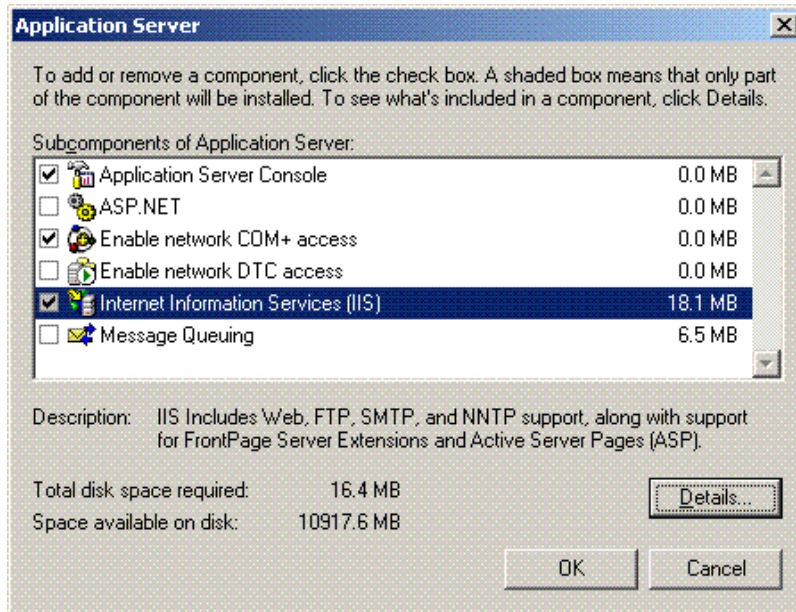
IP address: 192.168.100.1

Subnet mask: 255.255.255.0

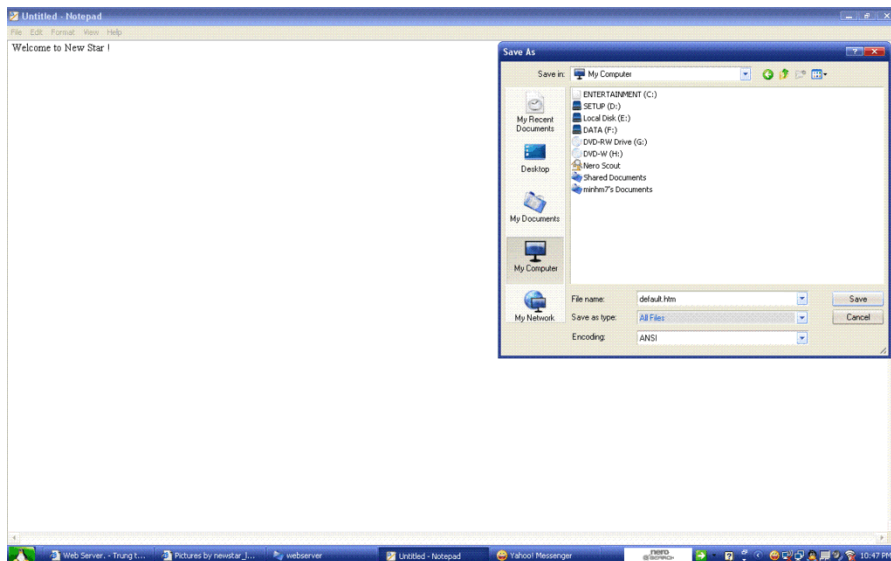
b) Cấu hình Web server

Các bước thực hiện:

- Cài đặt dịch vụ IIS: vào Control Panel -> Add or remove programs -> Add/remove windows components -> Application Server



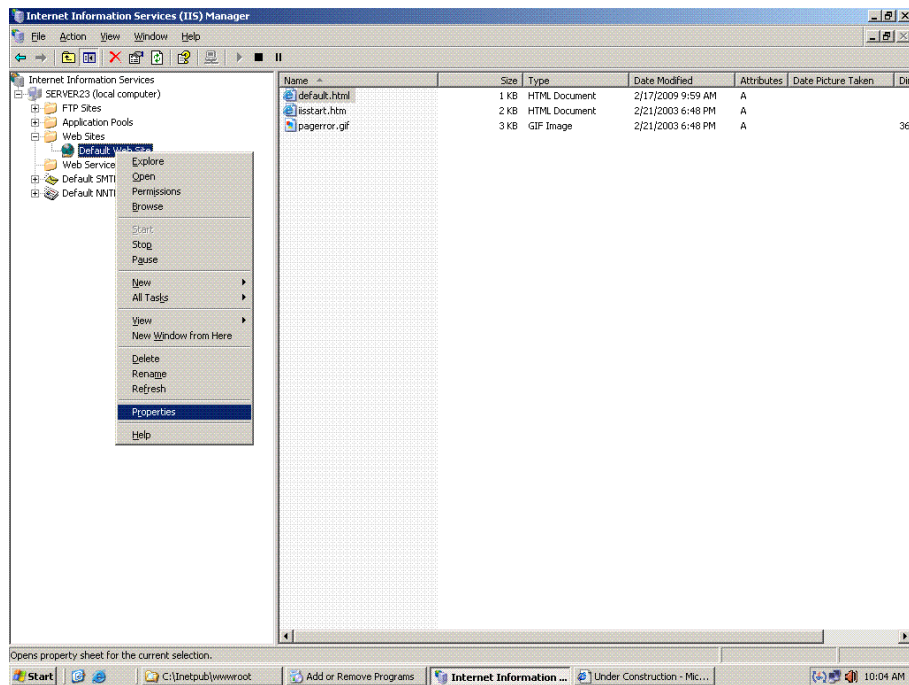
- Thiết kế một trang Web đơn giản (sử dụng Notepad)



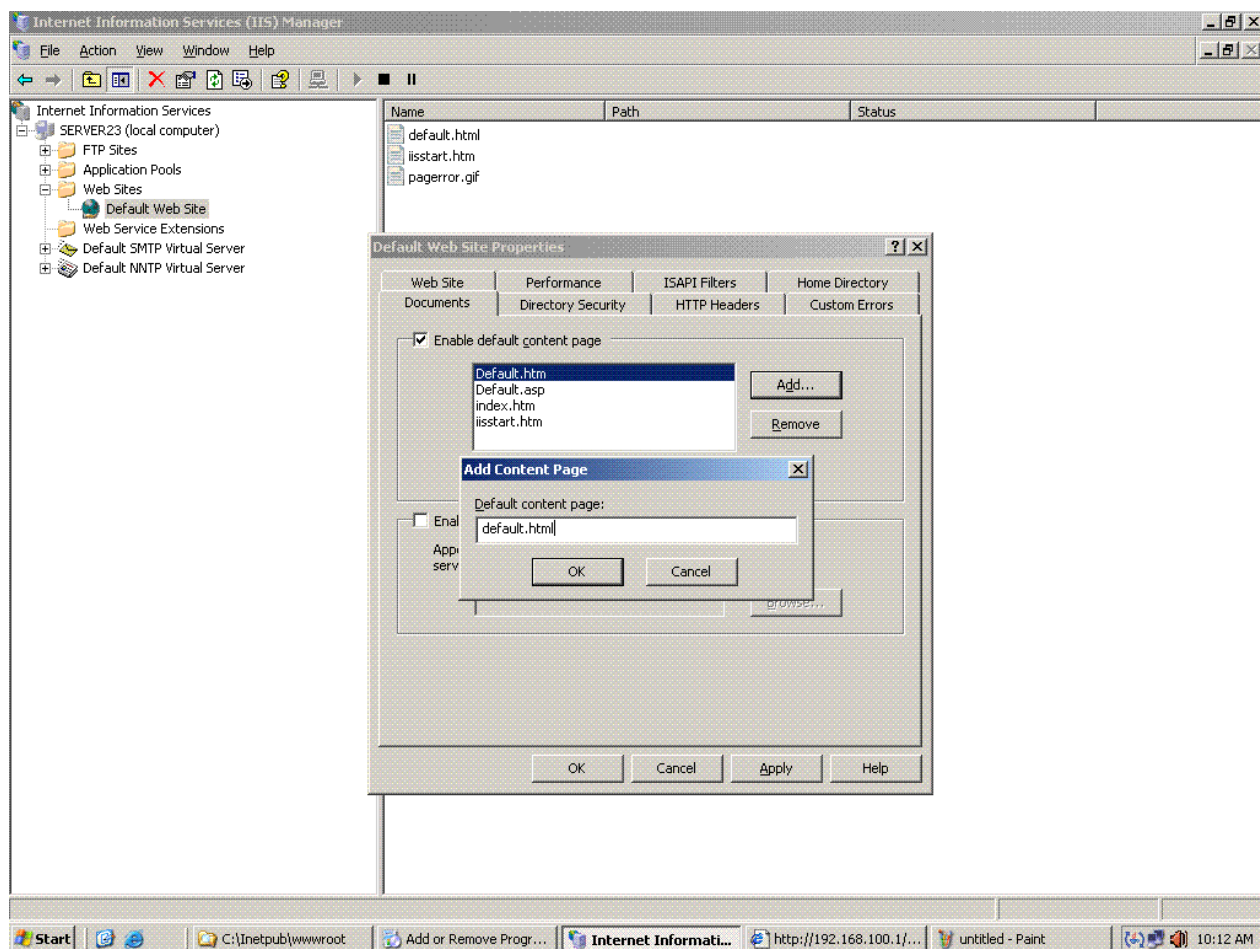
- Cấu hình các thông số trong IIS.

Vào Start => Administrative Tools => Internet Information Services(IIS) Manager

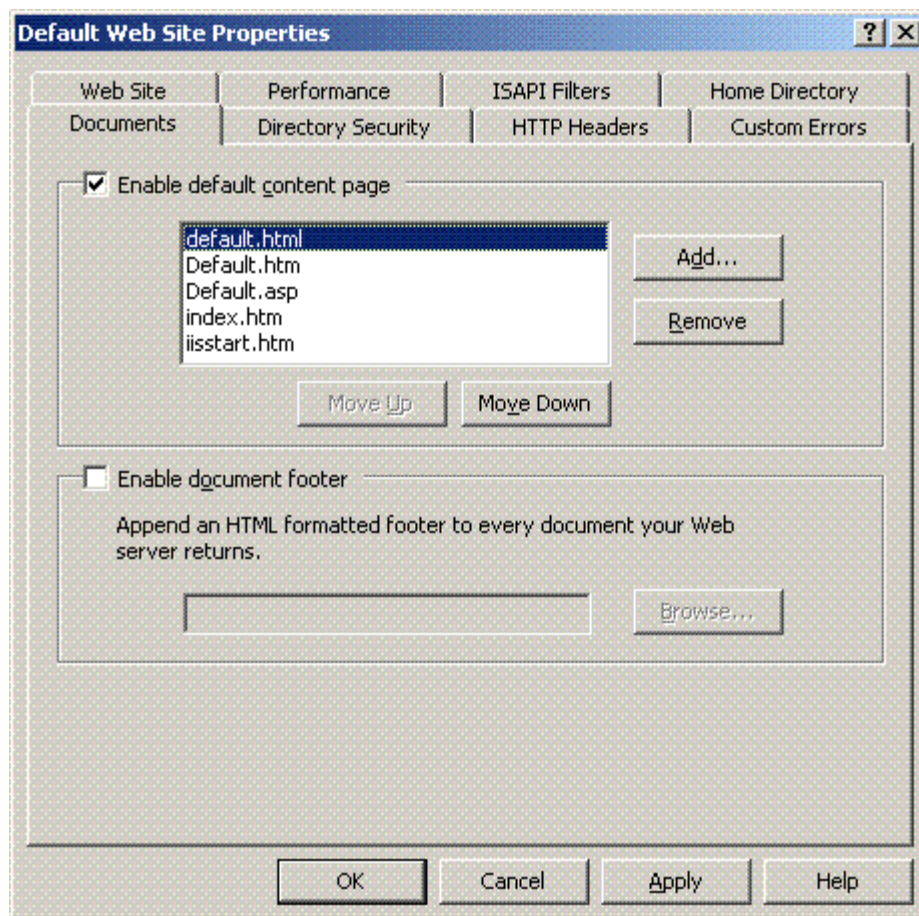
Vào Web Sites => click chuột phải vào Default Web Site => chọn Properties



Vào tab Documents => Click vào Add => Chọn trang web cần truy cập

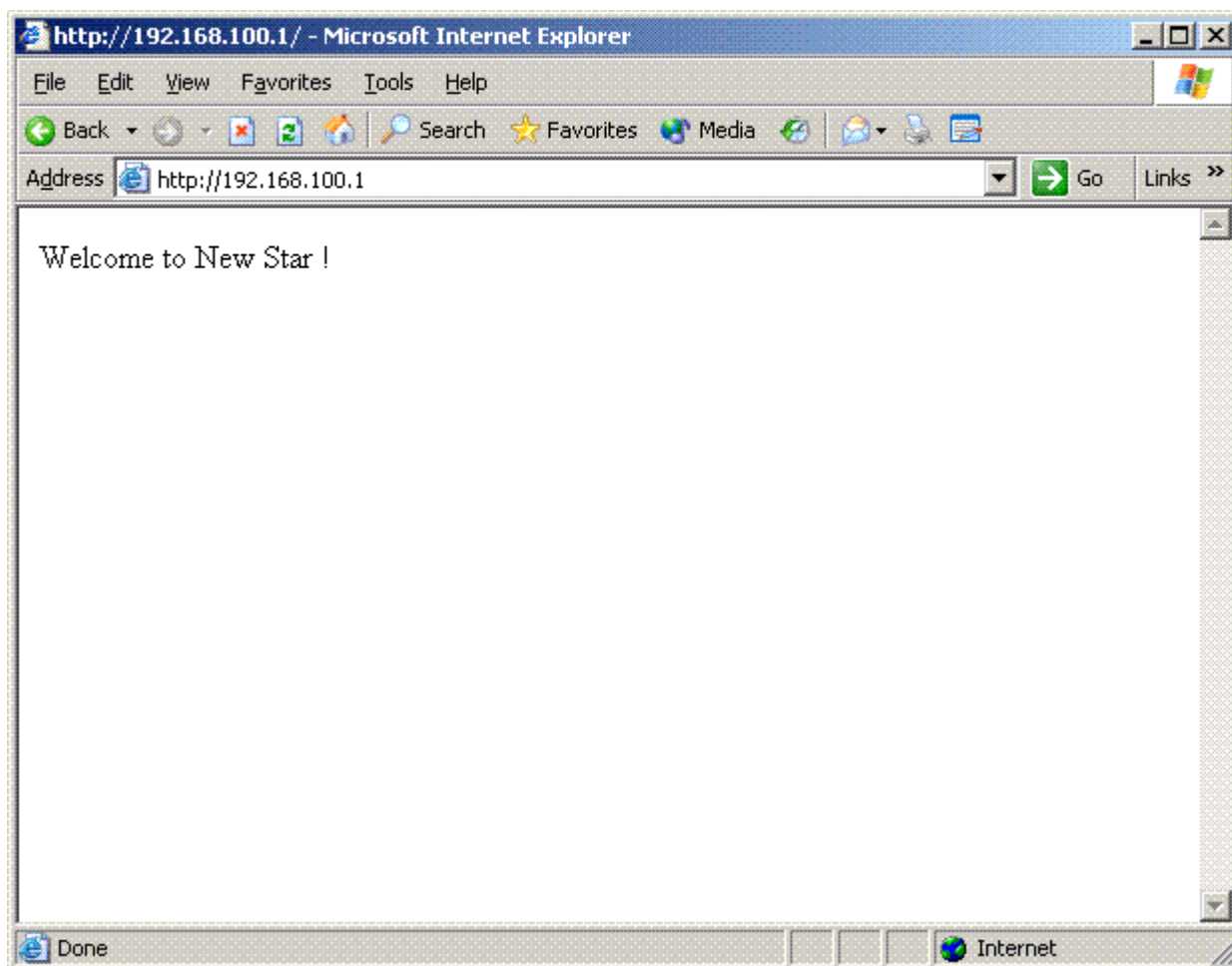


Sau đó nhấn Move Up để đưa trang web cần truy cập thành trang web mặc định.



c) Kiểm tra

Dùng các chương trình Web Browser: IE, Firefox, ... để kiểm tra.



Bài 5 : Cấu hình một số ADSL Router

I/Giới thiệu:

ADSL là từ viết tắt của [Tiếng Anh: Asymmetric Digital Subscriber Line](#) dịch sang tiếng Việt là **đường dây thuê bao số bất đối xứng**, là một dạng của [DSL](#).^[1] ADSL cung cấp một phương thức truyền dữ liệu với băng thông rộng, tốc độ cao hơn nhiều so với giao thức truy cập qua đường dây [điện thoại](#) truyền thống theo phương thức [truy cập quay số](#) (Dial up). Khi truyền băng thông trên đường dây điện thoại được tách ra làm 2 phần, 1 phần nhỏ dùng cho các tín hiệu như [Phone](#), [Fax](#). Phần lớn còn lại dùng cho truyền tải tín hiệu ADSL. Ý nghĩa của cụm từ "bất đối xứng" trong ADSL là do lượng dữ liệu tải xuống và tải lên là không bằng nhau, với dữ liệu chủ yếu là tải xuống.

1.Tổng quan



Một router ADSL hỗ trợ chuẩn Wi-Fi 802.11 b-g dùng để kết nối mạng Internet.

ADSL là sự thay thế với tốc độ cao cho thiết bị Modem hoặc ISDN giúp truy nhập Internet với tốc độ cao và nhanh hơn. Các biểu đồ sau chỉ ra các tốc độ cao nhất có thể đạt được giữa các dịch vụ cung cấp.

- **Asymmetric:** Tốc độ truyền không giống nhau ở hai chiều. Tốc độ của chiều xuống (từ mạng tới thuê bao) có thể nhanh gấp hơn 10 lần so với tốc độ của chiều lên (từ thuê bao tới mạng). Điều này phù hợp một phần cho việc khai thác [dịch vụ Internet](#) khi mà chỉ cần kết nối (tương ứng với lưu lượng nhỏ thông tin mà thuê bao gửi đi) là có thể nhận được một lưu lượng lớn dữ liệu tải về từ Internet.
- **Digital:** Các [Modem](#) ADSL hoạt động ở mức bit (0 & 1) và dùng để chuyển thông tin số hoá giữa các thiết bị số như các máy tính PC. Chính ở khía cạnh này thì ADSL không có gì khác với các Modem thông thường.
- **Subscriber Line:** ADSL tự nó chỉ hoạt động trên đường dây thuê bao bình thường nối tới tổng đài nội hạt. Đường dây thuê bao này vẫn có thể được tiếp tục sử dụng cho các cuộc gọi đi hoặc

nghe điện thoại cùng một thời điểm thông qua thiết bị gọi là "Splitters" có chức năng tách thoại và dữ liệu trên đường dây.

2. Ứng dụng

ADSL xác lập cách thức dữ liệu được truyền giữa thuê bao (nhà riêng hoặc công sở) và tổng đài thoại nội hạt trên chính đường dây điện thoại bình thường, thường gọi các đường dây này là [local loop](#). Thực chất của ứng dụng ADSL không phải ở việc truyền dữ liệu đi/đến tổng đài điện thoại nội hạt mà là tạo ra khả năng truy nhập Internet với tốc độ cao. Như vậy, vấn đề nằm ở việc xác lập kết nối dữ liệu tới Nhà cung cấp dịch vụ [Internet](#). Mặc dù ADSL được sử dụng để truyền dữ liệu bằng các giao thức Internet, nhưng trên thực tế việc thực hiện điều đó như thế nào lại không phải là đặc trưng kỹ thuật của ADSL. Hiện nay, phần lớn ADSL được dùng cho truy nhập Internet tốc độ cao và sử dụng các dịch vụ trên Internet một cách nhanh hơn.

II/Cơ chế hoạt động



Chip [DSL](#)

ADSL tìm cách khai thác phần băng thông tương tự còn chưa được sử dụng trên đường dây nối từ thuê bao tới tổng đài nội hạt. Đường dây này được thiết kế để chuyển tải [dải phổ tần số](#) (frequency spectrum) chiếm bởi cuộc thoại bình thường. Tuy nhiên, nó cũng có thể chuyển tải các tần số cao hơn dải phổ tương đối hạn chế dành cho thoại. Đó là dải phổ mà ADSL sử dụng.

Toạ cơ bản sử dụng dải tần số từ 300 Hz tới 3,400 Hz. Trên thực tế, các Splitter được sử dụng để đảm bảo dữ liệu và thoại không xâm phạm lẫn nhau trên đường truyền. Các tần số mà mạch vòng có thể chuyển tải, hay nói cách khác là khối lượng dữ liệu có thể chuyển tải sẽ phụ thuộc vào các nhân tố sau:

- Khoảng cách từ tổng đài nội hạt.
- Kiểu và độ dày đường dây.
- Kiểu và số lượng các mối nối trên đường dây.
- Mật độ các đường dây chuyển tải ADSL, ISDN và các tín hiệu phi thoại khác.
- Mật độ các đường dây chuyển tải tín hiệu radio.

III-Các thành phần của ADSL

Trong phần này chúng ta sẽ lần lượt mô tả chức năng của từng thành phần của ADSL, bắt đầu từ Modem ADSL tới Nhà cung cấp dịch vụ Internet. Chúng ta cũng xem xét ở phía ISP để lọc ra những thành phần cơ bản mà họ sử dụng để cung cấp dịch vụ ADSL.

Modem ADSL

Modem ADSL kết nối vào đường dây điện thoại (còn gọi là local loop) và đường dây này nối tới thiết bị tổng đài nội hạt. Modem ADSL sử dụng kết hợp một loạt các kỹ thuật xử lý tín hiệu tiên tiến nhằm đạt được tốc độ băng thông cần thiết trên đường dây điện thoại thông thường với khoảng cách tới vài km giữa thuê bao và tổng đài nội hạt.

Hoạt động của Modem ADSL

ADSL hoạt động bằng cách vận hành cùng lúc nhiều Modem, trong đó mỗi Modem sử dụng phần băng thông riêng có thể.

Sơ đồ trên đây chỉ mô phỏng một cách tương đối, nhưng qua đó ta có thể nhận thấy ADSL sử dụng rất nhiều Modem riêng lẻ hoạt động song song để khai thác băng thông tối đa và cung cấp một tốc độ rất cao. Mỗi đường kẻ sọc đen ở trên thể hiện một Modem và chúng hoạt động tại các tần số hoàn toàn khác nhau. Trên thực tế có thể tới 255 Modem hoạt động trên một đường ADSL. Điểm đặc biệt ở chỗ ADSL sử dụng dải tần số từ 26 kHz tới 1.1 MHz trong 10 MHz của băng thông thoại. Tất cả 255 Modems này được vận hành chỉ trên một con chip đơn.

Lượng dữ liệu mà mỗi Modem có thể truyền tải phụ thuộc vào các đặc điểm của đường dây tại tần số mà Modem đó chiếm. Một số Modem có thể không làm việc một chút nào vì sự gây nhiễu từ nguồn tín hiệu bên ngoài chẳng hạn như bởi một đường dây (local loop) khác hoặc nguồn phát vô tuyến nào đó. Các Modem ở tần số cao hơn thông thường lại truyền tải được ít dữ liệu hơn bởi lý ở tần số càng cao thì sự suy hao càng lớn, đặc biệt là trên một khoảng cách dài.

Mạch vòng/Local Loop

"Local loop" là thuật ngữ dùng để chỉ các đường dây điện thoại bình thường nối từ vị trí người sử dụng tới công ty điện thoại. Nguyên nhân xuất hiện thuật ngữ local loop - đó là người nghe (điện thoại) được kết nối vào hai đường dây mà nếu nhìn từ tổng đài điện thoại thì chúng tạo ra một mạch vòng local loop.

IV/Các thành phần ADSL từ phía nhà cung cấp dịch vụ

Phạm vi Nhà cung cấp dịch vụ gồm có ba thành phần quan trọng bao gồm: [DSLAM](#) - DSL Access Multiplexer, [BAS](#) - Broadband Access Server và [ISP](#) - Internet Service Provider.

DSLAM

Một thiết bị [DSLAM](#) có thể tập hợp nhiều kết nối thuê bao ADSL - có thể nhiều tới hàng trăm thuê bao - và tụ lại trên một kết nối cáp quang. Sợi cáp quang này thường được nối tới thiết bị gọi là [BAS](#) - Broadband Access Server, nhưng nó cũng có thể không nối trực tiếp tới BAS vì BAS có thể được đặt tại bất cứ đâu. DSLAM là thiết bị đặt ở phía tổng đài, là điểm cuối của kết nối ADSL. Nó chứa vô số các Modem ADSL bố trí về một phía hướng tới các mạch vòng và phía kia là kết nối cáp quang.

BAS

Broadband Access Server (BAS) là thiết bị đặt giữa DSLAM và POP của ISP. Một thiết bị BAS có thể phục vụ cho nhiều DSLAM. Các giao thức truyền thông được đóng gói để truyền dữ liệu thông qua kết nối ADSL, vì vậy mục đích của BAS là mở gói để hoàn trả lại các giao thức đó trước khi đi vào Internet. Nó cũng đảm bảo cho kết nối của bạn tới ISP được chính xác giống như khi bạn sử dụng Modem quay số hoặc ISDN. Như chú giải ở trên, ADSL không chỉ rõ các giao thức được sử dụng để tạo thành kết nối tới Internet. Phương pháp mà PC và Modem sử dụng bắt buộc phải giống như BAS sử dụng để cho kết nối thực hiện được. Thông thường ADSL sử dụng hai giao thức chính là: [PPPoE](#) (PPP over Ethernet Protocol) và [PPPoA](#) (Point to Point Protocol over ATM).

V/Kết nối [mạng](#)

Kết nối các thành phần

Dưới đây sẽ trình bày về những giao thức truyền thông được sử dụng trên kết nối ADSL. Khi kết nối vào Internet, bạn sử dụng các giao thức chạy ở tầng vận chuyển TCP/IP (chẳng hạn như HTTP - giao thức được sử dụng bởi các Web Browser). Quá trình này là giống nhau với các kiểu truy nhập quay số qua PSTN, ISDN và ADSL.

Các giao thức được sử dụng giữa Modem và BAS

Khi quay số PSTN/ISDN để truy nhập vào Internet, chúng ta sử dụng giao thức gọi là PPP để vận chuyển dữ liệu TCP/IP và kiểm tra cũng như xác thực tên và mật khẩu người truy nhập. Trong ADSL, PPP cũng thường được sử dụng để kiểm tra tên và mật khẩu truy nhập, và ATM thì luôn được sử dụng ở mức thấp nhất. Kết nối điển hình như dưới đây:

Vai trò của ATM

ATM - Asynchronous Transfer Mode, được sử dụng như là công cụ chuyển tải cho ADSL ở mức thấp. Lý do vì đó là cách thuận tiện và mềm dẻo đối với các công ty thoại muốn kéo dài khoảng cách kết nối từ DSLAM tới BAS giúp họ có thể đặt BAS ở bất cứ đâu trên mạng. Có hai tham số cần phải thiết lập cấu hình một cách chính xác trên Modem ADSL để đảm bảo kết nối thành công tại mức ATM với DSLAM: VPI (Virtual Path Identifier) và VCI (Virtual Channel Identifier).

VI.Cấu trúc của ADSL

PPP là giao thức dùng để vận chuyển lưu lượng Internet tới ISP dọc theo các kết nối Modem và ISDN. PPP kết hợp chặt chẽ các yếu tố xác thực - kiểm tra tên/mật khẩu - và đó là lý do chính mà người ta dùng PPP với ADSL. Mặc dù BAS thực thi giao thức PPP và tiến hành việc xác thực, nhưng thực ra việc đó được thực hiện bằng cách truy nhập vào các cơ sở dữ liệu khách hàng đặt tại ISP. Bằng cách đó, ISP biết được rằng các kết nối do BAS định tuyến tới - đã được xác thực thông qua giao dịch với cơ sở dữ liệu riêng của ISP.

VII.Modem ADSL trên thực tế

Modem ADSL thông minh bản thân nó đã tích hợp sẵn các giao thức truyền thông cần thiết (chẳng hạn thiết bị Modem ADSL Router hoặc Modem được sử dụng kết nối qua cổng Card [Ethernet](#) 10/100Mb) nên chỉ việc lựa chọn và khai báo [VPI/VCI](#) cho [Modem](#).

Còn Modem ADSL thụ động thì phải hoạt động dựa trên hệ điều hành của máy tính để cung cấp các giao thức cần thiết. Các loại Modem này bắt buộc phải cài đặt phần mềm điều khiển Modem và thiết lập các giao thức PPP, VPI/VCI. Việc cấu hình như vậy phức tạp và đòi hỏi thời gian nhiều hơn.

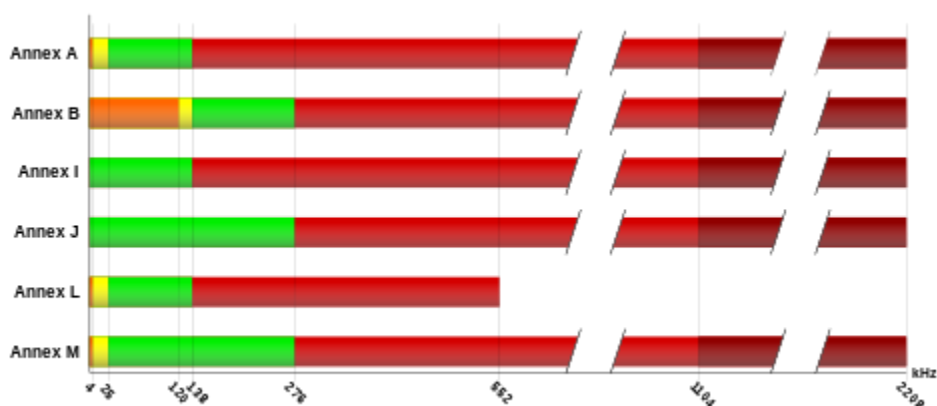
Chỉ có [Windows 98SE](#), [Windows ME](#), Windows 2000/XP và các Windows thế hệ mới là có cài sẵn cơ chế thực thi [ATM](#), vì thế người ta ít sử dụng các Modem thụ động trên thực tế. Mặc dù các Modem thông minh có hỗ trợ các giao thức cần thiết nhưng chúng vẫn có thể được dùng cho các hệ điều hành nói trên. Các Modem thụ động có thể nối với PC thông qua giao diện USB, hoặc có thể được sản xuất dưới dạng PCI Card để cắm thẳng trên bảng mạch chủ của PC. Lưu ý là việc khai thác giao thức ATM không có nghĩa là cần phải có Card mạng ATM cho PC - đó chỉ là cơ chế hỗ trợ bằng phần mềm trong hệ điều hành.

VIII.Mối tương quan giữa điện thoại và ADSL

ADSL cho phép cùng lúc vừa truy nhập Internet tốc độ cao lại vừa có thể thực hiện cuộc gọi cũng trên đường dây đó. Thiết bị chuyên dụng Splitters được sử dụng để tách riêng các tần số cao dùng cho ADSL và các tần số thấp dùng cho thoại. Như vậy, thông thường đặt các Splitters tại mỗi đầu của đường dây - phía thuê bao và phía DSLAM. Tại phía thuê bao, các tần số thấp được chuyển đến máy điện thoại còn các tần số cao đi đến modem ADSL. Tại các tổng đài, các tần số thấp được chuyển sang mạng thoại PSTN còn các tần số cao đi đến ISP.

Tốc độ của kết nối giữa modem ADSL và DSLAM phụ thuộc vào khoảng cách đường truyền và tốc độ tối đa được cấu hình sẵn trên cổng của DSLAM. Ngược lại, tốc độ kết nối vào Internet lại còn phụ thuộc vào nhiều yếu tố khác nữa như số người dùng kết nối, tốc độ kết nối giữa DSLAM và BAS, số lượng card DSLAM cùng nối vào một BAS và số lượng người thực tế đang kết nối.

IX.Các chuẩn ADSL



Tần số các chuẩn ADSL phổ biến

Phiên bản	Tên chuẩn	Tên phổ biến	Tốc độ tải về	Tốc độ tải lên	Ứng dụng năm
ADSL	ANSI T1.413-1998 Issue 2	ADSL	8.0 Mbit/s	1.0 Mbit/s	1998
ADSL	ITU G.992.1	ADSL (G.DMT)	8.0 Mbit/s	1.3 Mbit/s	1999-07
ADSL	ITU G.992.1 Annex A	ADSL over POTS	12.0 Mbit/s	1.3 Mbit/s	2001
ADSL	ITU G.992.1 Annex B	ADSL over ISDN	12.0 Mbit/s	1.8 Mbit/s	2005
ADSL	ITU G.992.2	ADSL Lite (G.Lite)	1.5 Mbit/s	0.5 Mbit/s	1999-07
ADSL2	ITU G.992.3	ADSL2	12.0 Mbit/s	1.3 Mbit/s	2002-07
ADSL2	ITU G.992.3 Annex J	ADSL2	12.0 Mbit/s	3.5 Mbit/s	
ADSL2	ITU G.992.3 Annex L	RE-ADSL2	5.0 Mbit/s	0.8 Mbit/s	
ADSL2	ITU G.992.4	splitterless ADSL2	1.5 Mbit/s	0.5 Mbit/s	2002-07
ADSL2+	ITU G.992.5	ADSL2+	20.0 Mbit/s	1.1 Mbit/s	2003-05
ADSL2+	ITU G.992.5 Annex M	ADSL2+M	24.0 Mbit/s	3.3 Mbit/s	2008
ADSL2++	(up to 3.75 MHz)	ADSL4	52.0 Mbit/s ?	5.0 Mbit/s ?	Đang phát triển

Bài 6 : Các kỹ thuật về chia sẻ Internet

I-Cách sử dụng Chia sẻ Kết nối Internet

Để sử dụng Chia sẻ Kết nối Internet để chia sẻ kết nối Internet của bạn, máy chủ phải có một bộ điều hợp mạng được cấu hình để kết nối mạng nội bộ, và một bộ điều hợp mạng hoặc modem được cấu hình để kết nối với Internet.

II-Trên máy chủ

Trên máy chủ, hãy làm theo các bước sau để chia sẻ kết nối Internet:

1. Đăng nhập vào máy tính chủ với tư cách Quản trị viên hoặc với tư cách Chủ nhân.
2. Bấm **Bắt đầu**, rồi bấm **Pa-nen Điều khiển**.
3. Bấm **Kết nối Mạng và Internet**.
4. Bấm **Kết nối Mạng**.
5. Bấm chuột phải vào kết nối bạn sử dụng để kết nối với Internet. Ví dụ, nếu bạn muốn kết nối với Internet bằng cách sử dụng modem, hãy bấm chuột phải vào kết nối bạn muốn thực hiện dưới **Quay số**.
6. Bấm **Thuộc tính**.
7. Bấm tab **Nâng cao**.
8. Trong **Chia sẻ Kết nối Internet**, hãy chọn hộp kiểm **Cho phép người dùng khác trong mạng kết nối thông qua kết nối Internet của máy tính này**.
9. Nếu bạn đang chia sẻ kết nối Internet quay số, hãy chọn hộp kiểm **Thiết lập một kết nối quay số bất kì khi nào một máy tính trong mạng của tôi định truy nhập Internet** nếu bạn muốn cho phép máy tính của mình tự động kết nối với Internet.
10. Bấm **OK**. Bạn nhận được thông báo sau:

Khi Chia sẻ Kết nối Internet có hiệu lực, bộ điều hợp mạng LAN của bạn sẽ được đặt để dùng địa chỉ IP 192.168.0.1. Máy tính của bạn có thể mất khả năng kết nối với máy tính khác trong mạng của bạn. Nếu những máy tính khác này có địa chỉ IP tĩnh, bạn nên đặt chúng để nhận địa chỉ IP tự động. Bạn có chắc bạn muốn cho phép Chia sẻ Kết nối Internet không?

11. Bấm **Có**.

Kết nối với Internet đã được chia sẻ tới các máy tính khác trên mạng cục bộ (LAN). Bộ điều hợp mạng đã kết nối với mạng nội bộ (LAN) được cấu hình với địa chỉ IP tĩnh là 192.168.0.1 và mặt nạ mạng là 255.255.255.0

Để xem video về cách để cấu hình máy chủ cho Chia sẻ Kết nối Internet , hãy bấm vào nút **Chạy** (



) trên trình xem Windows Media Player sau:

<http://support.microsoft.com/servicedesks/ShowMeHow/3061261.aspx>

Chú ý Để xem video này, máy tính của bạn phải được cài đặt Windows Media Player 7.0 hoặc phiên bản mới hơn.

Để biết thêm thông tin về cách có được Windows Media Player phiên bản 7.1, bấm vào số bài viết sau đây để xem bài viết trong Cơ sở Kiến thức Microsoft:

[299321](#) Mô tả và khả năng sẵn có của Windows Media Player 7.1

III-Trên máy khách

Để kết nối với Internet bằng cách sử dụng kết nối được chia sẻ, bạn phải xác nhận cấu hình IP bộ điều hợp mạng LAN, và sau đó để cấu hình máy khách. Để xác nhận cấu hình IP bộ điều hợp mạng LAN, hãy làm theo các bước sau:

1. Đăng nhập vào máy tính chủ với tư cách Quản trị viên hoặc với tư cách Chủ nhân.
2. Bấm **Bắt đầu**, rồi bấm **Pa-nen Điều khiển**.
3. Bấm **Kết nối Mạng và Internet**.
4. Bấm **Kết nối Mạng**.
5. Bấm chuột phải **Kết nối Mạng cục bộ**, sau đó bấm **Các đặc tính**.
6. Bấm vào tab **Chung**, bấm **Giao thức Internet (TCP/IP)** trong danh sách **Kết nối này dùng các khoản mục sau**, rồi bấm **Thuộc tính**.
7. Trong hộp thoại **Thuộc tính Giao thức Internet (TCP/IP)**, bấm **Tự động nhận địa chỉ IP** (nếu nó chưa được chọn), rồi bấm **OK**.

Chú ý Bạn cũng có thể gán địa chỉ IP tĩnh trong phạm vi từ 192.168.0.2 tới 192.168.0.254. Ví dụ, bạn có thể gán địa chỉ IP tĩnh, mặt nạ mạng và cổng nối mặc định sau:

8. Địa chỉ IP 192.168.0.2
9. Mặt nạ mạng 255.255.255.0
10. Cổng nối Mặc định 192.168.0.1

11. Trong hộp thoại **Thuộc tính Kết nối Nội mạng**, bấm **OK**.
12. Đóng Pa-nen Điều khiển.

Để xem video về cách để cấu hình máy chủ cho Chia sẻ Kết nối Internet, hãy bấm vào nút **Chạy** (



) trên trình xem Windows Media Player sau:

<http://support.microsoft.com/servicedesks/ShowMeHow/3061262.aspx>

Chú ý Để xem video này, máy tính của bạn phải được cài đặt Windows Media Player 7.0 hoặc phiên bản mới hơn.

Để biết thêm thông tin về cách có được Windows Media Player phiên bản 7.1, bấm vào số bài viết sau đây để xem bài viết trong Cơ sở Kiến thức Microsoft:

[299321](#) Mô tả và khả năng sẵn có của Windows Media Player 7.1

Để cấu hình máy khách sử dụng kết nối Internet được chia sẻ, hãy làm theo các bước sau:

1. Bấm **Bắt đầu**, rồi bấm **Pa-nen Điều khiển**.
 2. Bấm **Kết nối Mạng và Internet**.
 3. Bấm **Tùy chọn Internet**.
 4. Trong hộp thoại **Thuộc tính Hệ thống**, bấm tab **Khôi phục Hệ thống**.
 5. Bấm nút **Thiết lập**.
- Thuật sĩ Kết nối Mới khởi động.
6. Trên trang **Chào mừng bạn đến với Thuật sĩ Kết nối Mới**, bấm **Tiếp theo**.
 7. Bấm **Kết nối với Internet**, sau đó bấm **Tiếp theo**.
 8. Bấm **Thiết lập thủ công kết nối của tôi** rồi bấm **Tiếp theo**.
 9. Bấm **Kết nối sử dụng kết nối bằng thông rộng luôn được bật**, sau đó bấm **Tiếp theo**.
 10. Trên trang **Đang hoàn thành Thuật sĩ Kết nối Mới**, bấm **Kết thúc**.
 11. Đóng Pa-nen Điều khiển.

Khi bạn khởi động Microsoft Internet Explorer, máy khách sẽ cố kết nối với Internet bằng cách sử dụng kết nối Internet được chia sẻ của máy chủ.

Để xem video về cách để cấu hình máy khách cho Chia sẻ Kết nối Internet, hãy bấm vào nút **Chạy** (



) trên trình xem Windows Media Player sau:

<http://support.microsoft.com/servicedesks/ShowMeHow/3061263.aspx>

Chú ý Để xem video này, máy tính của bạn phải được cài đặt Windows Media Player 7.0 hoặc phiên bản mới hơn.

Để biết thêm thông tin về cách có được Windows Media Player phiên bản 7.1, bấm vào số bài viết sau đây để xem bài viết trong Cơ sở Kiến thức Microsoft:

[299321](#) Mô tả và khả năng sẵn có của Windows Media Player 7.1

IV-Khắc phục sự cố

Khi bạn bật Chia sẻ Kết nối Internet trên máy chủ, bộ điều hợp mạng LAN của máy chủ tự động được gán địa chỉ IP là 192.168.0.1. Do đó, một trong các tình huống sau đây có thể xảy ra:

- **Xung đột địa chỉ IP**
Mỗi máy tính trên mạng LAN phải có một địa chỉ IP duy nhất. Nếu hai máy tính trở lên có cùng một địa chỉ IP, xung đột IP xảy ra, và một trong các bộ điều hợp mạng tắt cho đến khi xung đột được giải quyết. Để giải quyết xung đột, hãy để cấu hình máy khách tự động nhận địa chỉ IP, hoặc gán cho máy khách một địa chỉ IP duy nhất.
- **Mất kết nối mạng**
Nếu mạng của bạn được cấu hình trong dải địa chỉ IP khác nhau so với việc dùng Chia sẻ Kết nối Internet, bạn sẽ mất kết nối mạng với máy chủ. Để giải quyết sự cố, hãy để cấu hình các máy

khách tự động nhận địa chỉ IP, hoặc gán cho mỗi máy khách một địa chỉ IP duy nhất trong phạm vi từ 192.168.0.2 tới 192.168.0.254.

Bài 7 : Định tuyến mạng

I-Giới thiệu tổng quan

Trong ngành [mạng máy tính](#), **định tuyến** ([tiếng Anh](#): *routing* hay *routeing*) là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó. Việc định tuyến được thực hiện cho nhiều loại mạng, trong đó có [mạng điện thoại](#), [liên mạng](#), [Internet](#), mạng giao thông.

[Routing](#) chỉ ra hướng, sự di chuyển của các gói (dữ liệu) được đánh địa chỉ từ mạng nguồn của chúng, hướng đến đích cuối thông qua các node trung gian; thiết bị phần cứng chuyên dùng được gọi là router (bộ định tuyến). Tiến trình định tuyến thường chỉ hướng đi dựa vào bảng định tuyến, đó là bảng chứa những lộ trình tốt nhất đến các đích khác nhau trên mạng. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

Routing khác với bridging (bắc cầu) ở chỗ trong nhiệm vụ của nó thì các cấu trúc địa chỉ gọi nên sự gần gũi của các địa chỉ tương tự trong mạng, qua đó cho phép nhập liệu một bảng định tuyến đơn để mô tả lộ trình đến một nhóm các địa chỉ. Vì thế, routing làm việc tốt hơn bridging trong những mạng lớn, và nó trở thành dạng chiếm ưu thế của việc tìm đường trên mạng Internet.

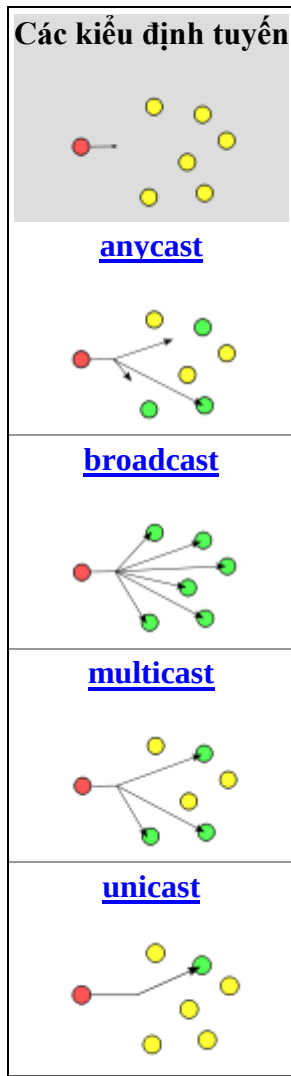
Các mạng nhỏ có thể có các bảng định tuyến được cấu hình thủ công, còn những mạng lớn hơn có topo mạng phức tạp và thay đổi liên tục thì xây dựng thủ công các bảng định tuyến là vô cùng khó khăn. Tuy nhiên, hầu hết mạng điện thoại chuyển mạch chung (public switched telephone network - PSTN) sử dụng bảng định tuyến được tính toán trước, với những tuyến dự trữ nếu các lộ trình trực tiếp đều bị nghẽn. Định tuyến động (dynamic routing) cố gắng giải quyết vấn đề này bằng việc xây dựng bảng định tuyến một cách tự động, dựa vào những thông tin được giao thức định tuyến cung cấp, và cho phép mạng hành động gần như tự trị trong việc ngăn chặn mạng bị lỗi và nghẽn.

Định tuyến động chiếm ưu thế trên Internet. Tuy nhiên, việc cấu hình các giao thức định tuyến thường đòi hỏi nhiều kinh nghiệm; đừng nên nghĩ rằng kỹ thuật nối mạng đã phát triển đến mức hoàn thành tự động việc định tuyến. Cách tốt nhất là nên kết hợp giữa định tuyến thủ công và tự động.

Những mạng trong đó các gói thông tin được vận chuyển, ví dụ như Internet, chia dữ liệu thành các gói, rồi dán nhãn với các đích đến cụ thể và mỗi gói được lập lộ trình riêng biệt. Các mạng xoay vòng, như mạng điện thoại, cũng thực hiện định tuyến để tìm đường cho các vòng (ví dụ như cuộc gọi điện thoại) để chúng có thể gửi lượng dữ liệu lớn mà không phải tiếp tục lặp lại địa chỉ đích.

Định tuyến IP truyền thống vẫn còn tương đối đơn giản vì nó dùng cách định tuyến bước kế tiếp (next-hop routing), router chỉ xem xét nó sẽ gửi gói thông tin đến đâu, và không quan tâm đường đi sau đó của gói trên những bước truyền còn lại. Tuy nhiên, những chiến lược định tuyến phức tạp hơn có thể được, và thường được dùng trong những hệ thống như MPLS, ATM hay Frame Relay, những hệ thống này đôi khi được sử dụng như công nghệ bên dưới để hỗ trợ cho mạng IP.

II-Các kiểu định tuyến



III-Các lớp thuật toán định tuyến

1-Thuật toán vector

(distance-vector routing protocols)

Thuật toán này dùng thuật toán Bellman-Ford. Phương pháp này chỉ định một con số, gọi là chi phí (hay trọng số), cho mỗi một liên kết giữa các node trong mạng. Các node sẽ gửi thông tin từ điểm A đến điểm B qua đường đi mang lại tổng chi phí thấp nhất (là tổng các chi phí của các kết nối giữa các node được dùng).

Thuật toán hoạt động với những hành động rất đơn giản. Khi một node khởi động lần đầu, nó chỉ biết các node kề trực tiếp với nó, và chi phí trực tiếp để đi đến đó (thông tin này, danh sách của các đích, tổng chi phí của từng node, và bước kế tiếp để gửi dữ liệu đến đó tạo nên bảng định tuyến, hay bảng khoảng cách). Mỗi node, trong một tiến trình, gửi đến từng "hàng xóm" tổng chi phí của nó để đi đến các đích mà nó biết. Các node "hàng xóm" phân tích thông tin này, và so sánh với những thông tin mà chúng đang "biết"; bất kỳ điều gì cải thiện được những thông tin chúng đang có sẽ được đưa vào các bảng định tuyến của những "hàng xóm" này. Đến khi kết thúc, tất cả node trên mạng sẽ tìm ra bước truyền kế tiếp tối ưu đến tất cả mọi đích, và tổng chi phí tốt nhất.

Khi một trong các node gặp vấn đề, những node khác có sử dụng node hỏng này trong lộ trình của mình sẽ loại bỏ những lộ trình đó, và tạo nên thông tin mới của bảng định tuyến. Sau đó chúng chuyển thông tin này đến tất cả node gần kề và lặp lại quá trình trên. Cuối cùng, tất cả node trên mạng nhận được thông tin cập nhật, và sau đó sẽ tìm đường đi mới đến tất cả các đích mà chúng còn tới được.

2-Thuật toán trạng thái kết nối

(Link-state routing protocols)

Khi áp dụng các thuật toán trạng thái kết nối, mỗi node sử dụng dữ liệu cơ sở của nó như là một bản đồ của mạng với dạng một đồ thị. Để làm điều này, mỗi node phát đi tới tổng thể mạng những thông tin về các node khác mà nó có thể kết nối được, và từng node góp thông tin một cách độc lập vào bản đồ. Sử dụng bản đồ này, mỗi router sau đó sẽ quyết định về tuyến đường tốt nhất từ nó đến mọi node khác.

Thuật toán đã làm theo cách này là Dijkstra, bằng cách xây dựng cấu trúc dữ liệu khác, dạng cây, trong đó node hiện tại là gốc, và chứa mọi node khác trong mạng. Bắt đầu với một cây ban đầu chỉ chứa chính nó. Sau đó lần lượt từ tập các node chưa được thêm vào cây, nó sẽ thêm node có chi phí thấp nhất để đến một node đã có trên cây. Tiếp tục quá trình đến khi mọi node đều được thêm.

Cây này sau đó phục vụ để xây dựng bảng định tuyến, đưa ra bước truyền kế tiếp tốt nhất, ... để từ một node đến bất kỳ node khác trên mạng.

3-So sánh các thuật toán định tuyến

Các giao thức định tuyến với thuật toán vector tỏ ra đơn giản và hiệu quả trong các mạng nhỏ, và đòi hỏi ít (nếu có) sự giám sát. Tuy nhiên, chúng không làm việc tốt, và có tài nguyên tập hợp ít ỏi, dẫn đến sự phát triển của các thuật toán trạng thái kết nối tuy phức tạp hơn nhưng tốt hơn để dùng trong các mạng lớn. Giao thức vector kém hơn với rắc rối về đếm đến vô tận.

Ưu điểm chính của định tuyến bằng trạng thái kết nối là phản ứng nhanh nhạy hơn, và trong một khoảng thời gian có hạn, đối với sự thay đổi kết nối. Ngoài ra, những gói được gửi qua mạng trong định tuyến bằng trạng thái kết nối thì nhỏ hơn những gói dùng trong định tuyến bằng vector. Định tuyến bằng vector đòi hỏi bảng định tuyến đầy đủ phải được truyền đi, trong khi

định tuyến bằng trạng thái kết nối thì chỉ có thông tin về "hàng xóm" của node được truyền đi. Vì vậy, các gói này dùng tài nguyên mạng ở mức không đáng kể. Khuyết điểm chính của định tuyến bằng trạng thái kết nối là nó đòi hỏi nhiều sự lưu trữ và tính toán để chạy hơn định tuyến bằng vector.

IV-Giao thức được định tuyến và giao thức định tuyến

Sự nhầm lẫn thường xảy ra giữa "giao thức được định tuyến" và "giao thức định tuyến" ("routed protocols" và "routing protocols").

1-Giao thức được định tuyến (routed protocols hay routable protocols)

Một giao thức đã được định tuyến là bất kỳ một giao thức mạng nào cung cấp đầy đủ thông tin trong địa chỉ tầng mạng của nó để cho phép một gói tin được truyền đi từ một máy chủ (host) đến máy chủ khác dựa trên sự sắp xếp về địa chỉ, không cần biết đến đường đi tổng thể từ nguồn đến đích. Giao thức đã được định tuyến định nghĩa khuôn dạng và mục đích của các trường có trong một gói. Các gói thông thường được vận chuyển từ hệ thống cuối đến một hệ thống cuối khác. Hầu như tất cả giao thức ở tầng 3 các giao thức khác ở các tầng trên đều có thể được định tuyến, IP là một ví dụ. Nghĩa là gói tin đã được định hướng (có địa chỉ rõ ràng) giống như lá thư đã được ghi địa chỉ rõ chỉ còn chờ routing (tìm đường đi đến địa chỉ đó)

Các giao thức ở tầng 2 như Ethernet là những giao thức không định tuyến được, vì chúng chỉ chứa địa chỉ tầng liên kết, không đủ để định tuyến: một số giao thức ở tầng cao dựa trực tiếp vào đây mà không có thêm địa chỉ tầng mạng, như NetBIOS, cũng không định tuyến được.

2-Giao thức định tuyến (routing protocols)

Giao thức định tuyến được dùng trong khi thi hành thuật toán định tuyến để thuận tiện cho việc trao đổi thông tin giữa các mạng, cho phép các router xây dựng bảng định tuyến một cách linh hoạt. Trong một số trường hợp, giao thức định tuyến có thể tự chạy đè lên giao thức đã được định tuyến: ví dụ, BGP chạy đè trên TCP: cần chú ý là trong quá trình thi hành hệ thống không tạo ra sự lệ thuộc giữa giao thức định tuyến và đã được định tuyến.

Danh sách các giao thức định tuyến

- **Giao thức định tuyến trong**
 - Router Information Protocol (RIP)
 - Open Shortest Path First (OSPF)
 - Intermediate System to Intermediate System (IS-IS)
 - Hai giao thức sau đây thuộc sở hữu của Cisco, và được hỗ trợ bởi các router Cisco hay những router của những nhà cung cấp mà Cisco đã đăng ký công nghệ:
 - Interior Gateway Routing Protocol (IGRP)
 - Enhanced IGRP (EIGRP)
- **Giao thức định tuyến ngoài**
 - Exterior Gateway Protocol (EGP)
 - Border Gateway Protocol (BGP)

- Constrained Shortest Path First (CSPF)

V-Thông số định tuyến (Routing metrics)

Một thông số định tuyến bao gồm bất kỳ giá trị nào được dùng bởi thuật toán định tuyến để xác định một lộ trình có tốt hơn lộ trình khác hay không. Các thông số có thể là những thông tin như băng thông (bandwidth), độ trễ (delay), đếm bước truyền, chi phí đường đi, trọng số, kích thước tối đa gói tin (MTU - Maximum transmission unit), độ tin cậy, và chi phí truyền thông. Bảng định tuyến chỉ lưu trữ những tuyến tốt nhất có thể, trong khi cơ sở dữ liệu trạng thái kết nối hay topo có thể lưu trữ tất cả những thông tin khác.

Router dùng tính năng phân loại mức tin cậy (administrative distance -AD) để chọn đường đi tốt nhất khi nó "biết" hai hay nhiều đường để đến cùng một đích theo các giao thức khác nhau. AD định ra độ tin cậy của một giao thức định tuyến. Mỗi giao thức định tuyến được ưu tiên trong thứ tự độ tin cậy từ cao đến thấp nhất có một giá trị AD. Một giao thức có giá trị AD thấp hơn thì được tin cậy hơn, ví dụ: OSPF có AD là 110 sẽ được chọn thay vì RIP có AD là 120.

Bảng sau đây cho biết sự sắp xếp mức tin cậy được dùng trong các router Cisco

Giao thức	Administrative distance
Nối trực tiếp	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Không xác định	255

VI-Các lớp giao thức định tuyến

Dựa vào quan hệ của các dòng router với các hệ thống tự trị, có nhiều lớp giao thức định tuyến như sau:

- **Giao thức định tuyến trong mạng Ad-hoc** xuất hiện ở những mạng không có hoặc ít phương tiện truyền dẫn.
- **Interior Gateway Protocols (IGPs)** trao đổi thông tin định tuyến trong một AS. Các ví dụ thường thấy là:
 - IGRP (Interior Gateway Routing Protocol)
 - EIGRP (Enhanced Interior Gateway Routing Protocol)
 - OSPF (Open Shortest Path First)
 - RIP (Routing Information Protocol)
 - [RSMLT](#)
 - IS-IS (Intermediate System to Intermediate System)

Chú ý: theo nhiều tài liệu của Cisco, EIGRP không phân lớp như giao thức trạng thái kết nối.

- **Exterior Gateway Protocols (EGPs)** định tuyến giữa các AS. EGPs gồm:
 - EGP (giao thức cũ để nối mạng Internet trước đây, bây giờ đã lỗi thời)
 - BGP (Border Gateway Protocol: phiên bản hiện tại, BGPv4, có từ khoảng năm 1995)

Bài 8 : Ứng dụng và triển khai Internet, bảo mật hệ thống mạng

I-Giới thiệu tổng quan

Bảo mật (security) là việc bảo vệ những thứ có giá trị [1]. Bảo mật thông tin (information security) là một chủ đề rộng bao gồm tất cả các vấn đề bảo mật có liên quan đến lưu trữ và xử lý thông tin. Lĩnh vực nghiên cứu chính của bảo mật thông tin gồm các vấn đề pháp lý như hệ thống chính sách, các quy định, yếu tố con người; các vấn đề thuộc tổ chức như kiểm toán xử lý dữ liệu điện tử, quản lý, nhận thức; và các vấn đề kỹ thuật như kỹ thuật mật mã, bảo mật mạng, công nghệ thẻ thông minh...

Bảo mật máy tính (computer security) là lĩnh vực liên quan đến việc xử lý ngăn ngừa và phát hiện những hành động bất hợp pháp/trái phép (đối với thông tin và tài nguyên hệ thống) của người dùng trong một hệ thống máy tính. Có nhiều định nghĩa khác nhau về bảo mật máy tính nhưng hầu hết đều đề cập đến ba khía cạnh sau đây:

- Sự bí mật (confidentiality): ngăn ngừa việc làm lộ trái phép thông tin
- Sự toàn vẹn (Integrity): ngăn ngừa việc sửa đổi trái phép đối với thông tin
- Sự sẵn sàng (Availability): ngăn ngừa việc chiếm dụng trái phép thông tin hoặc tài nguyên.

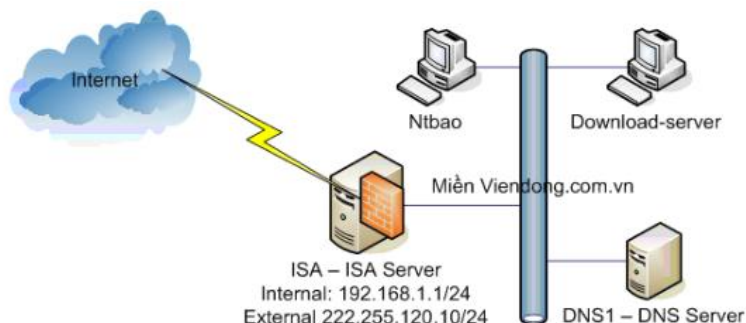
Trên thực tế, kỹ thuật mật mã được triển khai rộng rãi để đảm bảo tính bí mật và toàn vẹn của thông tin được lưu trữ hay truyền nhận nhưng kỹ thuật này không bảo đảm cho tính sẵn sàng của hệ thống.

Mạng máy tính được triển khai nhằm giúp máy tính mở rộng giao tiếp với môi trường bên ngoài đồng nghĩa việc tăng nguy cơ rủi ro. Chúng ta vì thế muốn kiểm soát cách người dùng hệ thống truy cập vào mạng, cách người dùng trên mạng truy cập vào hệ thống của chúng ta và cách thông tin được bảo vệ trên đường truyền. Do vậy, bảo mật mạng (network security) không chỉ đơn giản là mật mã mà còn đòi hỏi nhiều yêu cầu mới về kiểm soát truy xuất

II-Ứng dụng với công cụ ISA

LAB 1:

Mô hình mạng:



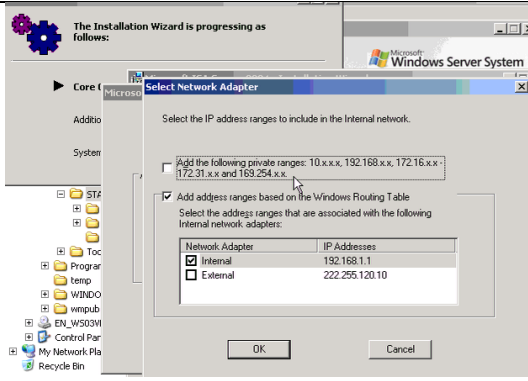
Anh/Chị có mô hình mạng như trên, Anh/Chị hãy cấu hình một máy chủ Proxy để quản lý và chia sẻ kết nối Internet cho các máy trạm.

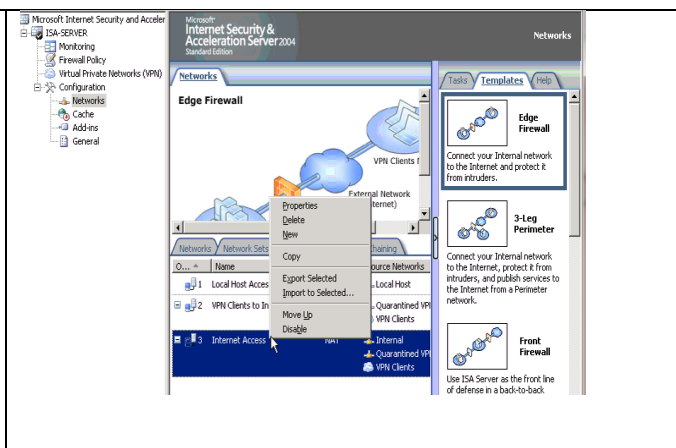
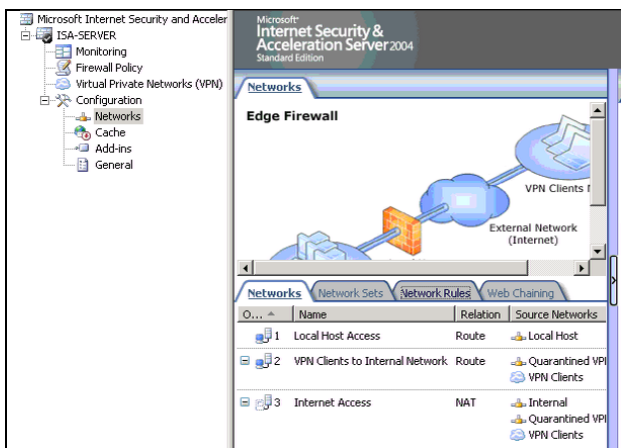
Triển khai:

Thiết lập dịch vụ Proxy theo yêu cầu

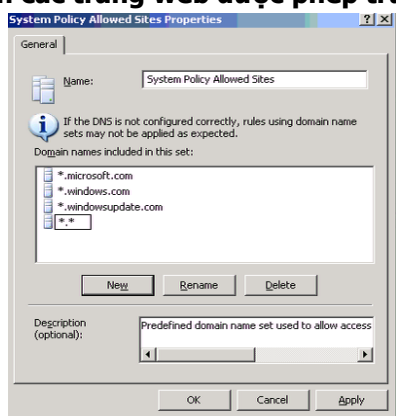
- Cài đặt chương trình ISA 2004 trên máy ISA
- Không cho phép máy Client đi Internet thông qua kỹ thuật NAT
- Hiệu chỉnh các trang Web được phép truy cập
- Bật tính năng Proxy Server
- Tạo Rule (luật) cho phép các máy bên trong (Internal Network) được truy cập internet.
- Thiết lập Cache cho ISA Server

Các bước thực hiện:

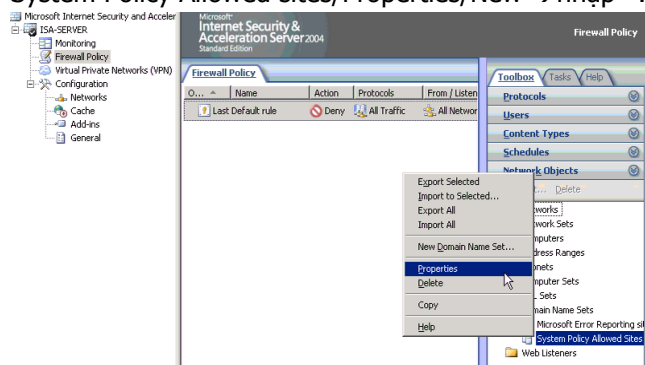
Cài đặt chương trình ISA	
Không cho các máy truy cập Internet bằng kỹ thuật NAT	Network/Network Rule/Right Click NAT → disable → Apply



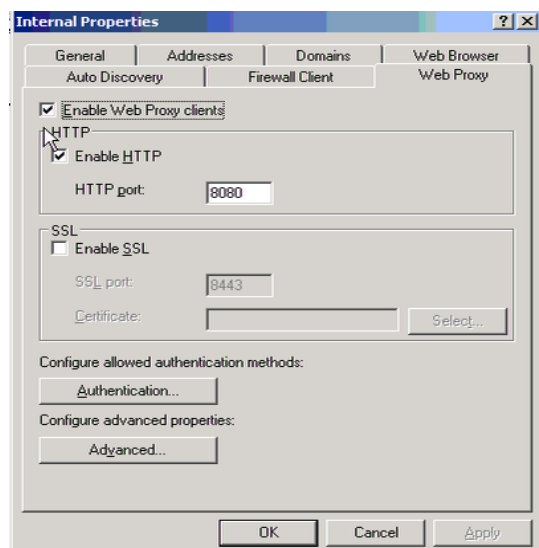
Hiệu chỉnh các trang web được phép truy cập



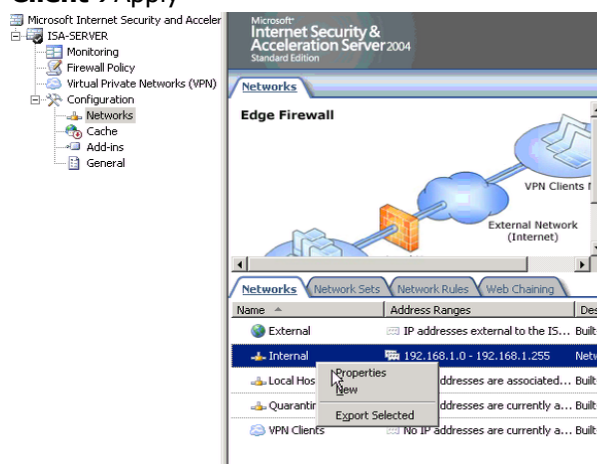
Firewall Policy/Toolbox/Domain Name Set/Right Click System Policy Allowed sites/Properties/New → nhập *.*



Bật tính năng Proxy Server

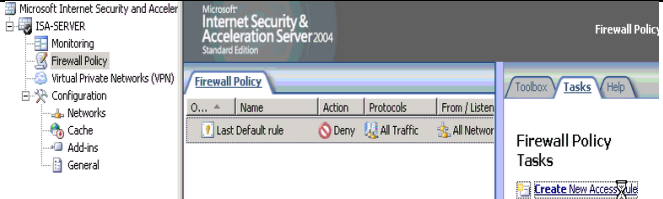
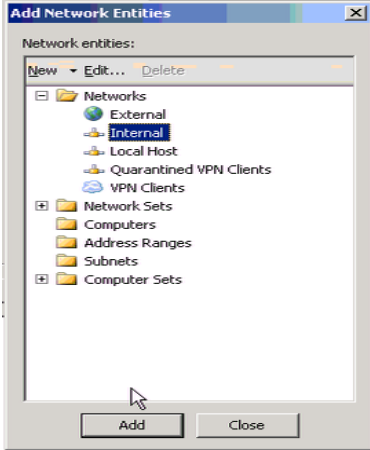
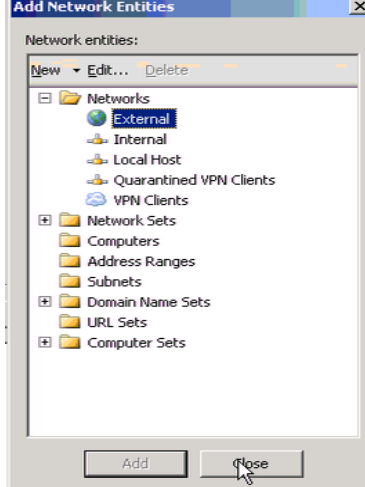
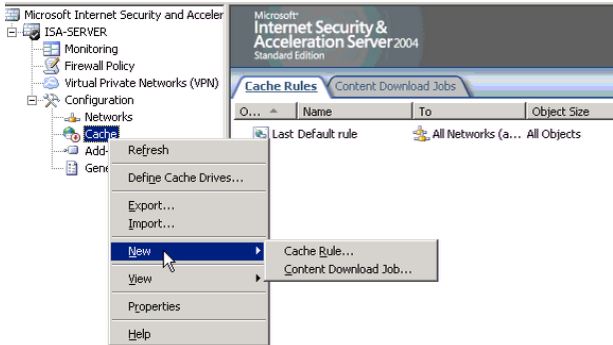
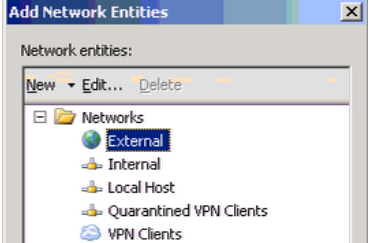
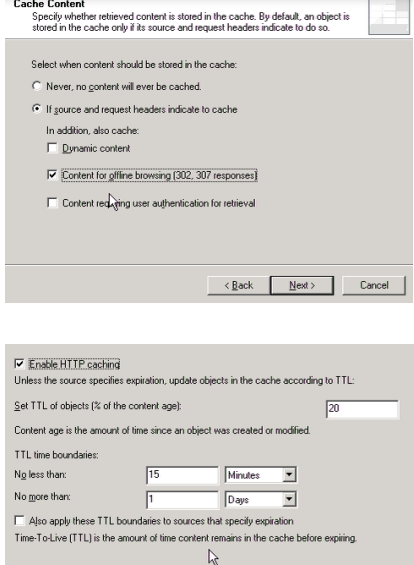


Network/network/right click Internal/Properties/Chọn Tab Web Proxy/ bật tính năng **Enable Web Proxy Client**→Apply

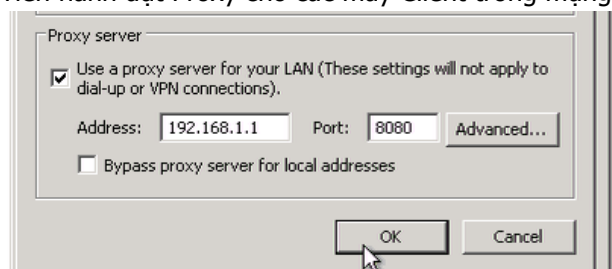


Tạo Rule(luật) cho phép các máy bên trong (internal) truy cập Internet

Firewall Policy/Task/Create new Access Rule/Đặt tên Rule/Next/Allow/All outbound Traffic/Next/Internal/Add

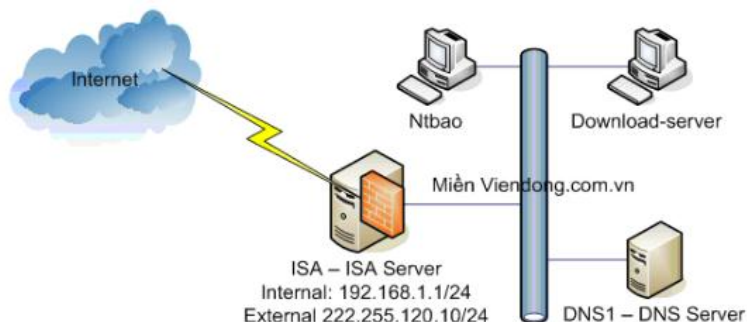
	
	
Thiết lập Cache cho ISA Server	Cache/New/Cache Rule...Đặt tên Rule/next 
	

Tiến hành đặt Proxy cho các máy Client trong mạng:



LAB 2:

Mô hình mạng:



Anh/Chị hãy cài đặt ISA 2004 để bảo vệ hệ thống mạng nội bộ theo các yêu cầu sau:

1. Cho phép máy download-server, địa chỉ 192.168.1.2 có thể truy xuất Internet thông qua cơ chế NAT
2. Cấm máy 192.168.1.10 truy cập Internet.
3. Trong giờ hành chính, không cho phép truy cập các địa chỉ: *.tuoitre.com.vn, *.thanhnien.com.vn.

Triển khai:

Thiết lập các luật theo yêu cầu

- Cho phép máy 192.168.1.2 được truy cập theo kỹ thuật NAT
 - Định nghĩa máy 192.168.1.2
 - Tạo luật theo yêu cầu
- Không cho phép máy 192.168.1.10 truy cập Internet.
 - Định nghĩa máy 192.168.1.10
 - Tạo luật theo yêu cầu

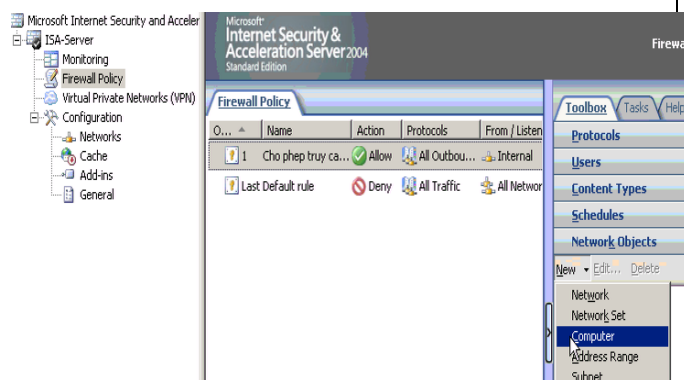
Các bước thực hiện:

Cho phép máy có địa chỉ IP 192.168.1.2 truy cập theo kỹ thuật NAT :

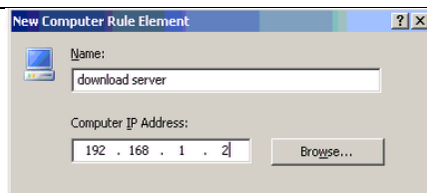
Bước 1: Định nghĩa máy có địa chỉ 192.168.1.2

Bước 2 : Tạo luật (bằng kỹ thuật NAT) theo yêu cầu cho máy vừa định nghĩa

Firewall Policy/Toolbox/Computer/New/computer

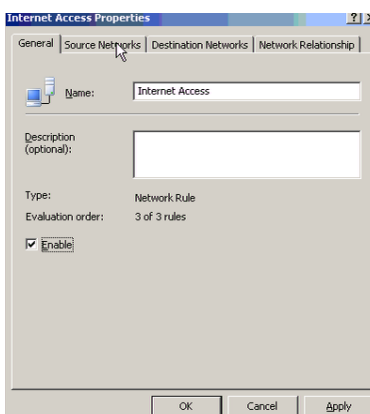


Hình 1

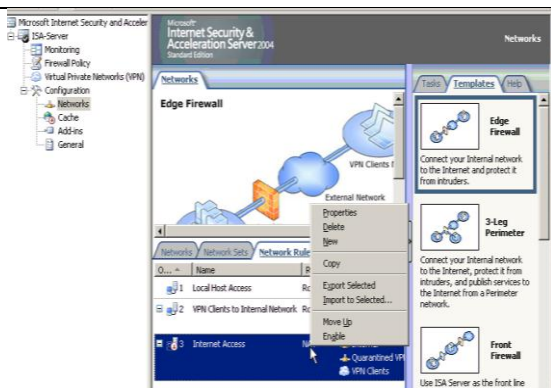


hình 2

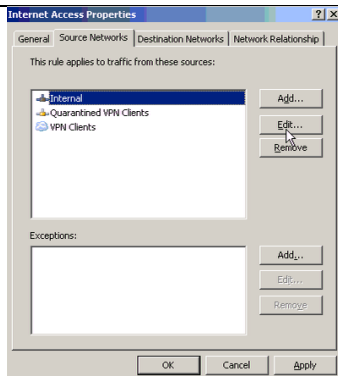
Nhấp chuột phải/Properties/check vào mục Enable/chọn Tab Source Network/Remove tất cả các mục trong danh sách để đưa Computer đã định nghĩa ở bước 1



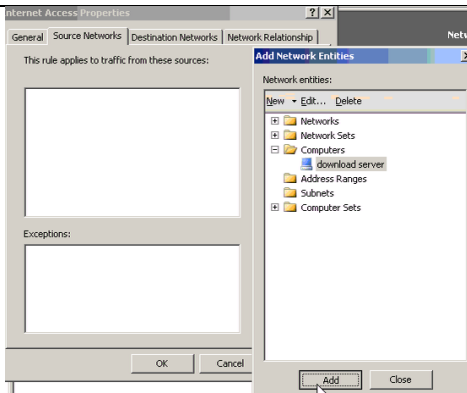
Hình 4



Hình 3

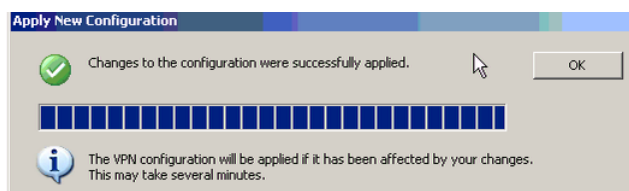


Hình 5

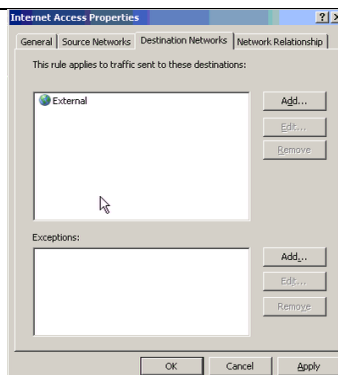


Hình 6

Cuối cùng chọn Apply



Hình 8

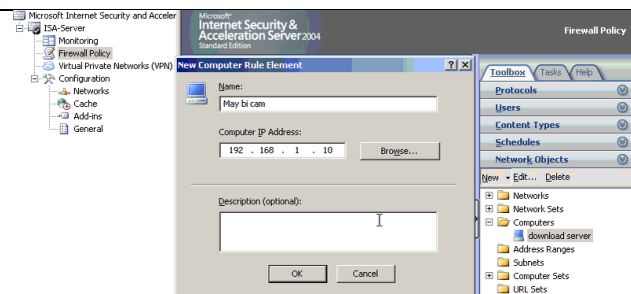


Hình 7

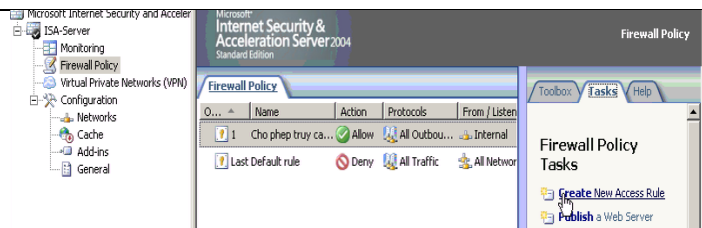
Không cho phép máy có địa chỉ IP 192.168.1.10 truy cập Internet

Bước 1: Định nghĩa máy có địa chỉ IP 192.168.1.10

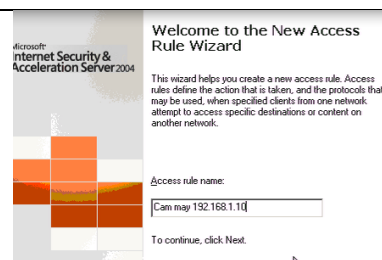
Bước 2 : Tạo luật cho máy vừa định nghĩa



Hình 1



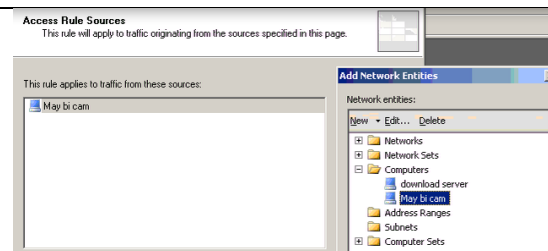
Hình 2



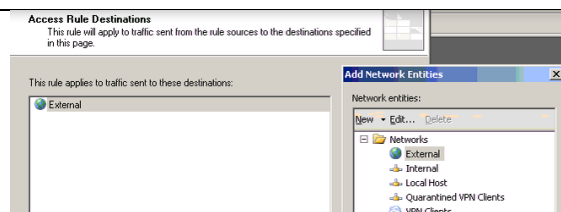
Hình 3



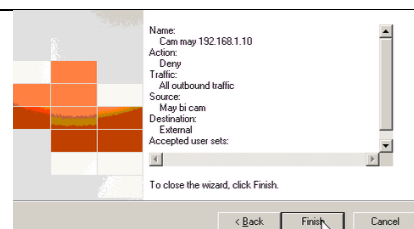
Hình 4



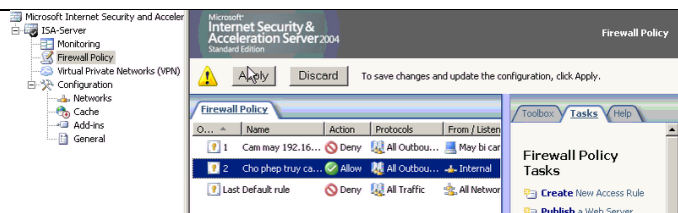
Hình 5



Hình 6



Hình 7



Hình 8

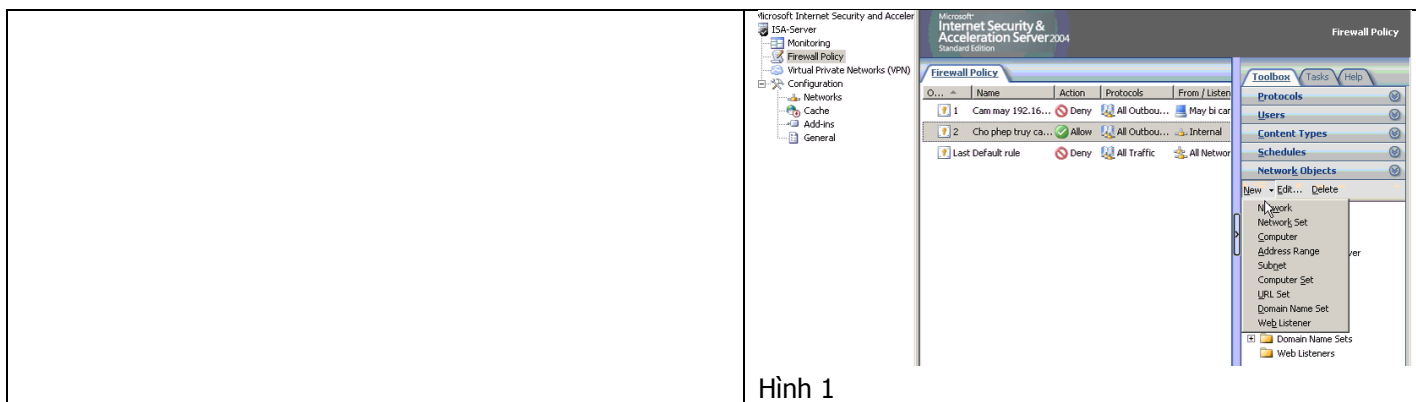
Trong giờ hành chính không cho truy cập các trang web *.tuoitre.com.vn và *.thanhnien.vn

Bước 1 : Định nghĩa các trang web cấm truy cập

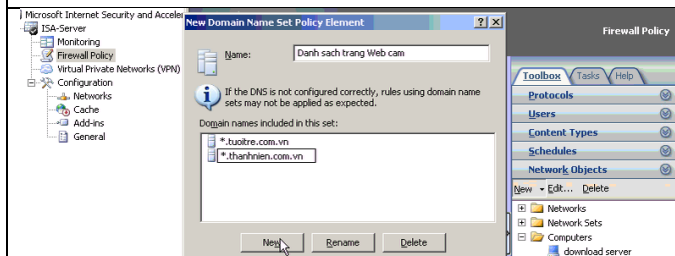
Bước 2 : Định nghĩa thời gian cấm

Bước 3 : Tạo luật theo yêu cầu từ bước 1 → bước 2

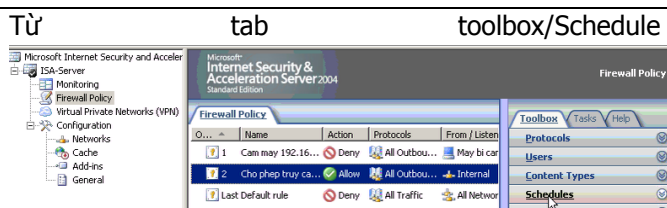
Firewall/Toolbox/Domain	Name	Set/New/Domain Name Set
-------------------------	------	-------------------------



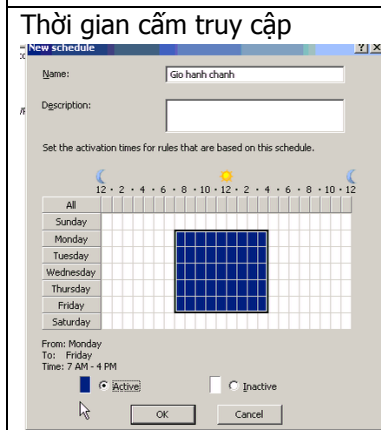
Hình 1



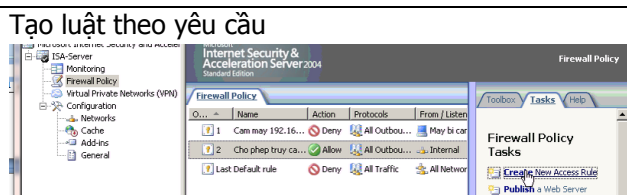
Hình 2



Hình 3

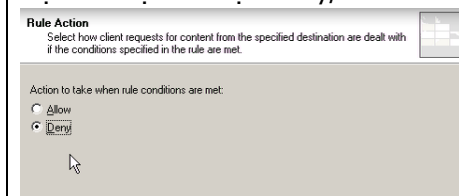


Hình 4



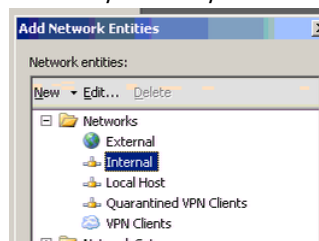
Hình 5

Đặt tên luật và chọn Deny/All outbound Traffic



Hình 6

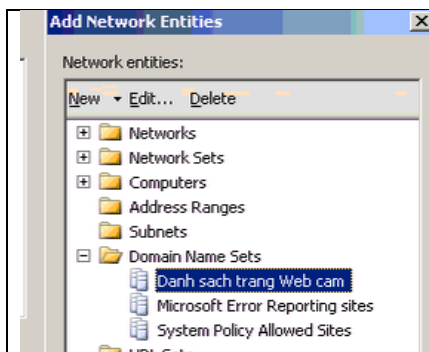
Network/Internal/add



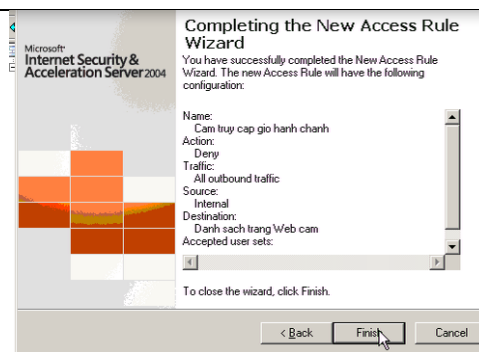
Hình 7

Add tên luật đã định nghĩa

Finish



Hình 8

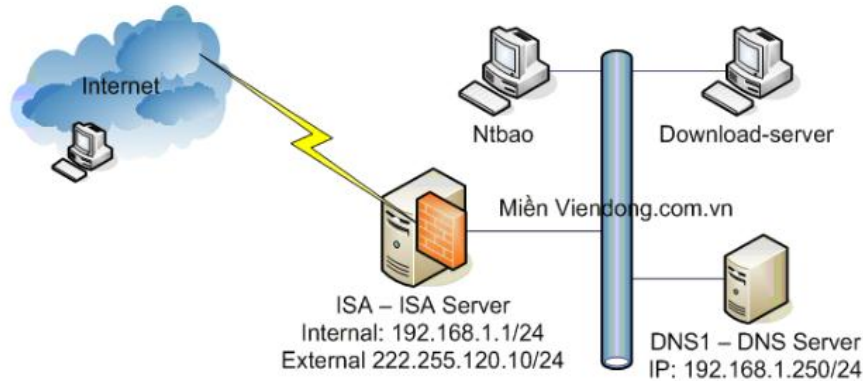


Hình 9

Mở trình duyệt để Test quá trình đã thực hiện

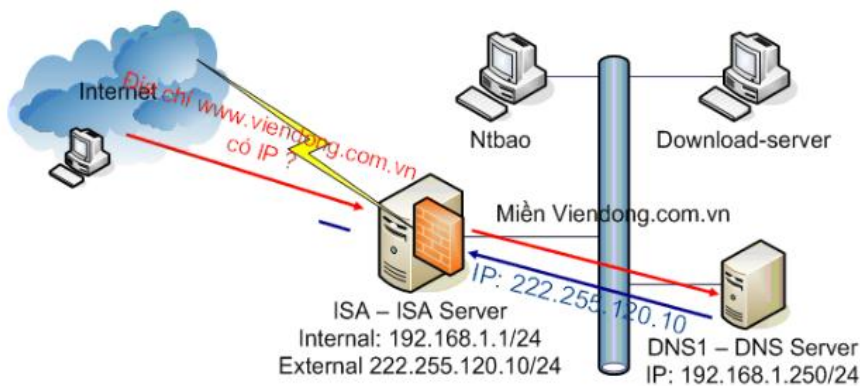
LAB 3:

Mô hình mạng:



Publishing DNS Server

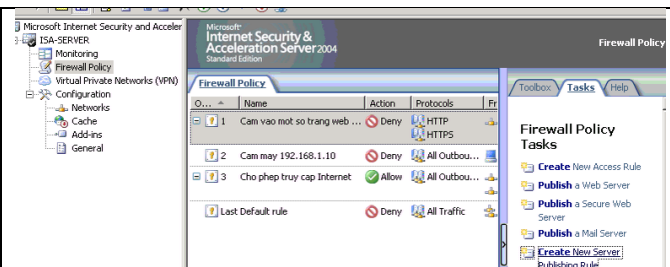
Triển khai:



Publishing DNS Server

Các bước thực hiện:

Firewall Policy/Create new server publishing Rule

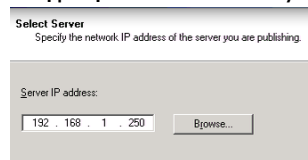


Hình 1



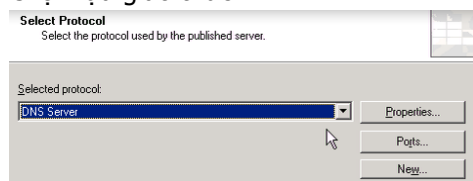
Hình 2

Nhập địa chỉ IP của máy DNS server cần publishing



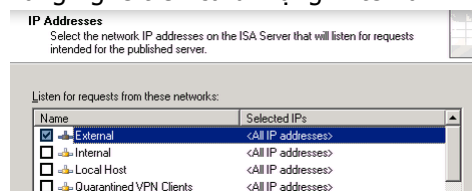
Hình 3

Chọn lựa giao thức



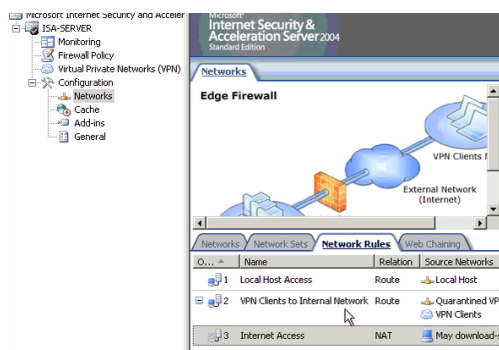
Hình 4

Lắng nghe trên card mạng External



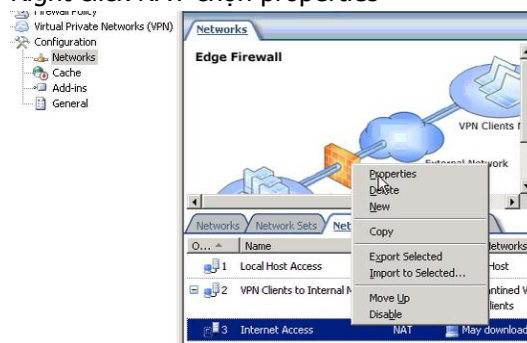
Hình 5

Cấu hình NAT cho máy DNS

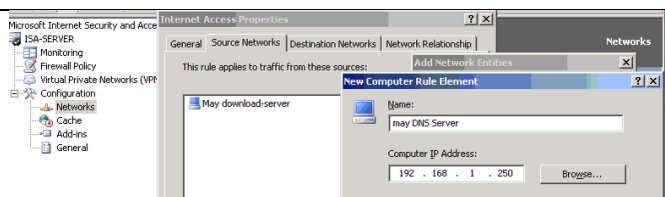


Hình 6

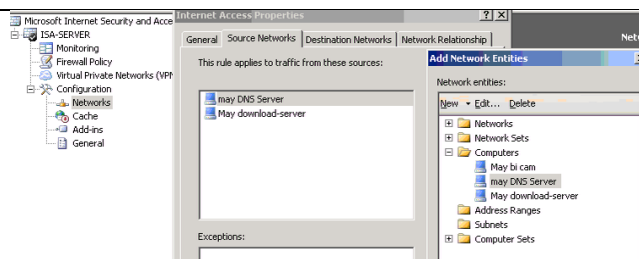
Right click NAT chọn properties



Hình 7

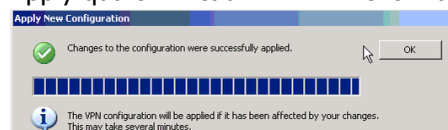


Hình 8



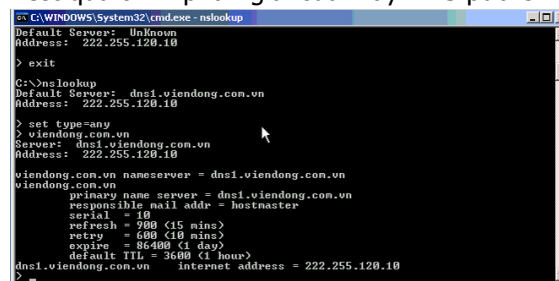
Hình 9

Apply quá trình cấu hình NAT cho máy DNS server



Hình 10

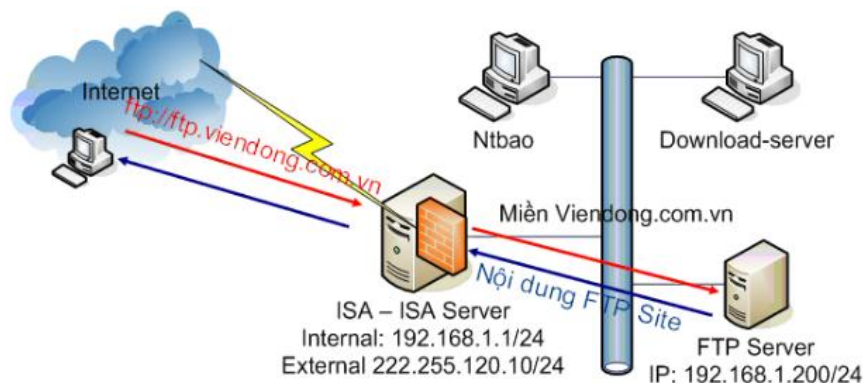
Test quá trình phân giải của máy DNS publishing



Hình 11

LAB 4:

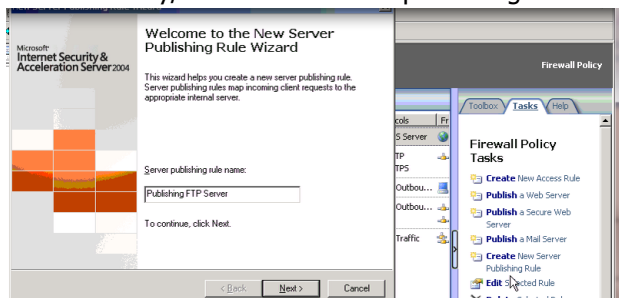
Mô hình mạng:



Publishing FTP Server

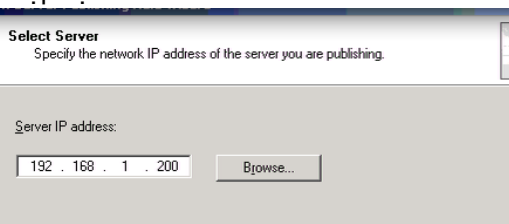
Các bước thực hiện:

Firewall Policy/Create new server publishing Rule



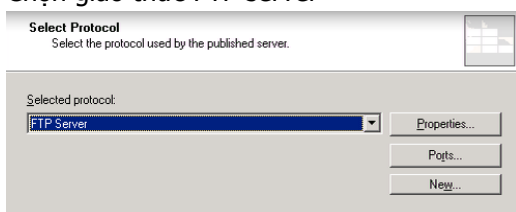
Hình 1

Nhập địa chỉ IP của FTP server cần Publishing



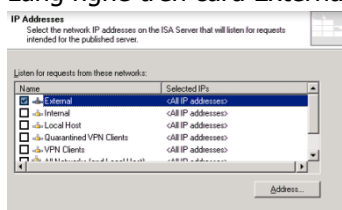
Hình 2

Chọn giao thức FTP server

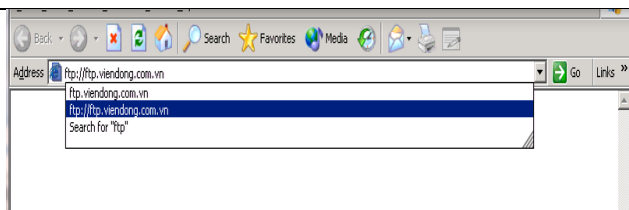


Hình 3

Lắng nghe trên card External

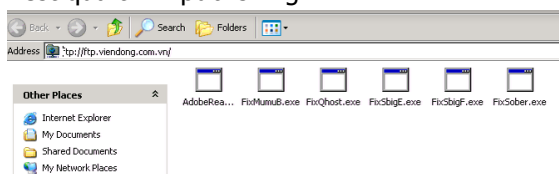


Hình 4



Hình 5

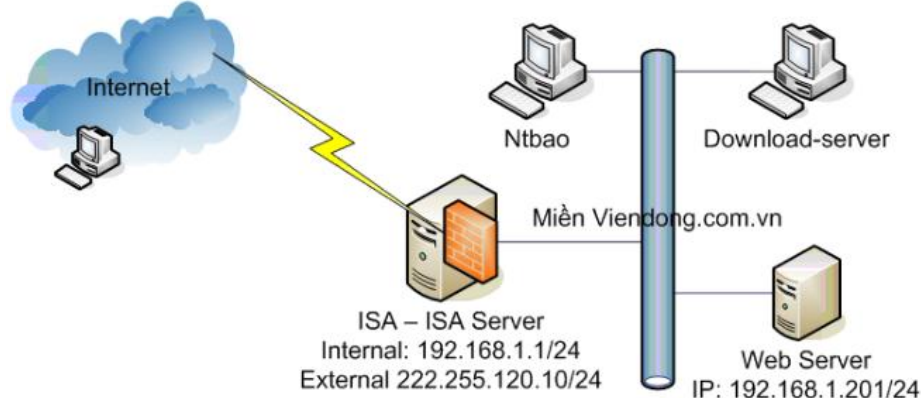
Test quá trình publishing



Hình 6

LAB 5:

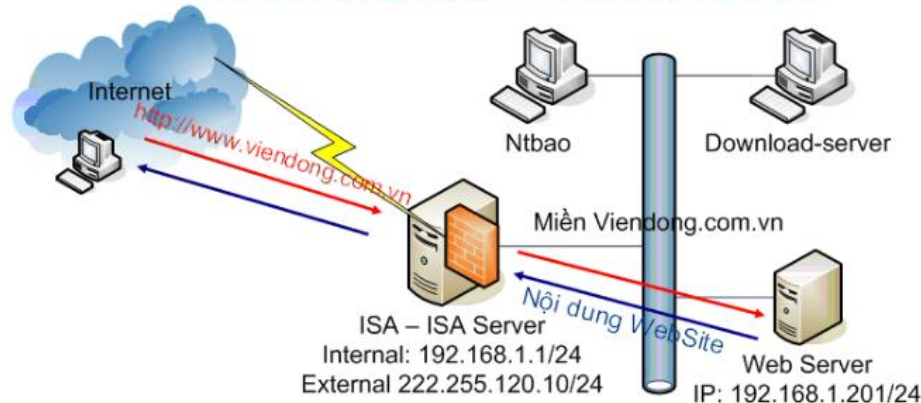
Mô hình mạng:



Publishing Web Server

Triển khai:

Port 80 trên card External → Port 80 trên Web Server



Publishing Web Server

Các bước thực hiện:

Firewall Policy/Publish a web server Hình 1	Nhập địa chỉ Web server Hình 2
--	---



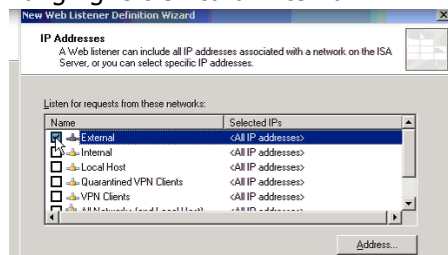
Hình 3

Định nghĩa Port cần lắng nghe : New button



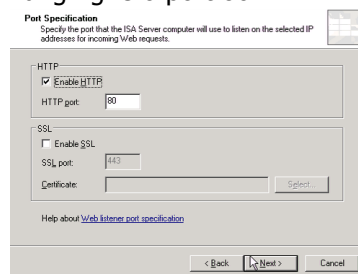
Hình 4

Lắng nghe trên card External

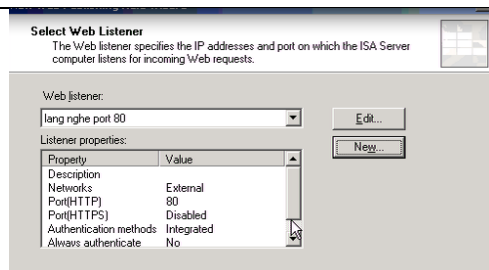


Hình 5

Lắng nghe ở port 80



Hình 6



Hình 7

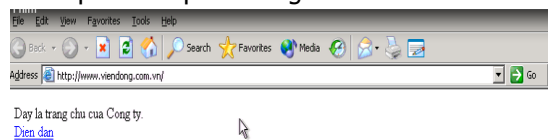


Hình 8



Hình 9

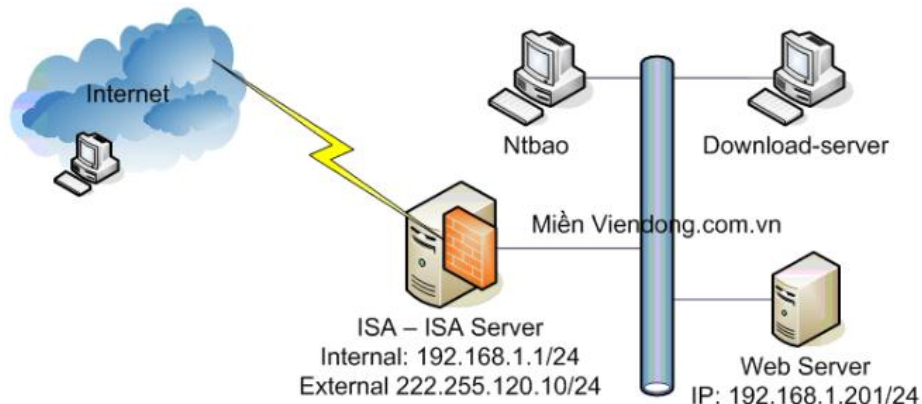
Test quá trình publishing



Hình 10

LAB 6:

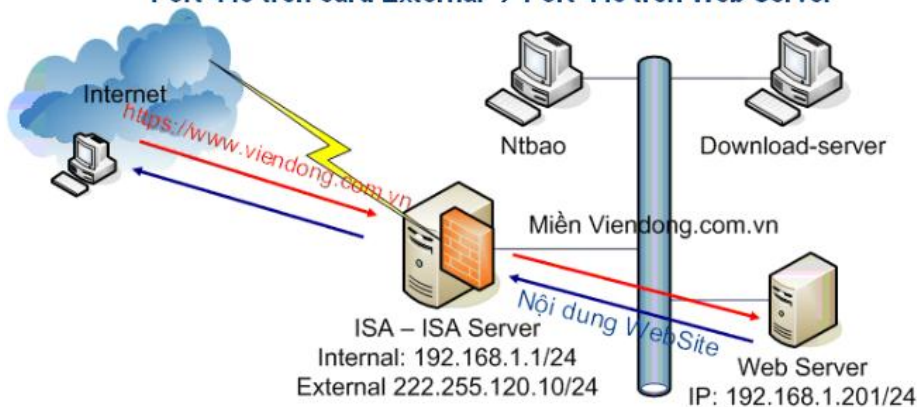
Mô hình mạng:



Publishing Web Server

Triển khai:

Port 443 trên card External → Port 443 trên Web Server

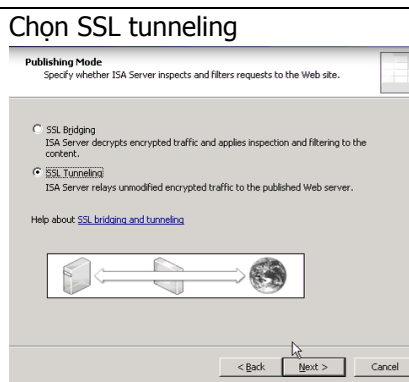


Publishing Web Server

Các bước thực hiện:



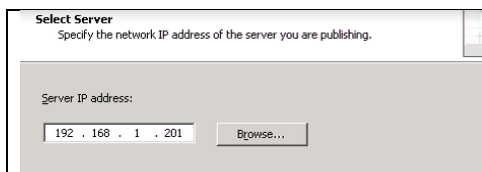
Hình 1



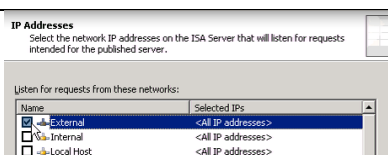
Hình 2

Nhập địa chỉ IP của Webserver

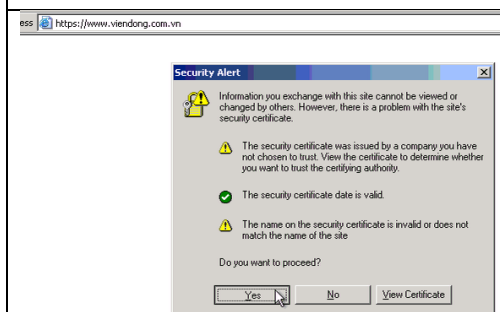
Lắng nghe trên card External



Hình 3



Hình 4



Hình 5

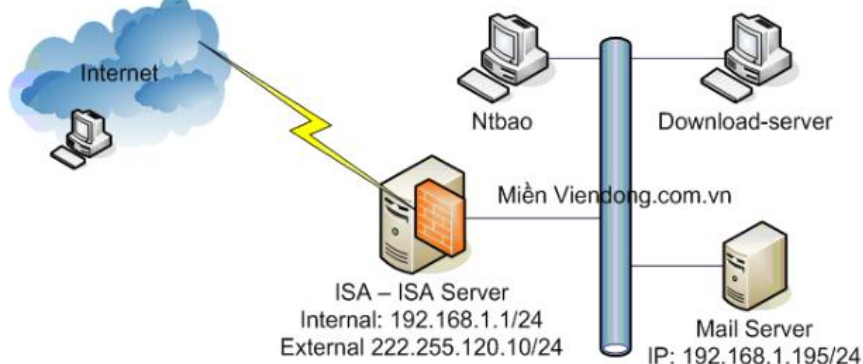
Test quá trình bằng giao thức https



Hình 6

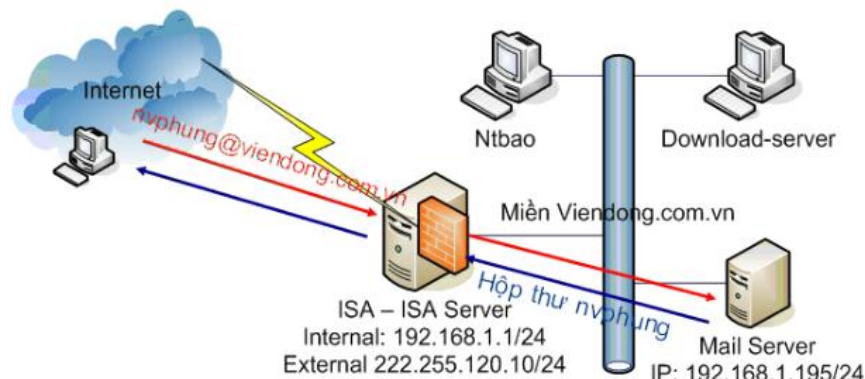
LAB 7

Mô hình mạng:



Publishing Mail Server

Triển khai:



Publishing Mail Server

Hình lab7.1

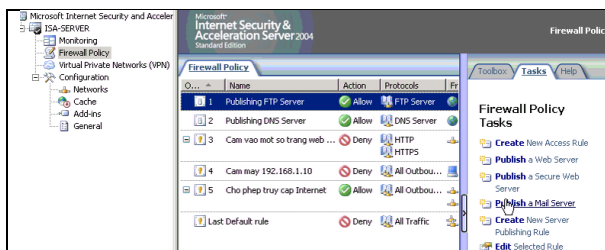
Thiết lập dịch vụ Web

- Cho phép sử dụng giao thức SMTP, POP3.
- Cho phép sử dụng Webmail
 - WorldClient - MDaemon
 - Outlook Web Access (OWA) – Mail Exchange

Hình lab7.2

Các bước thực hiện:

Firewall Policy/Publish a Mail Server	Đặt tên cho Rule
---------------------------------------	------------------

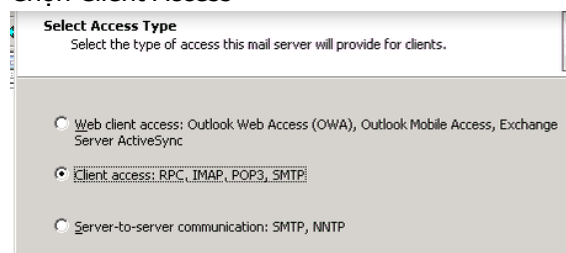


Hình 1



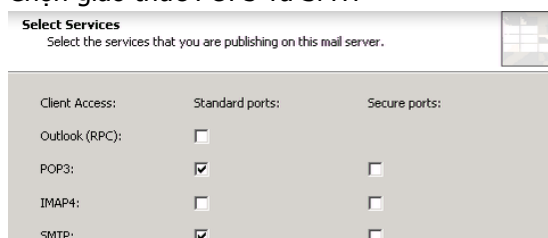
Hình 2

Chọn Client Access



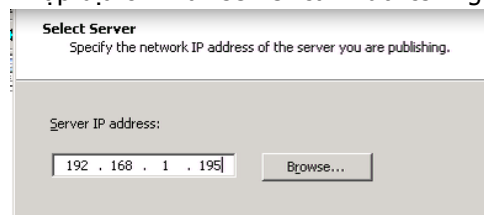
Hình 3

Chọn giao thức POP3 và SMTP



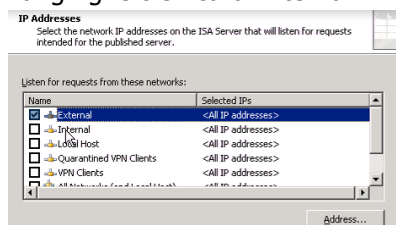
Hình 4

Nhập địa chỉ Mail server cần Publishing



Hình 5

Lắng nghe trên card External



Hình 6

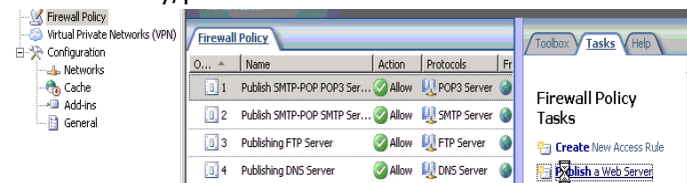
Thiết lập dịch vụ Web Mail

Thiết lập dịch vụ Web

- Cho phép sử dụng giao thức SMTP, POP3.
- Cho phép sử dụng Webmail
 - WorldClient - MDAemon
 - Outlook Web Access (OWA) – Mail Exchange

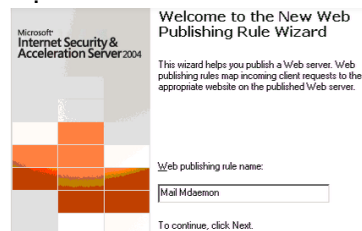
Hình 1

Firewall Policy/publish a Web server



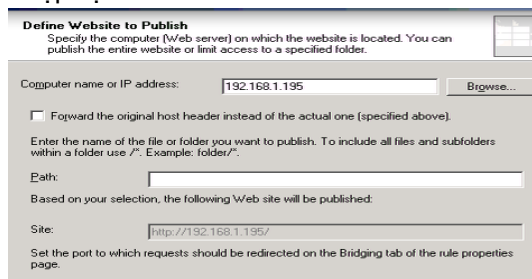
Hình 2

Đặt tên Rule cho Mdaemon



Hình 3

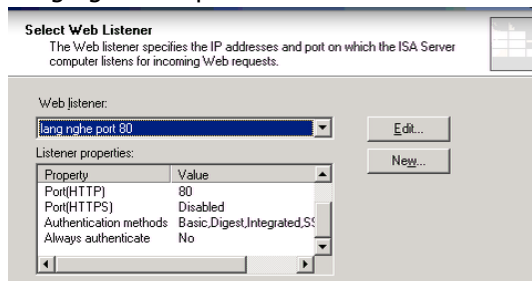
Nhập địa chỉ IP của Mail server





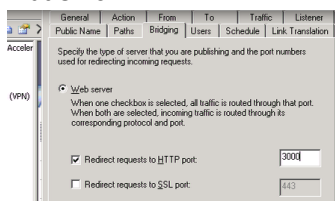
Hình 5

Lắng nghe trên port 80



Hình 6

Thiết lập Port 80 thành 3000 đối với chương trình Mdaemon



hình 7

Truy cập bằng port 3000 của mdaemon

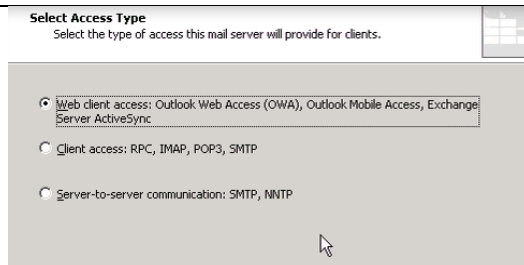


Hình 8

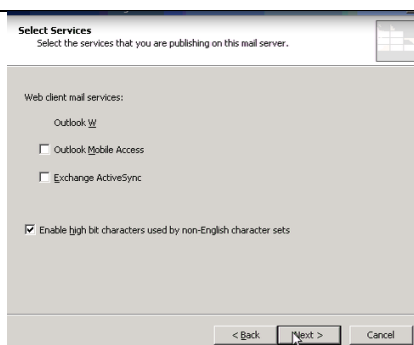
Sử dụng OWA của mail Exchange Firewall Policy/Publish a Mail Server



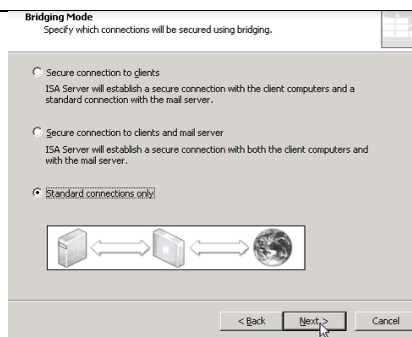
Hình 1



Hình 2



Hình 3



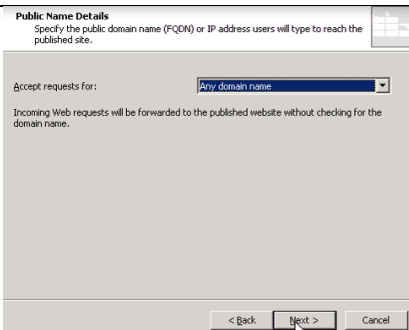
Hình 4

Nhập địa chỉ Mail Server

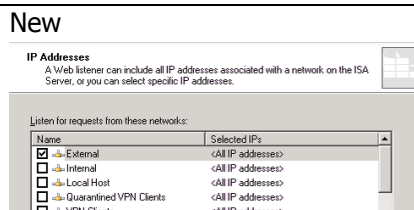


Hình 5

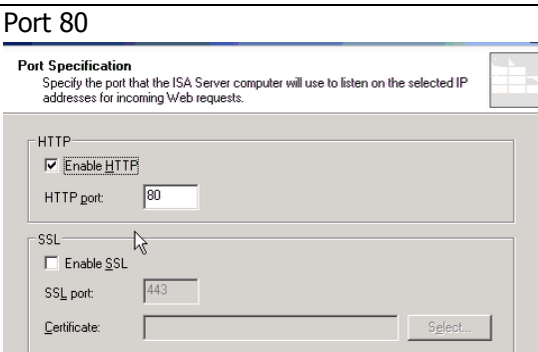
Lắng nghe từ bất kỳ Domain nào



Hình 6

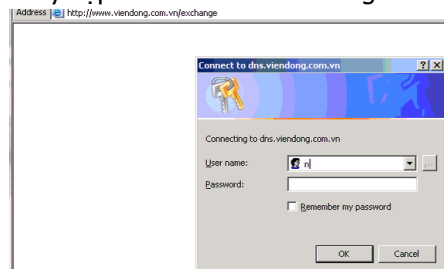


Hình 7



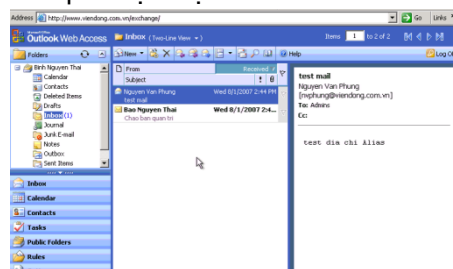
Hình 8

Truy cập web mail với Exchange



hình 9

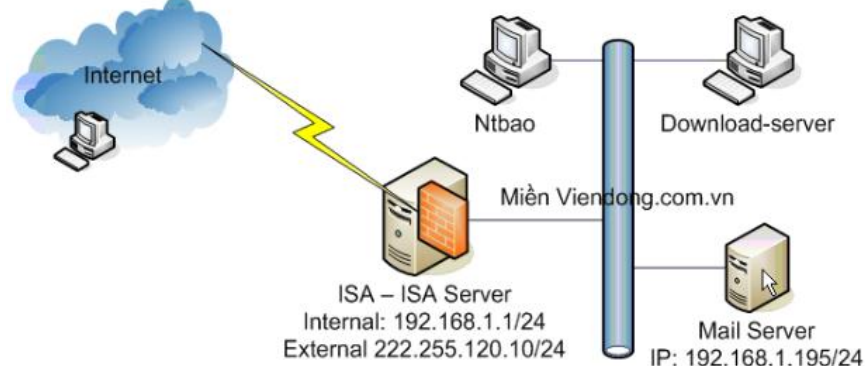
Kết quả thực hiện



hình 10

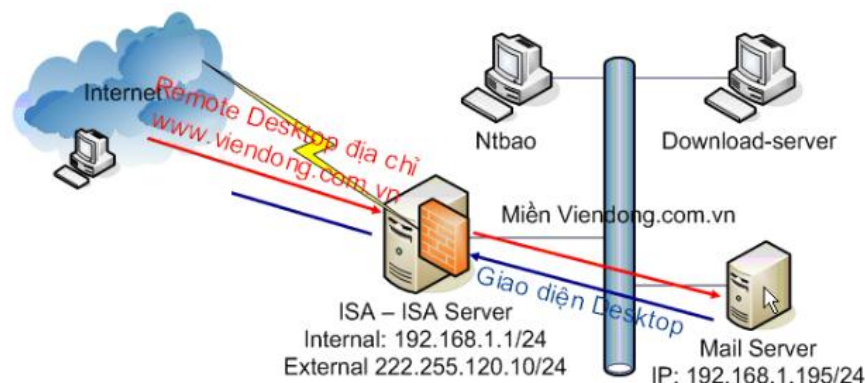
LAB 8:

Mô hình mạng:



Cho phép Remote Desktop Mail Server

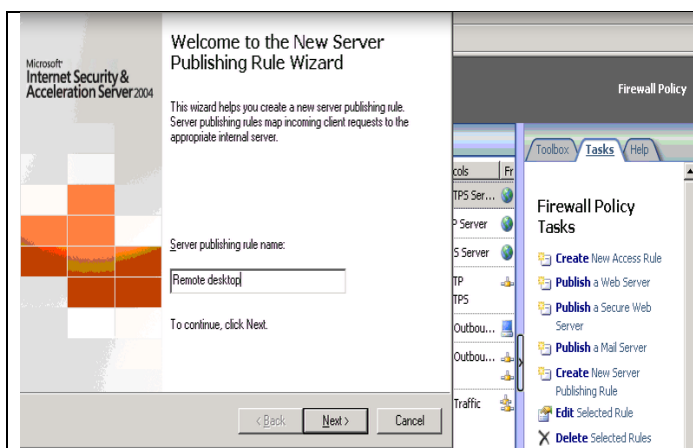
Triển khai:



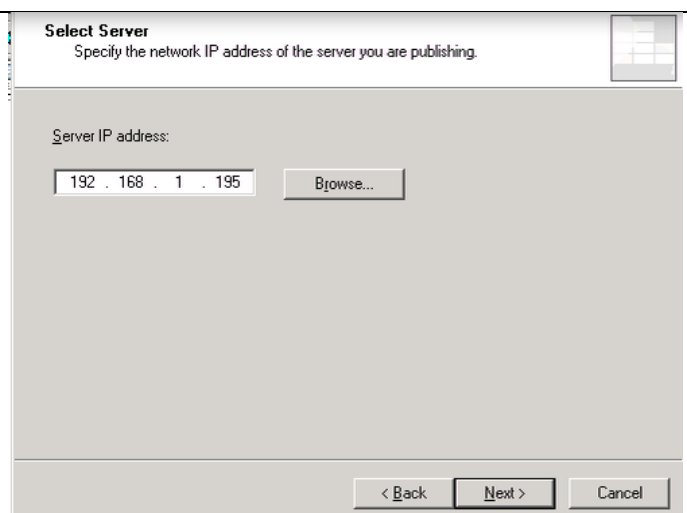
Cho phép Remote Desktop Mail Server

Các bước thực hiện:

Firewall Policy/Create New Server a Publishing Rule	Nhập địa chỉ IP của Mail Server cần Remote Desktop
---	--

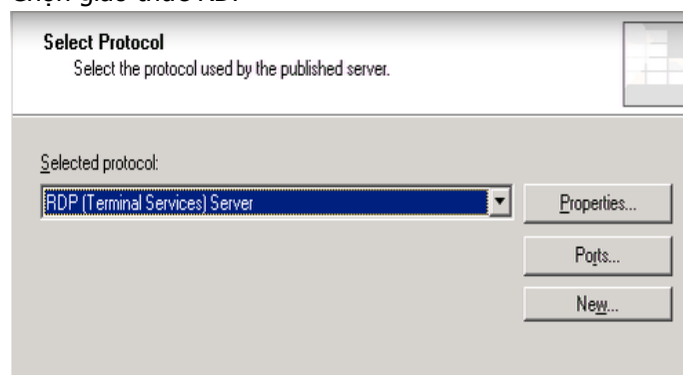


Hình 1



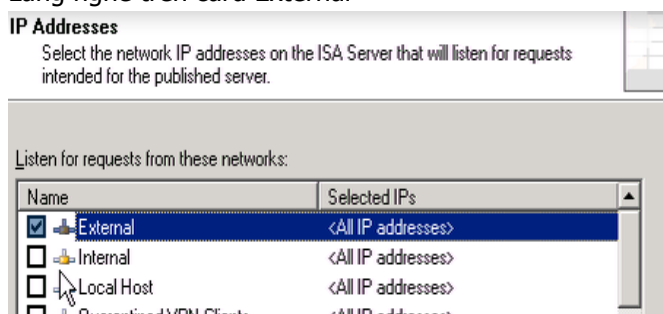
Hình 2

Chọn giao thức RDP



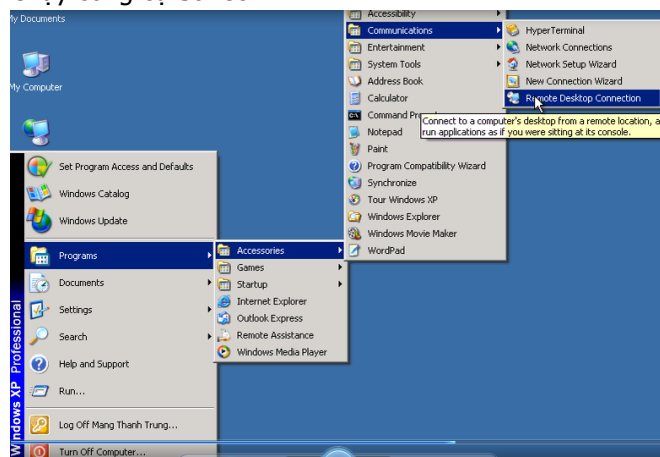
Hình 3

Lắng nghe trên card External

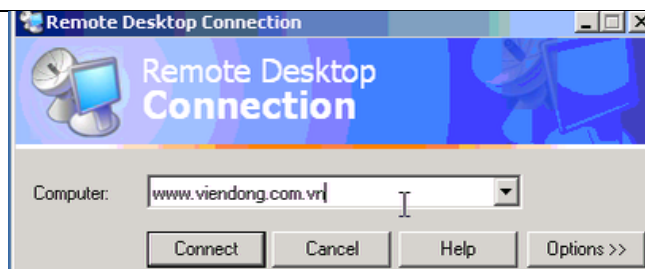


Hình 4

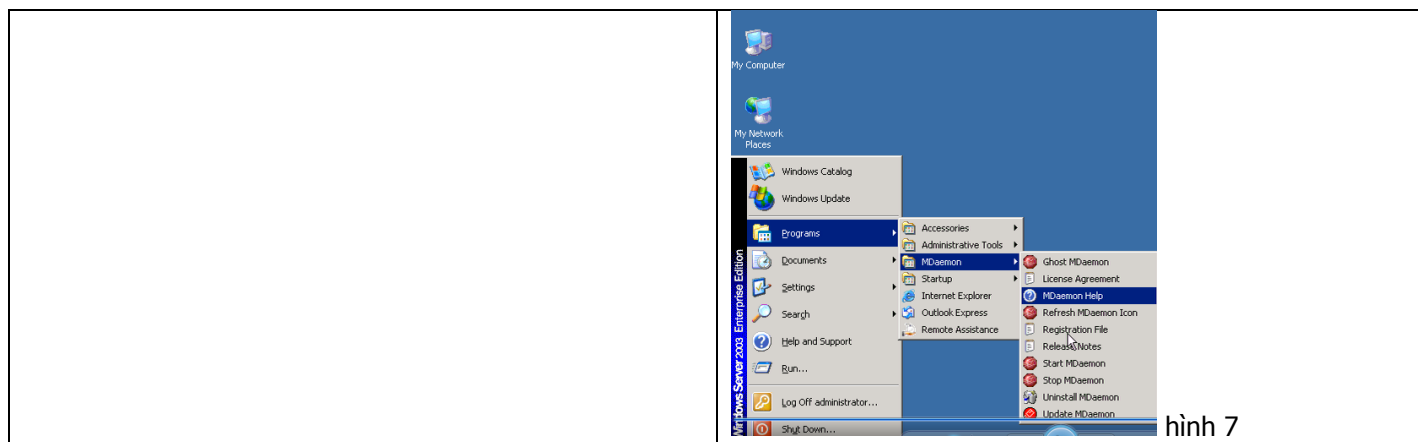
Chạy công cụ Stmsc



Hình 5

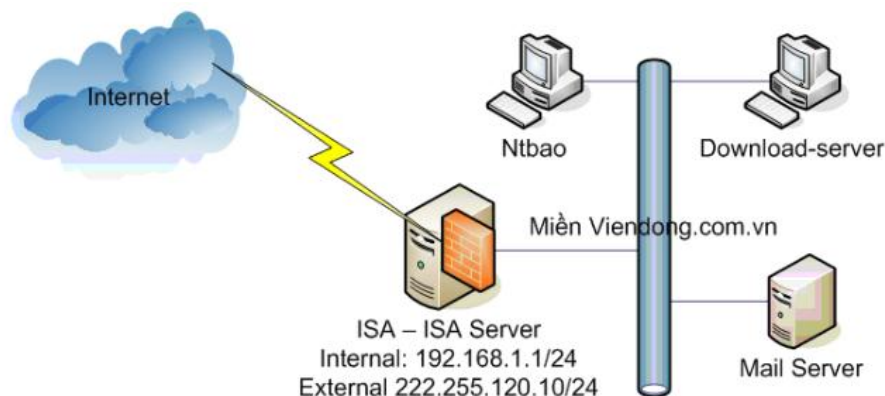


Hình 6



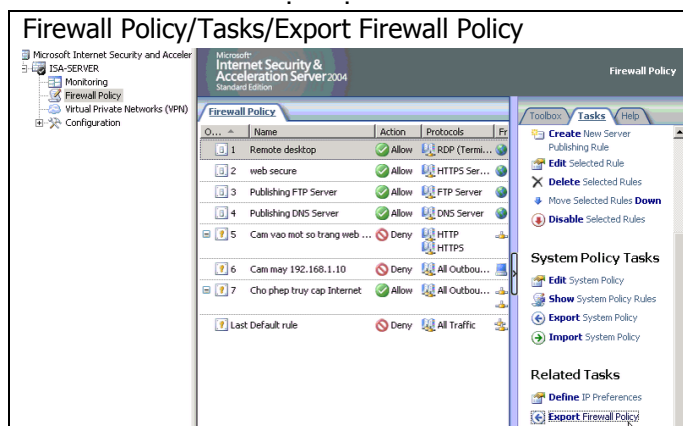
LAB9: LƯU VÀ BACKUP ISA

Mô hình mạng:



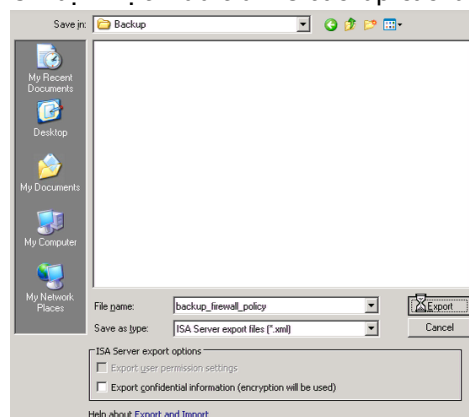
Trên máy ISA, Anh/Chị hãy backup lại các luật đã thiết lập.

Các bước thực hiện:



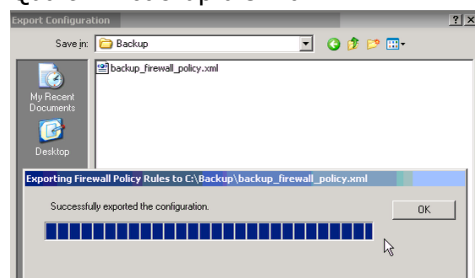
Hình 1

Chỉ định vị trí lưu trữ file backup các luật



Hình 2

Quá trình backup diễn ra



Hình 3

Bài 9 : Giám sát và tối ưu hóa Server.

Bài 10 : DỊCH VỤ TERMINAL SERVICE

I-Giới thiệu tổng quan

Bạn ở xa nhưng lại cần truy cập vào máy máy chủ trong công ty như là đang ngồi trên máy? Bài hướng dẫn sẽ từng bước hướng dẫn kích hoạt và cấu hình Remote Desktop for Administration trong Microsoft Windows Server 2003. Sau khi kích hoạt và cấu hình xong, bạn có thể truy cập vào máy chủ tại bất cứ nơi đâu có kết nối Internet như là đang sử dụng trực tiếp trên máy vậy.

II-Ứng dụng dịch vụ

Windows Server 2003 Terminal Services bao gồm hai thành phần sau:

- **Remote Desktop for Administration** (Công cụ quản trị máy tính từ xa)

Với Remote Desktop for Administration các quản trị viên có thể quản lý từ xa server dựa trên nền tảng Microsoft Windows 2000 và Windows Server 2003 từ bất kỳ client Terminal Services nào. Phục vụ cho mục đích thuyết trình và hợp tác, hai quản trị viên có thể chia sẻ một phiên làm việc. Ngoài ra quản trị viên còn có thể kết nối từ xa tới console thực của một server bằng cách dùng lệnh **-console**.

Chú ý:

- Bạn không cần phải có bản quyền truy cập Client Terminal Server khi dùng Remote Desktop for Administration. Tuy nhiên chỉ có các thành viên của nhóm quản trị mới có thể truy cập vào server.
- Mặc định Remote Desktop for Administration được cài cùng lúc với Windows Server 2003, nhưng được để ở chế độ không hoạt động vì một số lý do bảo mật.

- **Terminal Server**

Terminal Server cho phép nhiều client từ xa truy cập đồng thời tới các chương trình xây dựng trên nền tảng Windows chạy trên server cùng một lúc. Đây là hình thức triển khai Terminal Server thông thường.

Khi sử dụng mô hình Terminal Server, nhiều kết nối đồng thời do người dùng không thuộc nhóm quản trị (administrator) truy cập đến vẫn được chấp nhận. Bạn cũng có thể cài đặt dịch vụ Terminal Services Licensing trên bất kỳ server thành viên nào. Tuy nhiên bạn phải cấu hình một server có bản quyền trên tất cả server đích. Server này phải liên hệ với các server bản quyền không có bộ điều khiển tên miền nhưng được cấu hình như một server bản quyền tên miền. Server bản quyền tên miền doanh nghiệp được triển khai trên các bộ điều khiển không tên miền được phát hiện một cách tự động.

Trước khi sử dụng indows Server 2003 Terminal Services, các bạn nên xem lại một số thuật ngữ sau:

- **Server** (máy chủ)
Server là máy chủ, nơi chứa hầu hết tài nguyên máy tính. Server được dùng trong môi trường mạng Terminal Services. Server nhận và thực hiện thông tin từ bàn phím và chuột ở client. Sau đó hiển thị màn hình và các chương trình đang chạy trên server trong một cửa sổ ở máy client.
- **Messaging** (truyền tin)
Messaging là hoạt động liên lạc giữa server (máy chủ) và client (máy khách) thông qua Remote Desktop Protocol (RDP) 5.2. RDP là giao thức tầng chương trình dựa trên TCP/IP.

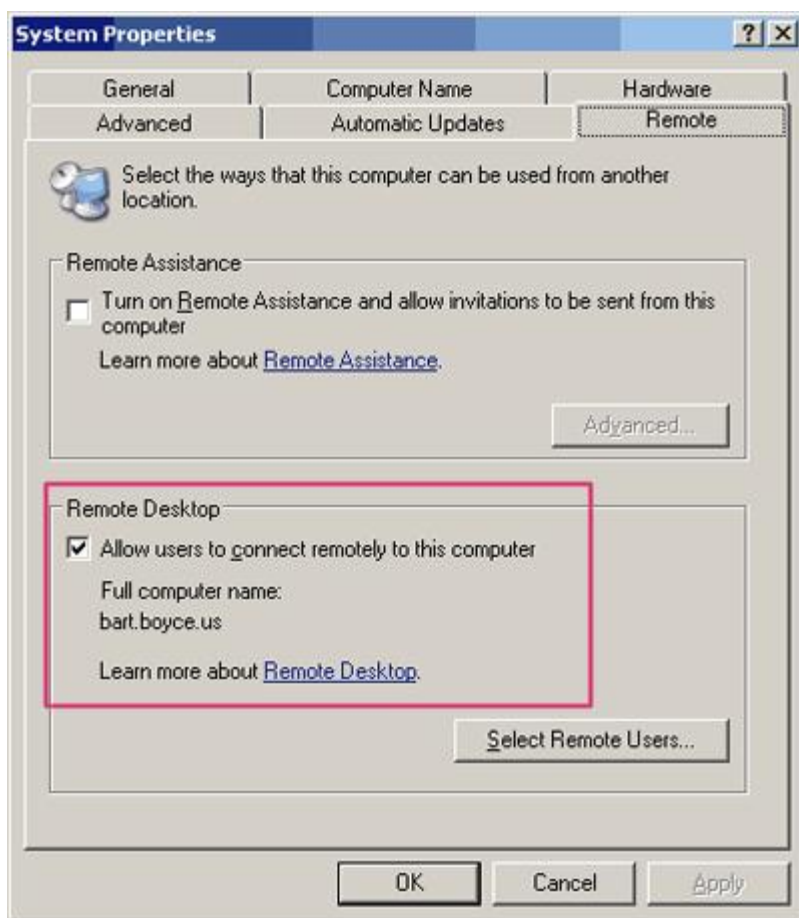
- **Client** (máy khách)

Máy để bàn từ xa đang chạy trên server được hiển thị trong một cửa sổ trên máy client. Khi khởi động một chương trình trên máy khách, thực tế các chương trình này đang chạy trên máy chủ. Remote Desktop Connection là tên được đặt cho client Terminal Services trong Windows 2000. Remote Desktop Connection sử dụng những cải tiến mới nhất của RDP 5.2, cung cấp khả năng nâng cao đáng kể so với các phiên bản trước đó. Remote Desktop Connection có thể được dùng để kết nối với các phiên bản cũ hơn của Terminal Services.

Sử dụng Remote Desktop for Administration

Mặc định, Remote Desktop for Administration được để ở chế độ không hoạt động. Muốn sử dụng nó, thực hiện theo các bước sau:

1. Vào **Start > Control Panel > System**.
2. Kích vào tab **Remote**, chọn **Allow users to connect remotely to your computer** (Cho phép người dùng kết nối từ xa tới máy tính của bạn) và kích **OK**.



Chú ý: Bạn không cần phải có Bản quyền truy cập client Terminal Server khi sử dụng Remote Desktop for Administration. Con số lớn nhất hai kết nối đồng thời được cho phép tự động trên server cuối khi Remote Desktop for Administration hoạt động.

Thay đổi mức mã hoá phiên

Mặc định mức mã hoá các phiên Terminal Services được thiết lập cho Client Compantible nhằm cung cấp mức mã hoá cao nhất hỗ trợ bởi client. Các thiết lập khác có thể sử dụng là:

- **High** - thiết lập này cung cấp khả năng bảo mật hai chiều sử dụng cơ chế mã hoá 128-bit.
- **Low** - thiết lập này sử dụng cơ chế mã hoá 56 bit.
- **FIPS Compliant**: tất cả dữ liệu được mã hoá bằng cách sử dụng các phương thức hợp lệ Federal Information Processing Standard 140-1.

Để kiểm tra mức mã hoá, thực hiện theo các bước sau:

1. Vào **Start > All Programs > Administrative Tools > Terminal Services Configuration**.
2. Ở khung bên trái, kích chọn **Connections**.
3. Ở khung bên phải, kích phải chuột lên **RDP-tcp** rồi chọn **Properties**.
4. Chọn **General** tab, chọn mức mã hoá bạn muốn trong danh sách **Encryption** rồi bấm **OK**.

Gỡ lỗi và sửa chữa

Nếu Terminal Services không ổn định, hãy kiểm tra lại địa chỉ IP. Các vấn đề có thể xuất hiện khi bạn cung cấp địa chỉ IP không hợp lệ. Nếu một chương trình chạy không như mong đợi, bạn có thể xem xét các vấn đề sau:

- Các chương trình có file khoá hoặc DLL không chạy chính xác. Vấn đề này xuất hiện khi có nhiều người dùng sử dụng cùng một lúc một chương trình nào đấy.
- Các chương trình sử dụng tên máy tính hoặc địa chỉ IP vào mục đích kiểm định có thể gặp sự cố. Vấn đề này xuất hiện khi nhiều người dùng cùng một lúc chạy chương trình khi dùng chung tên máy tính hoặc địa chỉ IP.

Để biết thêm thông tin về Windows Server 2003 Terminal Services, bạn có thể tìm trong Help and Support Center, dùng từ khoá "Terminal Services".

BÀI 11 : REMOTE INSTALLATION SERVICES

I-Giới thiệu dịch vụ

Ngày nay , trên toàn cầu đã có nhiều hệ điều hành mạng như Linux , WinNT và mới đây còn có công nghệ mới như Windows 2000 Server . Với Windows 2000 của Microsoft ra đời hỗ trợ một số tiện ích mà không có ở những hệ điều hành Win9x và WinNT về việc điều khiển từ xa , việc cài đặt hàng loạt các ứng dụng đến máy của những người dùng mạng từ một vị trí trung tâm .

Bước 1 : Cài đặt Remote Installation Services

Bước 2 : Cấu hình RIS server

Bước 3 : Cấu hình trên Server

Bước 4 : Cấu hình Group Policy

Bước 5: Cấp quyền khởi tạo cho các users.

Bước 6 : Chỉnh sửa Answer file cho image

Bước 7: Tiến hành cài đặt

Điều kiện thực hiện :

- * Hệ thống phải có Active Directory, các dịch vụ DNS, DHCP hoạt động tốt.
- * Server cài đặt RIS có 2 phân vùng khác nhau.
- * Phân vùng cài đặt RIS định dạng theo chuẩn NTFS.

Bước 1 : Cài đặt Remote Installation Services

- Vào Control Start -> Settings -> Control Panel -> Add/Remove Programs -> Add/Remove Windows Components.
- Chọn Remote Installation Services và click Next.



Trong quá trình cài đặt, đưa đĩa CD Windows Server 2k vào để chương trình copy các file cần thiết.

Bước 2 : Cấu hình RIS server

-Khởi động RIS: Start ->Run -> RISetup.exe



Click Next

-Chọn nơi để lưu các file cài đặt cho client (phải là phân vùng NTFS), Click Next



-Check vào mục Respond to client computer requesting service.



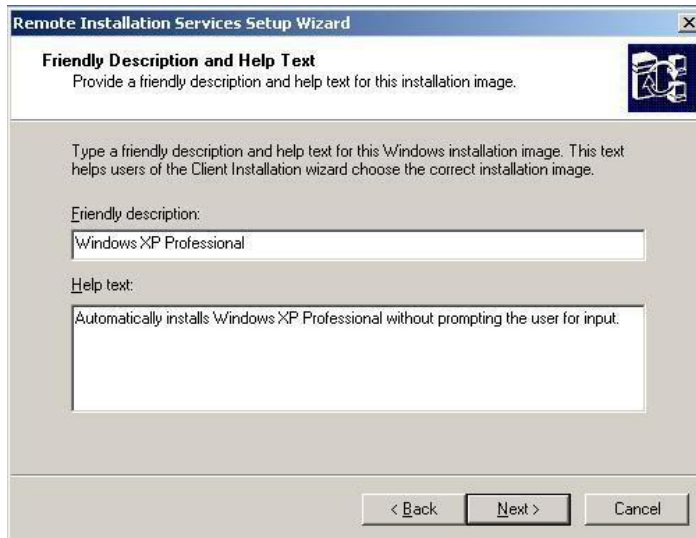
- Click Next.

-Chỉ đến nơi chứa source cài đặt HĐH(chỉ đến thư mục I386 trên CD-Rom chứa HĐH muốn cài), click Next



-Đặt tên và chú thích cho Image (mặc định)

- Click Next để tiếp tục.



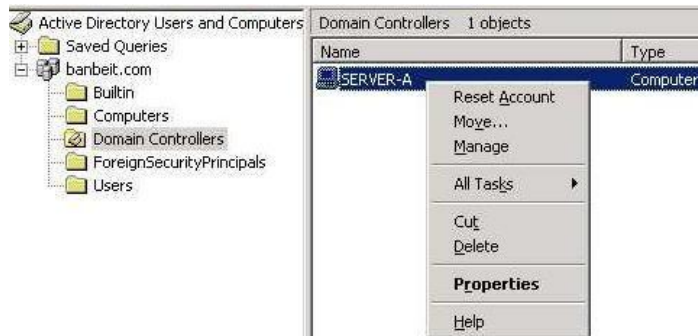
Click Next ->Next

-Quá trình copy files cần thiết từ CD cài đặt XP & tạo các file cấu hình

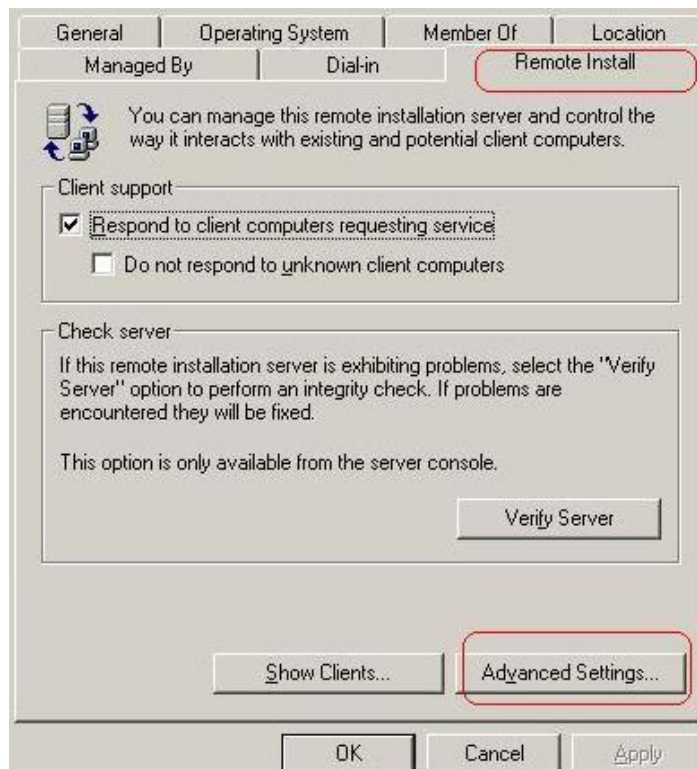


Bước 3 : Cấu hình trên Server

- Vào Active Directory User and Computers.
- >Chọn Domain -> Domain Controllers, click phải vào tên server, chọn Properties

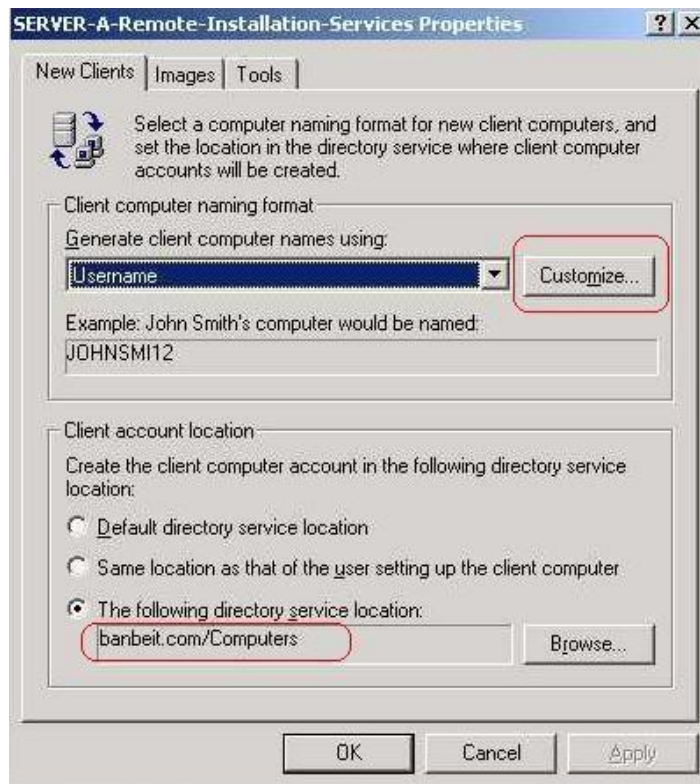


->Click tab Remote Install, chọn Advance Settings

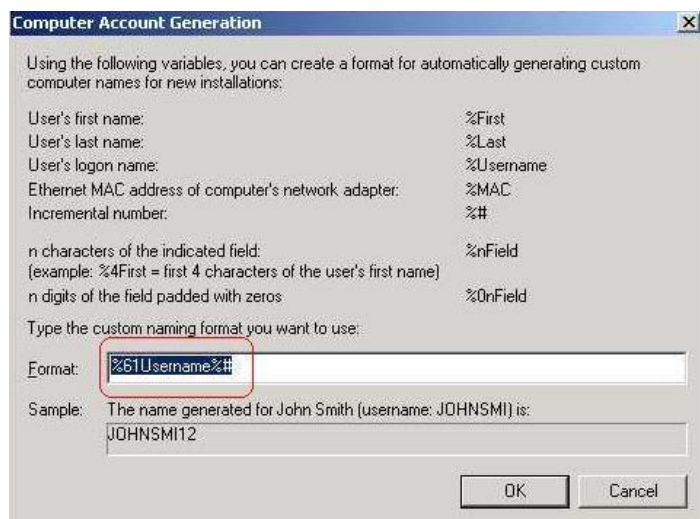


- Trong Advanced Settings ->Client Account location :

->Chọn The following directory service location,duyet đến tên domain/computers trong Active Directory



Ở hình trên, trong mục **Client computer naming format**, chọn **Customize** -> Trong hộp thoại Customize, trong mục Format nhập vào các tham số đặt tên cho máy.

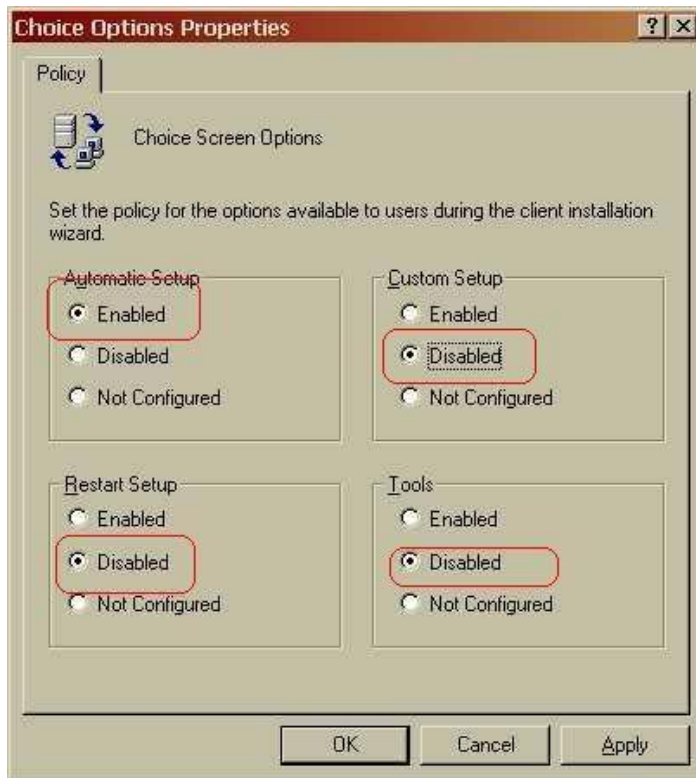


VD: tham số %Username, lấy tên người dùng để đặt tên máy tính.

Bước 4 : Cấu hình Group Policy

Việc này nhằm đảm bảo cho quá trình cài đặt được tự động hoàn toàn.

-Vào User Configuration > Windows Settings > Remote Installation Services, chỉnh theo hình sau:



Bước 5: Cấp quyền khởi tạo cho các users.

- Khi cài đặt, máy con sẽ tự join vào Domain. Vì vậy, User phải có quyền tạo tài khoản máy trên OU domain/computers trong Active Directory.

- Cấp quyền cho Users:

+ Tạo Group tên là RISInstall

+ Add tất cả các user sử dụng cho việc cài đặt máy vào RISInstall.

+ Add group RISInstall vào nhóm Account Operators.

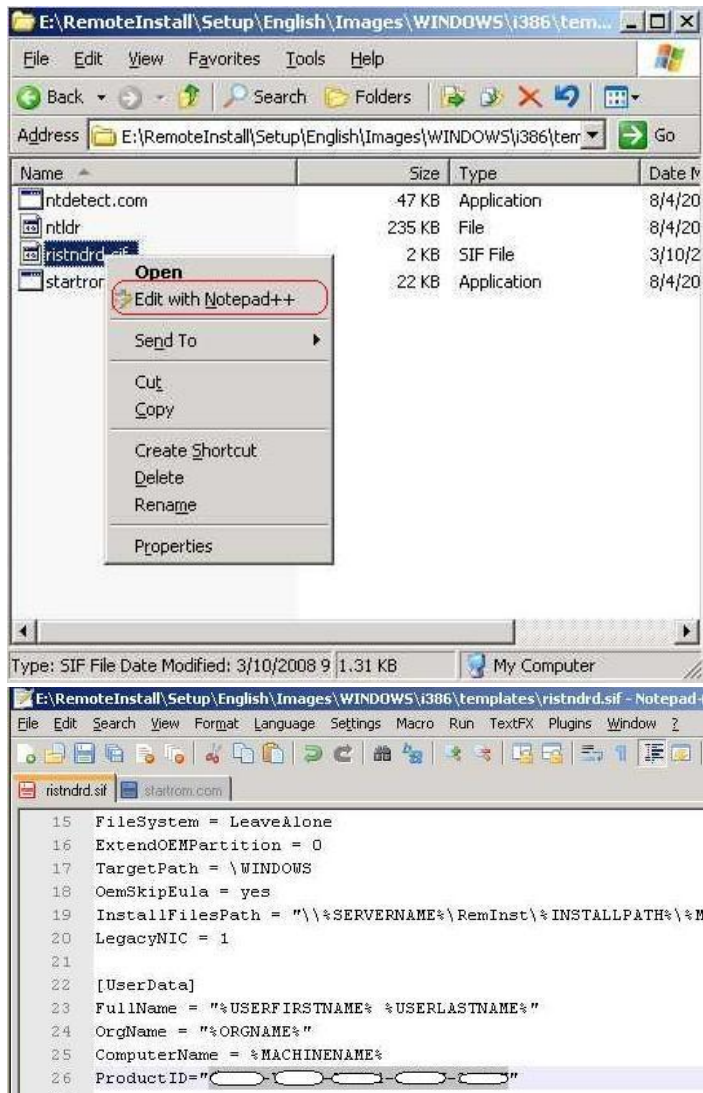
**Lưu ý: Khi kết thúc quá trình cài đặt, cần remove nhóm RISInstall ra khỏi nhóm Account Operator hoặc xóa nhóm này.

Bước 6 : Chỉnh sửa Answer file cho image:

Trong quá trình cài đặt tạo Image ở trên, RIS Server đã tạo sẵn file Answer nhưng chưa đầy đủ. Chúng ta cần chỉnh sửa lại, nếu không trong lúc cài đặt sẽ bị hỏi thông tin.

- Vào thư mục \\Setup\\English\\Images\\Windows\\i386\\templates.

Mở file **ristndrd.sif**, tìm đến đoạn [UserData] và thêm vào dòng ProductID= "số CD-Key" và lưu lại.



- Tại mục Re- partition --> sửa lại là NO
- Tại mục Use Whole disk --> sửa lại là NO

```
[RemoteInstall]
Repartition = NO
UseWholeDisk = NO
```

(Nếu không chỉnh 2 mục trên thì các client sẽ bị mất các partition sau khi cài xong!)

Bước 7: Tiến hành cài đặt

Để cho các máy chưa có HĐH liên lạc được với RIS Server, Card mạng của máy muốn cài đặt HĐH phải có tính năng boot qua mạng (PXE), hoặc chúng ta có thể dùng đĩa mềm hay đĩa CD ROM có chức năng Boot từ mạng.

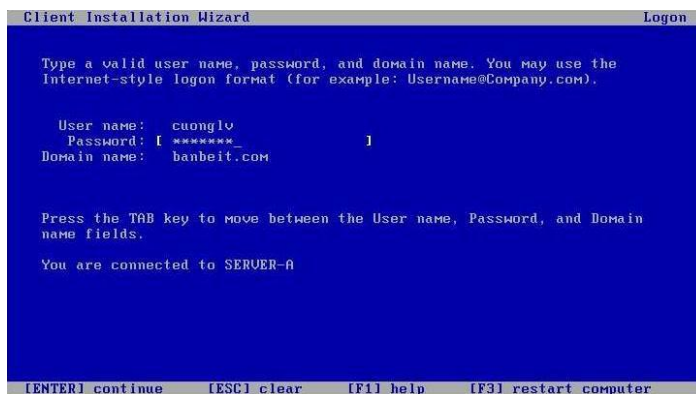
Đa số các loại máy hiện nay card mạng đều hỗ trợ PXE.

- Vào BIOS cho phép boot từ card mạng để boot qua mạng hoặc boot từ CD boot mạng.
- Bật máy cần cài đặt, máy sẽ tìm kiếm DHCP server và khởi động Client Installation Wizard



Nhấn Enter để tiếp tục.

- Nhập vào tài khoản khởi tạo.



II-Ứng dụng cài đặt

Bước 1 : Cài đặt Remote Installation Services

Bước 2 : Cấu hình RIS server

Bước 3 : Cấu hình trên Server

Bước 4 : Cấu hình Group Policy

Bước 5: Cấp quyền khởi tạo cho các users.

Bước 6 : Chỉnh sửa Answer file cho image

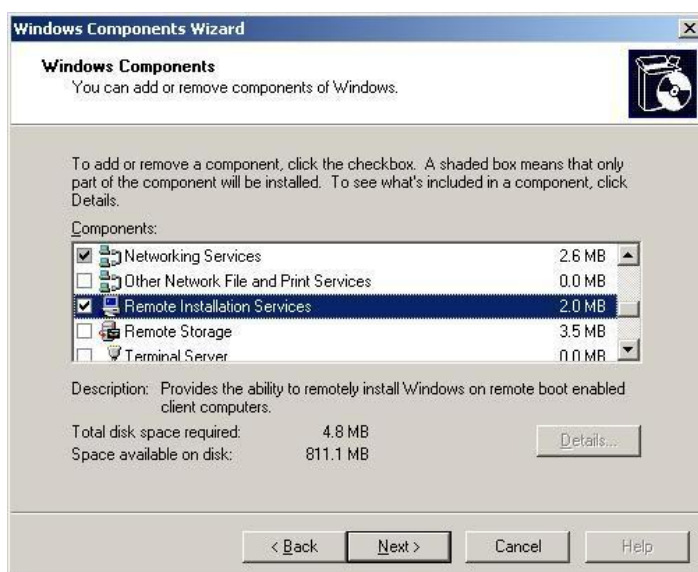
Bước 7: Tiến hành cài đặt

Điều kiện thực hiện :

- * Hệ thống phải có Active Directory, các dịch vụ DNS, DHCP hoạt động tốt.
- * Server cài đặt RIS có 2 phân vùng khác nhau.
- * Phân vùng cài đặt RIS định dạng theo chuẩn NTFS.

Bước 1 : Cài đặt Remote Installation Services

- Vào Control Start -> Settings -> Control Panel -> Add/Remove Programs -> Add/Remove Windows Components.
- Chọn Remote Installation Services và click Next.



Trong quá trình cài đặt, đưa đĩa CD Windows Server 2k vào để chương trình copy các file cần thiết.

Bước 2 : Cấu hình RIS server

-Khởi động RIS: Start ->Run -> RISetup.exe

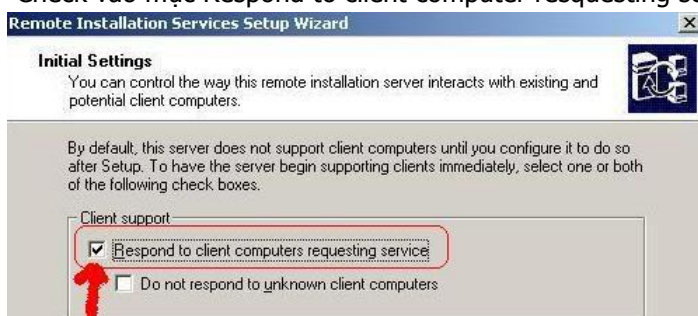


Click Next

-Chọn nơi để lưu các file cài đặt cho client (phải là phân vùng NTFS), Click Next



-Check vào mục Respond to client computer requesting service.



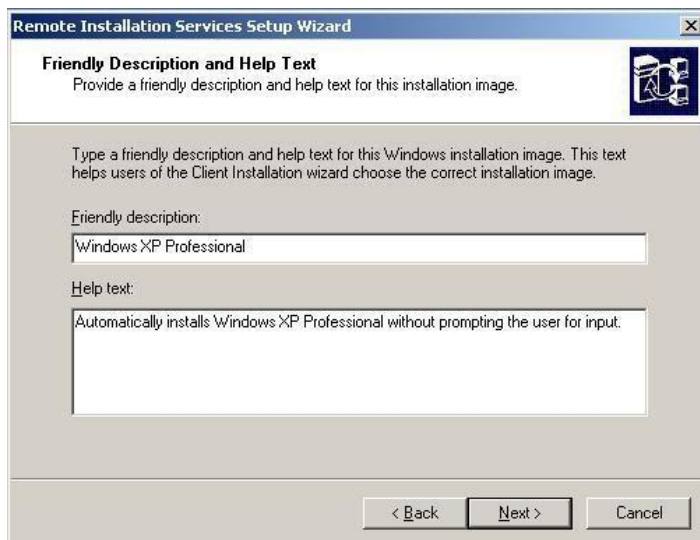
- Click Next.

-Chỉ đến nơi chứa source cài đặt HĐH(chỉ đến thư mục I386 trên CD-Rom chứa HĐH muốn cài), click Next



-Đặt tên và chú thích cho Image (mặc định)

- Click Next để tiếp tục.



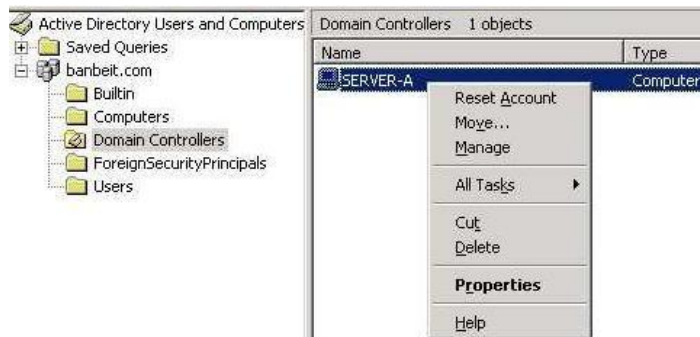
Click Next ->Next

-Quá trình copy files cần thiết từ CD cài đặt XP & tạo các file cấu hình

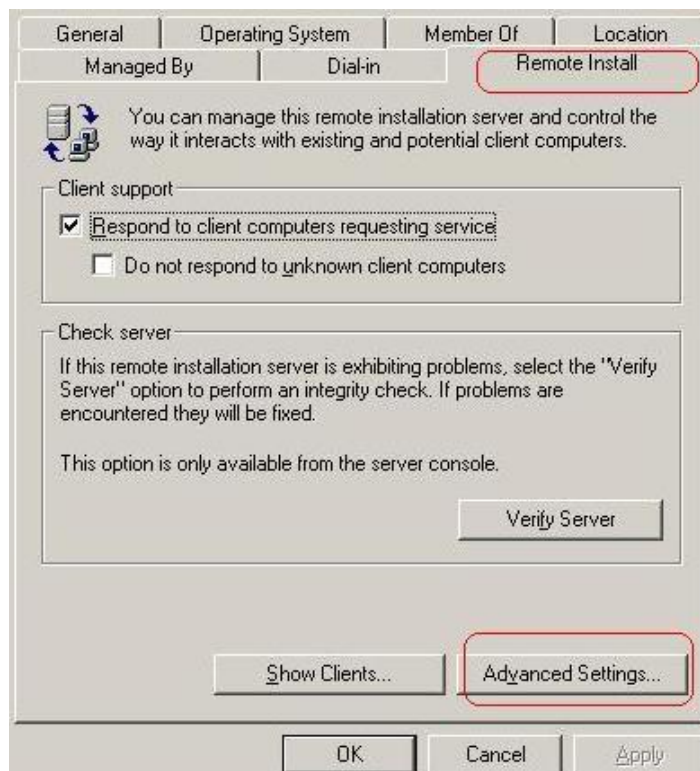


Bước 3 : Cấu hình trên Server

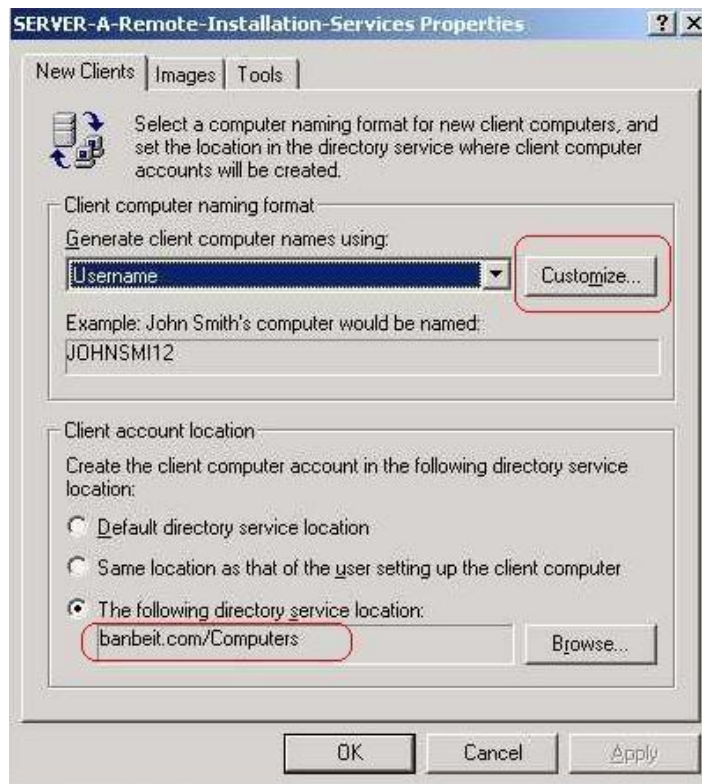
- Vào Active Directory User and Computers.
- >Chọn Domain -> Domain Controllers, click phải vào tên server, chọn Properties



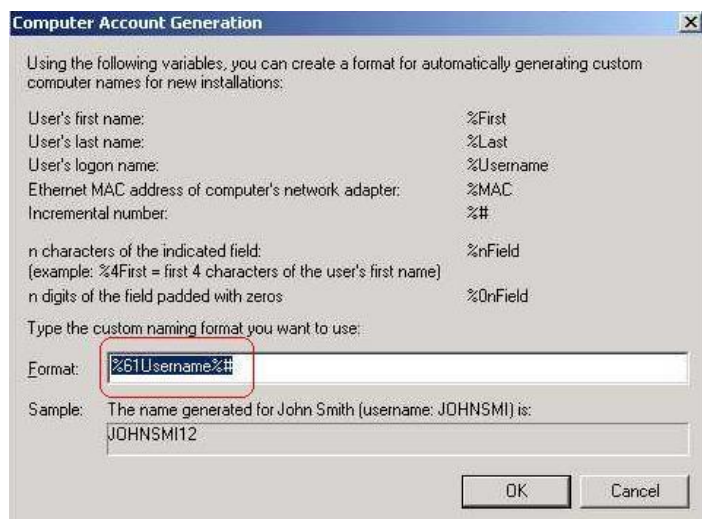
- >Click tab Remote Install, chọn Advance Settings



- Trong Advanced Settings ->Client Account location :
- >Chọn The following directory service location, duyệt đến tên domain/computers trong Active Directory



Ở hình trên, trong mục **Client computer naming format**, chọn **Customize** -> Trong hộp thoại Customize, trong mục Format nhập vào các tham số đặt tên cho máy.

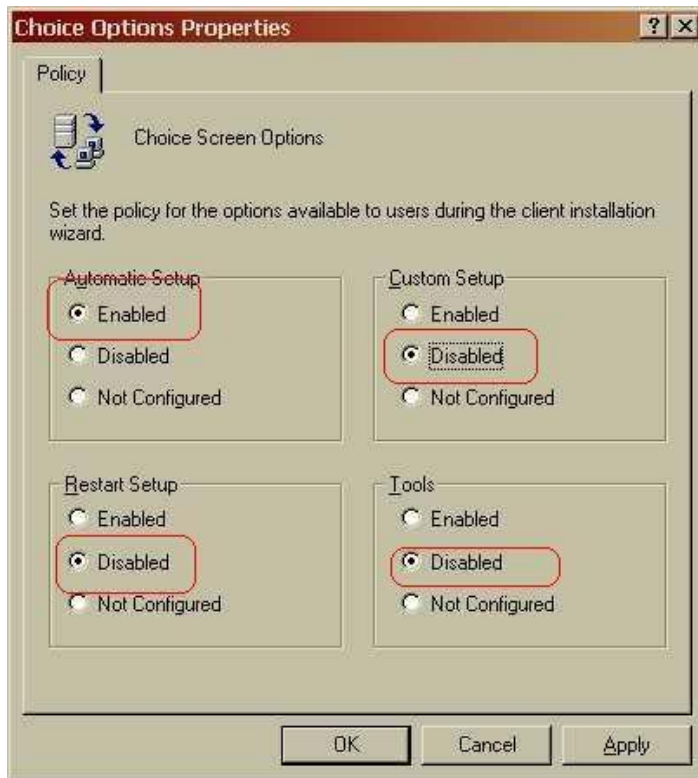


VD: tham số %Username, lấy tên người dùng để đặt tên máy tính.

Bước 4 : Cấu hình Group Policy

Việc này nhằm đảm bảo cho quá trình cài đặt được tự động hoàn toàn.

-Vào User Configuration > Windows Settings > Remote Installation Services, chỉnh theo hình sau:



Bước 5: Cấp quyền khởi tạo cho các users.

- Khi cài đặt, máy con sẽ tự join vào Domain. Vì vậy, User phải có quyền tạo tài khoản máy trên OU domain/computers trong Active Directory.

-Cấp quyền cho Users:

+Tạo Group tên là RISInstall

+Add tất cả các user sử dụng cho việc cài đặt máy vào RISInstall.

+Add group RISInstall vào nhóm Account Operators.

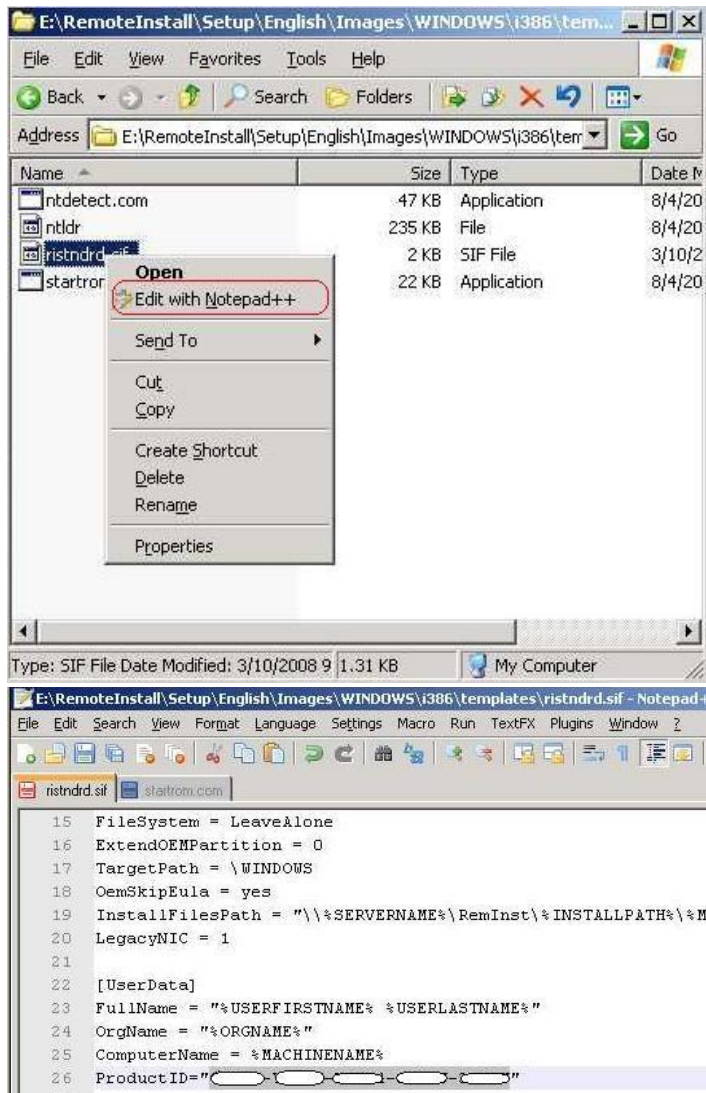
**Lưu ý: Khi kết thúc quá trình cài đặt, cần remove nhóm RISInstall ra khỏi nhóm Account Operator hoặc xóa nhóm này.

Bước 6 : Chỉnh sửa Answer file cho image:

Trong quá trình cài đặt tạo Image ở trên, RIS Server đã tạo sẵn file Answer nhưng chưa đầy đủ. Chúng ta cần chỉnh sửa lại, nếu không trong lúc cài đặt sẽ bị hỏi thông tin.

-Vào thư mục \\Setup\English\Images\Windows\i386\templates.

Mở file **ristndrd.sif**, tìm đến đoạn [UserData] và thêm vào dòng ProductID= "số CD-Key" và lưu lại.



- Tại mục Re- partition --> sửa lại là NO
- Tại mục Use Whole disk --> sửa lại là NO

```
[RemoteInstall]
Repartition = NO
UseWholeDisk = NO
```

(Nếu không chỉnh 2 mục trên thì các client sẽ bị mất các partition sau khi cài xong!)

Bước 7: Tiến hành cài đặt

Để cho các máy chưa có HĐH liên lạc được với RIS Server, Card mạng của máy muốn cài đặt HĐH phải có tính năng boot qua mạng (PXE), hoặc chúng ta có thể dùng đĩa mềm hay đĩa CD ROM có chức năng Boot từ mạng.

Đa số các loại máy hiện nay card mạng đều hỗ trợ PXE.

- Vào BIOS cho phép boot từ card mạng để boot qua mạng hoặc boot từ CD boot mạng.
- Bật máy cần cài đặt, máy sẽ tìm kiếm DHCP server và khởi động Client Installation Wizard



Nhấn Enter để tiếp tục.

-Nhập vào tài khoản khởi tạo.



Bài 12 : Xây dựng hệ thống mạng Bootrom.**GIỚI THIỆU KHÁI QUÁT VỀ MẠNG BOOT-ROM****1. GIỚI THIỆU:**

Từ bài viết này, sẽ hướng dẫn cách thực hiện một hệ thống mạng LAN sử dụng kỹ thuật BOOTROM (hay còn gọi là khởi động máy từ xa – remote boot) cho phép một số máy tính thành viên trong mạng không gắn đĩa cứng riêng mà vẫn có thể hoạt động như một máy tính thông thường. Hệ thống mạng đặc biệt này được gọi một cách ngắn gọn là Mạng BOOT-ROM. Trong Phần 1 sẽ giới thiệu mô hình mạng BOOT-ROM và tìm hiểu nguyên lý hoạt động cơ bản của hệ thống mạng này.

2. CHUẨN BỊ:

Chúng ta sẽ xây dựng mạng BOOT-ROM trong đó các máy khách sẽ dùng chung một ổ đĩa ảo (thực chất là một tập tin ảnh dùng chung - Share Image) chứa HĐH Windows XP, với những chuẩn bị và qui ước như sau:

- Máy chủ có cấu hình Pentium 4, HDD 40GB, RAM 512 MB, HĐH Windows Server 2003 kèm theo dịch vụ cấp phát địa chỉ động DHCP
- Các máy trạm có cấu hình đồng bộ Celeron, RAM 128MB, HĐH Windows XP và các ứng dụng cần thiết.
- Sử dụng card mạng Realtek 8139 tốc độ 10/100 Mb/s gắn kèm BOOT-ROM hỗ trợ chuẩn PXE 2.0
- Phần mềm tạo và quản lý tập tin ảnh của đĩa cứng ảo BXP 2.5 của hãng Venturcom.

3. MÔ HÌNH HOẠT ĐỘNG:

Để thực hiện hệ thống mạng BOOT-ROM này, chúng ta cần có những kiến thức cơ bản về mạng máy tính và TCP/IP, tuy nhiên bạn cũng có thể chấp nhận một số kết quả trong quá trình thực hiện. Những vấn đề này chúng ta sẽ có dịp hiểu kỹ hơn khi thực hành nhiều lần cũng như tham khảo thêm các tài liệu liên quan và tài liệu đi kèm với phần mềm. Trước khi bắt tay vào việc, chúng ta cần nắm được một cách khái quát về mô hình hoạt động của hệ thống mạng này.

MÔ HÌNH 01:

Trước tiên, ta xem xét mô hình hoạt động gồm 03 máy tính:

- Máy A là P4 được cài đặt HĐH Windows Sever 2003
- 02 máy còn lại B & C là máy Celeron được cài đặt HĐH Windows XP và ứng dụng cần thiết

Các máy này đều có thể hoạt động độc lập nhờ các HĐH được cài đặt trên đĩa cứng riêng của từng máy.

MÔ HÌNH 02:

Khi các máy có nhu cầu trao đổi thông tin hoặc sử dụng các dịch vụ từ một máy khác thì ta sẽ kết nối chúng lại thông qua các thiết bị mạng.

Trong hệ thống mạng này ta gọi máy tính A được cài HĐH Windows Server 2003 là máy chủ và 02 máy còn lại B & C là các máy khách. Ở mô hình này các máy vừa chạy độc lập vừa có thể trao đổi thông tin hay sử dụng các dịch vụ của nhau thông qua hệ thống mạng vừa thiết lập.

MÔ HÌNH 03:

Bây giờ có 1 câu hỏi đặt ra là nếu chúng ta bỏ đĩa cứng đang chứa HĐH Windows XP ra ngoài thì máy khách B hoặc C có thể hoạt động bình thường như trước đó hay không? Câu trả lời là hoạt động được. Để làm được điều này ta cần có thêm trợ giúp từ một phần mềm thứ 3 mà trong chương trình sử dụng phần mềm BXP 2.5 của hãng Venturcom. Phần mềm BXP gồm 2

thành phần:

- BXP server được cài đặt trên máy chủ A
- BXP Client trên 2 máy khách B, C.

Nhiệm vụ của phần mềm BXP là

- Mã hoá toàn bộ HĐH Windows XP đang cài đặt trên đĩa cứng của máy B hoặc C thành một tập tin ảnh.
- Chép tập tin ảnh này đặt trên đĩa cứng của máy chủ A và làm sao để máy khách có thể truy xuất nó như là một ổ đĩa ảo có chứa HĐH Windows XP.
- Quản lý và phối hợp các hoạt động giữa đĩa ảo với từng máy khách

MÔ HÌNH 04:

Trong mạng BOOT-ROM các máy khách không ổ cứng khởi động vào hệ điều hành dựa vào sự hỗ trợ hoàn toàn từ máy chủ. Nghĩa là HĐH Windows XP điều khiển máy khách sẽ được nạp vào từ tập

tin ảnh ảo trên ổ cứng của máy chủ thay vì trên máy khách. Để làm được điều này, đầu tiên card mạng trên các máy khách cần gắn thêm BOOT-ROM hỗ trợ chuẩn PXE version V.99J hoặc cao hơn.

Khi bạn bật nguồn cho máy khách, đoạn mã chương trình chứa trong BOOT-ROM trên card mạng được khởi động và phát ra một yêu cầu nhận cấp phát địa chỉ IP và các thông tin cấu hình khác đến máy chủ. Dịch vụ cấp phát địa chỉ IP động DHCP được cài đặt trên máy chủ sẽ nhận yêu cầu và cấp cho máy khách một địa chỉ IP, các thông tin cấu hình liên quan và địa chỉ của máy chủ cài đặt các dịch vụ của BXP (như dịch vụ Boot và Login).

Sau khi đã nhận đầy đủ các thông tin này, BOOT-ROM trên máy khách sẽ sử dụng giao thức truyền tập tin TFTP (Trivial File Transfer Protocol) để nạp một tập tin ảnh chứa thông tin khởi động (Bootstrap File VLDRMIL13.BIN) đã được lưu trên đĩa cứng của máy chủ.

Giao thức TFTP cũng được sử dụng để truyền tập tin giữa máy chủ và máy khách. Sau đó máy khách sẽ khởi động từ tập tin Bootstrap này và thông qua sự hỗ trợ của các dịch vụ chứa trong BXP để truy xuất tập tin ảnh ảo của HĐH Windows XP dưới hình thức một ổ đĩa ảo lưu trên đĩa cứng của máy chủ.

4. KẾT PHẦN I:

Đến đây chúng ta đã biết mạng BOOT-ROM là gì và nguyên tắc hoạt động của nó ra sao. Trong bài tới chúng ta sẽ bắt đầu các bước cài đặt.

HƯỚNG DẪN BẰNG HÌNH ẢNH QUÁ TRÌNH SETUP BOOTROM – BXP 5.0.1a

Quá trình xây dựng 1 server Boot rom + server game gồm các bước sau:

- 1/ Bước 1: Cài đặt WINDOW SERVER (Phần này các bạn tự tìm hiểu)
- 2/ Bước 2: Cài đặt DHCP cung cấp IP cho các máy client
- 3/ Bước 3: Cài đặt Dot Net 3.0 (Microsoft .NET Framework 3.0)
- 4/ Bước 4: Cài đặt SQL Server 5.0
- 5/ Bước 5: Cách Download Citrix Provisioning Server BXP 5.0.2
- 6/ Bước 6: Cài đặt Citrix Provisioning Server BXP 5.0.1.a (Boot Rom)
- 7/ Bước 7: Cài đặt máy client.

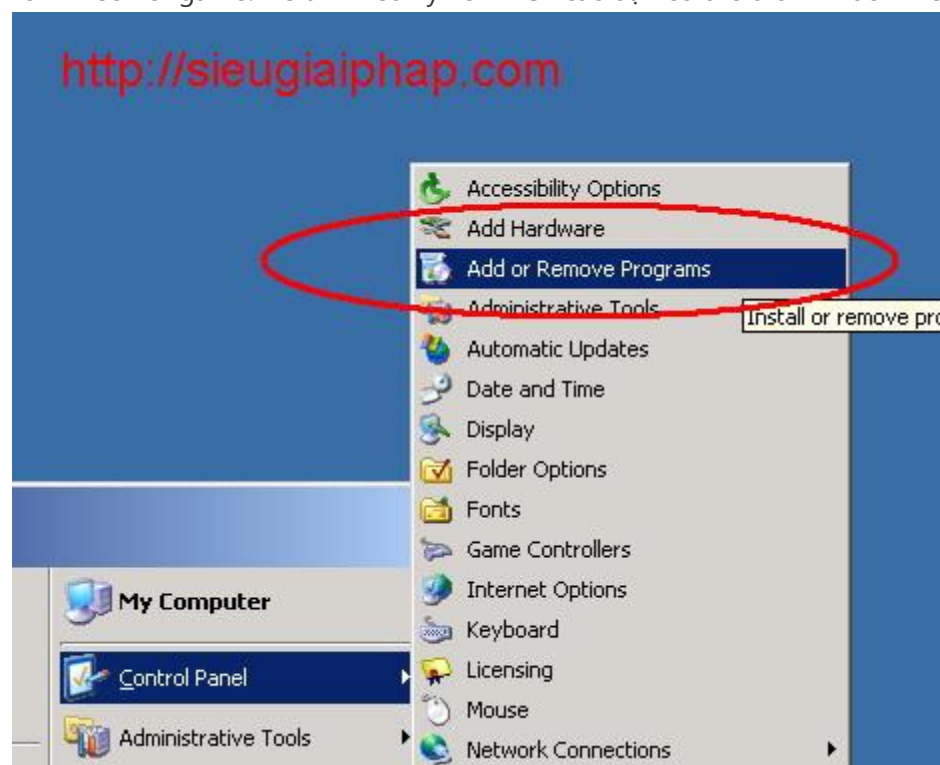
Bắt đầu nào

1/ Bước 1: Quá trình setup WIN SERVER 2003 hay WIN SERVER 2008 các bạn có thể tìm hiểu trong nhiều tài liệu. Xem như việc cài đặt hệ điều hành WIN SERVER các bạn đã thực hiện xong. Trong phần bài hướng dẫn này mình sử dụng hệ điều hành WIN SERVER 2003.

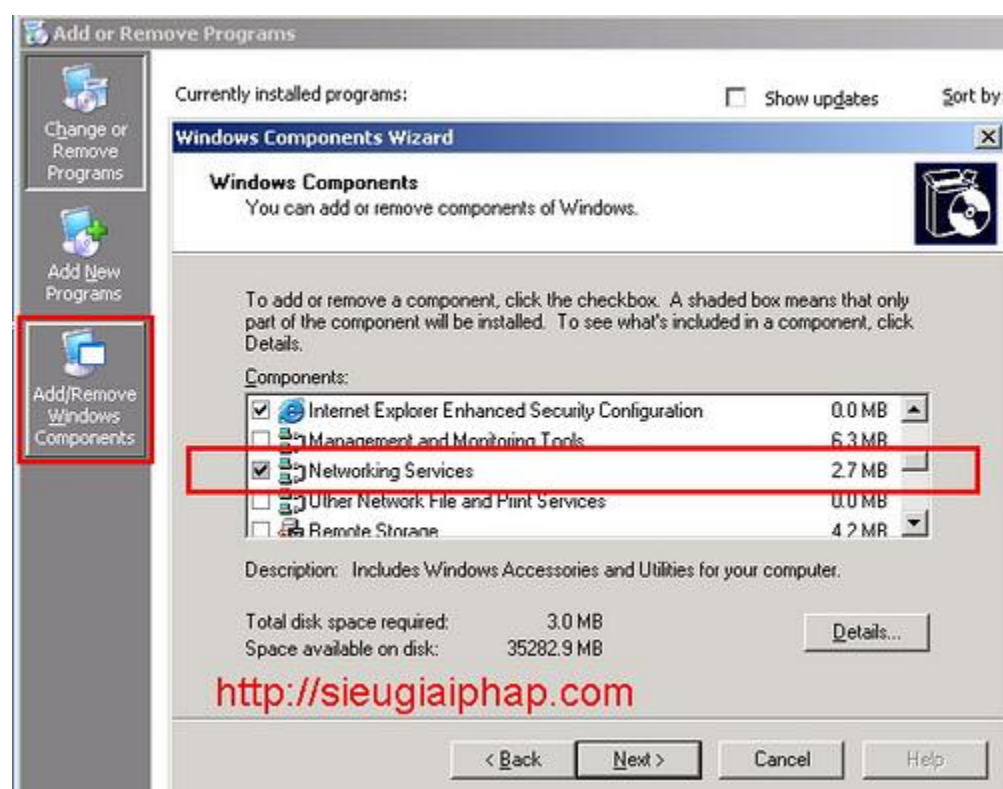
2/ Bước 2: Cài đặt DHCP.

Dịch vụ DHCP có công dụng cung cấp IP cho các máy client 1 cách tự động.

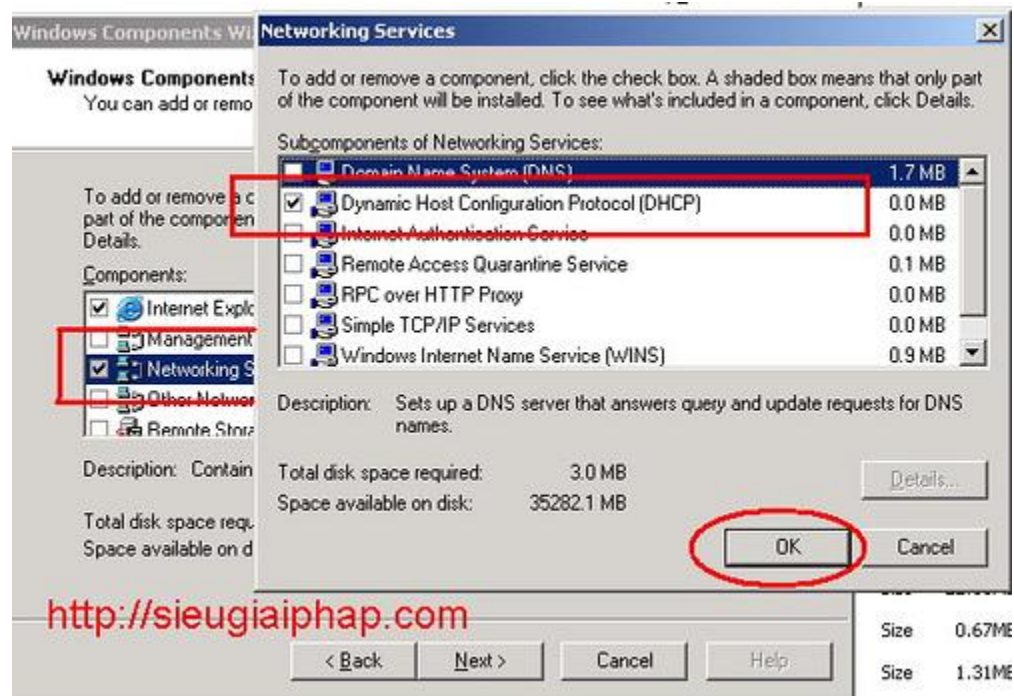
Trong phần hướng dẫn này mình nói nhanh các bước cài đặt phục vụ cho việc xây dựng server boot rom + server game. Để tìm hiểu kỹ về DHCP các bạn có thể tham khảo nhiều tài liệu khác.



Chọn "Add or Remove Programs"



Chọn "Add/Remove Windows Components", check "Networking Services", sau đó click vào nút "Details..."



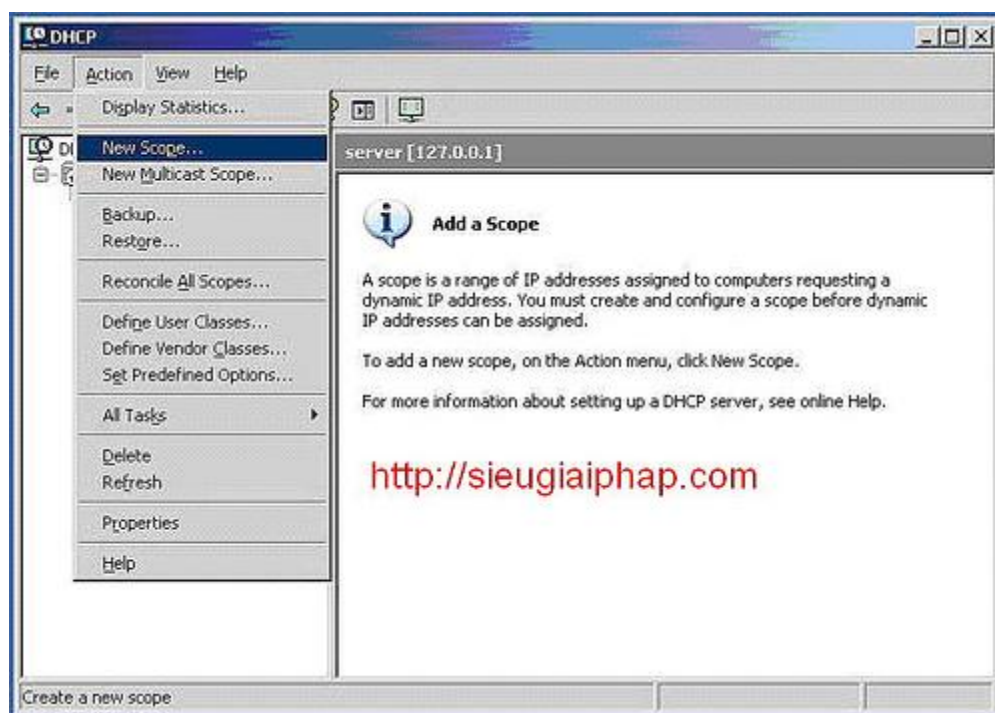
Check vào ô "Dynamic Host Configuration Protocol (DHCP)".

Chú ý: Trong quá trình cài DHCP, Windows đòi phải có đĩa WINDOWS trong ổ CD.



Bạn đã cài đặt thành công DHCP cho máy server của mình.

Tiếp đến chúng ta cấu hình DHCP server để cấp IP cho client:



Đầu tiên chọn New Scope



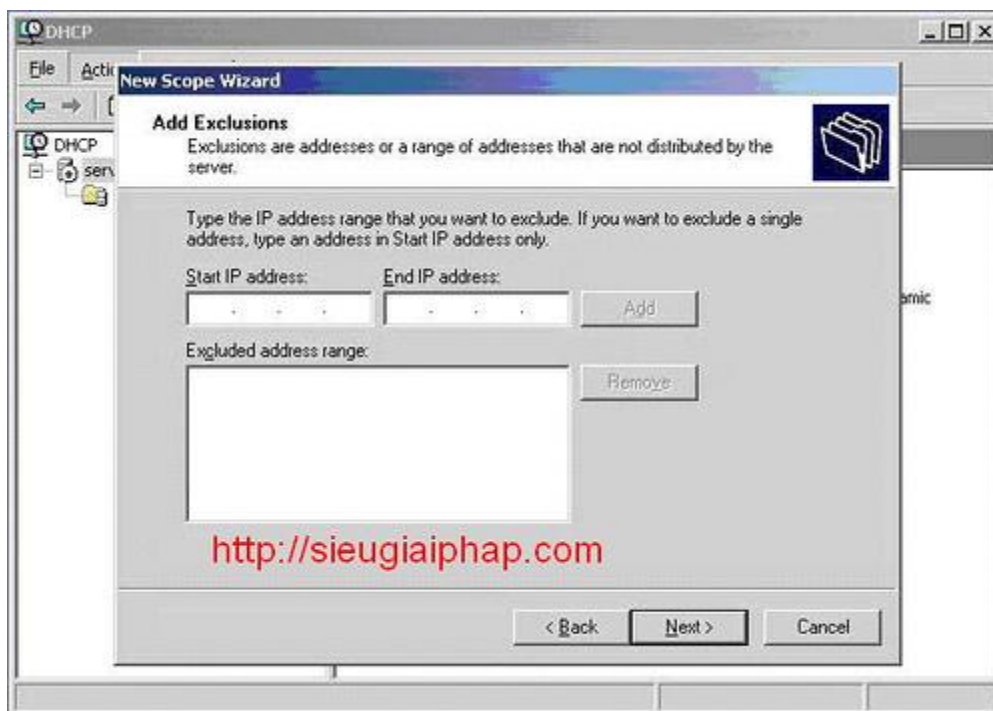
Click Next>



Điền Name và Description vào rồi Next>



Phần này là khoảng phạm vi IP mà DHCP server sẽ cấp cho Client, với tôi giới hạn từ IP 192.168.1.100 đến 192.168.1.150

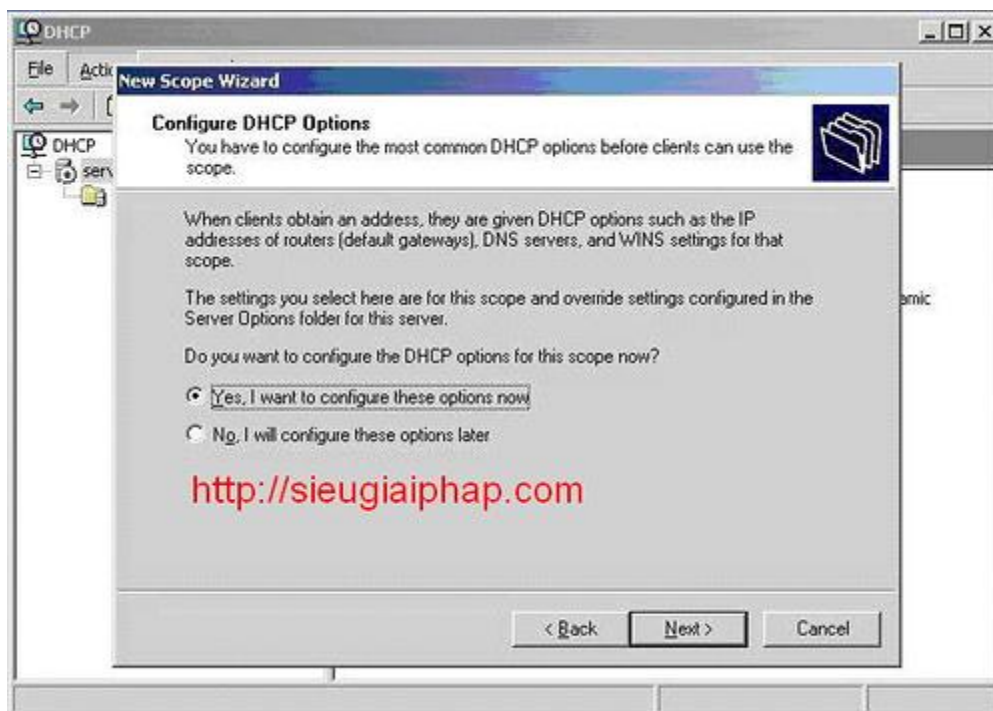


Những IP mà bạn ko muốn DHCP cung cấp cho máy Client.

Nghĩa là: Nếu bạn muốn DHCP không cung cấp IP nào mà nằm trong khoảng phạm vi IP của bạn vừa điền ở trên, bạn có thể điền số IP đó vào chỗ này. Và cứ Next nha



Cứ để mặc định 8h sau khi cấu hình xong chúng ta sẽ chỉnh lại unlimited, và chọn Next>

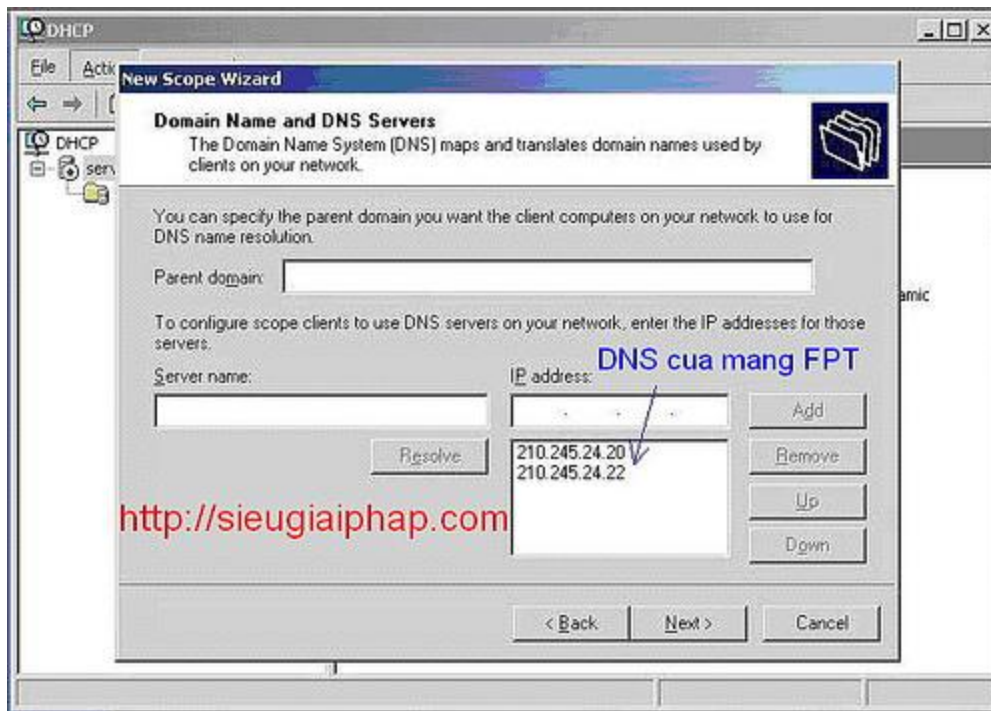


Theo trong hình rồi chọn Next> nha



Điền địa chỉ gateway rồi Add > và Next >

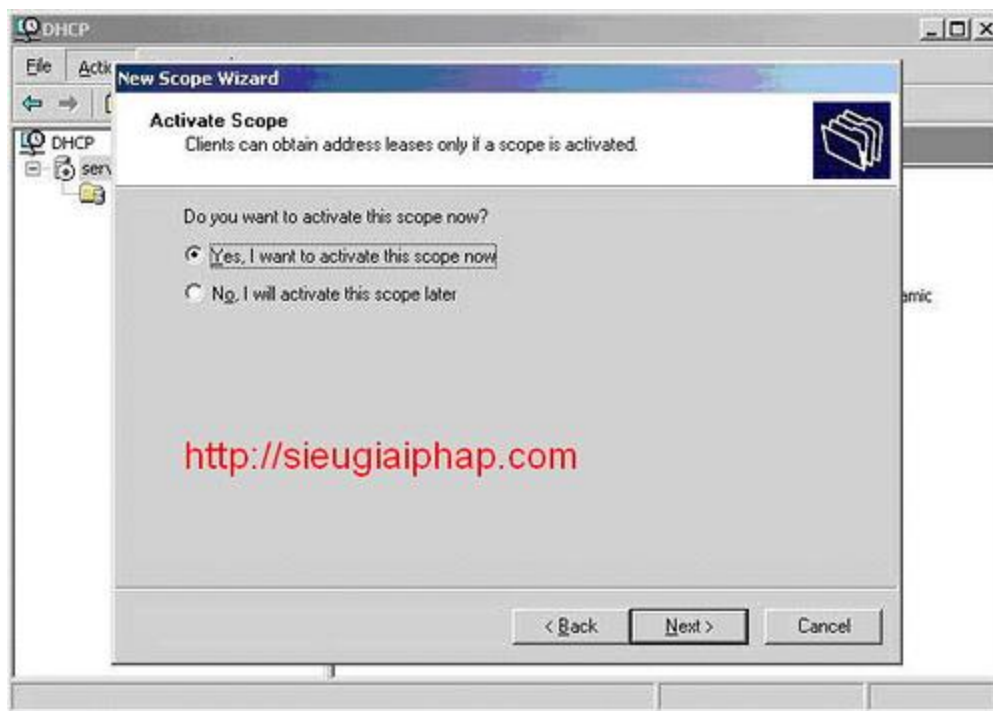
Chú ý: gateway là địa chỉ của modem đó, của mình là 192.168.1.1, còn của bạn?



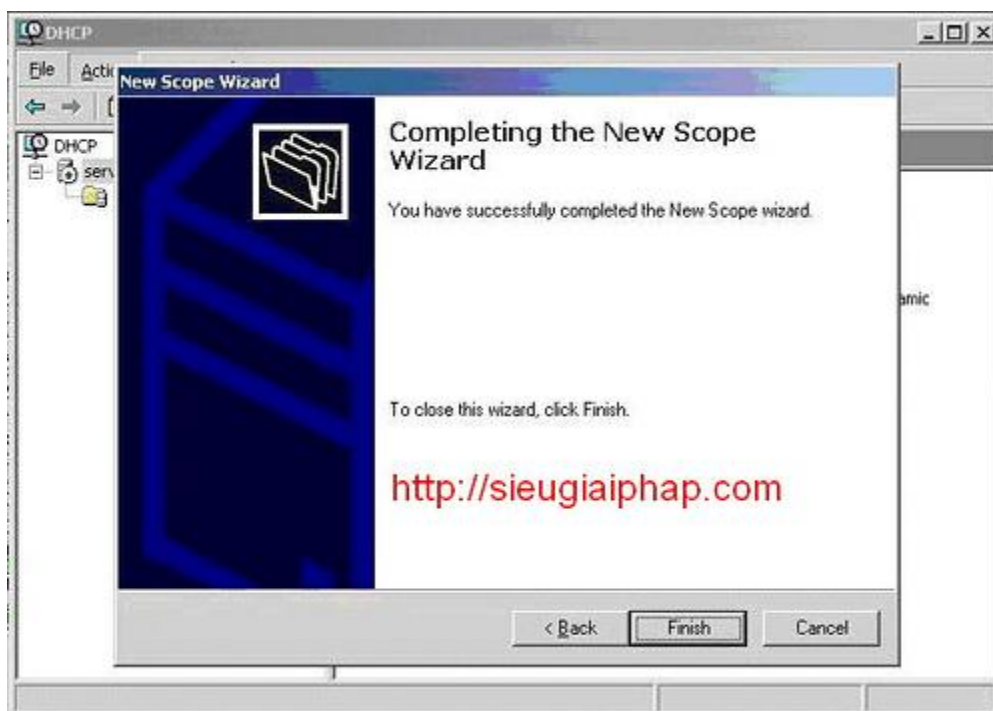
Điền DNS server, mạng mình dùng là FPT, nên là số này, còn VNN và Viettel thì khác nha.



Chọn Next >

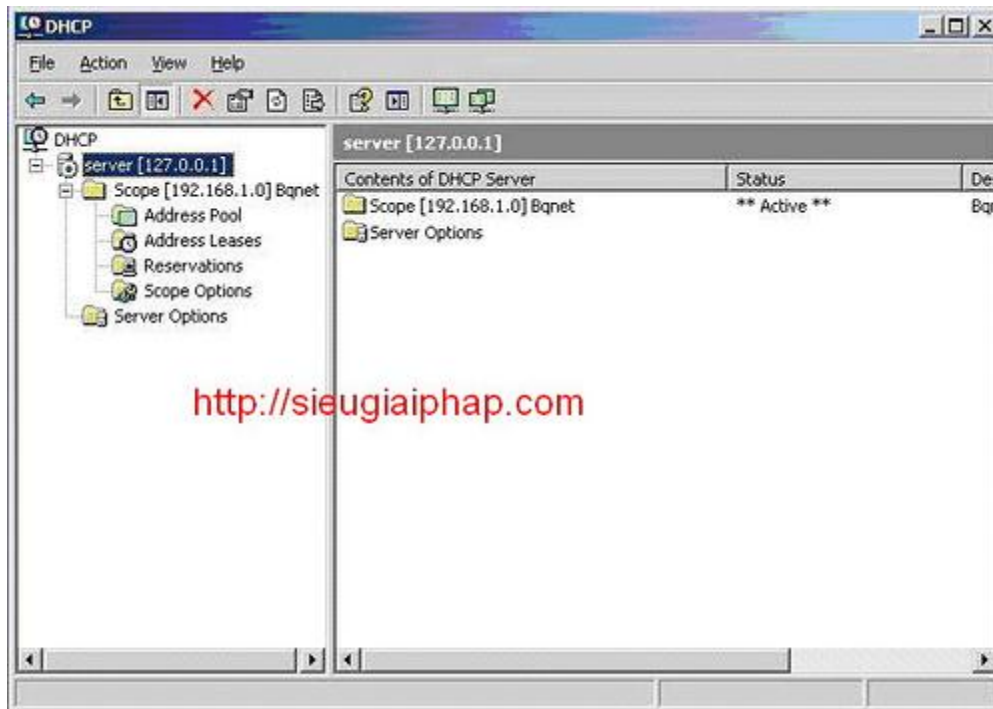


Như trong hình rồi chọn Next > (sẽ chạy DHCP ngay sau khi cấu hình xong)



Chọn Finish là chúng ta đã cấu hình xong DHCP server

Và đây là thành quả của mình - giao diện chính của DHCP server như sau:

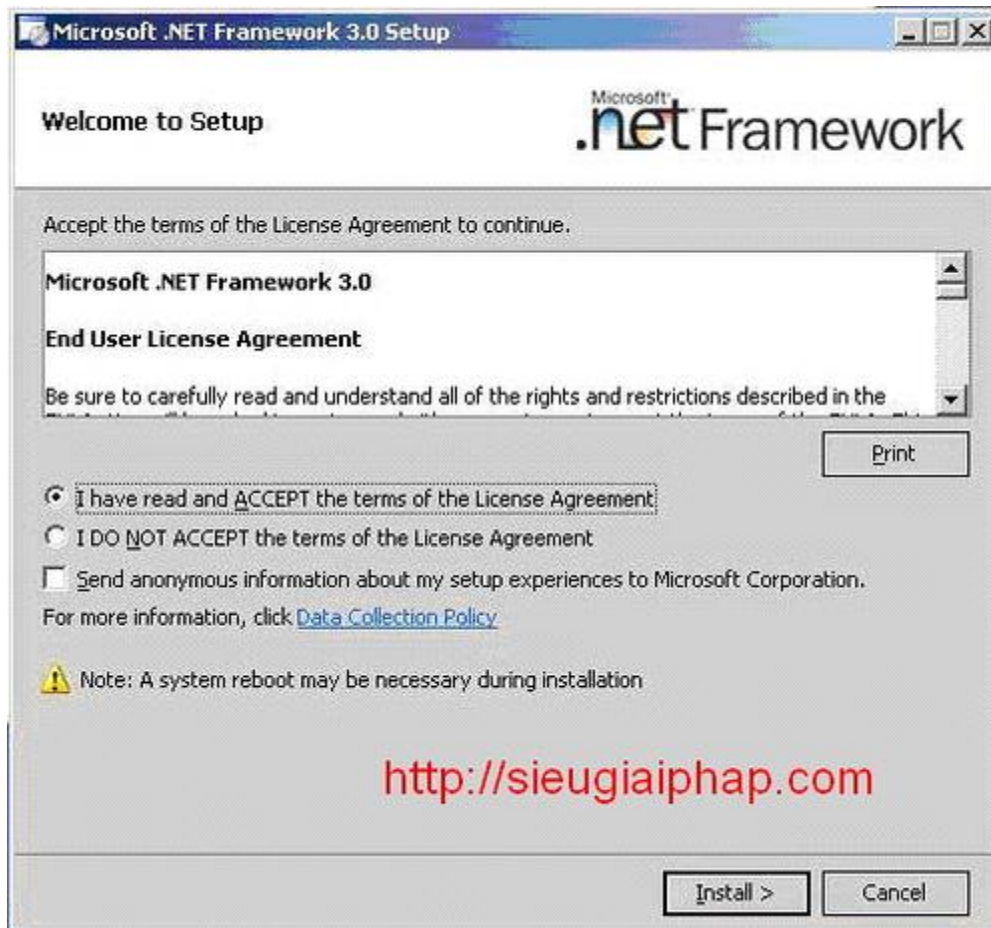


Bước 3: Cài đặt .Net Framework 3.0

Khi sử dụng Bootrom bằng phần mềm Citrix BXP 5.01.a thì cấu hình đòi hỏi chúng ta phải có .Net Framework 3.0 và SQL Server 5.0 (bước 4).

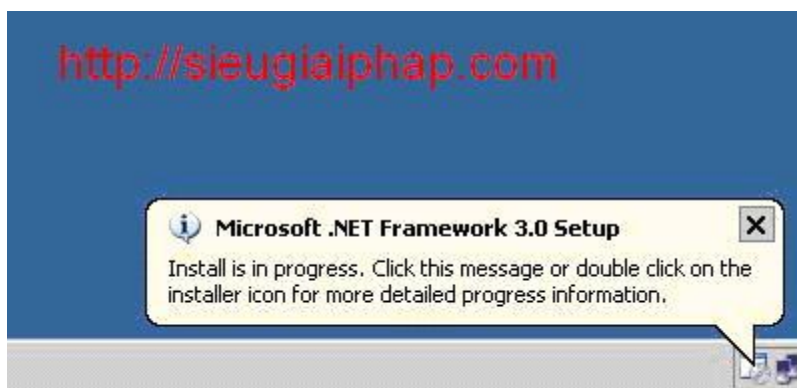
Hai phần mềm này sẽ có sẵn trong đĩa CD setup Citrix BXP5.0.1a. (bước 6)

Bắt đầu nào, trong CD Citrix BXP5.0.1a có 2 phiên bản .Net Framework 3.0 cho 2 win tương ứng (32 bit và 64 bit). Vì mình sử dụng win server 2003 – 32 bit nên sẽ cài bản 32 bit. Chạy file setup ta sẽ có hình như sau:

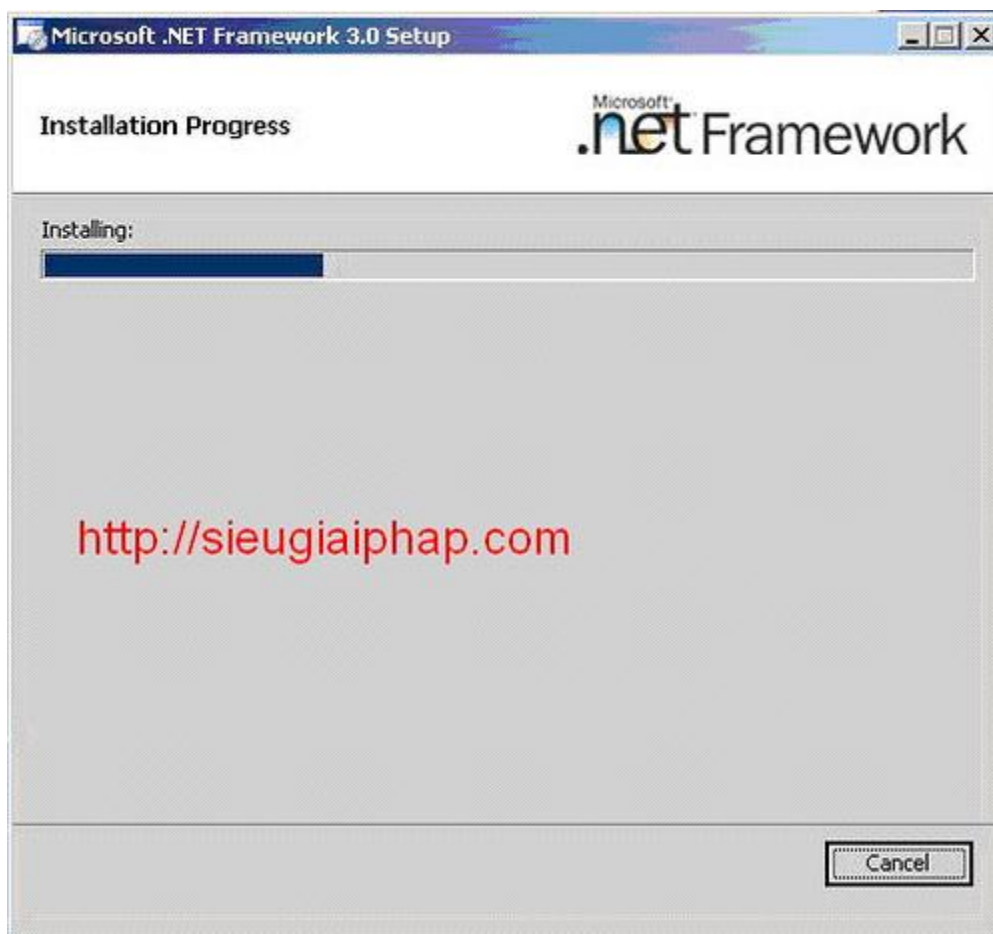


Chọn "I have read and ACCEPT" Và nhấn Install>

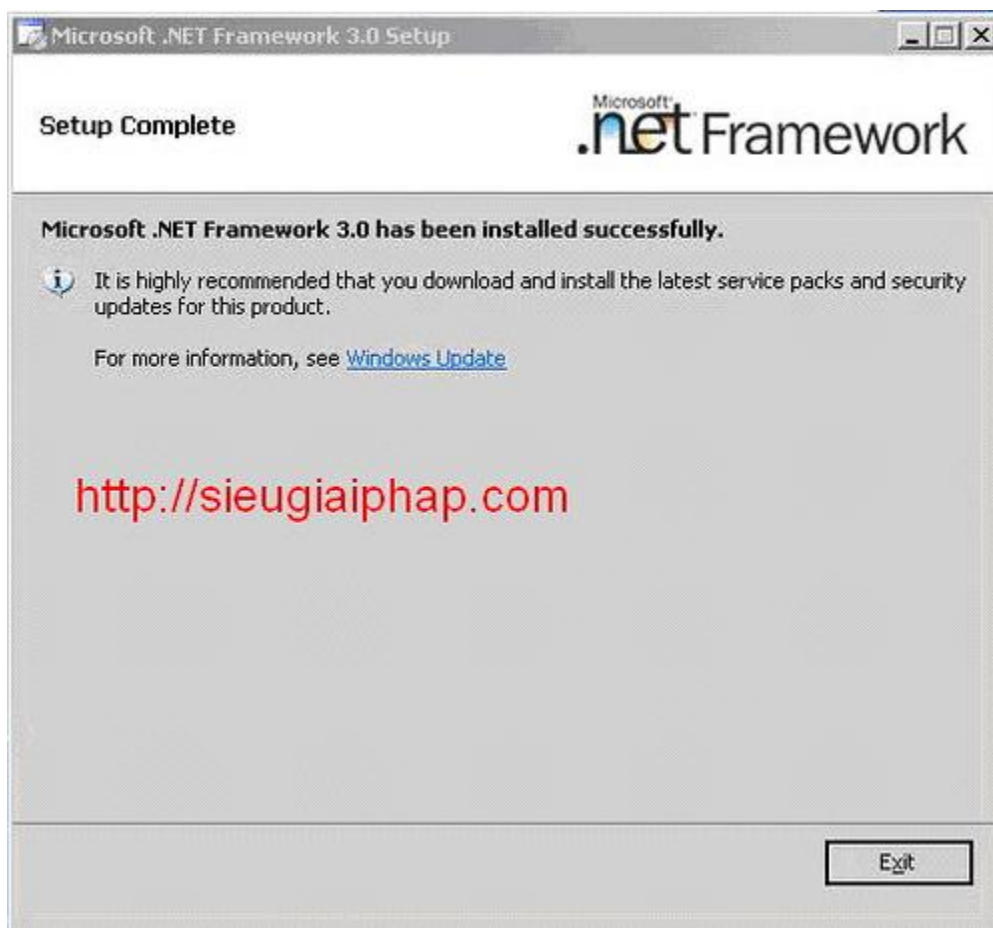
Chương trình cài đặt sẽ chạy ẩn (hide) dưới icon tray...



Double Click vào icon đó để hiện cửa sổ cài đặt .NET Framework

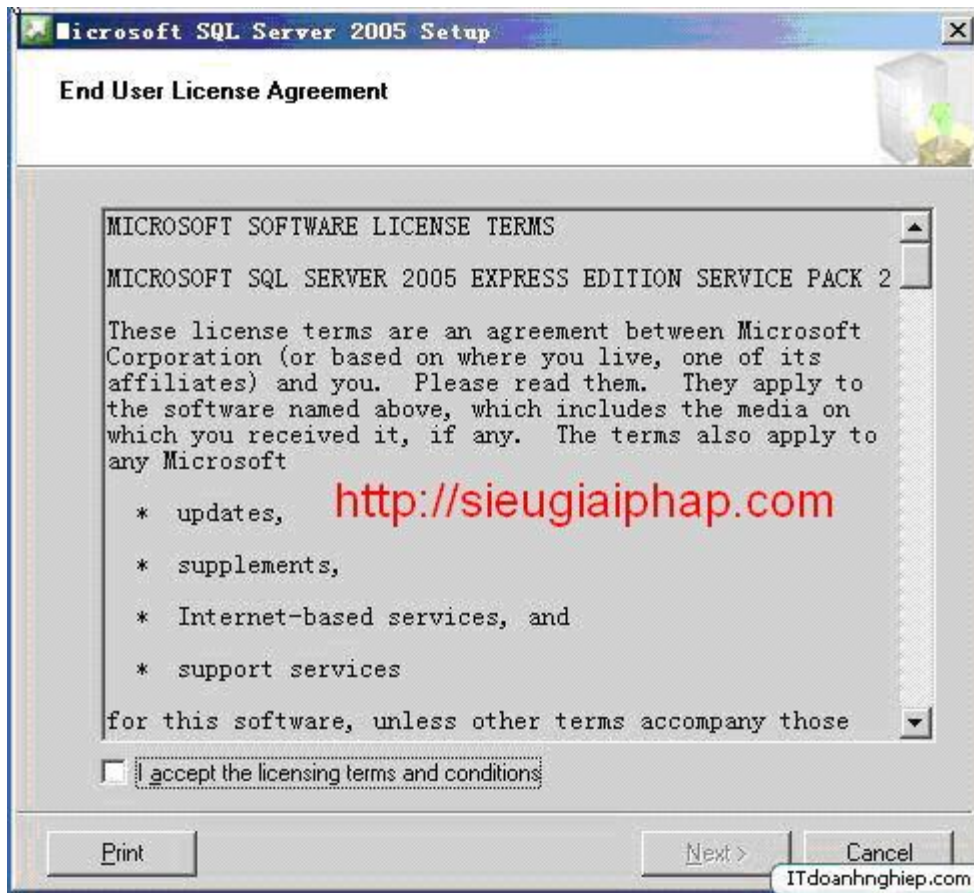


Sau khi cài đặt xong bấm vào Exit để kết thúc cài đặt .NET Framework.

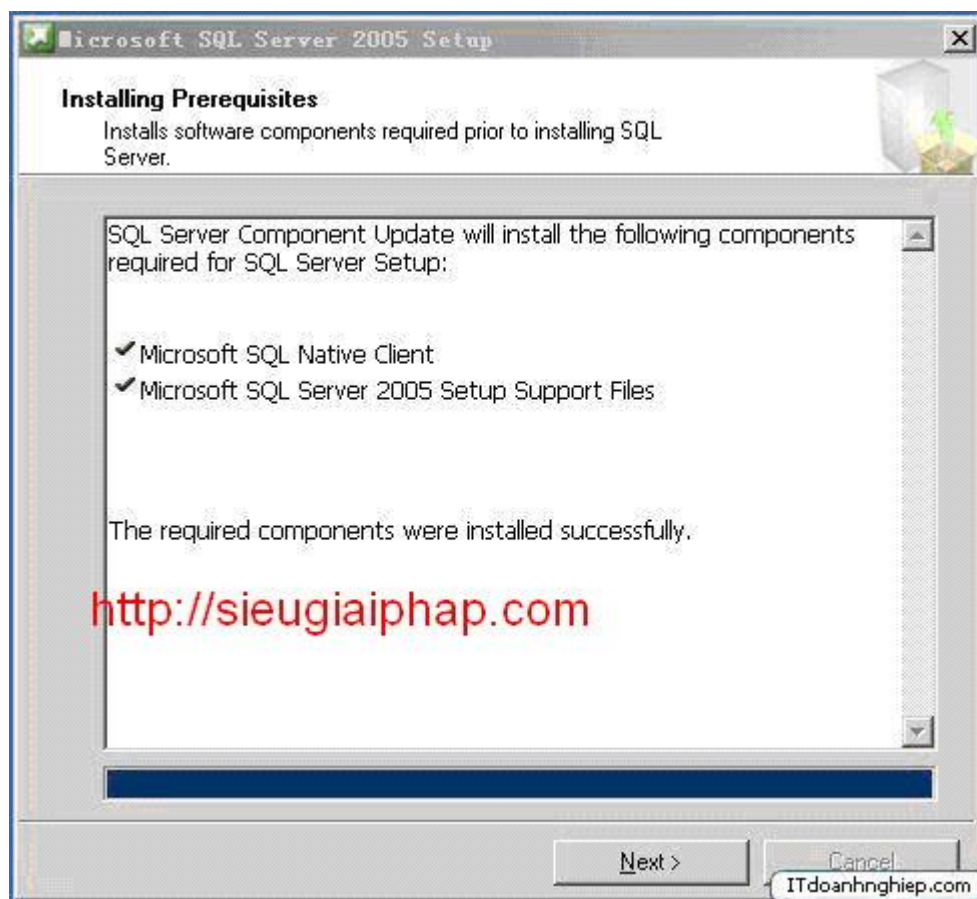


Bước 4: Cài đặt MS-SQLserver 2005 theo các bước sau:

Chú ý cũng có 2 phiên bản cho win 32 bit và 64 bit. Mình cũng lại sử dụng phiên bản cho win 32 bit



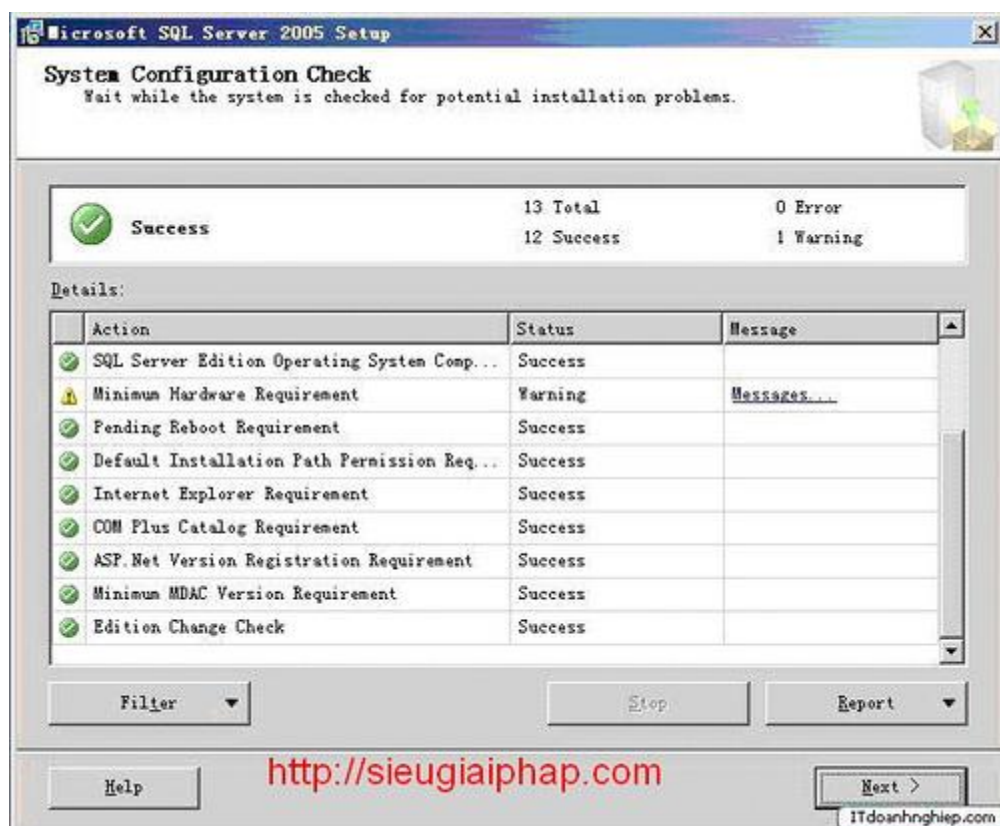
Click vào ô vuông đồng ý và Next>



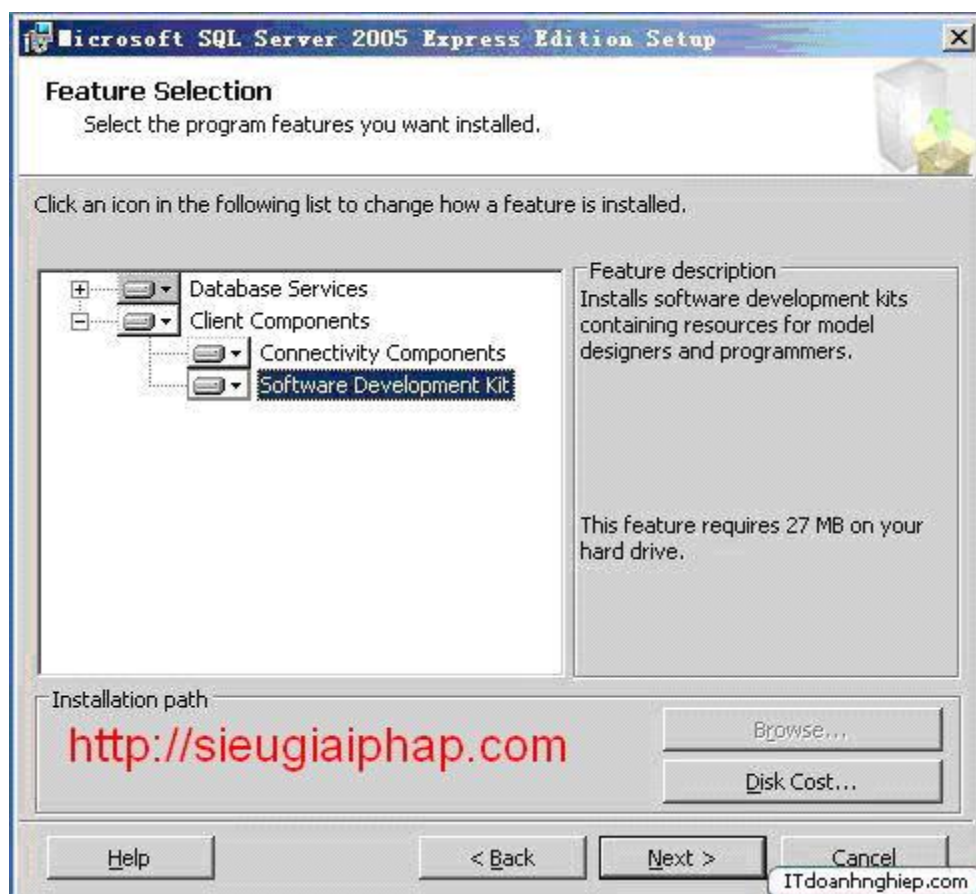
Next>



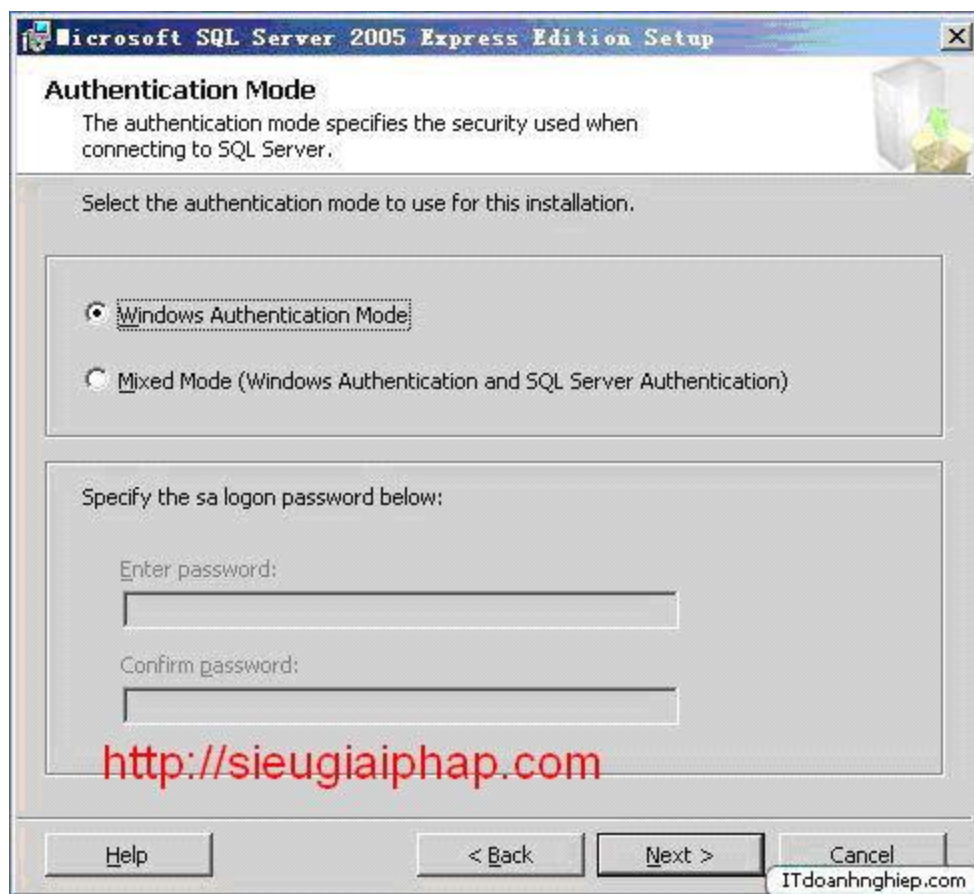
Next>



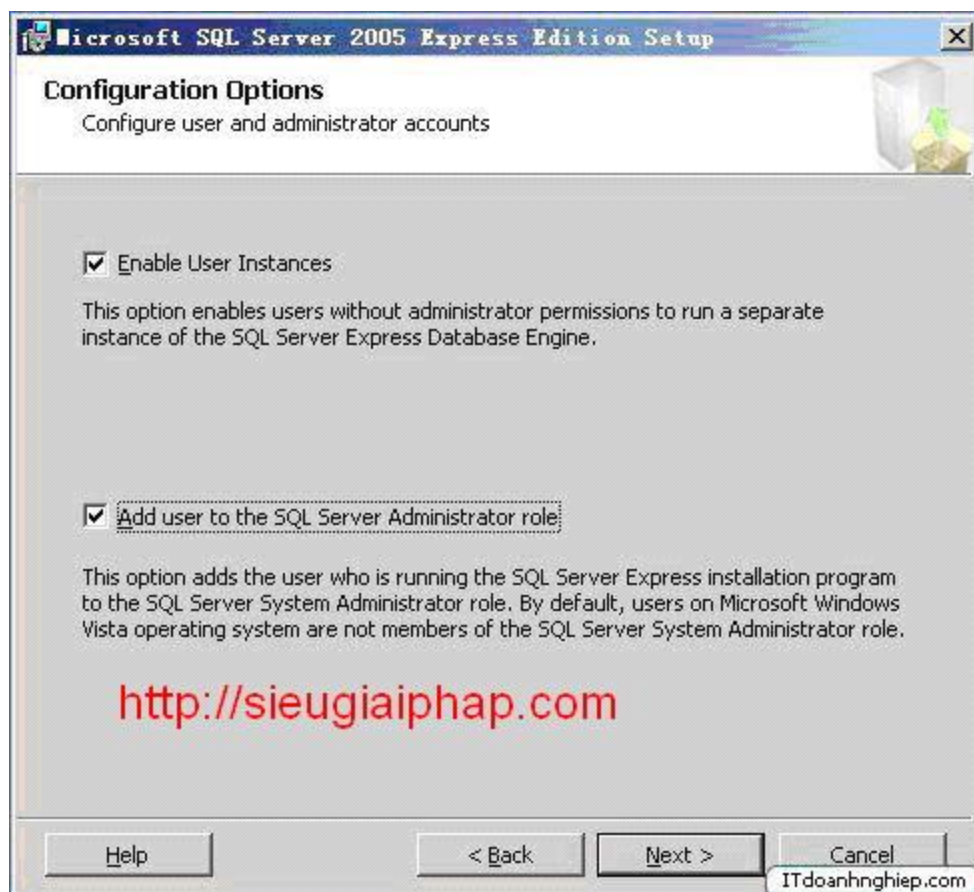
Next>



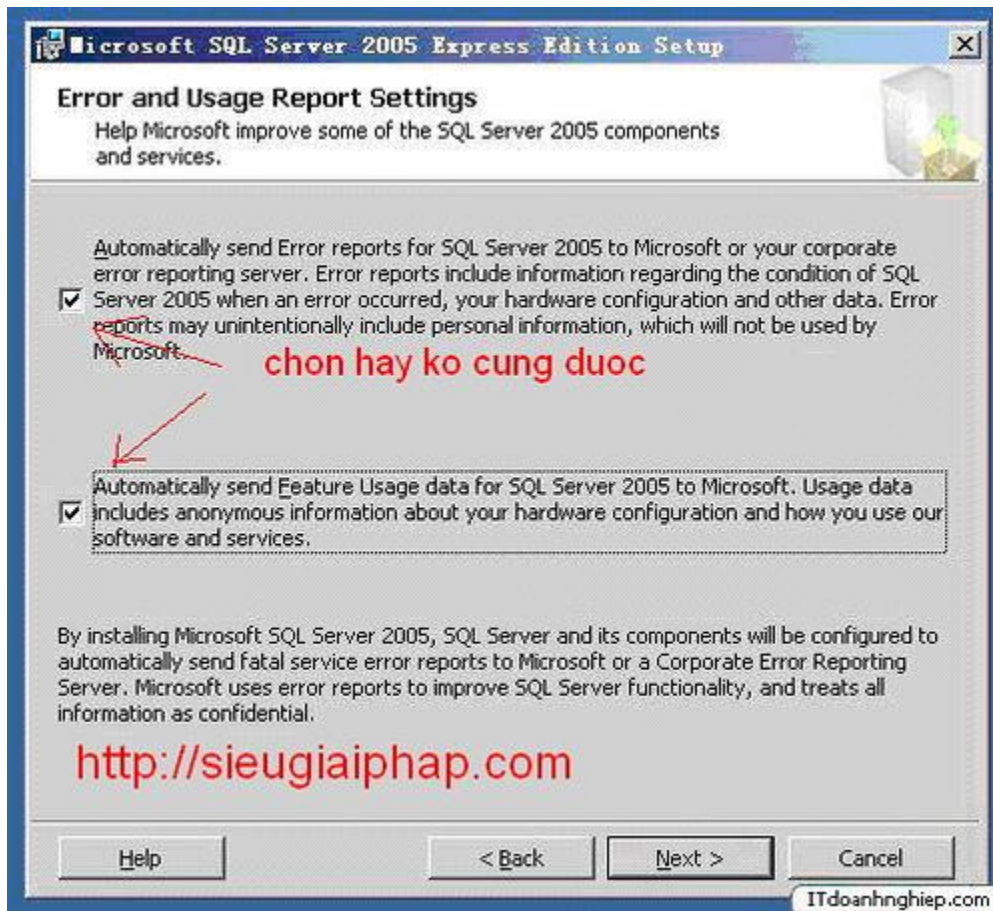
Next> (cài trên HDD)



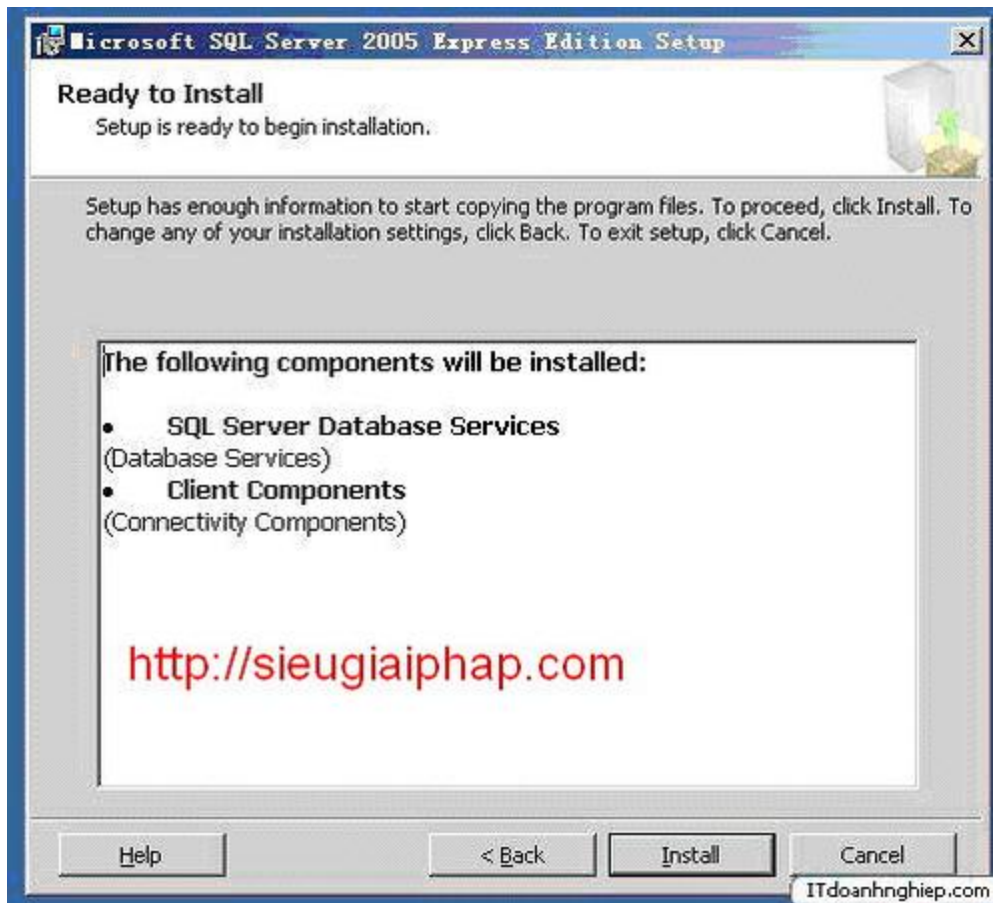
Check vào Windows Authentication Mode và Next>



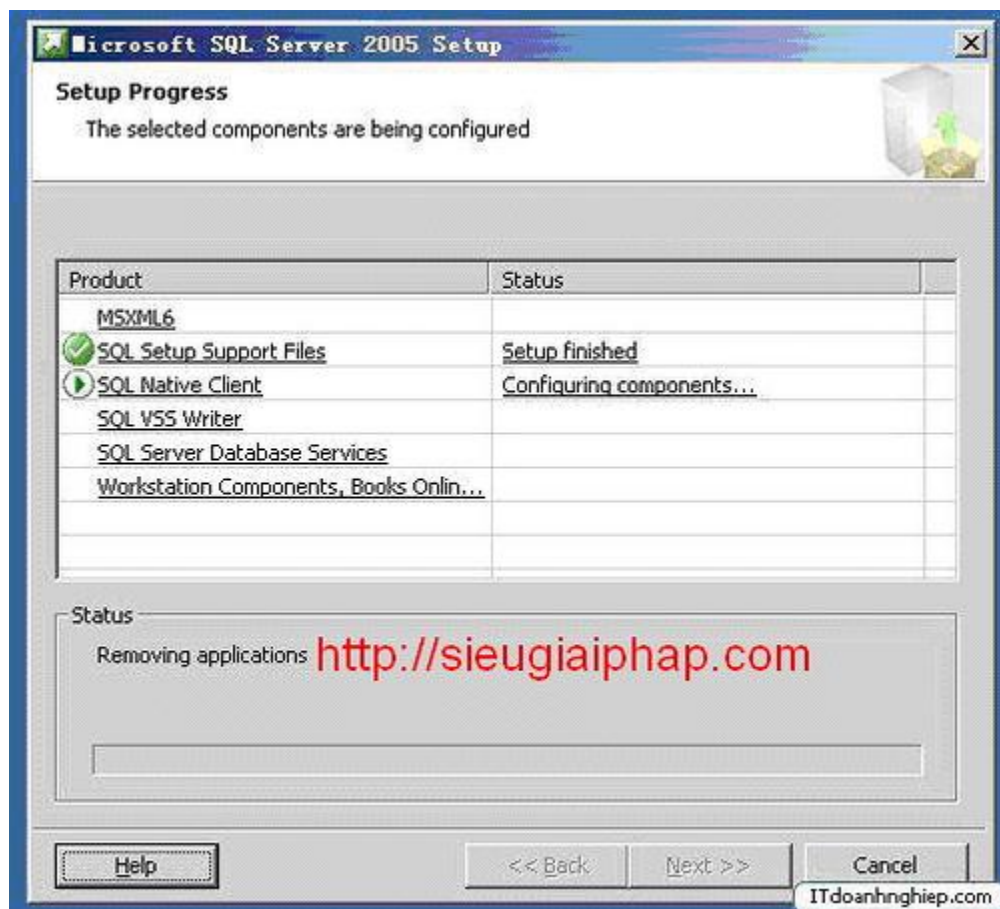
Check Enable User Instances và Add user to the SQL Server Administrator role rồi chọn Next>



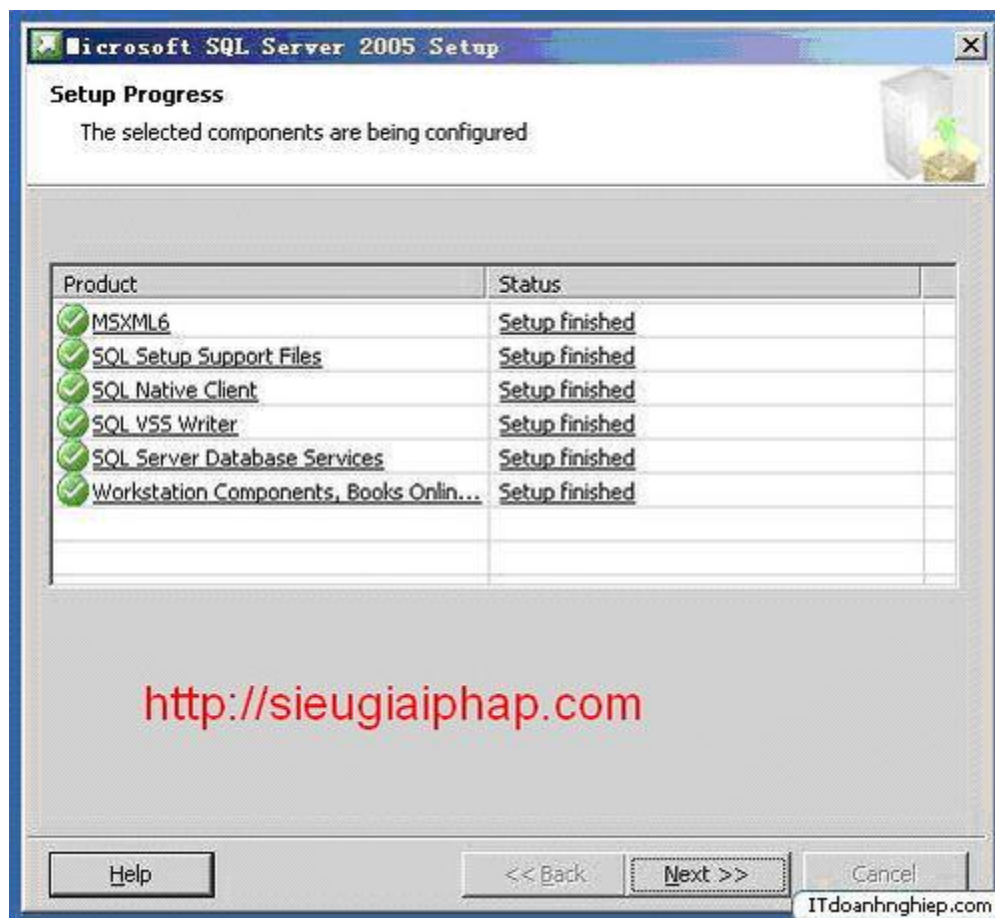
chọn Next>



Chọn Install để chương trình bắt đầu cài ...



Sau khi chương trình cài đặt xong chọn Next>



Và cuối cùng là chọn Finish.

Bước 5: Cách Download Citrix Provisioning Server BXP 5.0.2

Download software BXP 5.x từ <http://citrix.com>

Đăng ký 1 tài khoản.



Home > My Citrix > New Users

My Citrix

Username:

Password:

Log In

[Forgot Your Password](#)

[New Users](#)

[More Options](#)

<http://sieugiaiphap.com>

Create a new My Citrix account

My Citrix Registration 1 of 2

*Required information is preceded by an asterisk.

Preferred Language

* Email Address

* First Name

* Last Name

* Company

* Address

* Country

* State or Province

* City

ZIP/Postal Code

Phone country Code

* Phone

(Area code) (Phone number)

Continue

Điền thông tin xong thì Click vào đây

Important
Please verify if your company account, before you submit.
Find your company account
Attention Citrix Partner
Please call your Business MyCitrix account.
Find your Business Center

Create a new My Citrix account

My Citrix Registration 2 of 2

<http://sieugiaiphap.com>

Chú ý:

Tên tài khoản nhiều hơn 6 ký tự

Mật khẩu nhiều hơn 8 ký tự và phải bao gồm ít nhất 2 trong 3 trường hợp sau:

Có 1 con số,

Có 1 chữ viết hoa,

Có 1 ký tự đặc biệt.

Ví dụ: SIEUGIAIPHAP123

*Required information is preceded by an asterisk.

* Login ID:

* Password:

* Confirm Password:

Please enter your preferred login ID and password and click the submit button to complete your registration. Your login ID must have at least 6 characters and your password must be (8) or more characters in length and meet at least two of the following criteria:

- contain at least one (1) digit
- contain at least one (1) UPPERCASE letter
- include at least one (1) of these symbols: ! @ # \$ % ^ * ? + = -

Continue

Điền xong thông tin thì Click vào đây

bui quang duoc >> ID: 49983924
My Profile

My Tools

Access your applications and utilities from anywhere in My Citrix.

Choose a Toolbox ▶

My Citrix

► Useful Links & Resources
Reference Desk

<http://sieugiaiphap.com>

Vay la ban da dang ky xong va website tu dong dang nhap.

Hay chon software ma minh muon download.

Vi du:phan mem Bootrom
Citrix Provisioning Services

Citrix Receiver for iPhone

Thousands of Windows apps in the palm of your hand. [LEARN MORE](#)

Featuring: Download the Citrix Essentials for Hyper-V

Reference Desk [Show only last 30 days](#)

Find a Resource

Find everything you need in one simple place:

Resources by product

Choose a product

Choose a product
-- Access Gateway
-- Branch Repeater (WANScaler)
-- Essentials for Hyper-V
-- GoToAssist
-- GoToMeeting
-- GoToMyPC
-- GoToWebinar
-- NetScaler
-- Receiver
-- XenApp
-- XenDesktop
-- XenServer
Application Firewall
Citrix Cloud Center
Citrix Delivery Center
Citrix Provisioning Services
Command Center
EasyCall
EdgeSight

Literature

[Show Details](#)

2/29/2008 Citrix Provisioning Server for Datacenters 4.5
2/28/2008 Citrix Provisioning Server for Datacenters 4.5 Product Overview Brochure
1/1/2008 Citrix Provisioning Server Fact Sheet
1/1/2008 Citrix Provisioning Server Customer Story: Amstelveen
1/1/2008 Installing Citrix Pres. Server Inside a Provisioning Server for BCenter vDisk

More ▶

<http://sieugiaiphap.com>

Software Downloads

[Show](#)

6/8/2009 Provisioning Services 5.1
8/19/2008 Provisioning Services 5.0
4/28/2008 Provisioning Server 4.5 Hotfixes

Vay con cho gi nua ma ko
download cai minh can. ^^
Tai lieu hay software.....

White Papers

[Show Details](#)

2/2/2008 Citrix Provisioning Server for Datacenters Freeze.com Real World Solutions
2/1/2008 Del. a Highly Available Prov. Server Using Leading Edge Shared Storage Tech.
2/1/2008 Delivering Citrix Provisioning Server in an 802.1x Secure Network

Bước 6: Cài đặt Citrix Provisioning Server BXP 5.0.1.a - Phần mềm Bootrom

Chạy file PVSSRV_server để cài đặt:



Next>



Next>



Install



Finish cài đặt xong BXP5.01a...



Tiếp theo phần cài đặt BXP5.01a có 1 bản thông báo cấu hình server sẽ xuất hiện chúng ta sẽ cấu hình như sau :



Chọn Next >

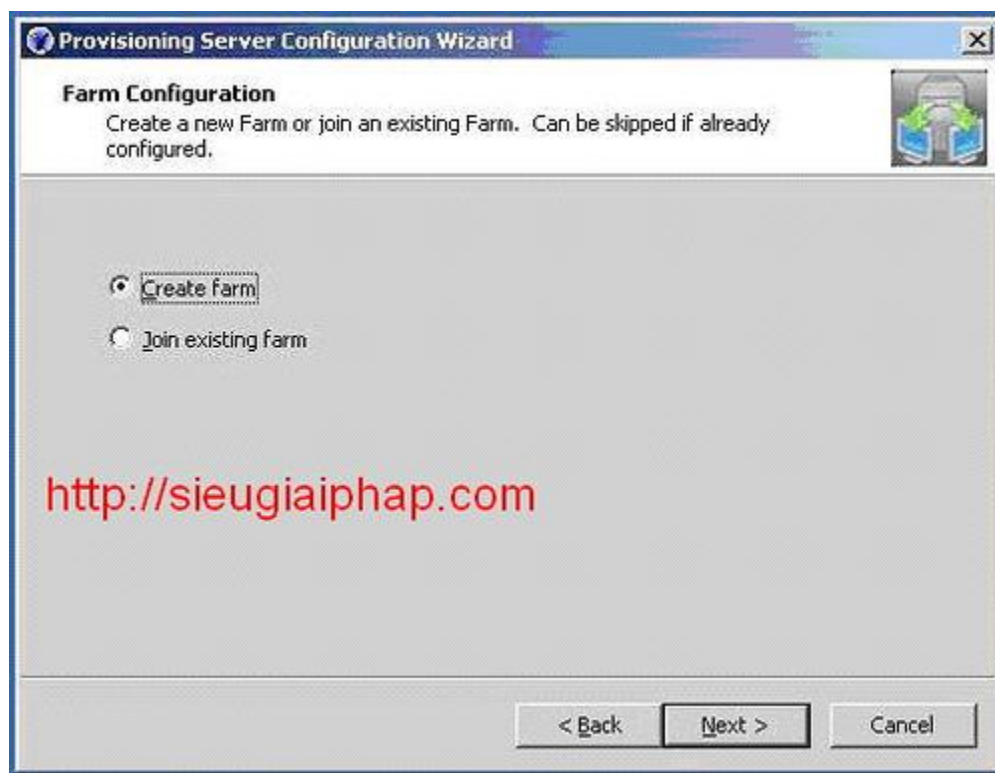


Check như trong hình rồi chọn Next >



Chọn dòng thứ 2 - Provisioning Server PXE Service

Next>



Next>

Provisioning Server Configuration Wizard

Database Server
Enter the Server and Instance names.

Server name:

Instance name:

Note: Leaving this blank indicates the default instance.
Default SQL Server Express instance name is 'SQLExpress'.

<http://sieugiaiphap.com>

< Back Next > Cancel

Click Browse để chọn server SQL như đã cài đặt ở trên rồi chọn Next >

Provisioning Server Configuration Wizard

New Farm
Enter the new Database and Farm names.

Database name:

Farm name:

Site name:

Collection name:

☐ Use Active Directory groups for security

☒ Use Windows groups for security

Farm Administrator group:

<http://sieugiaiphap.com>

< Back Next > Cancel

Điền thông tin cơ sở dữ liệu hoặc giữ mặc định rồi chọn Next >



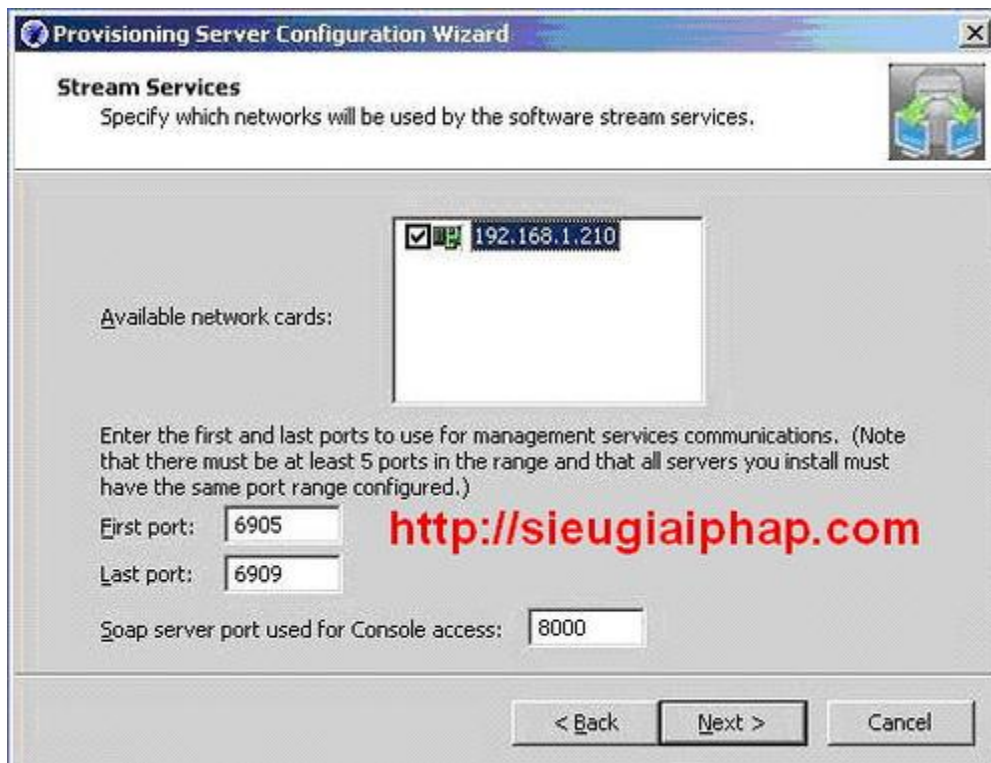
The screenshot shows the 'License Server' step of the 'Provisioning Server Configuration Wizard'. The window title is 'Provisioning Server Configuration Wizard'. The subtitle is 'License Server' with the instruction 'Enter the license server hostname and port.' Below this, there are two text input fields: 'License server name:' with the value 'SERVER' and 'License server port:' with the value '27000'. A checkbox labeled 'Use Datacenter licenses for desktops if no Desktop licenses are available' is checked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A large red watermark 'http://sieugiaiphap.com' is overlaid on the center of the window.

Không bận tâm và Next >

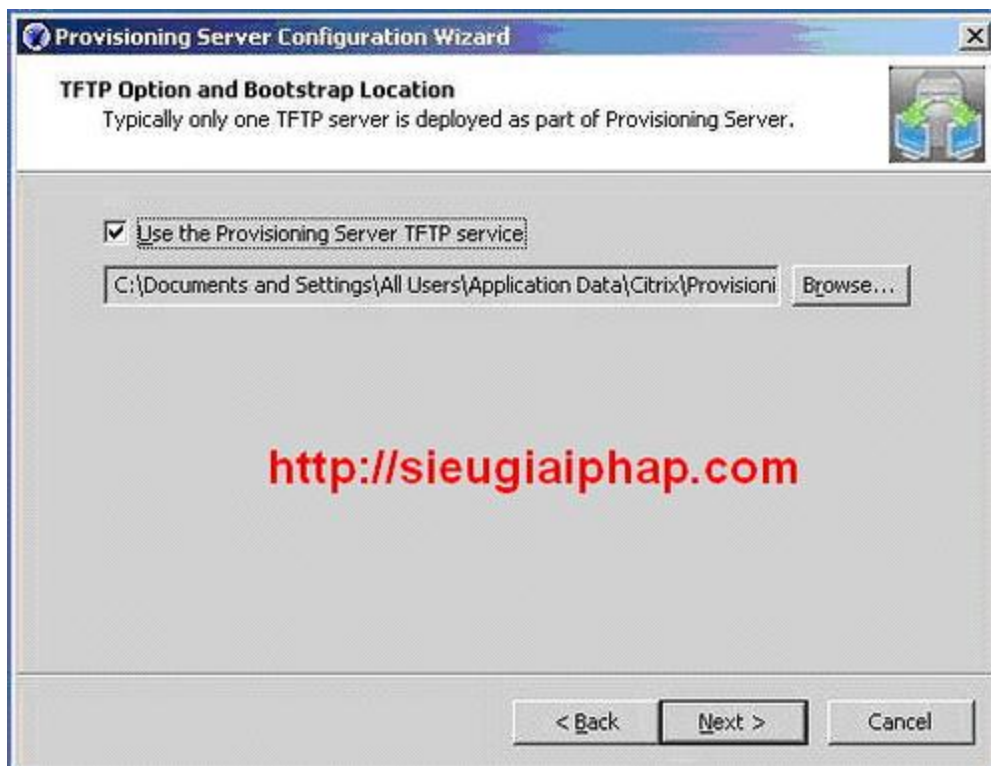


The screenshot shows the 'User account' step of the 'Provisioning Server Configuration Wizard'. The window title is 'Provisioning Server Configuration Wizard'. The subtitle is 'User account' with the instruction 'The Stream and Soap Services will run under a user account. Please select what user account you will use.' Below this, there are two radio button options: 'Network service account' and 'Specified user account (Required when using a Windows Share)'. The 'Specified user account' option is selected. Below these options are four text input fields: 'User name:', 'Domain:', 'Password:', and 'Confirm password:'. A large red watermark 'http://sieugiaiphap.com' is overlaid on the center of the window. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

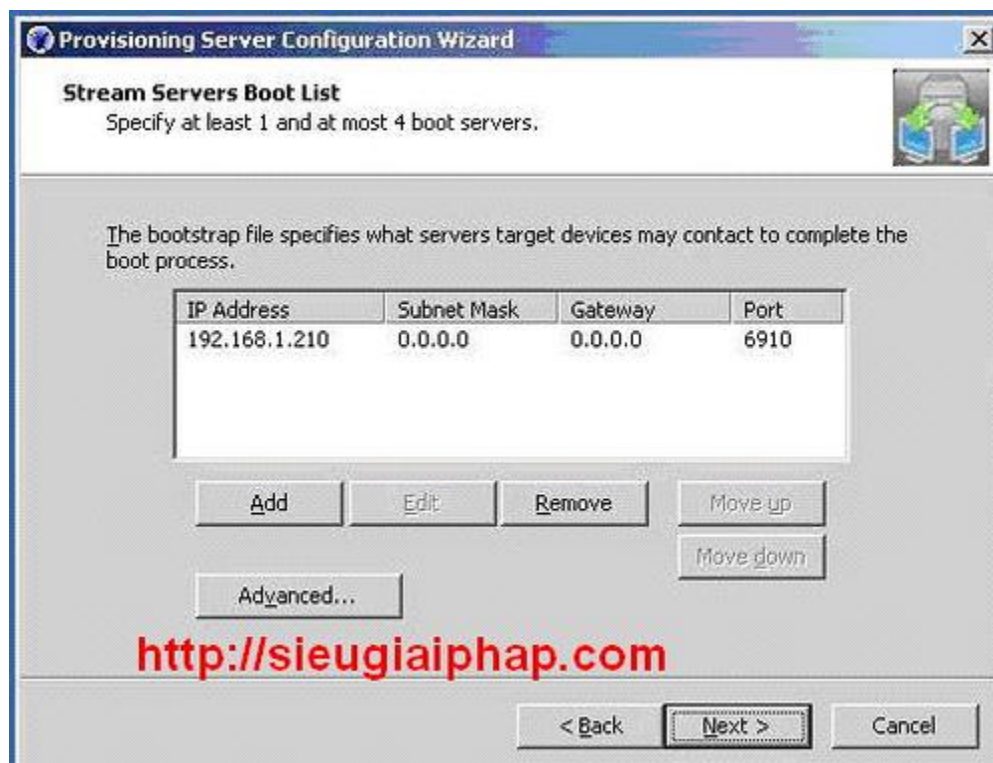
Chọn như hình vẽ và Next >



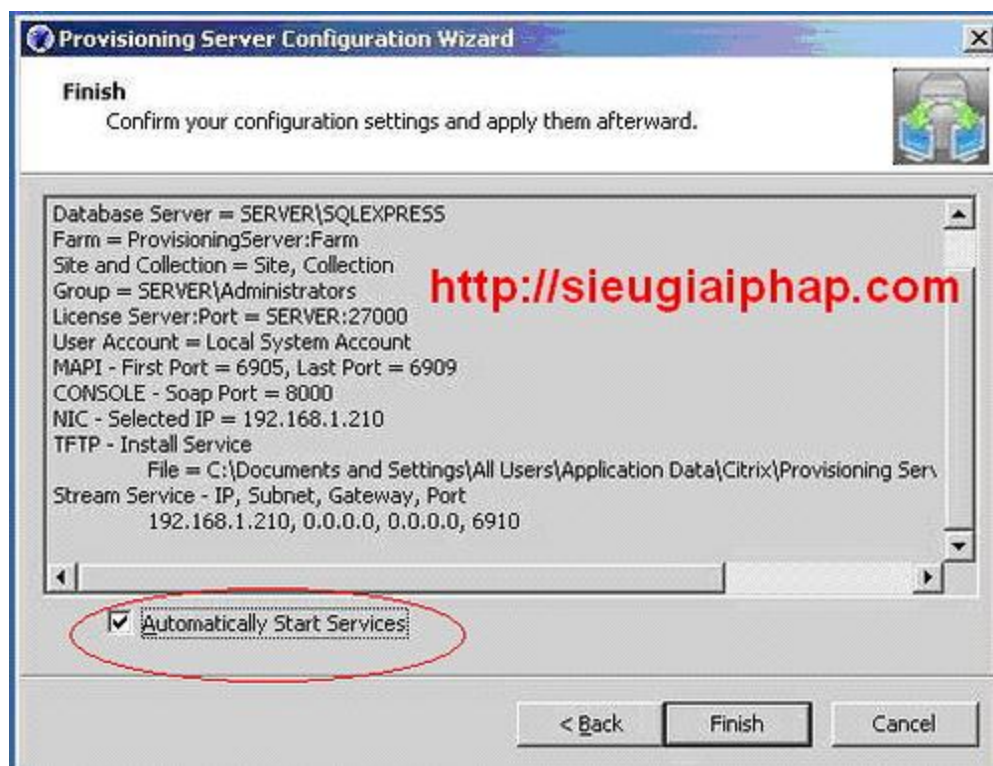
Phần này là phần chọn Card LAN dùng làm card để Bootrom cho Client, Chọn xong thì rồi Next >



Như hình vẽ và Next>



Không có gì cần chỉnh sửa thì Next >



Finish để chương trình sẽ tự động load services...



Nhấn Done.

Vậy là chúng ta đã cấu hình xong phần Server

A/ Phần tạo ảnh để client nhận HDD ảo (thiết lập vdisk)

Sau khi cài đặt xong Citrix BXP server + cấu hình phần NIC LAN làm boot rom, chúng ta sẽ chạy Provisioning Server.

1/ Tạo STORE - nơi chứa file Image (file ảnh hay còn gọi là vDisk, chứa client)

Nếu bạn có nhiều cấu hình máy khác nhau thì phải tạo số lượng STORE cũng như vDisk tương ứng.

2/ Tạo vDisk - như 1 vùng chứa toàn bộ Client.(vDisk này có thể nói cho dễ hiểu như phân vùng HDD chứa file ghost của client - bạn nào ko thích hay phản đối thì tùy, miễn bình luận)

Và Format vDisk.

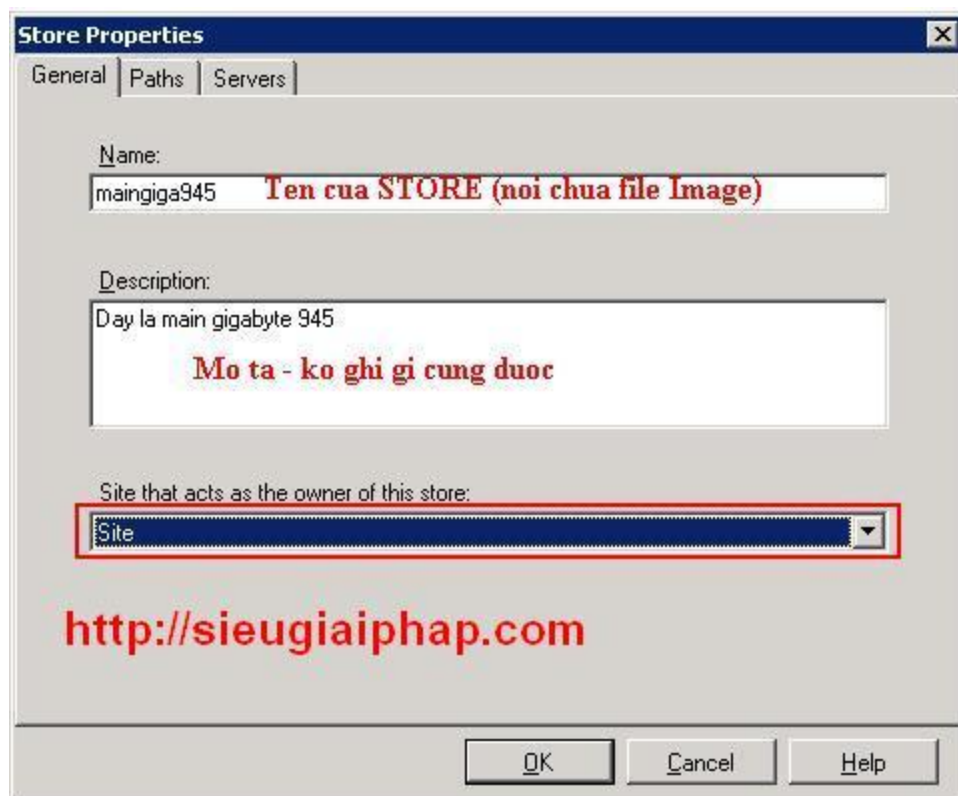
Chú ý: Khi bạn tạo vDisk xong thì window sẽ nhận CÁC vDisk này như 1 ổ Removable Disk - dĩ nhiên trong Windows Explorer sẽ xuất hiện thêm ổ này. Đừng có dại dột xóa nó hoặc tắt nó nha, bạn sẽ phải trả giá cho việc này đó.

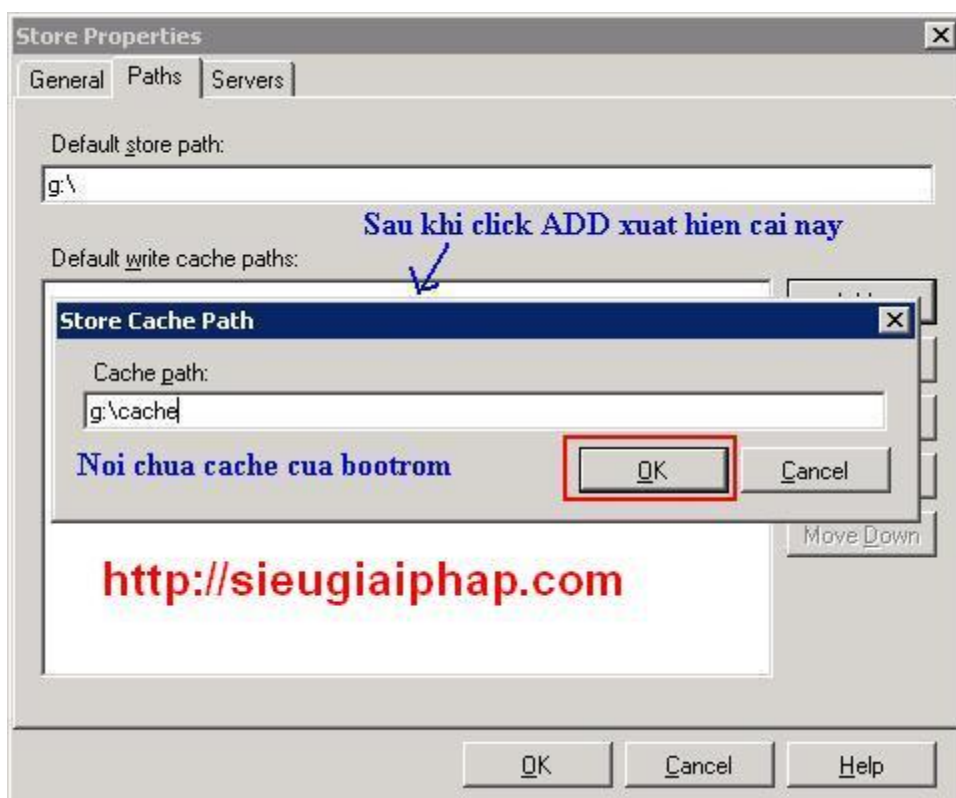
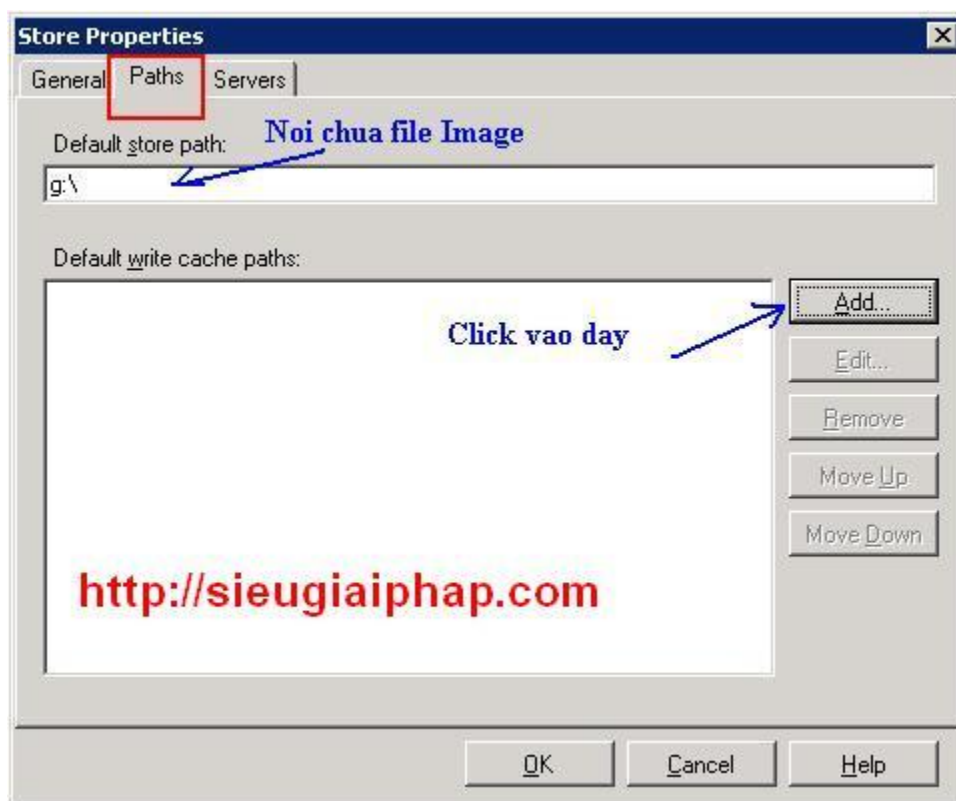
Back up vDisk phòng trường hợp HDD bị bad, còn có cái để mở cửa kinh doanh.

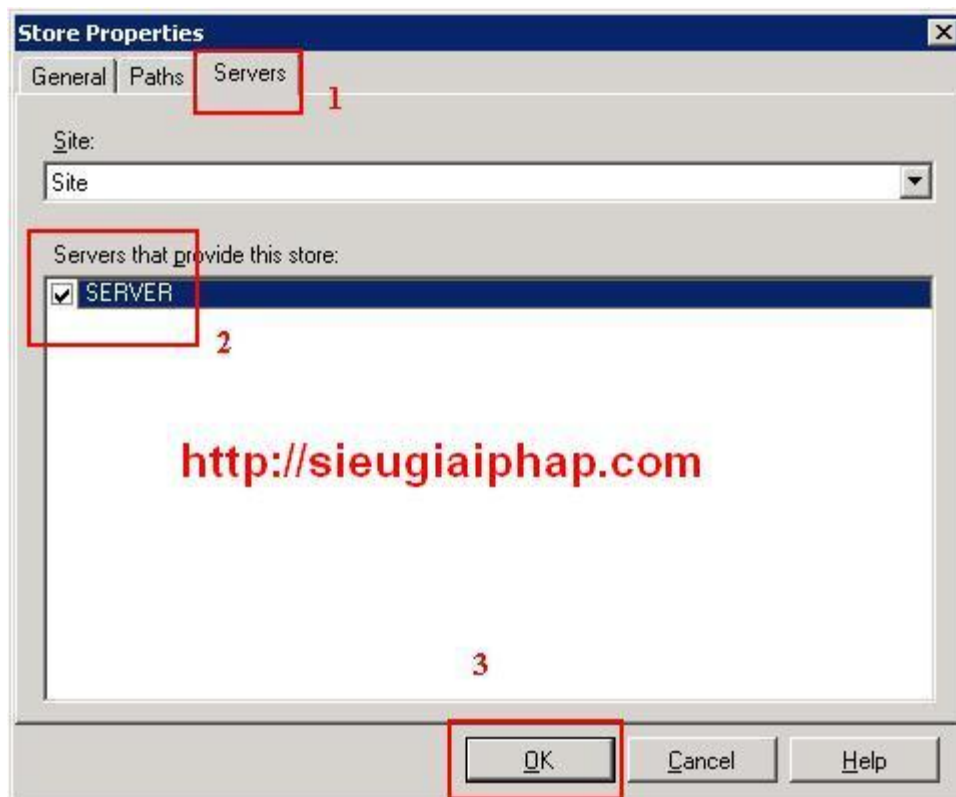
3/ Add Client vào Citrix Provisioning Server.

4/ Tìm hiểu các thuộc tính của Client và vDisk. Chuẩn bị cho Client build image.

Nào Let 's Go.











Trong trường hợp bạn đã có sẵn file vDisk thì không cần tạo mới. Khi đó chỉ cần tạo STORE và gán vDisk vào. Chúng ta làm như sau:





http://sieugiaiphap.com

Name	Store	Connections	Size	Mode	Class
☒ 915	915	0	6997 MB	Cache on Server	
☒ 945	945	0	6997 MB	Cache on Server	
☒ 9451g	9451g	0	6997 MB	Cache on Server	

Mình có 3 cấu hình nên đã tạo 3 Store để chứa 3 Image - Đây là 3 Vdisk đã được tạo

Để Format vDisk thì chúng ta phải Mount Disk. Và sau đó dùng Windows Explorer format ổ Removable Disk bình thường. (COI CHÚNG FORMAT NHẸM CÁI Ổ USB)

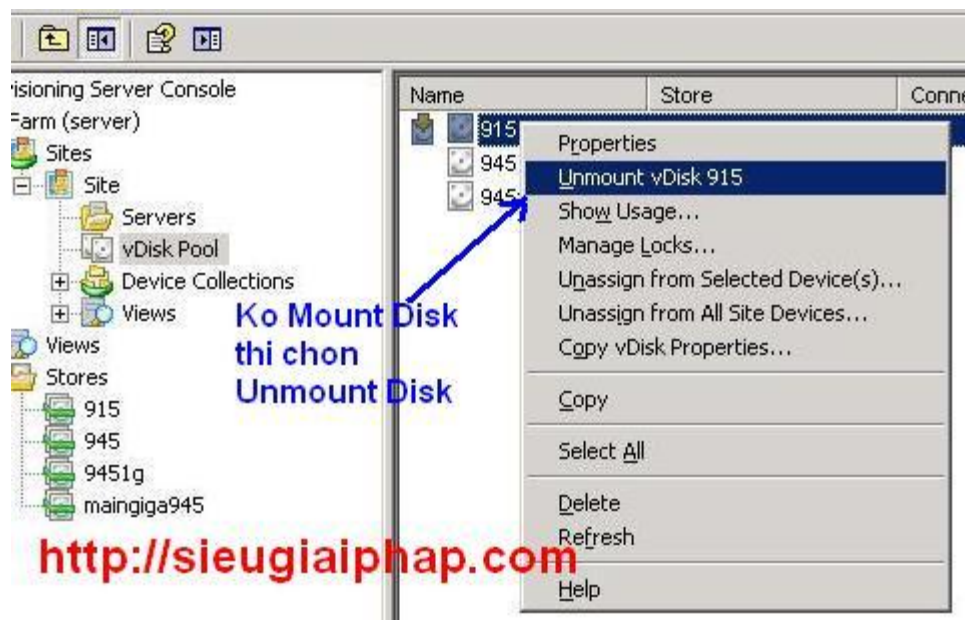
Chú ý: Trong quá trình Build Image, để Client nhận ra được vDisk thì vDisk phải được format trước.



Sau khi MOUNT DISK ta có hình sau



Không MOUNT DISK nữa thì làm như sau



Như vậy đến đây ta đã tạo được các Store và vDisk.

Mỗi vDisk được tạo sẽ có 3 file chứa trong HDD, nhưng ta chỉ cần copy 2 file như hình vẽ là có thể lưu trữ file Image cho client phòng trường hợp HDD bad.

915.lok	1 KB	LOK File	6/23/2009 9:44 AM	A
915.pvp	517 KB	PVP File	6/9/2009 2:30 AM	A
915.vhd	7,168,001 KB	VHD File	6/23/2009 7:68 AM	A
945.lok	1 KB	LOK File	6/23/2009 8:40 AM	A
945.pvp	517 KB	PVP File	6/9/2009 2:35 AM	A
945.vhd	7,168,001 KB	VHD File	6/9/2009 2:37 AM	A
9451g.lok	1 KB	LOK File	6/23/2009 8:29 AM	A
9451g.pvp	517 KB	PVP File	6/9/2009 2:33 AM	A
9451g.vhd	7,168,001 KB	VHD File	6/23/2009 3:01 AM	A

Muốn backup vDisk thì copy 2 file này save cho khác

Muốn gán vDisk cho Store thì làm như trên đã hướng dẫn

<http://sieugiaiphap.com>

B/Cài đặt PVSSRV_device cho máy Client kết nối với server

Tiếp theo chúng ta sẽ khai báo add client vào server.

Server nhận biết client thông qua địa chỉ MAC card LAN và nó sẽ gán vDisk cho client. Client sẽ nhận data này và boot + hoạt động.

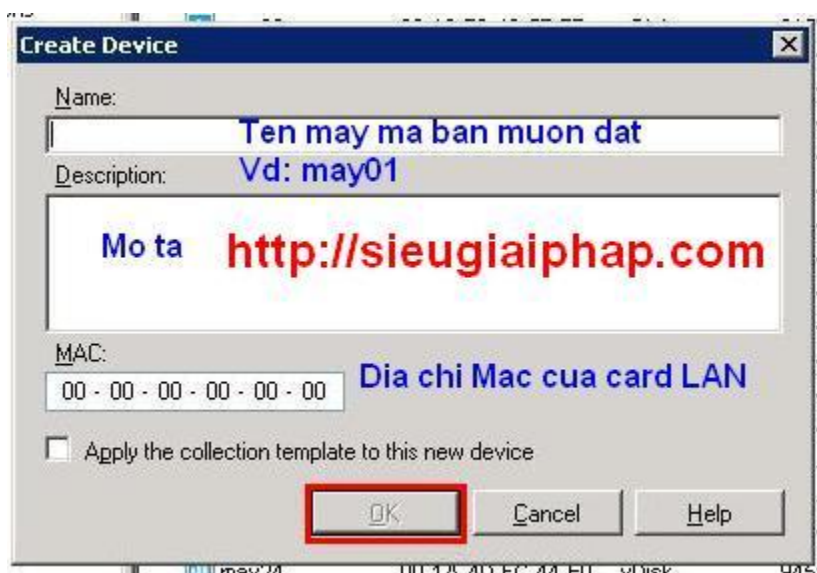
Chú ý: Các main mua cùng 1 lúc, cùng 1 hãng, cùng 1 version chưa chắc card LAN giống nhau. Và như vậy là cấu hình khác nhau đồng nghĩa phải cho nó 1 vDisk khác.

Có 2 cách để khai báo client cho server nhận.

* Cách thủ công, làm từng client 1

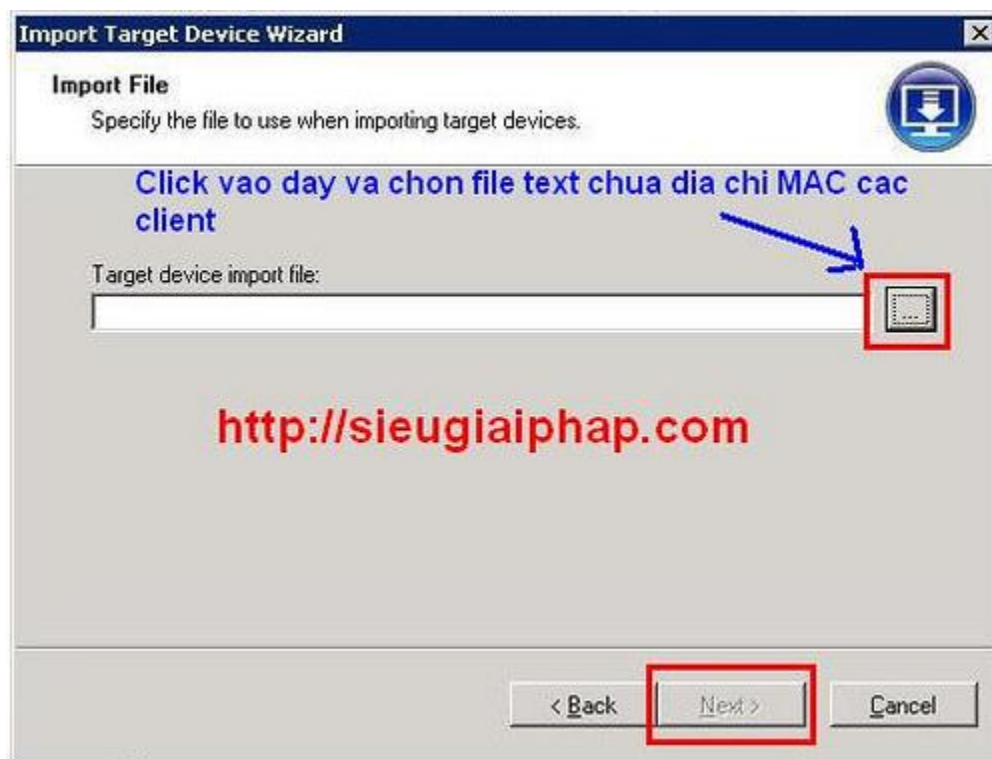
* Cách add hàng loạt, dùng file text chứa địa chỉ MAC của tất cả máy Client. Import vào server.

Cách thủ công



Cách hàng loạt







CẤU HÌNH FILE TEXT CHỨA MAC ĐỂ ADD CLIENT HÀNG LOẠT



Và kết quả là

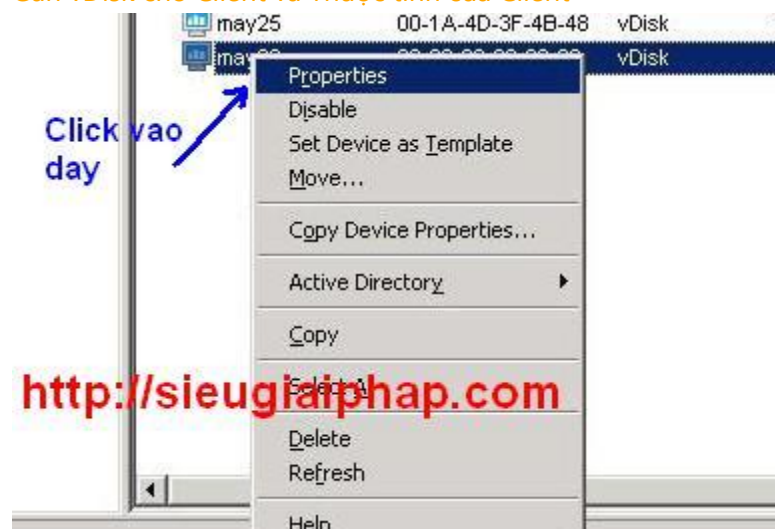


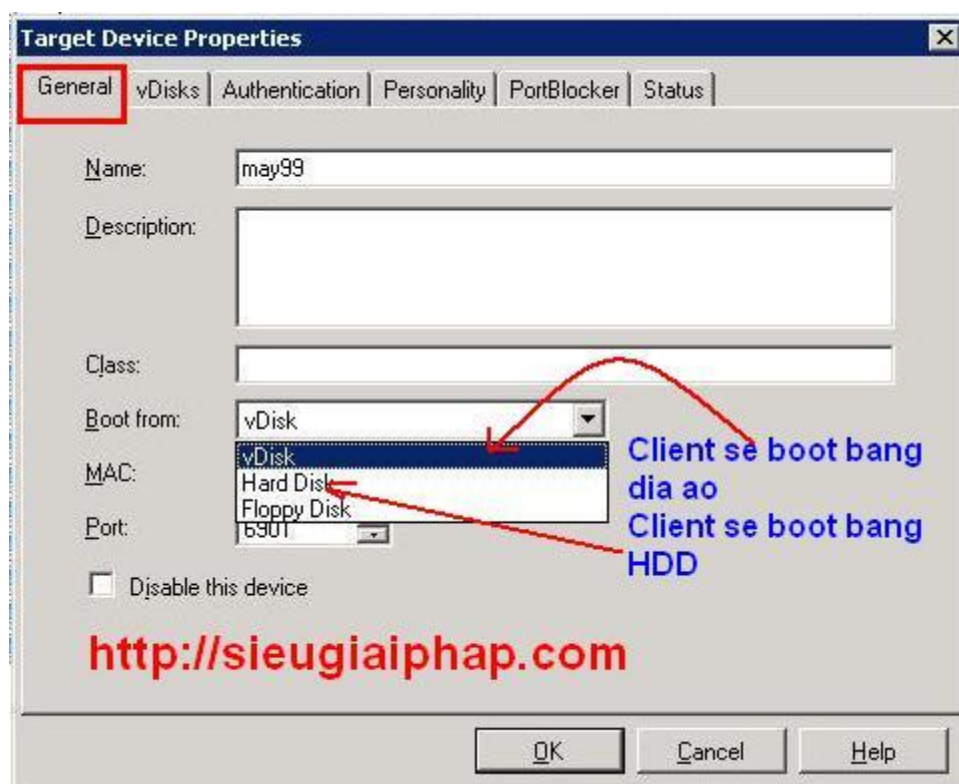
Tìm hiểu thuộc tính của Client, vDisk.

Gán vDisk cho Client có cấu hình tương ứng.

Chuẩn bị cho việc cài đặt Client + tạo file Image (build image)

Gán vDisk cho Client và Thuộc tính của Client

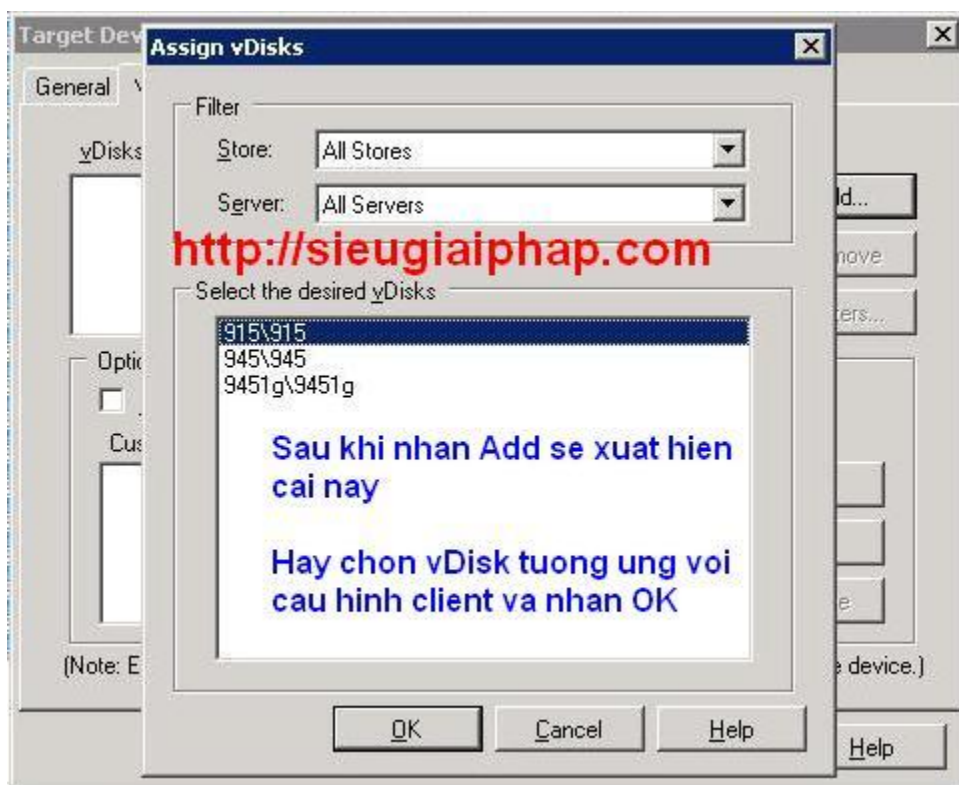
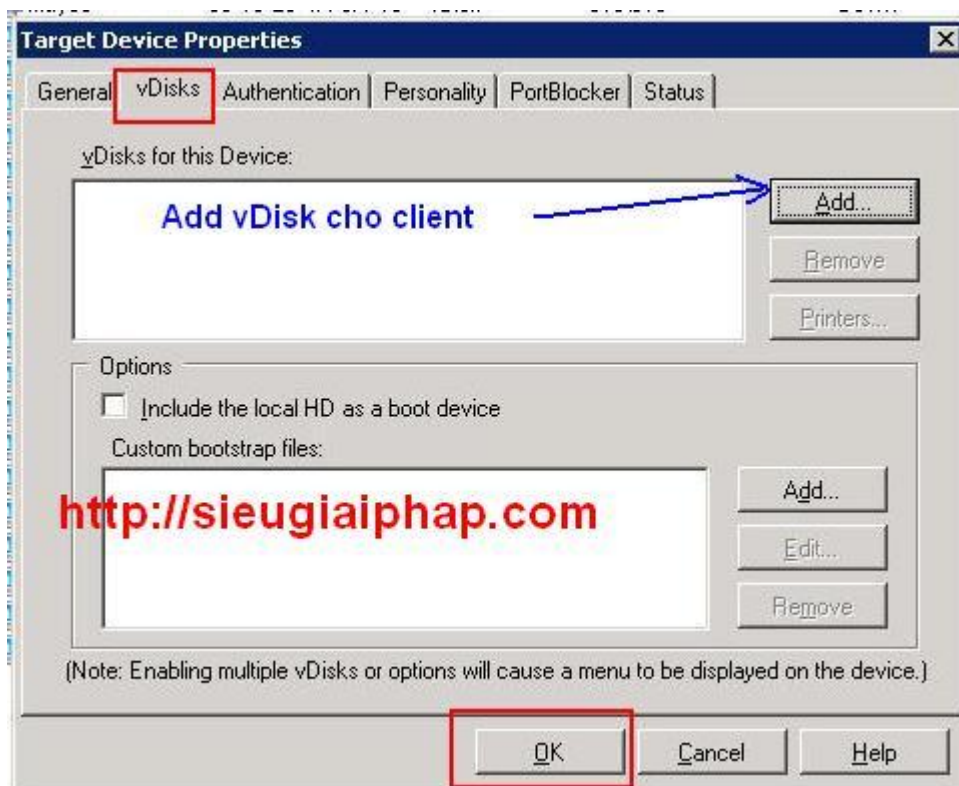


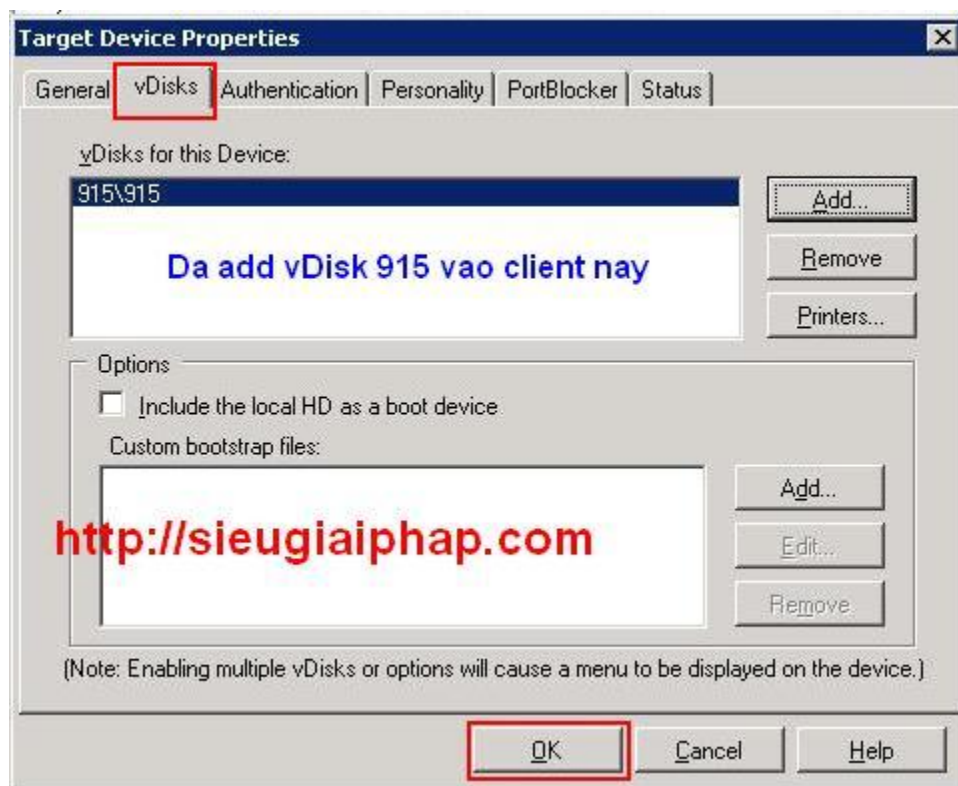


Mục Boot From:

Nếu chọn **vDisk** --> Client sẽ boot bằng image trên server (đây là chế độ boot rom)

Nếu chọn **Hard Disk** --> Client sẽ boot bằng HDD của nó (Đây là chế độ dùng để tạo file image)

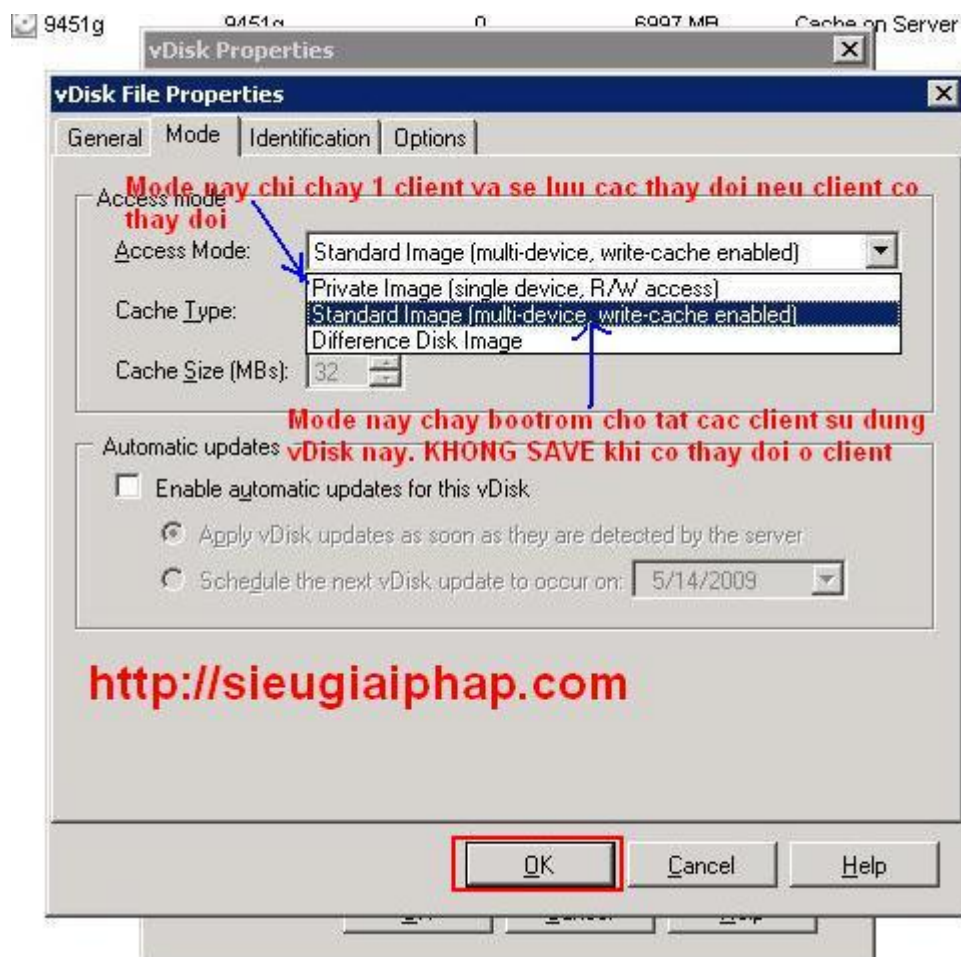




Thuộc tính của vDisk







khi vDisk ở chế độ:

Private Image: Thì chỉ 1 Client boot được. Nếu có thay đổi ở client thì file Image sẽ lưu lại hết. Dùng để chỉnh sửa file ảnh. Khuyến cáo khuya khuya khi không còn ai thì mới sử dụng chế độ này. (giống rã băng)

Standard Image: Đây là chế độ boot rom cho tất cả client sử dụng vDisk này.

Client có chỉnh sửa, copy, xóa, download thì chỉ có hiệu lực trên cache. File image ko bị thay đổi. Reset server thì trở lại như cũ.



ĐẾN LÚC NÀY CHÚNG TA ĐÃ CÀI ĐẶT XONG CÁC PHẦN MỀM CHO SERVER,
CÁC BƯỚC CHUẨN BỊ CHO VIỆC TẠO FILE IMAGE CŨNG XONG.

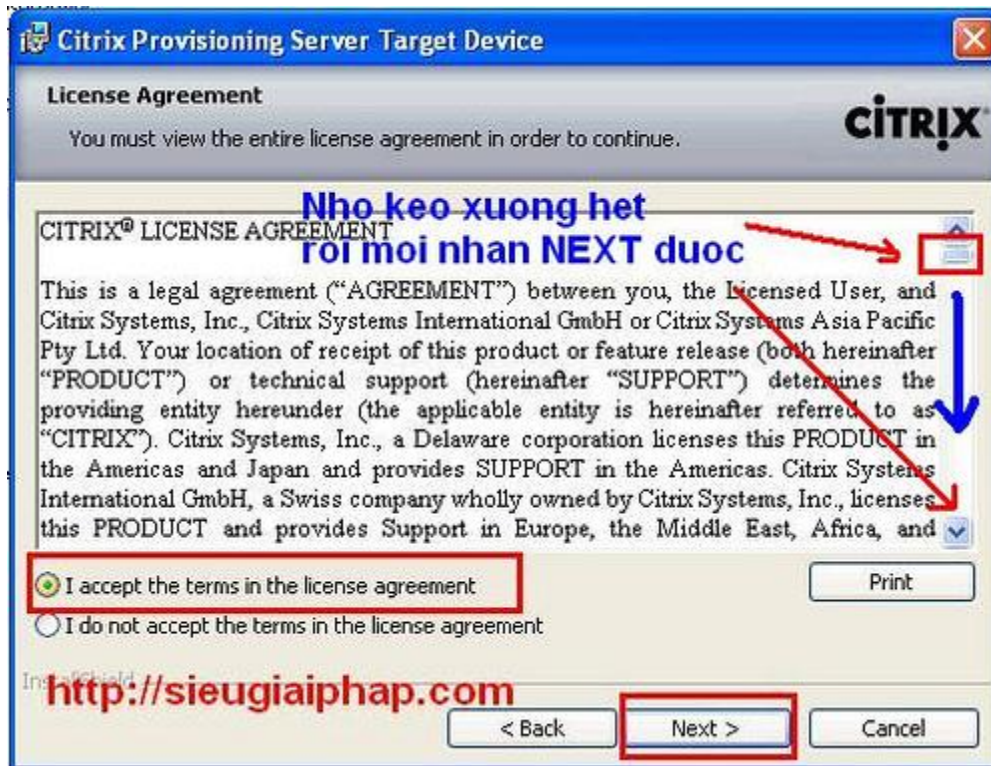
QUẢNG ĐƯỜNG ĐI ĐƯỢC 90% CÒN 10% LÀ
CHỜ CLIENT SETUP PHẦN CLIENT + TẠO FILE IMAGE LÀ HOÀN TẤT 100%

BƯỚC 7: CÀI ĐẶT CLIENT + TẠO FILE IMAGE

Lấy 1 máy client đã cài đầy đủ các phần mềm cần thiết để chuẩn bị làm image cho server. (cái này kỹ thuật ai làm cũng được).

Đầu tiên chạy PVSSRV_device.exe để cài đặt cho máy con phần mềm kết nối với server theo hình ảnh dưới đây:











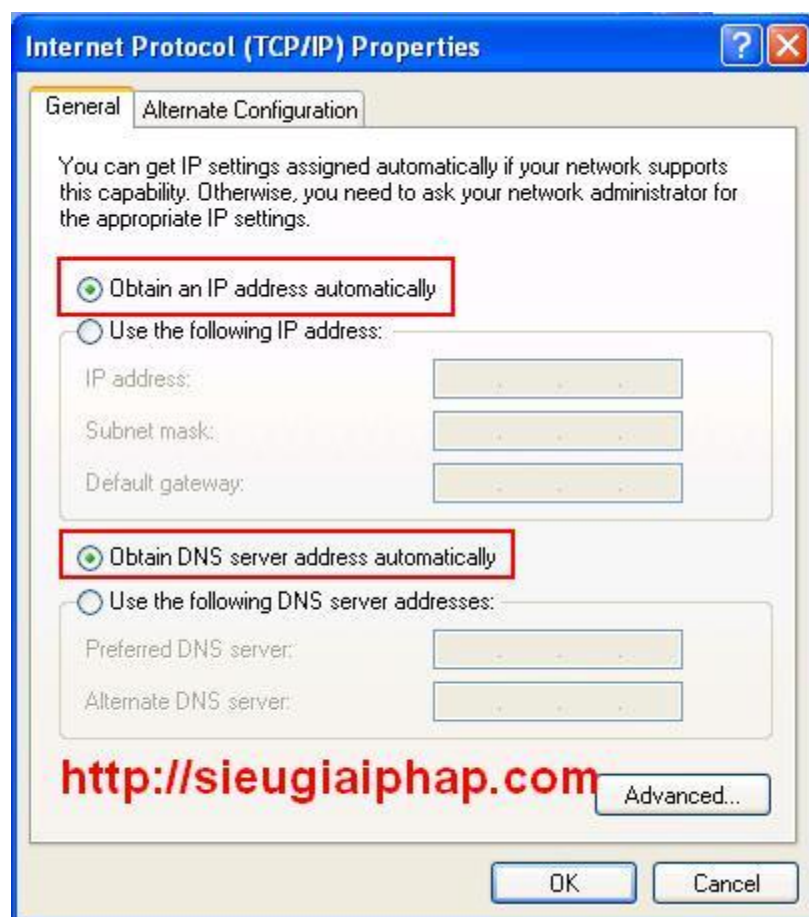
Vì chúng ta chưa cho boot bằng LAN nên biểu tượng kết nối server có dấu X màu đỏ, thông báo chưa kết nối với server.

Để kết nối với server chúng ta cần làm 2 bước sau

Bước 1: Trên máy server cho vDisk của client chuẩn bị kết nối ở chế độ Private Image và client ở chế độ boot bằng Hard Disk (xem phần trước để thực hiện)

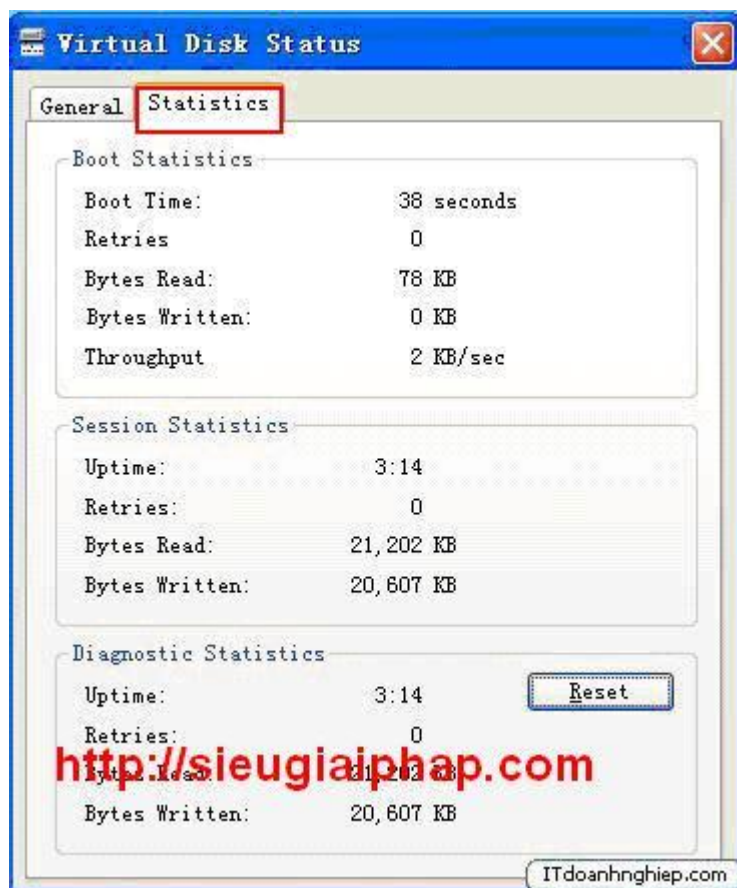
Bước 2: Cắm dây LAN kết nối server với Client. Vào BIOS của Client chỉnh khởi động bằng LAN (first boot = LAN) và chỉnh cho sử dụng chức năng boot LAN (BOOT LAN = Enable). Và khởi động máy client.

Chú ý: Card mạng của client lúc này phải ở chế độ Obtain an IP address automatically



Và như vậy sau khi vào win thì biểu tượng kết nối với server sẽ không còn dấu X màu đỏ. Chứng tỏ đã kết nối với server thành công. Chúng ta Double Click vào biểu tượng này để xem thông tin.





Và khi đó trong máy client sẽ xuất hiện thêm 1 ổ đĩa có dung lượng đúng bằng dung lượng vDisk mà mình đã tạo. (Ví dụ ổ E). Chúng ta cũng có thể format ổ này 1 lần nữa.

Bây giờ đã có thể tạo file ảnh cho server (build image), làm theo hình sau





(khoảng 5 phút tùy dung lượng)

Sau khi báo xong image thì các bạn sẽ làm gì nào??????

Bước 1: Chỉnh vDisk ở chế độ Standard Image hoặc Private Image đều được, Client ở chế độ vDisk (Xem kỹ phần trên)

Bước 2: Tháo HDD của Client. Và khởi động máy. WOW trên cả tuyệt vời. Nhưng nếu ko có license thì sau 5 phút sẽ bị shutdown.

Bài 14: PHẦN MỀM VISIO