



## Cấu hình Windows Server 2008 thành SSL VPN Server truy cập từ xa (Phần 2)

Nguồn : [quantrimang.com](http://quantrimang.com)

*Thomas Shinder*

**Trong phần thứ nhất, chúng tôi đã nói về một số giao thức VPN và máy chủ VPN của Microsoft trước kia. Để tiếp nối những gì đã giới thiệu trong phần một, chúng tôi sẽ đưa ra cho các bạn một mô tả ví dụ mạng sẽ sử dụng trong việc cấu hình gateway VPN để có thể hỗ trợ cho kết nối SSTP từ các máy khách Vista SP1.**

Chúng tôi sẽ không giới thiệu toàn bộ tất cả các bước mà sẽ thừa nhận rằng bạn đã cài đặt DC và đã kích hoạt các role như DHCP, DNS và Certificate Services trên máy chủ đó. Kiểu chúng chỉ máy chủ là Enterprise, nên bạn sẽ cấu hình một CA doanh nghiệp trên mạng của mình. Máy chủ VPN sẽ được nhập vào miền trước khi bắt đầu các bước dưới đây. Máy khách Vista cần phải được nâng cấp lên phiên bản SP1 trước khi thực hiện theo hướng dẫn này.

Chúng tôi cần thực hiện một số thủ tục dưới đây:

- Cài đặt IIS trên máy chủ VPN
- Yêu cầu một chứng chỉ máy tính cho máy chủ VPN bằng cách sử dụng IIS Certificate Request Wizard
- Cài đặt role RRAS server trên máy chủ VPN
- Kích hoạt máy chủ RRAS Server và cấu hình nó thành máy chủ VPN và NAT
- Cấu hình máy chủ NAT để xuất bản CRL
- Cấu hình User Account để cho phép các kết nối dial-up
- Cấu hình IIS trên Certificate Server để cho phép các kết nối HTTP cho thư mục CRL
- Cấu hình file HOSTS trên VPN client
- Sử dụng PPTP để kết nối với máy chủ VPN
- Thu được chứng chỉ CA từ Enterprise CA
- Cấu hình Client để có thể sử dụng SSTP và Connect đối với VPN Server bằng cách sử dụng SSTP

### **Cài đặt IIS trên máy chủ VPN Server**

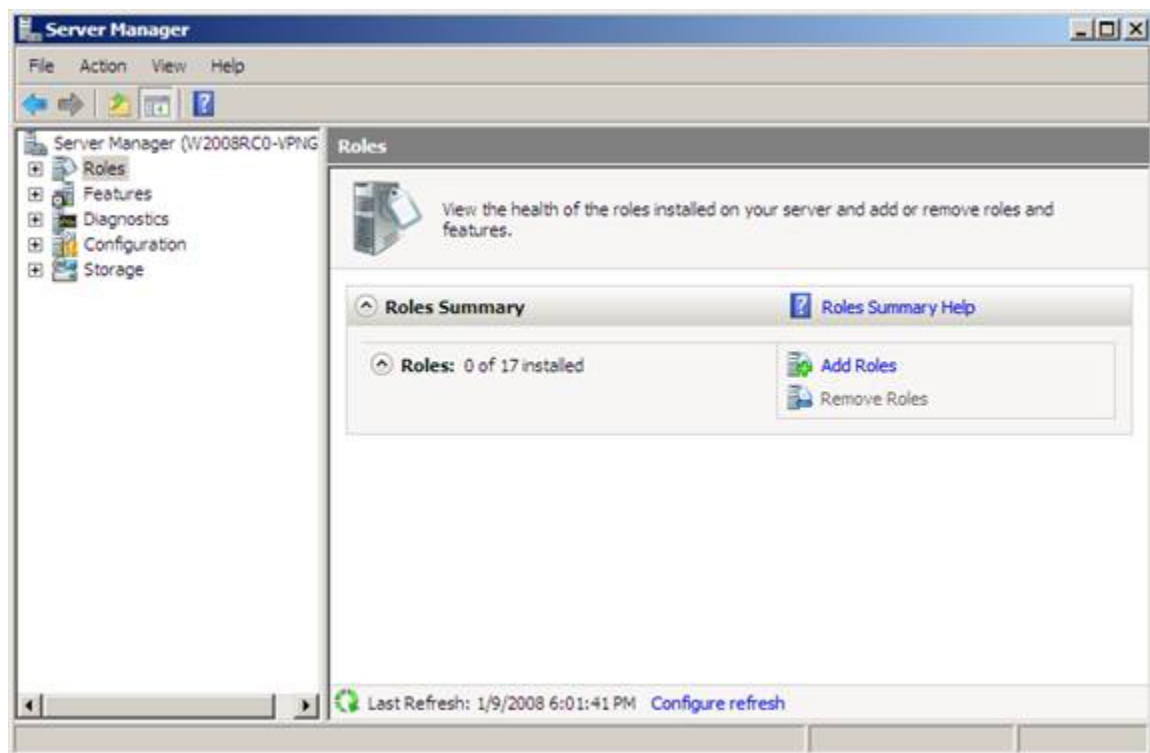
Có thể bạn sẽ thấy làm lạ vì thông thường chúng tôi vẫn gợi ý rằng đừng bao giờ đặt máy chủ web (Web server) trước một thiết bị bảo vệ mạng. Điều này là vì

chúng ta không cần giữ Web server trên một VPN server mà chỉ cần sử dụng nó trong một thời điểm nào đó. Bởi site kết nạp Web gồm có Windows Server 2008 Certificate Server không hữu dụng cho việc yêu cầu các chứng chỉ máy tính. Trong thực tế, nó hoàn toàn không được sử dụng. Những gì đáng quan tâm ở đây là bạn có thể có được chứng chỉ máy tính bằng sử dụng site kết nạp Web.

Để giải quyết vấn đề này, chúng ta sẽ lợi dụng enterprise CA. Khi sử dụng enterprise CA, bạn có thể tạo một yêu cầu đối với một máy chủ chứng chỉ trực tuyến. Yêu cầu trực tuyến cho một chứng chỉ máy tính được cho phép khi bạn sử dụng IIS Certificate Request Wizard và yêu cầu “Domain Certificate”- chứng chỉ miền. Vấn đề này chỉ làm việc khi máy tính yêu cầu chứng chỉ cùng với tên miền Enterprise CA.

Thực hiện theo các bước sau trên máy chủ VPN để cài đặt role IIS Web server:

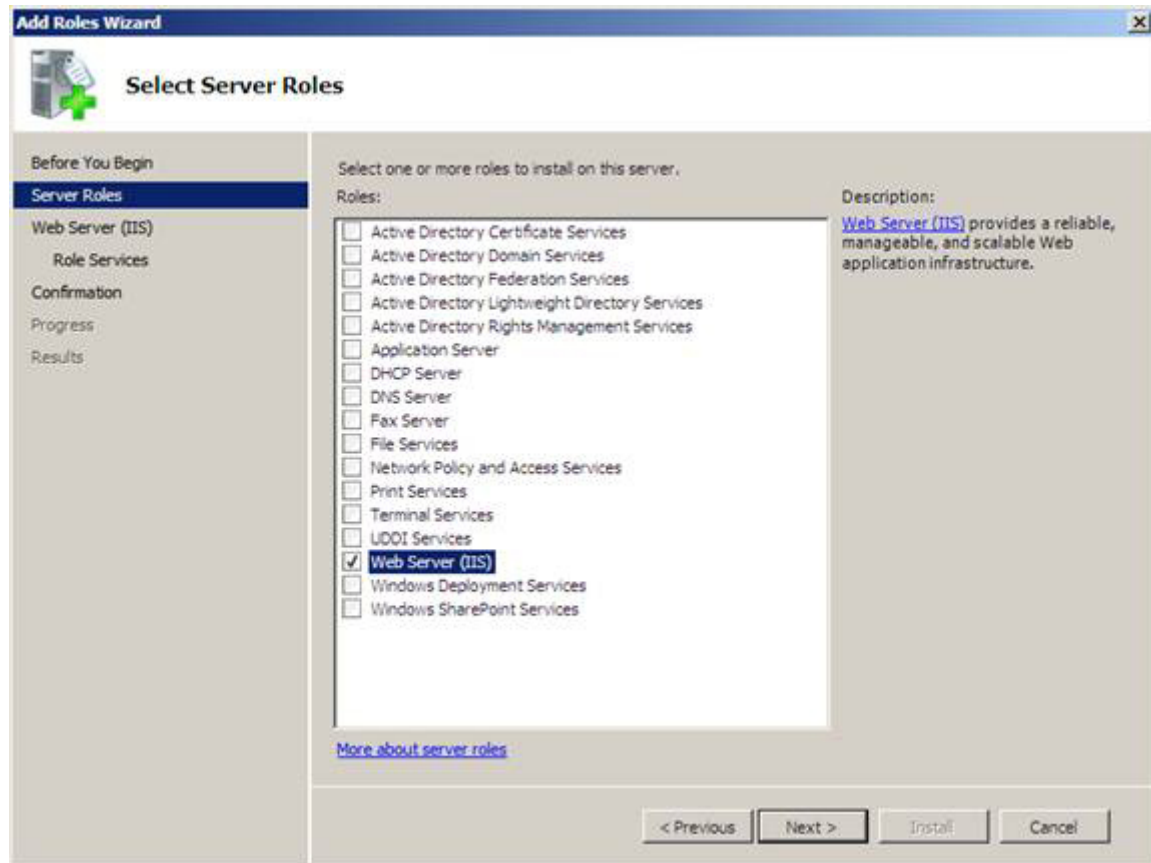
1. Mở **Server Manager** của Windows 2008
2. Trong phần panel bên phía trái của giao diện điều khiển, kích nút **Roles**



Hình 1

3. Kích vào liên kết **Add Roles** ở phần bên phải của panel bên phải.
4. Kích **Next** trên cửa sổ *Before You Begin*

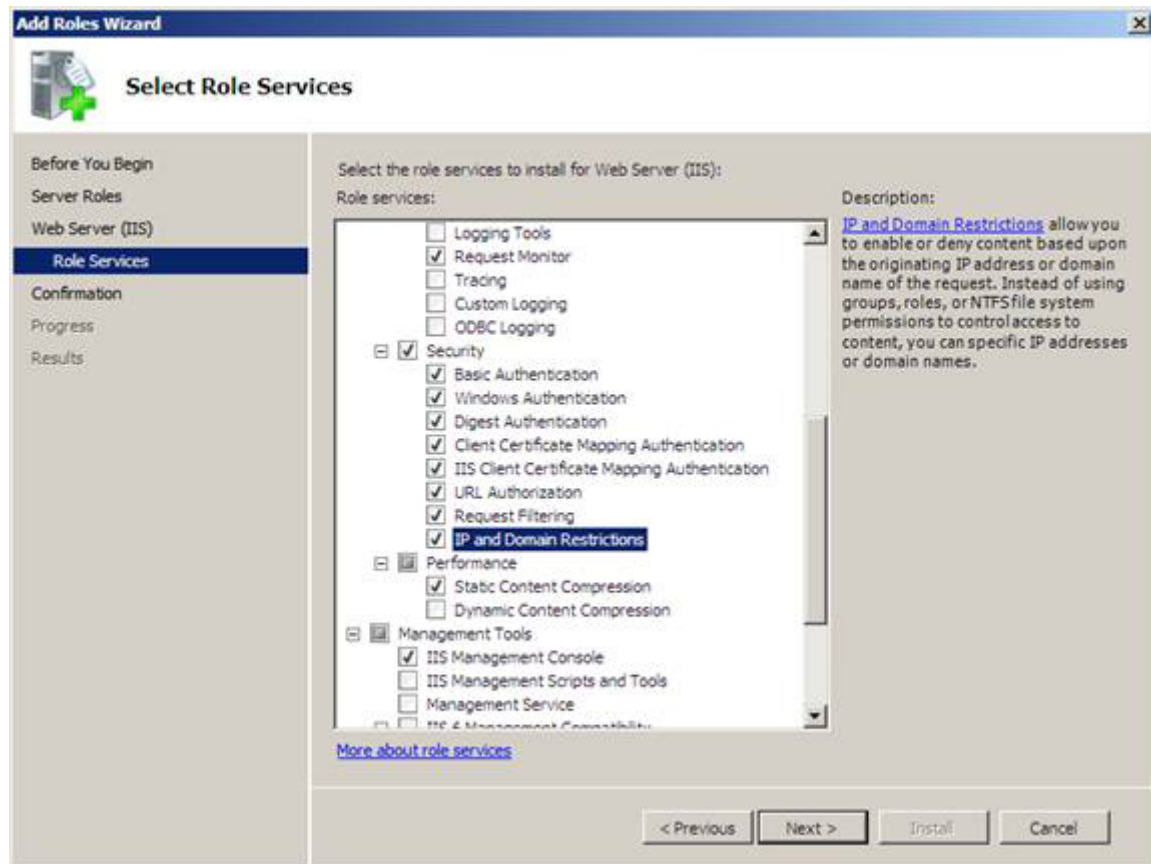
5. Tích vào hộp kiểm **Web Server (IIS)** trên cửa sổ *Select Server Roles* sau đó kích **Next**.



Hình 2

6. Đọc thông tin trên cửa sổ *Web Server (IIS)* nếu cần. Đây là một thông tin tổng quan rất tốt đối với việc sử dụng IIS7 như một máy chủ Web, tuy nhiên do chúng ta sẽ không sử dụng máy chủ Web IIS trên máy chủ VPN nên thông tin này không áp dụng cho kịch bản của chúng ta.

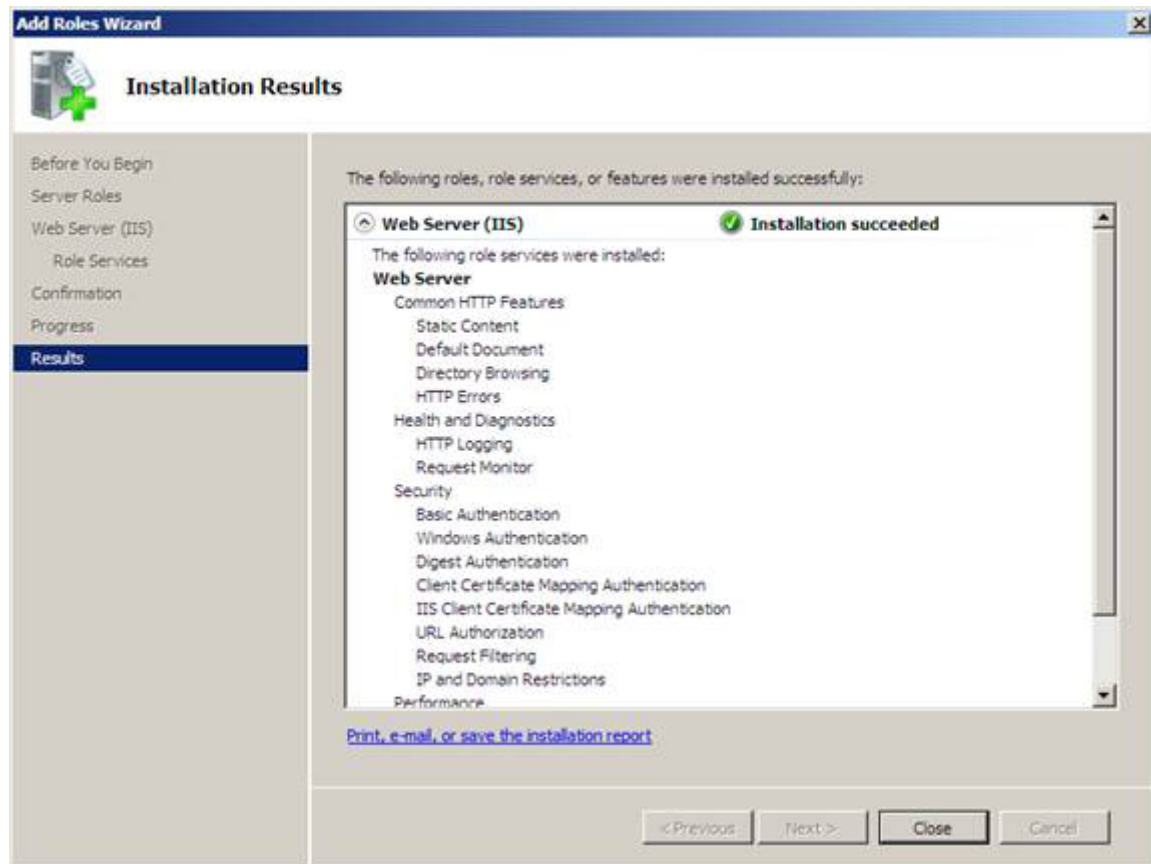
7. Trên cửa sổ *Select Role Services*, có một số tùy chọn đã được chọn sẵn. Kể cả bạn sử dụng các tùy chọn mặc định thì cũng không có nghĩa sẽ có được tùy chọn sử dụng Certificate Request Wizard. Chính vì vậy hãy tích vào các tùy chọn bảo mật **Security** để có *Role Service* cho Certificate Request Wizard và sau đó kích **Next**.



Hình 3

8. Xem lại các thông tin trên cửa sổ *Confirm Installation Selections* và kích **Install**.

9. Kích **Close** trên cửa sổ *Installation Results*



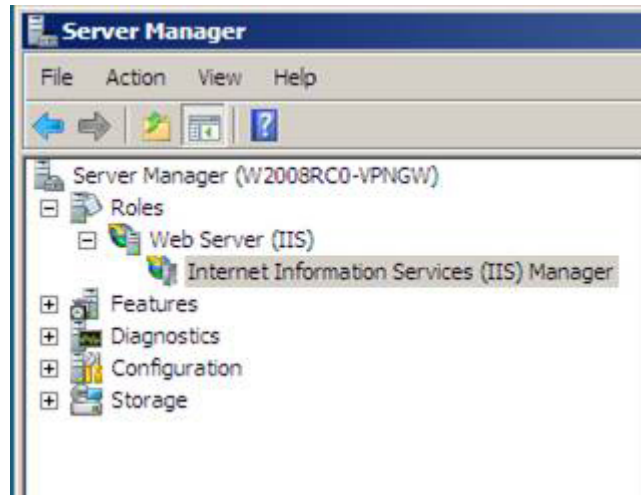
Hình 4

## Yêu cầu chứng chỉ máy tính cho VPN Server bằng sử dụng IIS Certificate Request Wizard

Bước tiếp theo là yêu cầu chứng chỉ máy tính cho VPN server. VPN server cần một chứng chỉ máy tính để có thể tạo kết nối SSL VPN với máy khách SSL VPN. Tên thường sử dụng trên chứng chỉ phải hợp lệ với tên mà máy khách VPN sẽ sử dụng để kết nối đến SSL VPN gateway. Điều này có nghĩa rằng bạn cần phải tạo một entry DNS chung cho tên trên chứng chỉ để giải quyết địa chỉ IP mở rộng trên VPN server, hoặc địa chỉ IP của thiết bị NAT nằm trước máy chủ VPN sẽ chuyển hướng kết nối đến SSL VPN server.

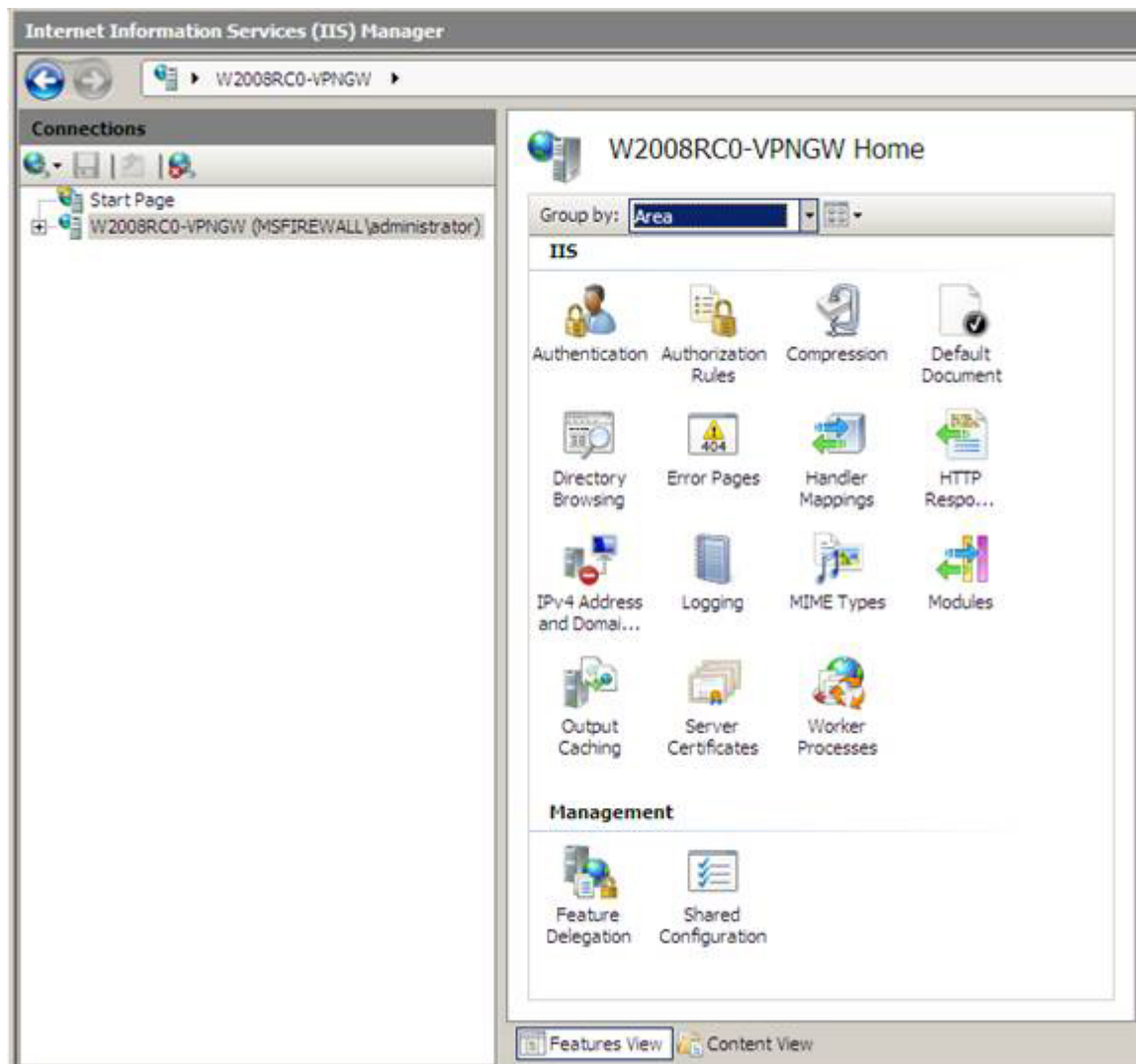
Thực hiện theo các bước dưới đây để yêu cầu và cài đặt một chứng chỉ máy tính trên SSL VPN server:

1. Trong *Server Manager*, mở rộng phần **Roles** ở trong panel bên trái, sau đó mở **Web Server (IIS)**. Kích vào **Internet Information Services (IIS) Manager**.



Hình 5

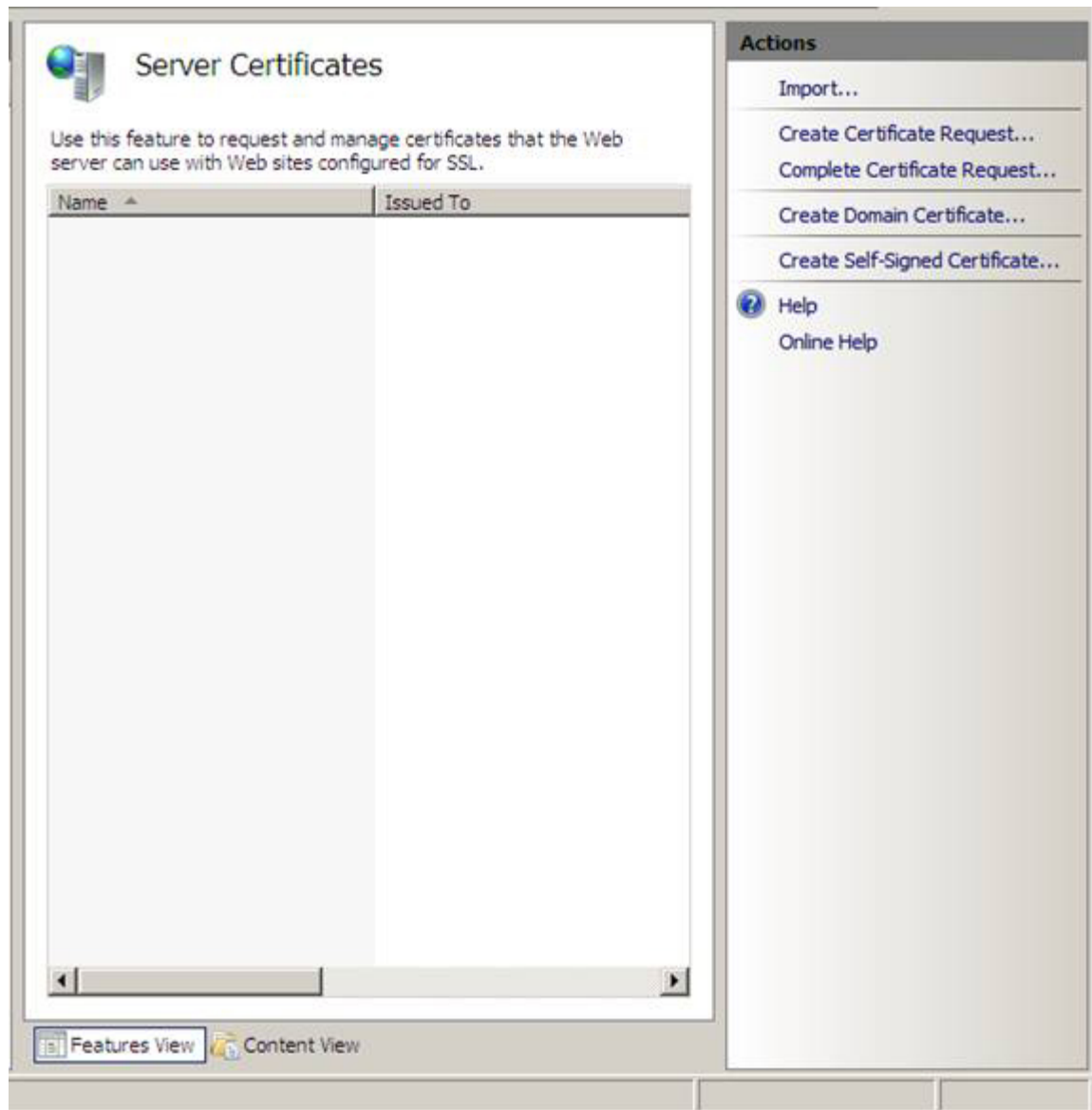
2. Trong giao diện điều khiển *Internet Information Services (IIS) Manager* xuất hiện ở panel bên phải, hãy kích tên của máy chủ. Trong ví dụ này, tên của máy chủ là **W2008RC0-VPNGW**. Kích vào biểu tượng **Server Certificates** trong panel bên phải của giao diện điều khiển IIS.



Hình 6

3. Trong panel bên phải của giao diện điều khiển, kích vào liên kết **Create Domain Certificate**.





Hình 7

4. Đọc các thông tin trên cửa sổ *Distinguished Name Properties*. Mục quan trọng nhất trên cửa sổ này là the **Common Name**. Tên này là tên mà các máy khách VPN sẽ sử dụng để kết nối với máy chủ VPN. Bạn sẽ cần có một entry DNS chung cho tên này để nó có thể giải quyết đối với giao diện bên ngoài của máy chủ VPN hoặc địa chỉ chung của thiết bị NAT trước máy chủ VPN. Trong ví dụ này, chúng tôi sẽ dùng tên chung **sstp.msfirewall.org**. Sau đó, chúng ta sẽ tạo các entry file HOSTS trên máy khách VPN để nó có thể thực hiện được với tên này. Kích **Next**.

**Create Certificate** [?] [X]

**Distinguished Name Properties**

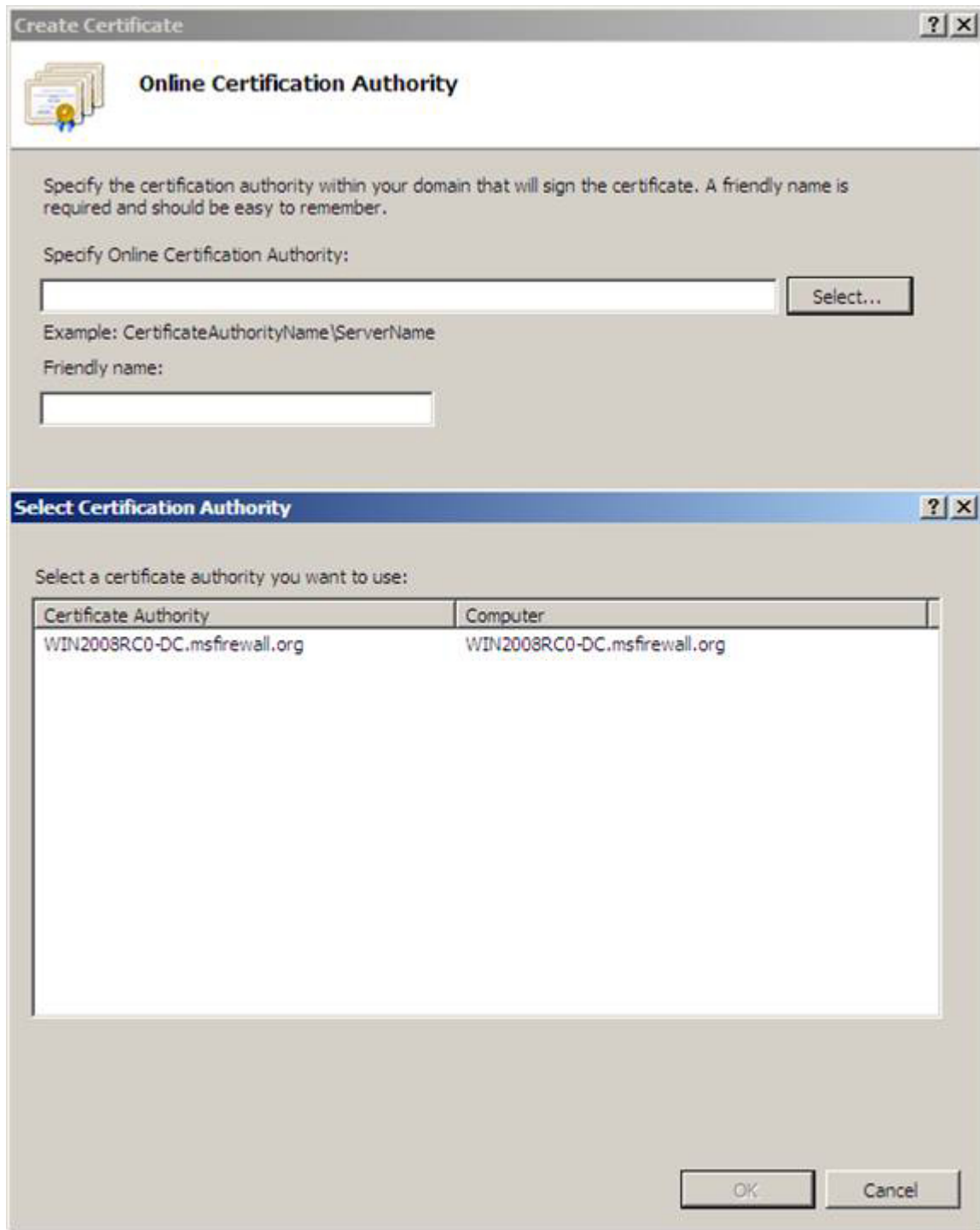
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="sstp.msfirewall.org"/>
Organization:	<input type="text" value="TACTEAM"/>
Organizational unit:	<input type="text" value="Dallas"/>
City/locality:	<input type="text" value="Dallas"/>
State/province:	<input type="text" value="Texas"/>
Country/region:	<input type="text" value="US"/>

Previous Next Finish Cancel

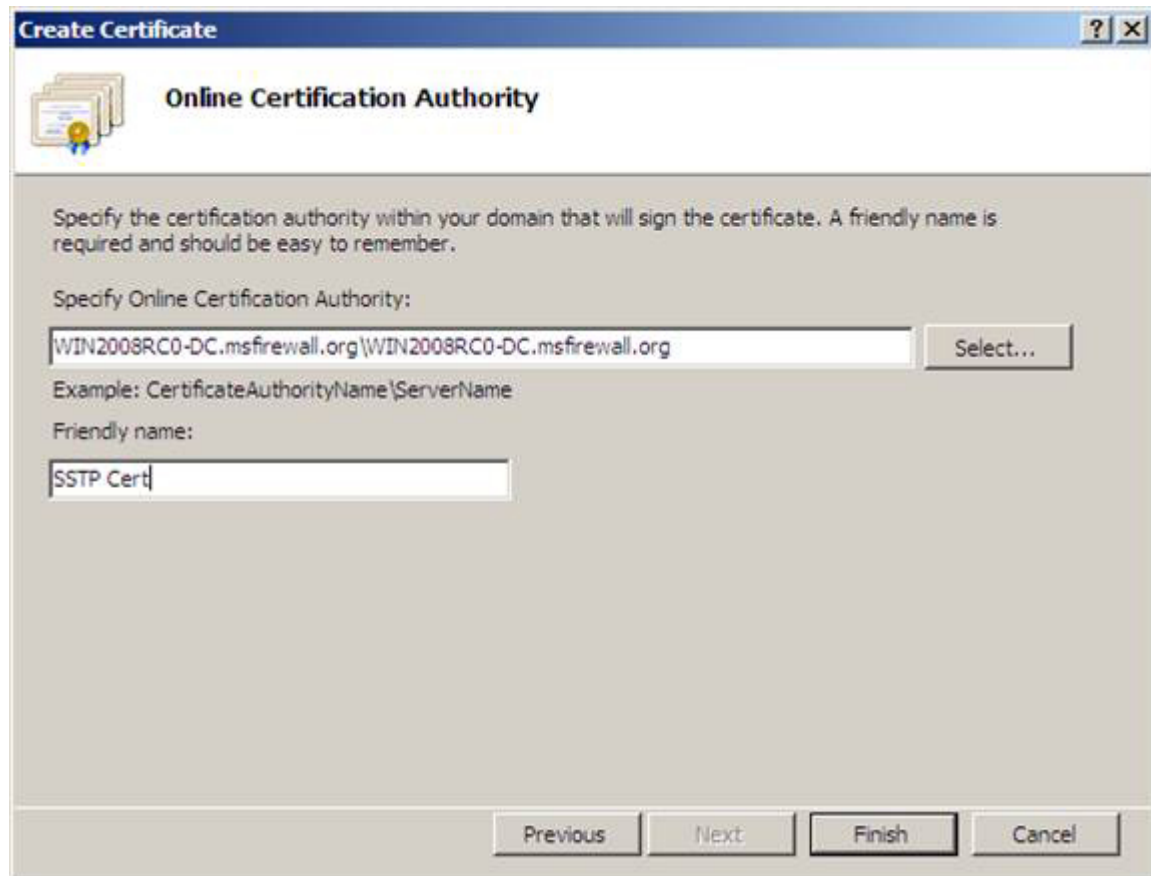
Hình 8

5. Trên cửa sổ *Online Certification Authority*, kích nút **Select**. Trong hộp thoại *Select Certification Authority*, kích tên của Enterprise CA sau đó kích **OK**. Nhập vào đó tên của chứng chỉ bên trong hộp văn bản **Friendly name**. Trong ví dụ này chúng tôi sử dụng tên **SSTP Cert** để biết rằng nó đang được sử dụng cho SSTP VPN gateway.



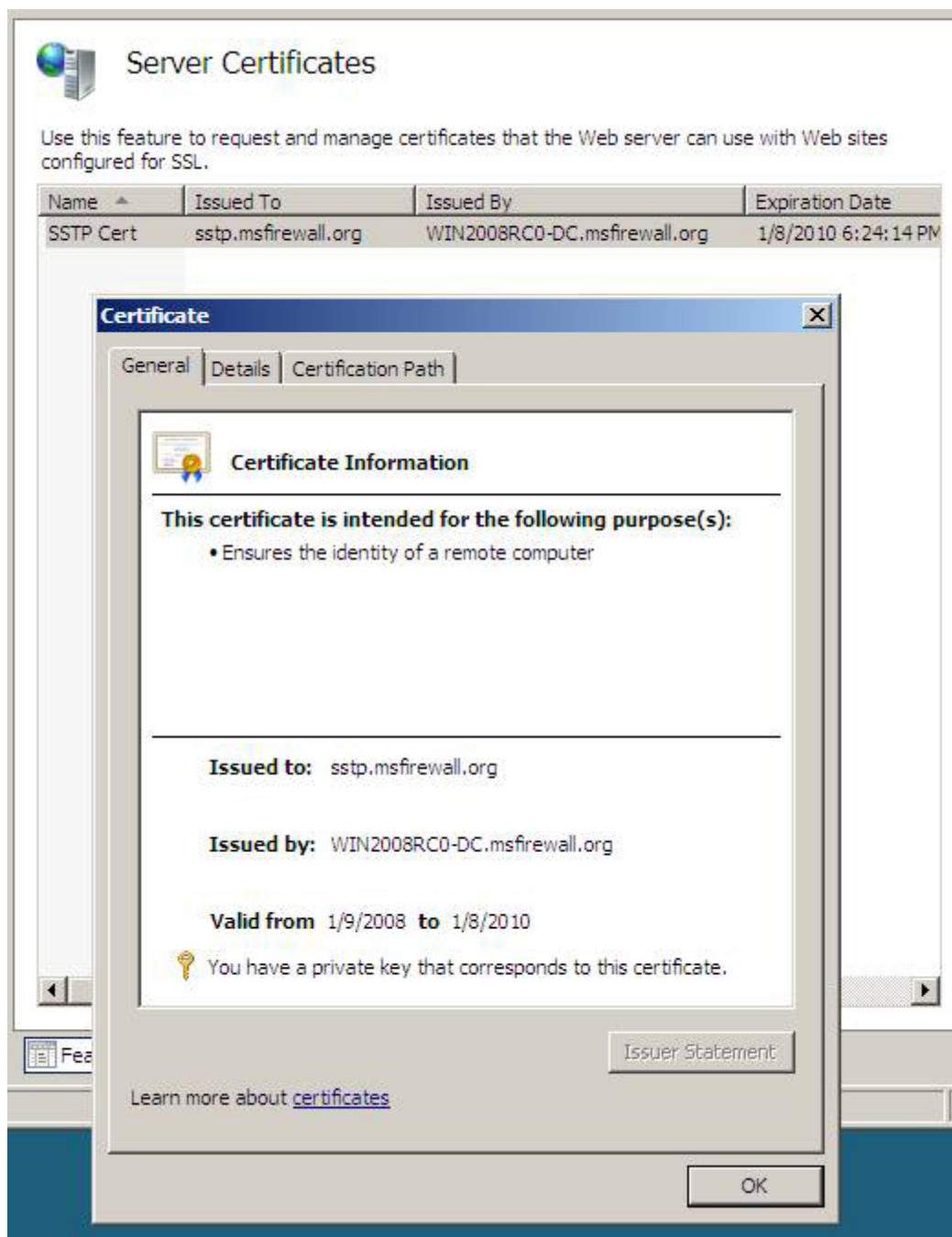
Hình 9

6. Kích **Finish** trên cửa sổ *Online Certification Authority*



Hình 10

7. Tiện ích sẽ chạy và sau đó không xuất hiện nữa. Sau thời điểm này, bạn sẽ nhìn thấy chứng chỉ xuất hiện trong giao diện điều khiển IIS. Kích đúp vào chứng chỉ và bạn có thể xem tên chung trong phần **Issued to** và chúng ta sẽ có một khóa riêng tương ứng với chứng chỉ. Kích **OK** để đóng hộp thoại *Certificate*.



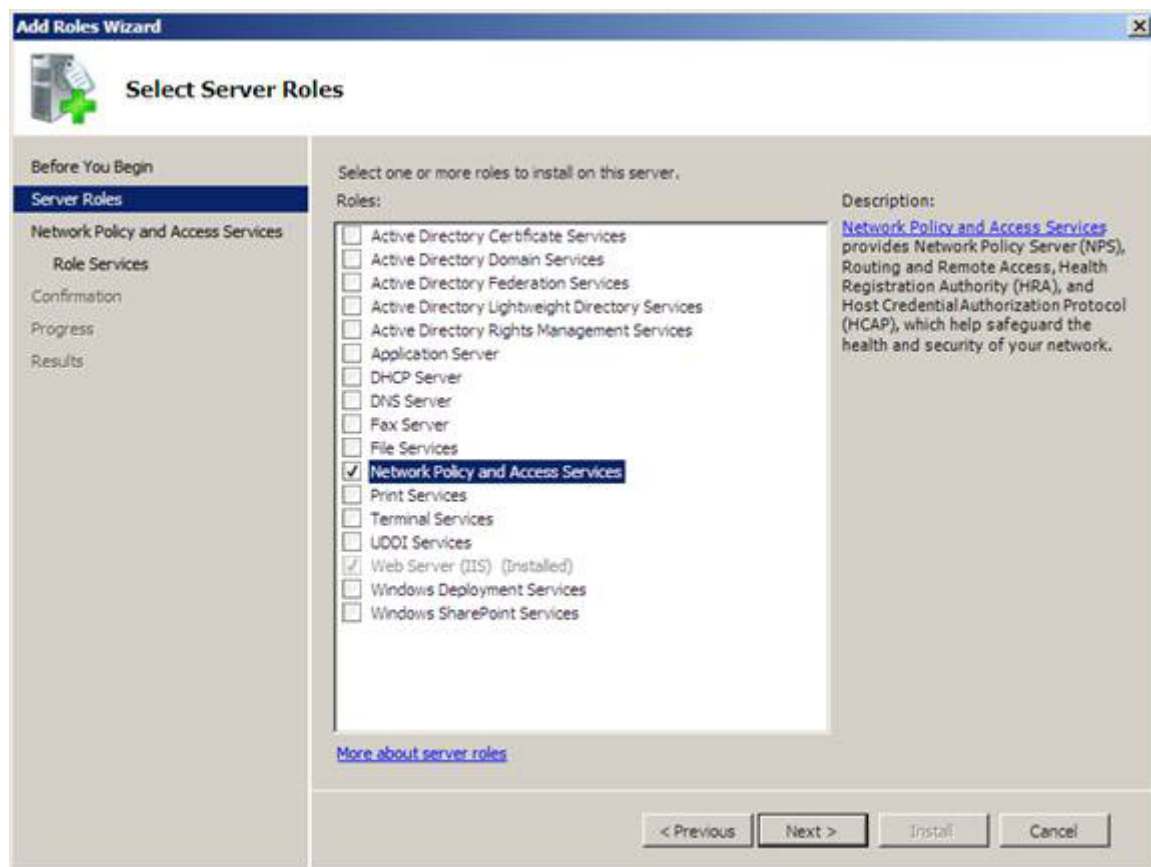
Hình 11

Bây giờ chúng ta đã có một chứng chỉ và có thể cài đặt RRAS Server Role. Lưu ý rằng bạn phải cài đặt chứng chỉ trước khi cài đặt RRAS Server Role. Không thực hiện như vậy bạn sẽ gặp phải một số vấn đề vì sẽ phải sử dụng một thường trình dòng lệnh khá phức tạp để kết nối chứng chỉ với bộ nghe SSL VPN.

### Cài đặt RRAS Server Role trên VPN Server

Để cài đặt RRAS Server Role, bạn thực hiện theo các bước dưới đây:

1. Trong *Server Manager*, kích nút **Roles** ở phần bên trái của giao diện điều khiển
2. Trong phần *Roles Summary*, kích vào liên kết **Add Roles**.
3. Kích **Next** trên cửa sổ *Before You Begin*
4. Trên cửa sổ *Select Server Roles*, bạn hãy tích vào hộp kiểm **Network Policy and Access Services**, sau đó kích **Next**.

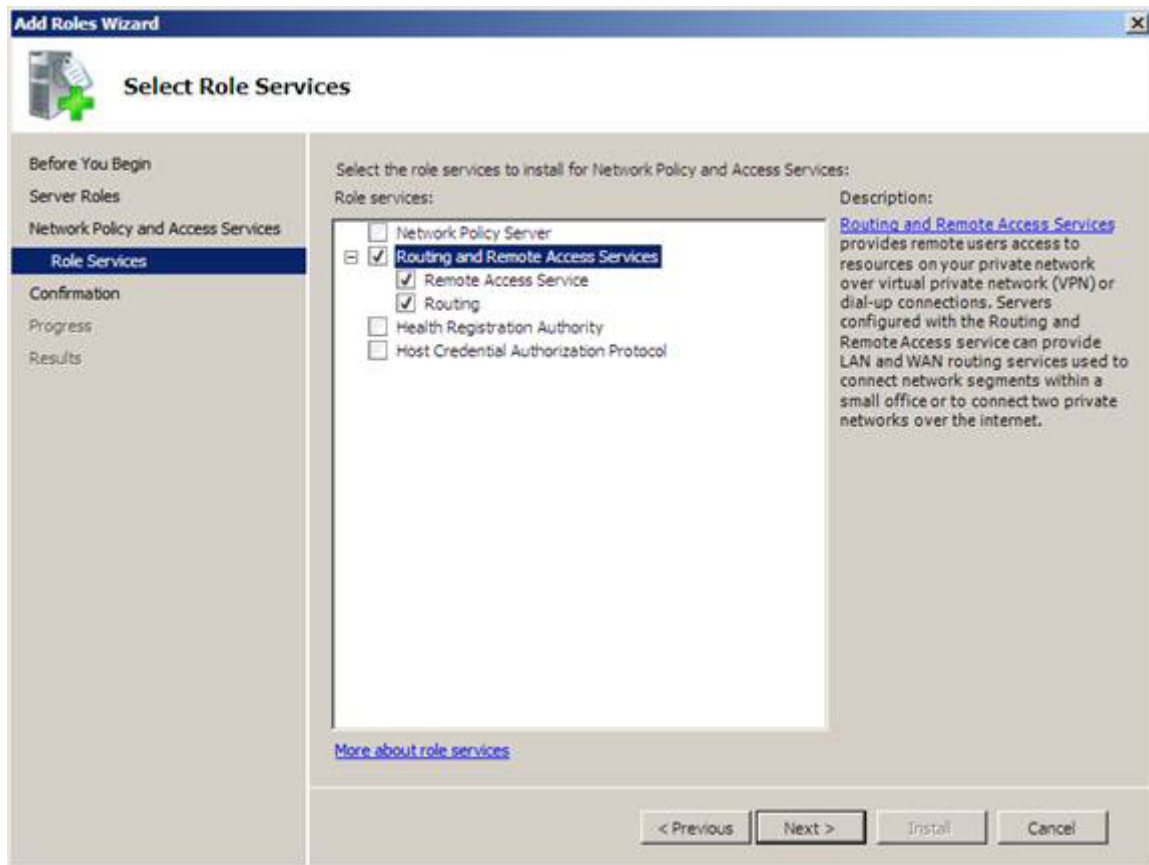


Hình 12

5. Đọc các thông tin trên cửa sổ *Network Policy and Access Services*. Hầu hết các thông tin này cho chúng ta biết về Network Policy Server mới (máy chủ chính sách vẫn được gọi là Internet Authentication Server [IAS] là RADIUS server), tất cả trong chúng hiện đều không áp dụng cho kịch bản của chúng ta. Kích **Next**.

6. Trên cửa sổ *Select Role Services*, hãy tích vào hộp kiểm **Routing and**

**Remote Access Services.** Khi tích vào hộp kiểm này, tiện ích cũng sẽ tự tích vào các hộp kiểm **Remote Access Service** và **Routing**. Kích **Next**.



Hình 13

7. Kích **Install** trên cửa sổ *Confirm Installation Selections*.

8. Kích **Close** trên cửa sổ *Installation Results*.

### **Kích hoạt RRAS Server và cấu hình nó trở thành một máy chủ NAT và VPN**

Lúc này role máy chủ RRAS server hiện đã được cài đặt, chúng ta cần phải kích hoạt dịch vụ RRAS, giống như cách đã thực hiện với nó trong các phiên bản trước đó của Windows. Chúng ta cần kích hoạt tính năng máy chủ VPN và dịch vụ NAT. Việc cần phải kích hoạt thành phần máy chủ VPN là hết sức rõ ràng nhưng rất có thể bạn phân vân rằng tại sao cần phải kích hoạt máy chủ NAT. Lý do là để các máy khách bên ngoài có thể tăng quyền truy cập vào Certificate Server để có thể kết nối với CRL. Nếu máy khách SSTP VPN không thể download được CRL thì kết nối SSTP VPN sẽ thất bại.

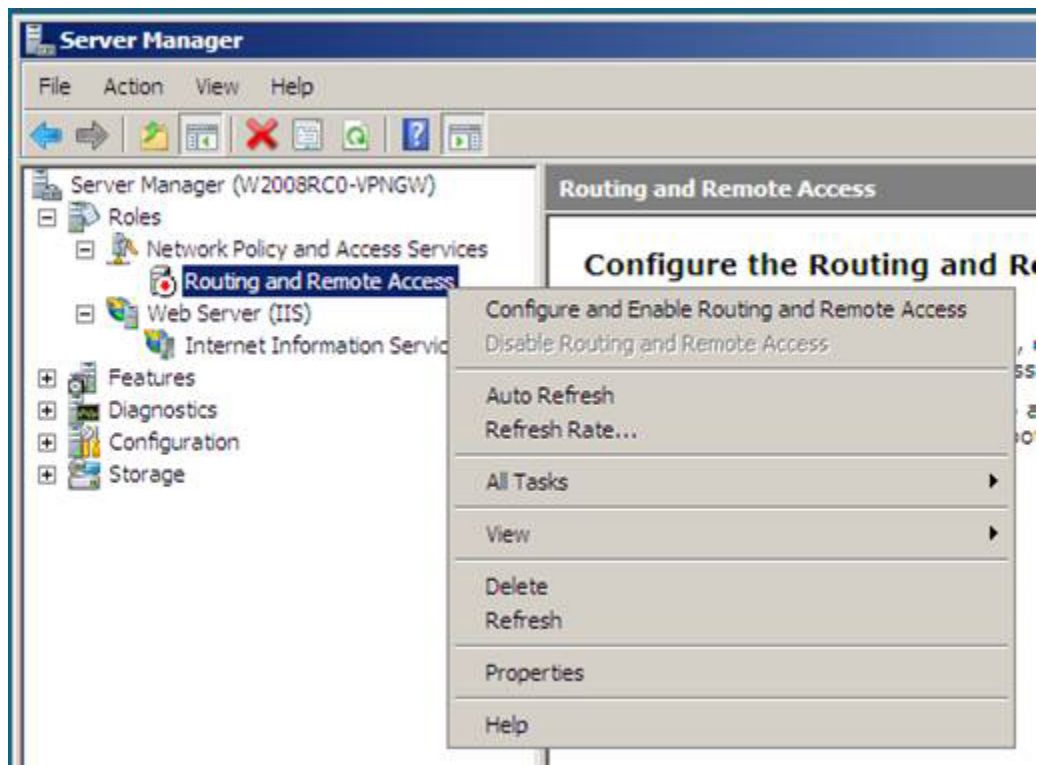
Để cho phép truy cập vào CRL chúng ta sẽ cấu hình máy chủ VPN thành một



máy chủ NAT và công bố CRL bằng cách sử dụng NAT đảo ngược. Trong môi trường thực tế bạn có thể sẽ có một tường lửa (như ISA Firewall chẳng hạn) nằm phía trước máy chủ chứng chỉ Certificate Server, vì vậy bạn sẽ công bố CRL bằng sử dụng tường lửa. Tuy vậy trong ví dụ này tường lửa sử dụng là Windows Firewall trên VPN server, chính vì vậy chúng ta cần phải cấu hình máy chủ VPN thành máy chủ NAT.

Thực hiện theo các bước dưới đây để có thể kích hoạt dịch vụ RRAS:

1. Trong *Server Manager*, mở phần **Roles** trong panel bên trái của giao diện điều khiển. Mở phần **Network Policy and Access Services** sau đó kích nút **Routing and Remote Access**. Kích chuột phải vào **Routing and Remote Access** sau đó kích **Configure and Enable Routing and Remote Access**.

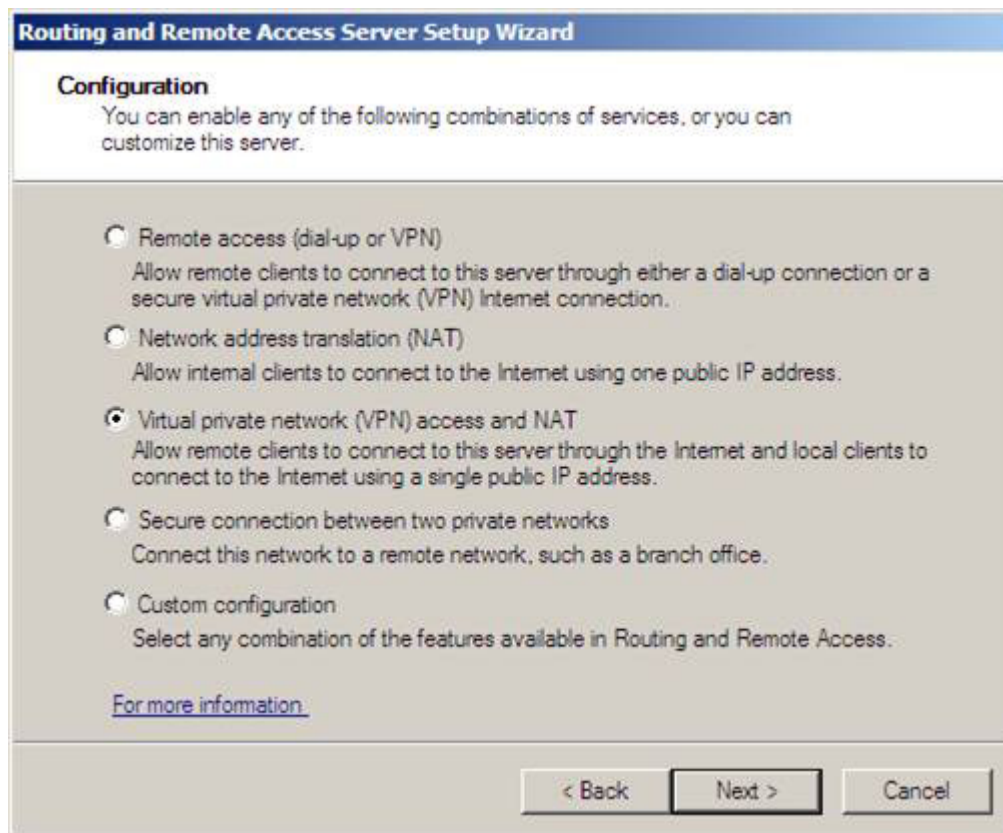


Hình 14

2. Kích **Next** trên cửa sổ *Welcome to the Routing and Remote Access Server Setup Wizard*

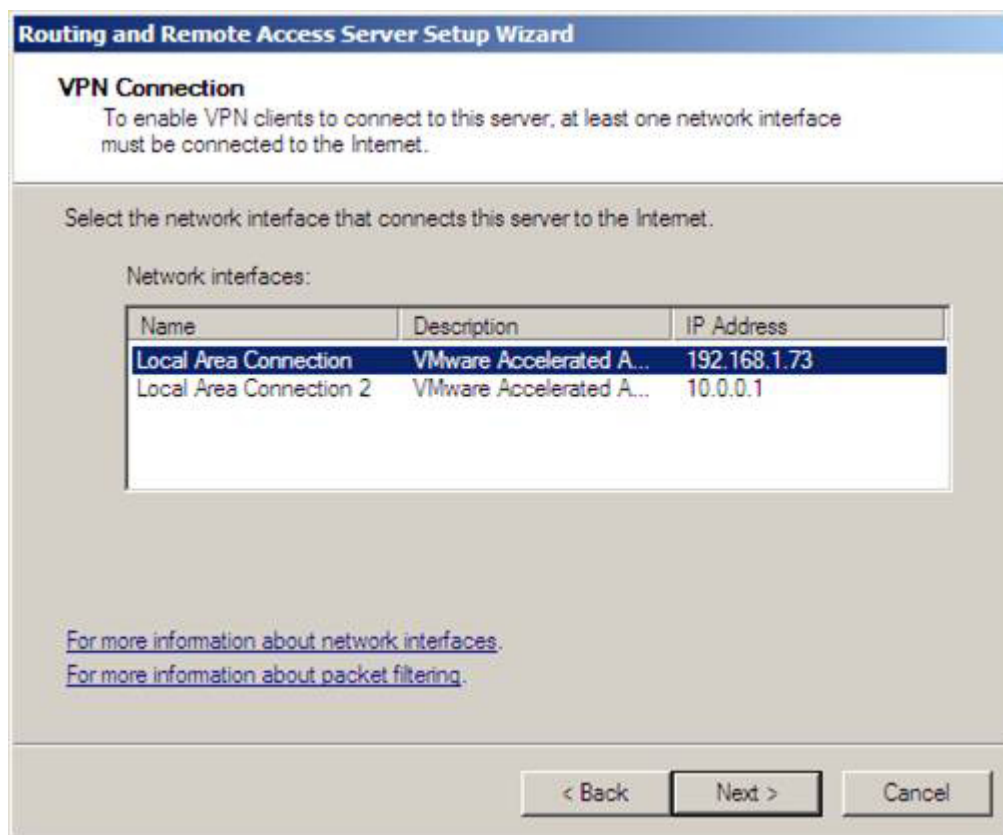
3. Trên cửa sổ *Configuration*, chọn tùy chọn **Virtual private network (VPN) access and NAT** và kích **Next**.





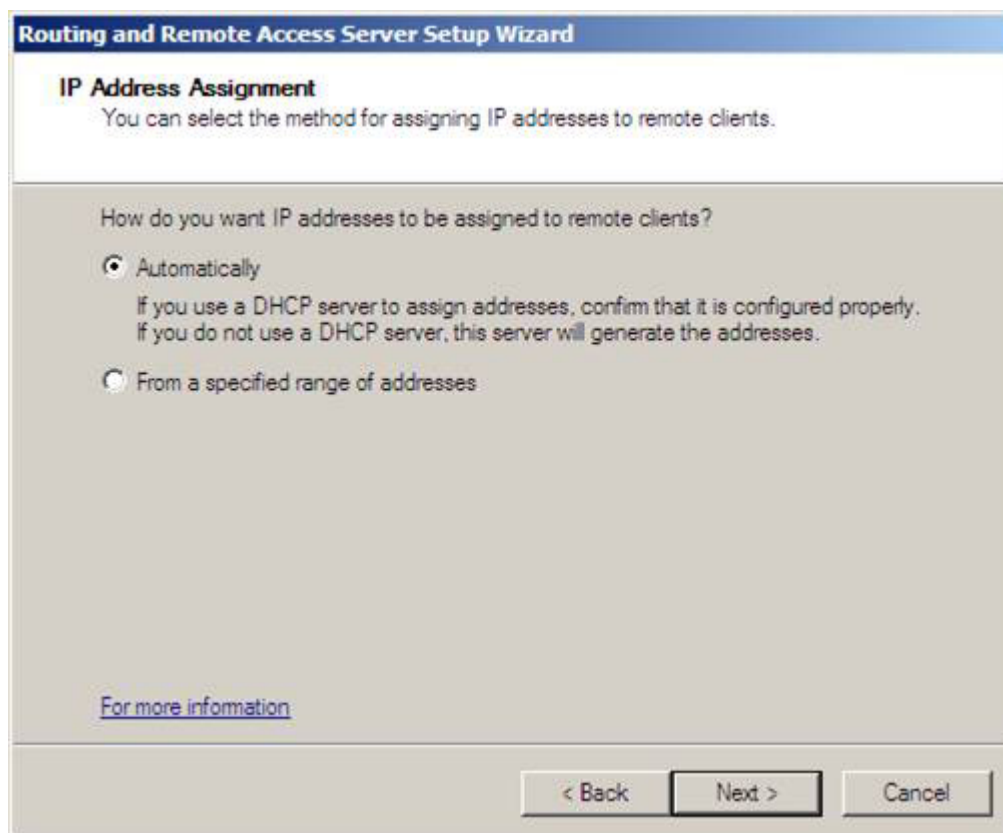
Hình 15

4. Trên cửa sổ *VPN Connection*, chọn NIC trong phần *Network interfaces*, phần có giao diện bên ngoài của máy chủ VPN. Sau đó kích **Next**.



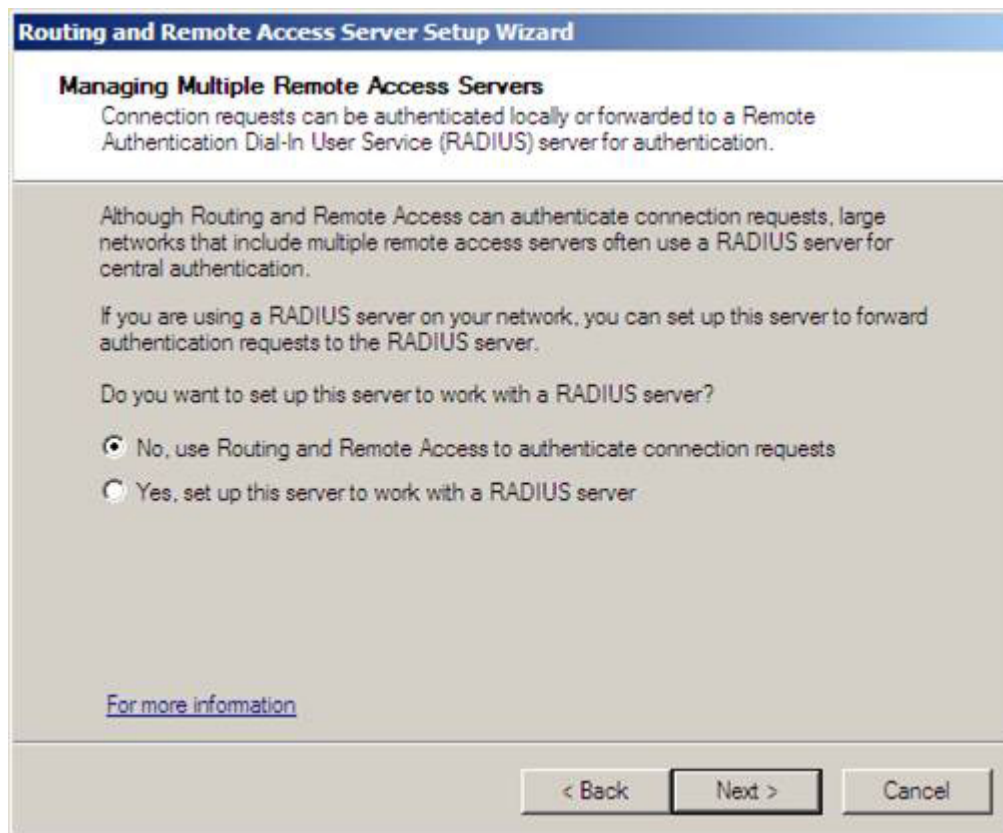
Hình 16

5. Trên cửa sổ *IP Address Assignment*, chọn tùy chọn **Automatically**. Chúng ta có thể chọn tùy chọn này vì đã cài đặt máy chủ DHCP trên bộ điều khiển miền phía sau máy chủ VPN. Nếu bạn chưa cài đặt máy chủ DHCP thì cần phải chọn tùy chọn **From a specified range of addresses** và sau đó cung cấp một danh sách các địa chỉ mà máy chủ VPN có thể sử dụng khi kết nối với mạng thông qua VPN gateway. Kích **Next**.



Hình 17

6. Trên cửa sổ *Managing Multiple Remote Access Servers*, chọn **No, use Routing and Remote Access to authenticate connection requests**. Đây là tùy chọn mà chúng ta sử dụng khi không có máy chủ NPS hay RADIUS. Vì máy chủ VPN là một thành viên của miền nên bạn có thể chứng thực người dùng bằng cách sử dụng các tài khoản miền. Nếu máy chủ VPN không phải là thành viên miền thì chỉ có các tài khoản cục bộ trên máy chủ VPN mới có thể được sử dụng, trừ khi bạn quyết định sử dụng máy chủ NPS. Kích **Next**.

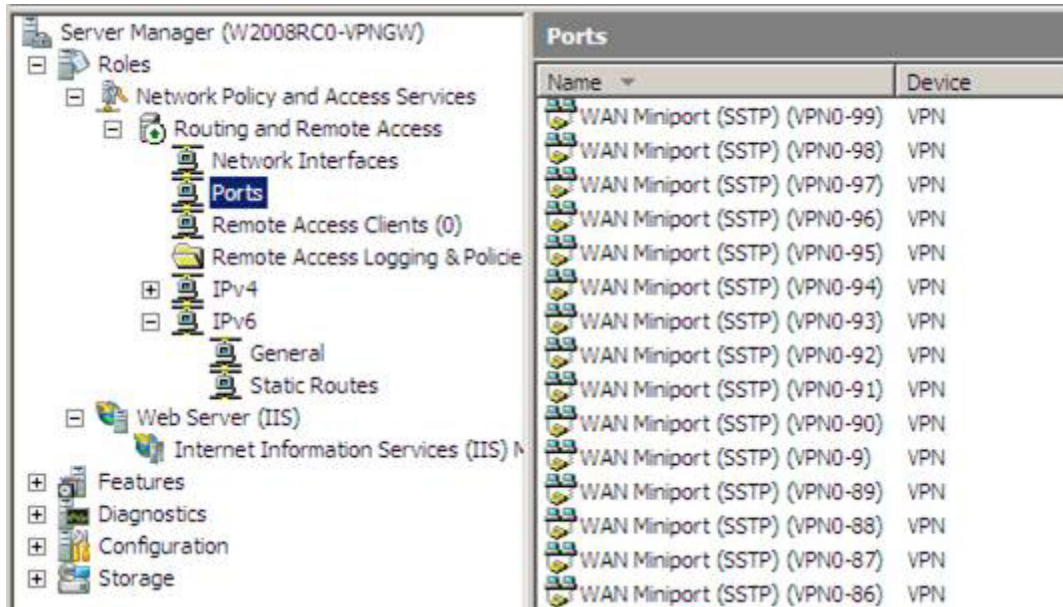


Hình 18

7. Đọc các thông tin tóm tắt trên cửa sổ *Completing the Routing and Remote Access Server Setup Wizard* và kích **Finish**.

8. Kích **OK** trong hộp thoại *Routing and Remote Access*, đây là hộp thoại thông báo cho bạn biết rằng việc chuyển tiếp các thông báo DHCP yêu cầu đến một tác nhân chuyển tiếp.

9. Trong phần panel bên trái của giao diện điều khiển, mở phần **Routing and Remote Access**, sau đó kích vào nút **Ports**. Ở phần giữa của panel, bạn sẽ thấy các kết nối cho SSTP.



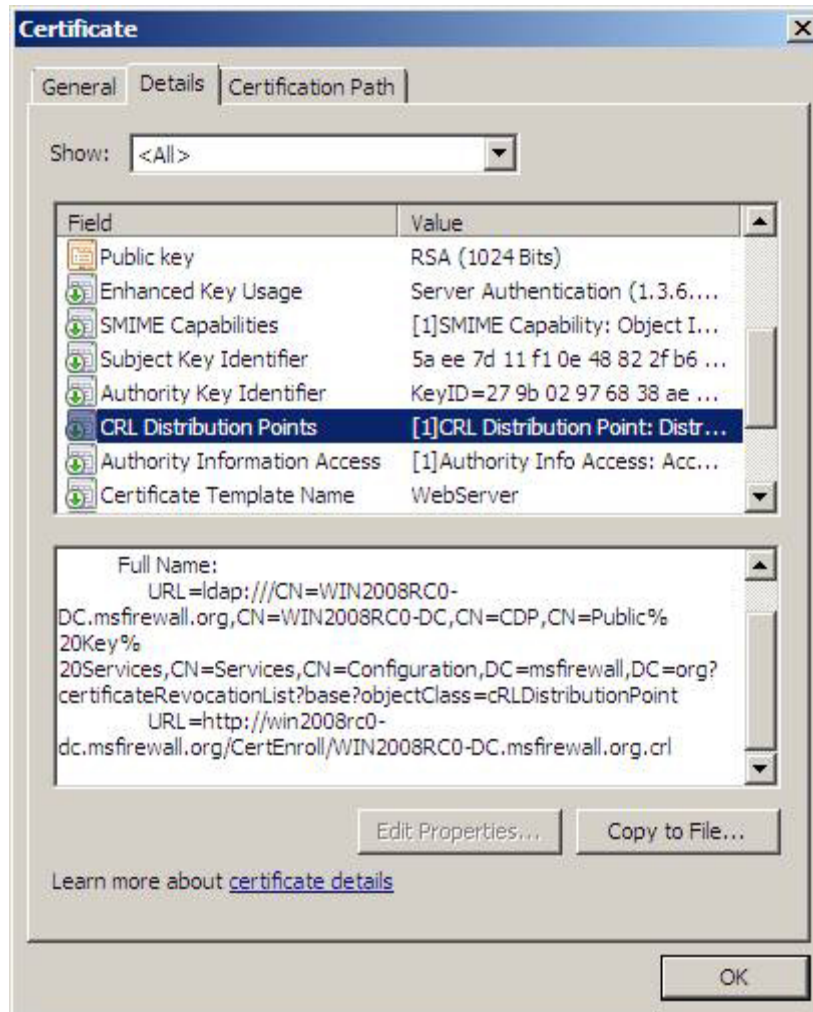
Hình 19

## Cấu hình máy chủ NAT để công bố CRL

Như chúng tôi đã đề cập từ trước, máy khách SSL VPN cần có thể download được CRL để xác nhận rằng chứng chỉ máy chủ trên máy chủ VPN đã không được hủy bỏ. Để thực hiện điều này, bạn cần cấu hình một thiết bị trước máy chủ chứng chỉ để chuyển tiếp các yêu cầu HTTP cho vị trí CRL đến được máy chủ chứng chỉ.

Vậy bạn đã biết được URL nào mà máy khách SSL VPN cần kết nối để thực hiện việc download CRL chưa? Các thông tin này được giới thiệu đến ngay bên trong bản thân mỗi chứng chỉ. Nếu bạn vào máy chủ VPN một lần nữa và kích đúp vào chứng chỉ trên giao diện điều khiển IIS (đây là do bạn đã thực hiện trước), thì bạn sẽ có thể tìm được các thông tin này. Kích vào tab Details của chứng chỉ và kéo xuống mục CRL Distribution Points, sau đó kích chuột vào mục đó. Trong panel thấp hơn, bạn có thể thấy các điểm phân phối khác nhau được dựa trên giao thức sử dụng để truy cập vào các điểm này. Trong màn hình chứng chỉ ở hình bên dưới, bạn có thể thấy được rằng chúng ta cần phải cho phép truy cập máy khách SSL VPN vào CRL thông qua URL:

***<http://win2008rc0-dc.msfirewall.org/CertEnroll/WIN2008RC0-DC.msfirewall.org.crl>***



Hình 20

Vì lý do này nên bạn cần tạo một entry DNS chúng đối với tên này để các máy khách VPN bên ngoài đều có thể thực thi được tên đó với địa chỉ IP trên thiết bị, thiết bị ở đây sẽ thực hiện đảo ngược NAT hoặc đảo ngược proxy để cho phép truy cập đến được website của Certificate Server. Trong ví dụ này, chúng ta cần phải có win2008rc0-dc.msfirewall.org để giải quyết địa chỉ IP trên giao diện bên ngoài của máy chủ VPN, máy chủ VPN sẽ đảo ngược NAT kết nối với Certificate Server.

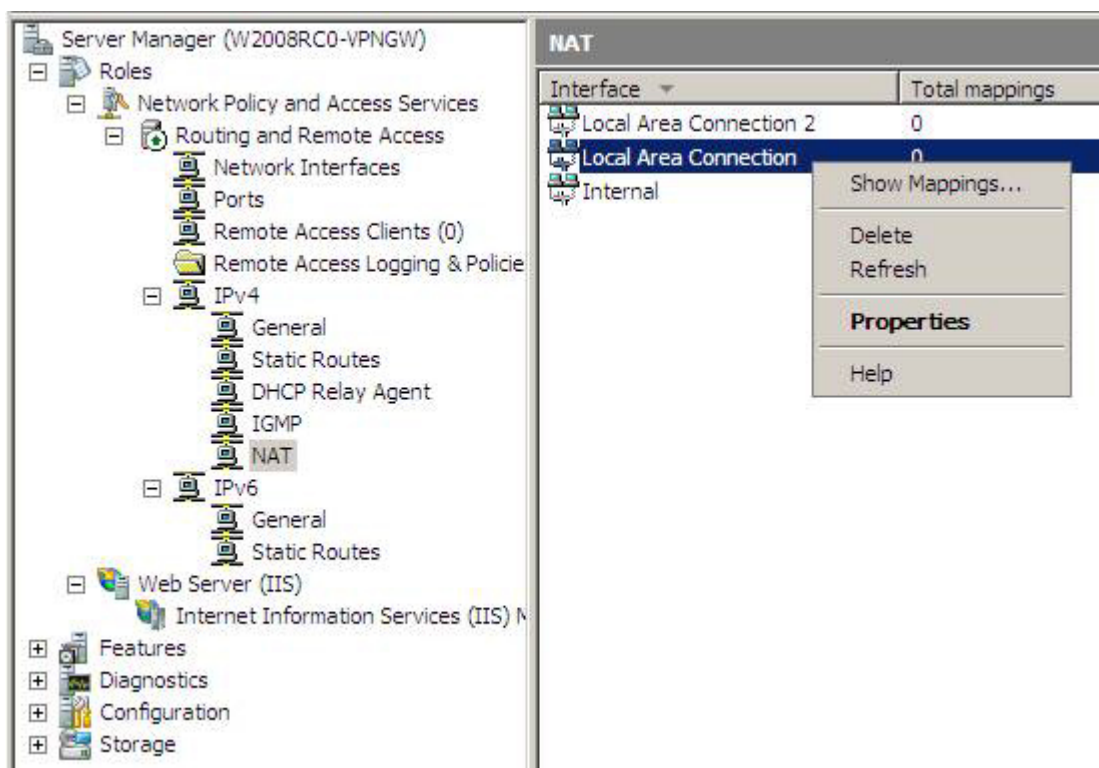
Nếu bạn đang sử dụng tường lửa “đời mới” (chẳng hạn như ISA Firewall) thì có thể thực hiện việc công bố site CRL an toàn hơn bằng cách cho phép chỉ truy cập vào CRL mà không vào toàn bộ site. Tuy vậy, trong bài này chúng tôi sẽ hạn chế trong khả năng một thiết bị NAT đơn giản như những gì RRAS NAT cung cấp. Bạn nên lưu ý ở đây rằng việc sử dụng tên site của CRL mặc định có thể không phải là cách an toàn vì nó lộ tên máy tính trên Internet. Bạn có thể tạo một CDP (CRL Distribution Point) để tránh điều này nếu cho rằng việc lộ tên riêng



của CA trong DNS chung là một vấn đề quan trọng.

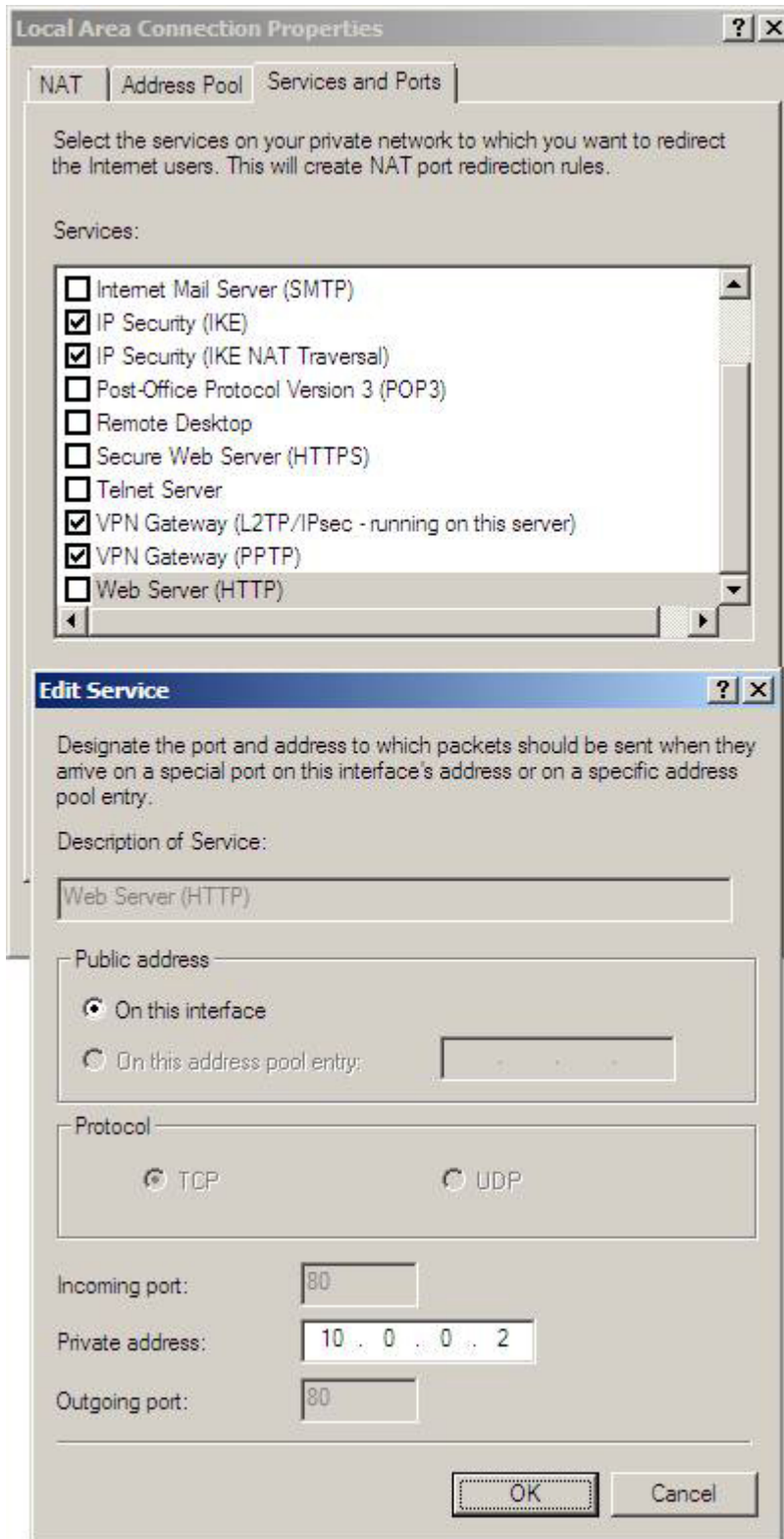
Thực hiện theo các bước dưới đây để cấu hình RRAS NAT có thể chuyển tiếp các yêu cầu HTTP tới Certificate Server:

1. Trong phần panel bên trái của *Server Manager*, bạn mở phần **Routing and Remote Access**, sau đó mở phần **IPv4**. Kích nút **NAT**.
2. Trong nút **NAT**, hãy kích chuột phải lên giao diện bên ngoài, ở giữa của giao diện điều khiển. Trong ví dụ này, tên của giao diện bên ngoài là **Local Area Connection**, sau đó kích **Properties**.



Hình 21

3. Trong hộp thoại *Local Area Connection Properties*, tích vào hộp kiểm **Web Server (HTTP)**. Khi thực hiện như vậy, hộp thoại **Edit Service** sẽ xuất hiện. Trong hộp văn bản **Private Address**, bạn nhập vào địa chỉ IP của máy chủ chứng chỉ trên mạng bên trong. Kích **OK**.



Hình 22

4. Kịch **OK** trong hộp thoại *Local Area Connection Properties*.





Hình 23

Lúc này, NAT server đã được cài đặt và được cấu hình, chúng ta có thể chuyển sự quan tâm của mình sang việc cấu hình máy chủ CA và máy khách SSTP VPN.

## Kết luận

Trong phần hai này, chúng tôi đã tiếp tục giới thiệu cho các bạn về việc cấu hình máy chủ SSL VPN bằng cách sử dụng Windows Server 2008. Chúng tôi đã đi vào các vấn đề cài đặt IIS trên máy chủ VPN, yêu cầu và cài đặt chứng chỉ máy chủ, cài đặt và cấu hình các dịch vụ RRAS và NAT. Trong phần tiếp theo của loạt bài này chúng tôi sẽ kết thúc bằng việc giới thiệu cách cấu hình máy chủ CA và máy khách SSTP VPN, mong các bạn đón đọc.

## Cấu hình Windows Server 2008 thành SSL VPN Server truy cập từ xa (Phần 3)

Nguồn : quantrimang.com

***Thomas Shinder***

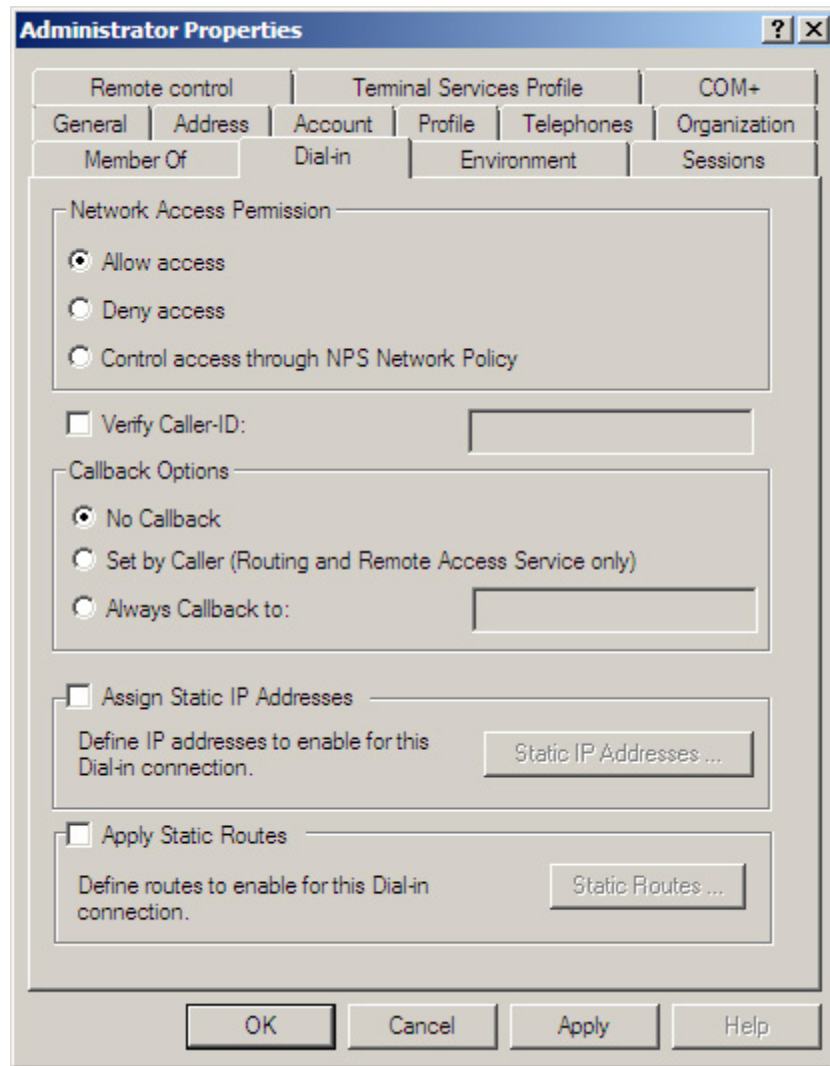
Trong hai phần trước của loạt bài giới thiệu cách tạo một máy chủ SSL VPN trên Windows Server 2008 này, chúng tôi đã giới thiệu các kiến thức cơ bản về vấn đề kết nối mạng VPN, sau đó đi sâu vào cấu hình của máy chủ. Trong quá trình này, chúng tôi đã thực hiện một số thay đổi cấu hình nhỏ trong Active Directory và trên CA Web. Sau khi thực hiện một số thay đổi, chúng tôi sẽ tập trung vào cấu hình máy khách VPN và kết thúc bằng việc thiết lập kết nối SSL VPN.

### Cấu hình tài khoản người dùng cho phép kết nối Dial-up

Các tài khoản người dùng cần những điều khoản cho việc truy cập dial-up trước khi họ có thể kết nối với máy chủ Windows VPN (một thành viên của miền Active Directory). Cách tốt nhất để thực hiện điều này là sử dụng Network Policy Server (NPS) và sử dụng điều khoản tài khoản người dùng mặc định, những điều khoản này là để cho phép truy cập từ xa được thiết lập dựa trên chính sách NPS. Tuy vậy, chúng ta đã không cài đặt máy chủ NPS trong kịch bản này, vì vậy sẽ phải cấu hình một cách thủ công các điều khoản này của người dùng.

Thực hiện các bước dưới đây để kích hoạt các điều khoản quay số trên tài khoản người dùng mà bạn muốn kết nối đến máy chủ SSL VPN. Trong ví dụ này, chúng tôi sẽ kích hoạt truy cập quay số của tài khoản quản trị viên miền mặc định:

1. Tại domain controller, mở giao diện điều khiển **Active Directory Users and Computers** từ menu **Administrative Tools**.
2. Trong phần panel bên trái của giao diện, mở rộng tên miền và kích vào nút **Users**. Kích đúp vào tài khoản **Administrator**.
3. Kích tab **Dial-in**. Thiết lập mặc định là **Control access through NPS Network Policy**. Vì chúng ta không có máy chủ NPS trong kịch bản này nên sẽ thay đổi thiết lập thành **Allow access**, như những gì bạn có thể thấy được trong hình bên dưới. Kích **OK** để tiếp tục.



Hình 1

### **Cấu hình IIS trên máy chủ chứng chỉ để cho phép các kết nối HTTP được thực hiện với CRL Directory**

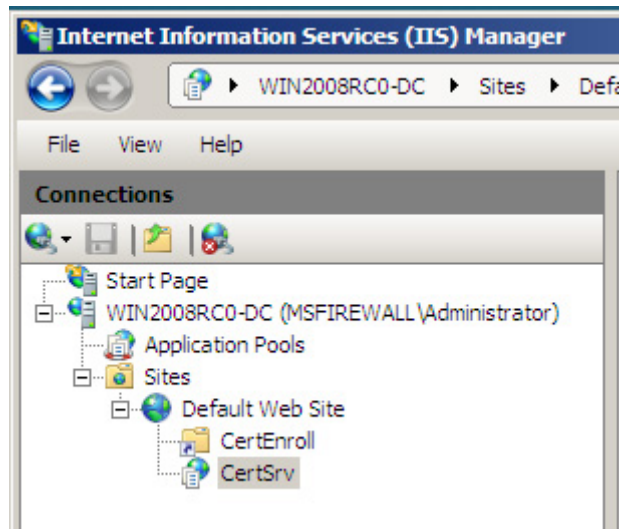
Vì một số lý do nên khi wizard đang cài đặt Certificate Services Web site, nó sẽ cấu hình thư mục CRL để yêu cầu một kết nối SSL. Điều này xét theo góc độ bảo mật dường như là một ý tưởng tốt, vấn đề bộc lộ ở đây là URL trên chứng chỉ không được cấu hình sử dụng SSL. Chúng tôi hy vọng bạn có thể tạo một entry CDP tùy chỉnh cho chứng chỉ để nó có thể sử dụng SSL, tuy nhiên bạn có thể sẽ tốn rất nhiều công sức vì Microsoft không có tài liệu cho vấn đề này. Chính vì chúng ta đang sử dụng các thiết lập mặc định cho CDP trong bài này nên cần tắt các yêu cầu SSL trên Web site của CA về đường dẫn của thư mục CRL.

Thực hiện các bước dưới đây để vô hiệu hóa yêu cầu SSL cho thư mục CRL

này:

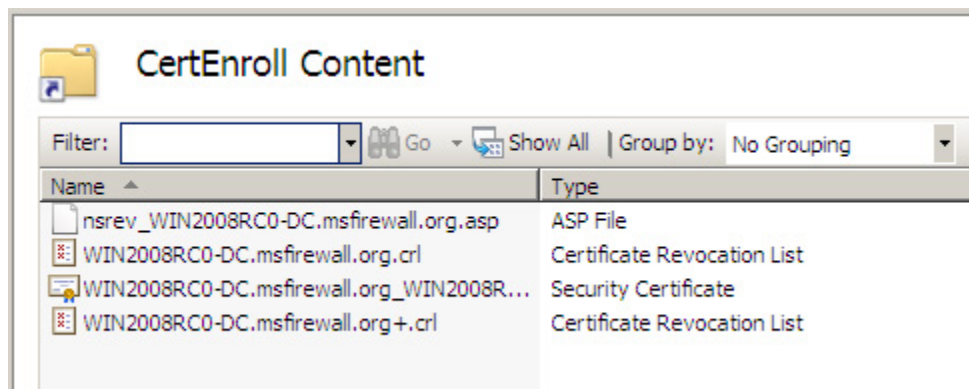
1. Từ menu **Administrative Tools**, mở **Internet Information Services (IIS) Manager**.

2. Trong phần panel bên trái của giao diện điều khiển, mở phần tên máy chủ và sau đó kích nút **Sites**. Mở nút **Default Web Site** và kích vào **CertEnroll**, bạn có thể xem những gì thực hiện trong hình vẽ bên dưới.



Hình 2

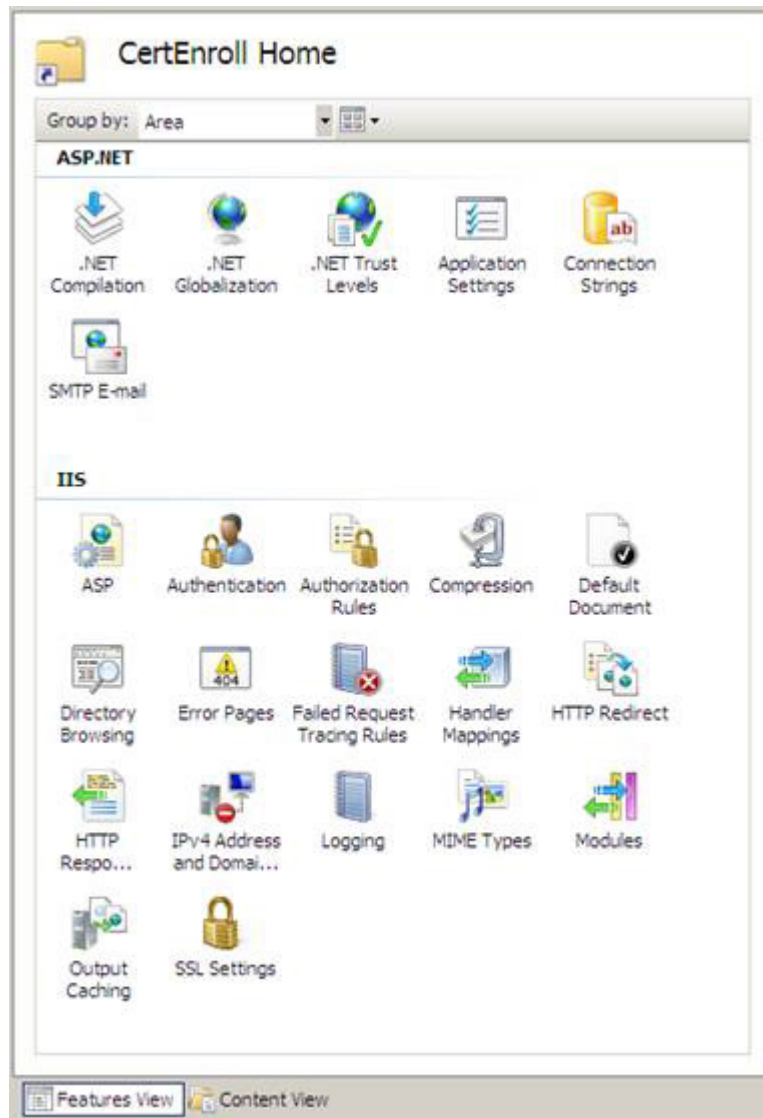
3. Nếu nhìn vào phần giữa của giao diện điều khiển thì bạn sẽ thấy CRL được đặt trong thư mục ảo này, như những gì trong hình bên dưới thể hiện. Để xem nội dung của thư mục ảo này, bạn cần phải kích vào nút **Content View** ở phần bên dưới của panel giữa.



Hình 3

4. Kích vào nút **Features View** ở phần bên dưới của panel giữa. Tại phần dưới

của panel giữa này, kích đúp vào biểu tượng **SSL Settings**.



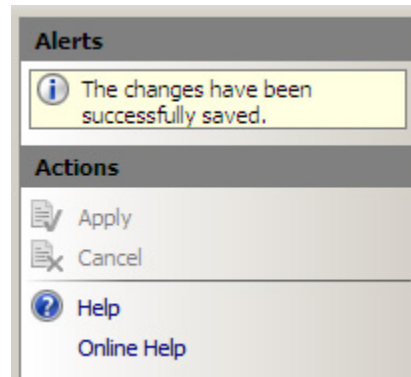
Hình 4

5. Trang **SSL Settings** xuất hiện ở giữa panel. Hủy bỏ dấu chọn từ hộp kiểm **Require SSL**. Kích vào liên kết **Apply** ở bên phải của giao diện điều khiển.



Hình 5

6. Đóng giao diện điều khiển IIS sau khi bạn thấy thông báo **The changes have been successfully saved.**



Hình 6

### Cấu hình File HOSTS trên máy khách VPN

Lúc này chúng ta có thể chuyển sự quan tâm sang máy khách VPN. Thứ đầu tiên cần thực hiện là cấu hình file HOSTS để có thể mô phỏng một cơ sở hạ tầng DNS công cộng. Có hai tên mà chúng ta cần nhập vào file HOSTS (và cũng vậy với máy chủ DNS công cộng mà bạn sẽ sử dụng trong môi trường sản xuất). Đầu tiên là tên của máy chủ VPN, như đã được định nghĩa bởi tên common/subject trên chứng chỉ mà bạn đã giới hạn cho máy chủ SSL VPN. Tên thứ hai cần nhập vào file HOSTS (và máy chủ DNS công cộng) là CDP URL, tên được tìm thấy trong chứng chỉ. Chúng ta đã thấy được vị trí của các thông tin CDP trong phần hai của loạt bài này.

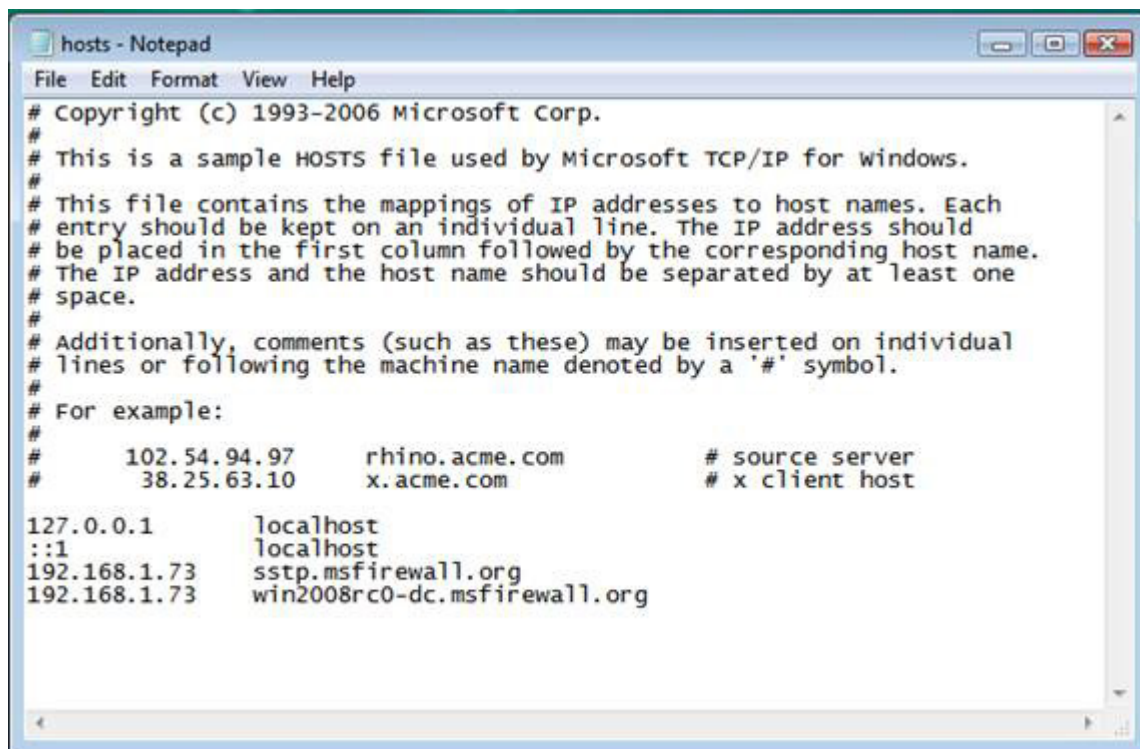
Hai tên cần nhập vào trong file HOSTS trong ví dụ này là:

**192.168.1.73 sstp.msfirewall.org**

## **192.168.1.73 win2008rc0-dc.msfirewall.org**

Thực hiện các bước dưới đây trên máy khách Vista SP1 VPN để cấu hình file HOSTS:

1. Kích nút **Start** và nhập vào dòng **c:\windows\system32\drivers\etc\hosts** trong hộp tìm kiếm và nhấn Enter.
2. Trong hộp thoại **Open With**, kích đúp vào **Notepad**.
3. Nhập vào các mục của file HOSTS bằng định dạng như những gì bạn có thể nhìn thấy trong hình bên dưới. Bảo đảm phải nhấn Enter sau dòng cuối cùng để con trỏ xuất hiện ở dưới dòng cuối cùng đó.



```
File Edit Format View Help
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host

127.0.0.1       localhost
::1            localhost
192.168.1.73   sstp.msfirewall.org
192.168.1.73   win2008rc0-dc.msfirewall.org
```

Hình 7

4. Đóng file và chọn tùy chọn save khi được hỏi.

### **Sử dụng PPTP để kết nối với máy chủ VPN**

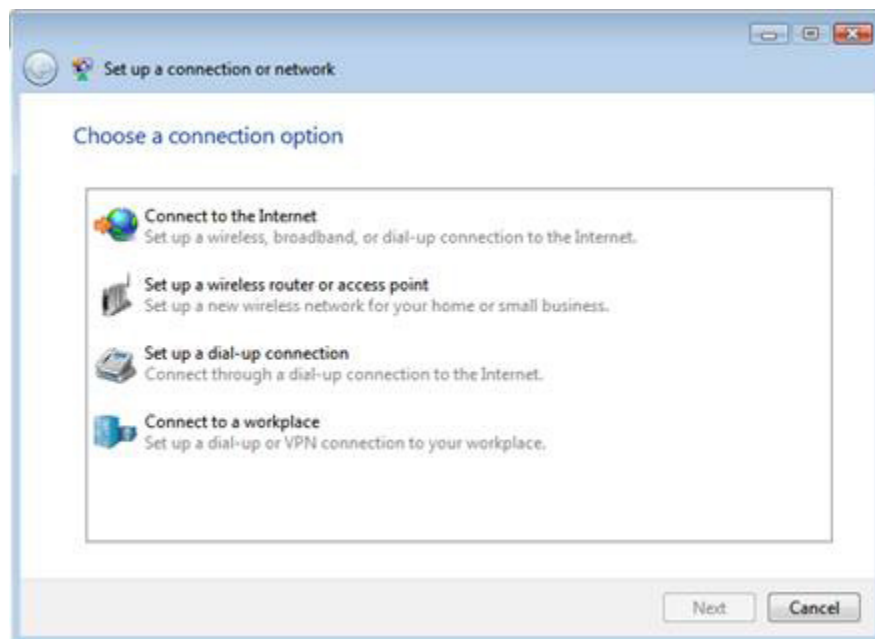
Chúng ta đang tiến gần hơn với việc tạo một kết nối SSL VPN! Bước tiếp theo là tạo một kết nối VPN trên máy khách Vista SP1 để cho phép có thể tạo một kết nối VPN ban đầu cho máy chủ VPN. Chúng ta cần thực hiện công việc này trong kịch bản hiện hành vì máy tính trình khách không phải là một thành viên miền.



Do máy tính này không nằm trong miền nên nó sẽ không có chứng chỉ CA được cài đặt một cách tự động trong kho lưu trữ chứng chỉ Trusted Root Certificate Authorities. Nếu máy tính này là một thành viên miền thì việc tự động kết nạp sẽ quan tâm đến vấn đề đó, vì đã cài đặt Enterprise CA. Cách đơn giản nhất để thực hiện điều này là tạo một kết nối PPTP từ máy khách Vista SP1 VPN đến máy chủ Windows Server 2008 VPN. Mặc định, máy chủ VPN sẽ hỗ trợ các kết nối PPTP và máy khách sẽ thử PPTP đầu tiên trước khi thử L2TP/IPSec và SSTP. Để thực hiện điều này, chúng ta cần phải tạo một kết nối VPN hoặc đối tượng kết nối.

Thực hiện các bước dưới đây trên máy khách VPN để tạo kết nối:

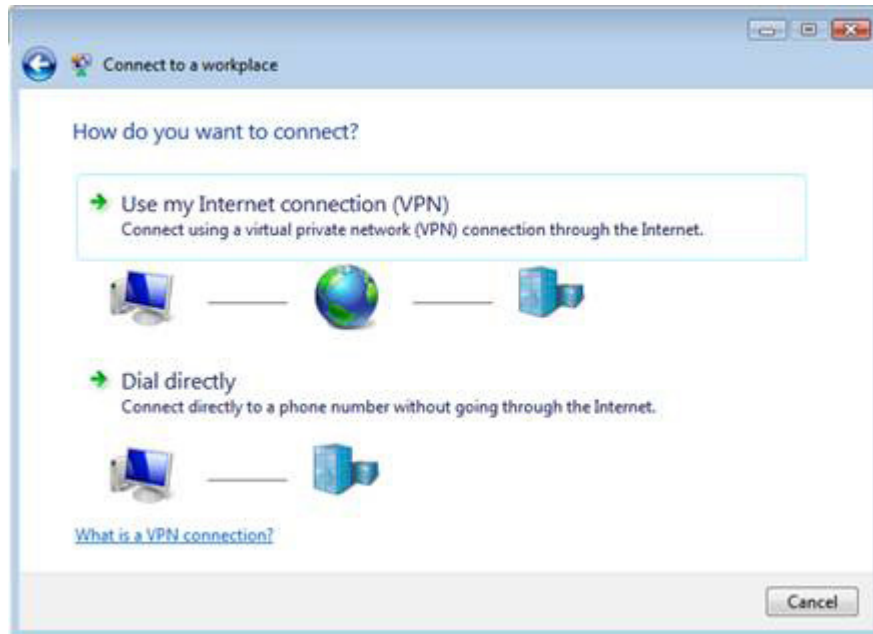
1. Trên máy khách VPN, kích chuột phải vào biểu tượng và sau đó kích **Network and Sharing Center**.
2. Trong cửa sổ Network Sharing Center, kích vào liên kết trên **Set up a connection or network** phía trái của cửa sổ.
3. Trên cửa sổ **Choose a connection option**, kích vào mục **Connect to a workplace** và sau đó kích **Next**.



Hình 8

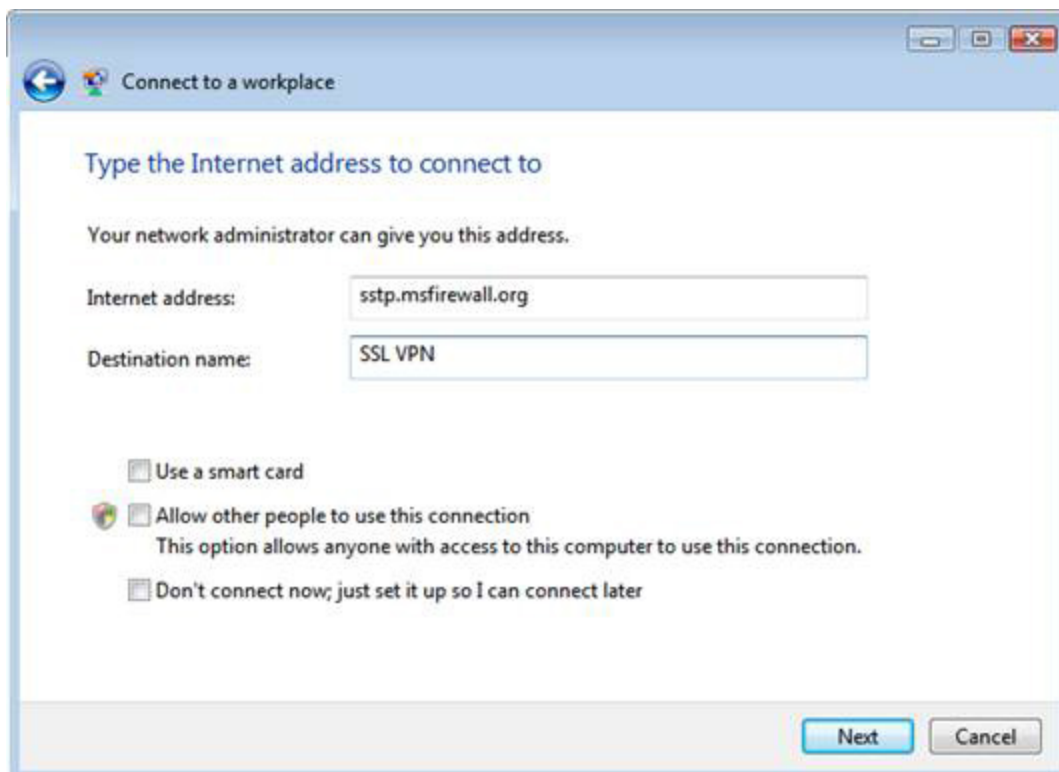
4. Trên cửa sổ **How do you want to connect**, chọn mục **Use my Internet connection (VPN)**.





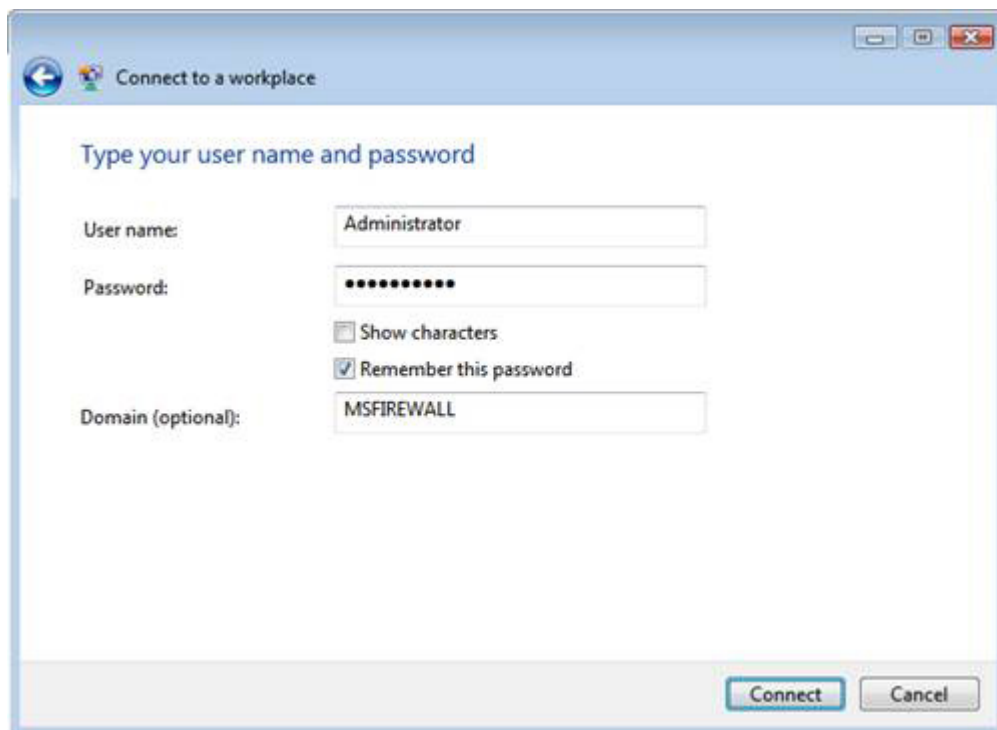
Hình 9

5. Trên cửa sổ **Type the Internet address to connect to**, nhập vào đó tên của máy chủ **SSL VPN**. Bảo đảm rằng tên này giống với tên chung trên chứng chỉ đã được sử dụng bởi máy chủ SSL VPN. Trong ví dụ này, tên của nó là **sstp.msfirewall.org**. Nhập vào **Destination Name**. Trong ví dụ này chúng tôi sẽ đặt tên **SSL VPN** đích. Kịch **Next**.



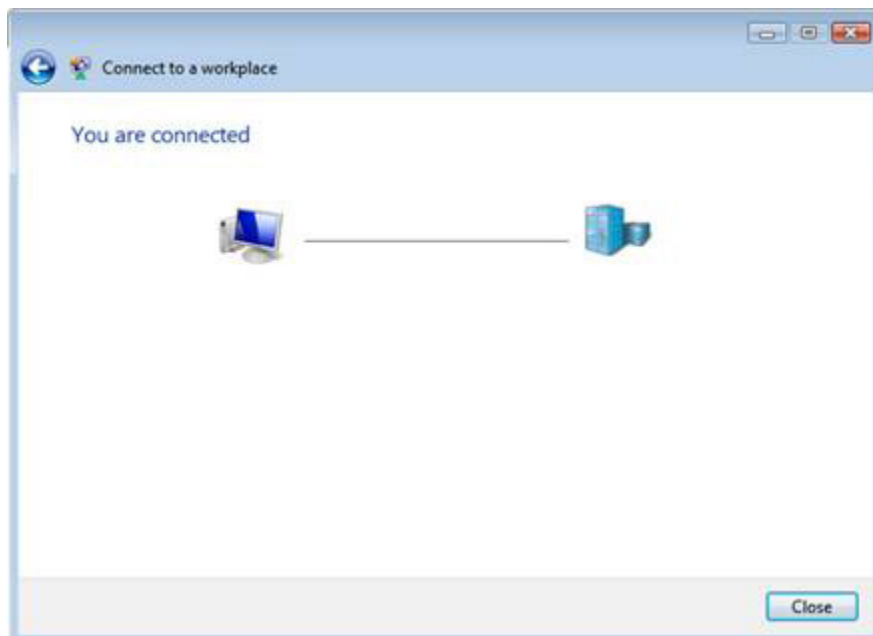
Hình 10

6. Trên cửa sổ **Type your user name and password**, nhập vào **Password** và **Domain**. Kích **Connect**.



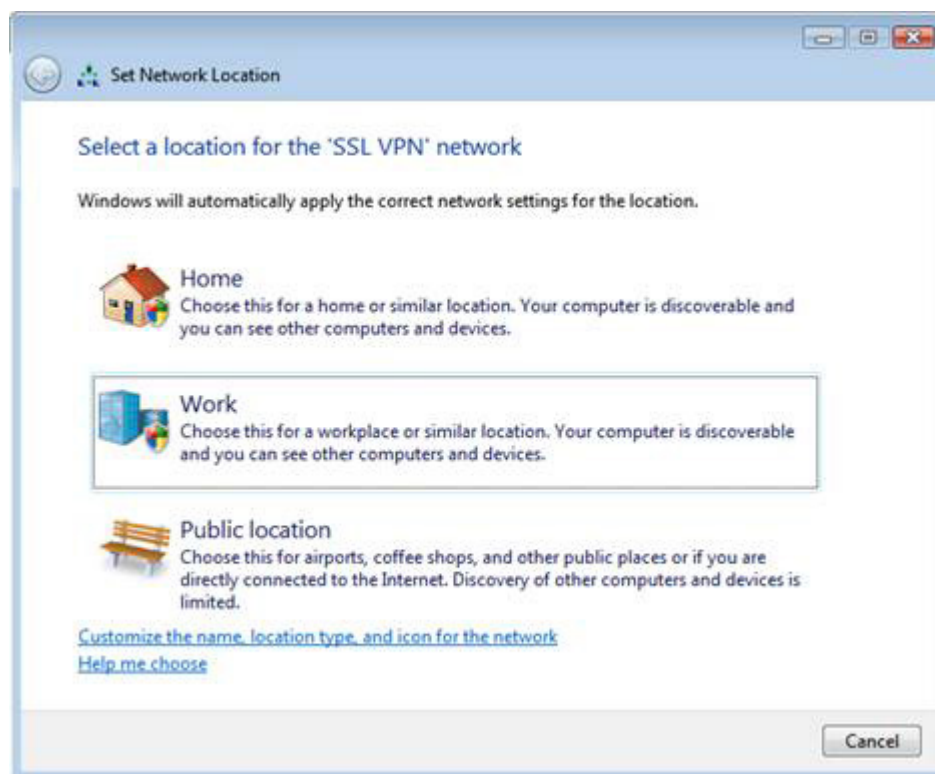
Hình 11

7. Kích **Close** trên cửa sổ **You are connected**.



Hình 12

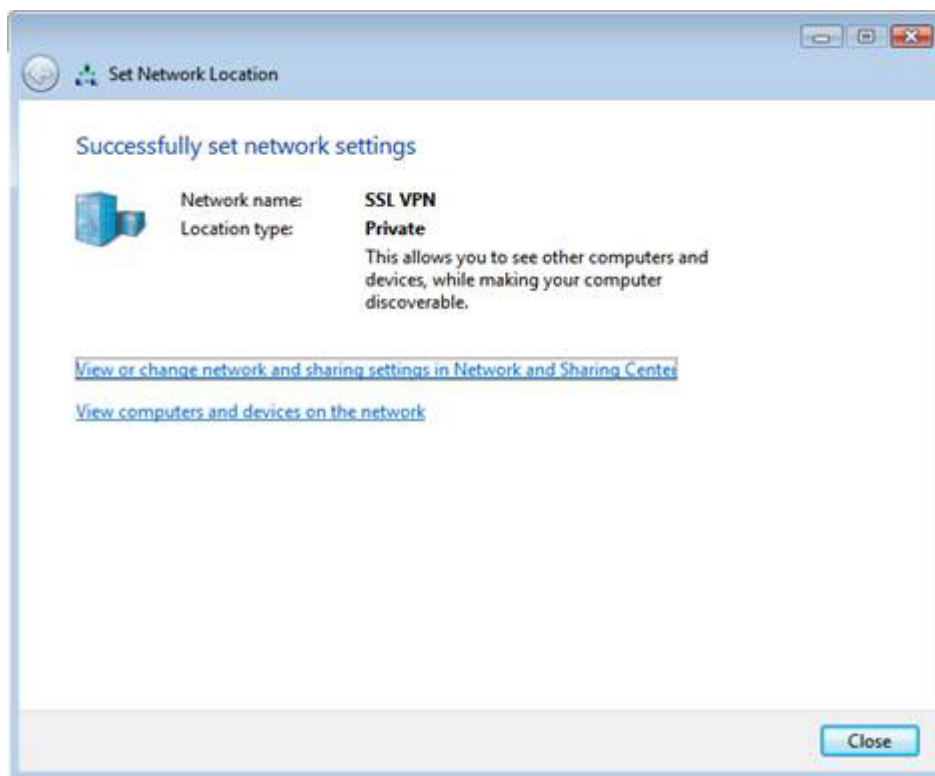
8. Trên cửa sổ **Select a location for the “SSL VPN” network**, chọn tùy chọn **Work**.



Hình 13

9. Kích **Continue** trong lời nhắc của UAC.

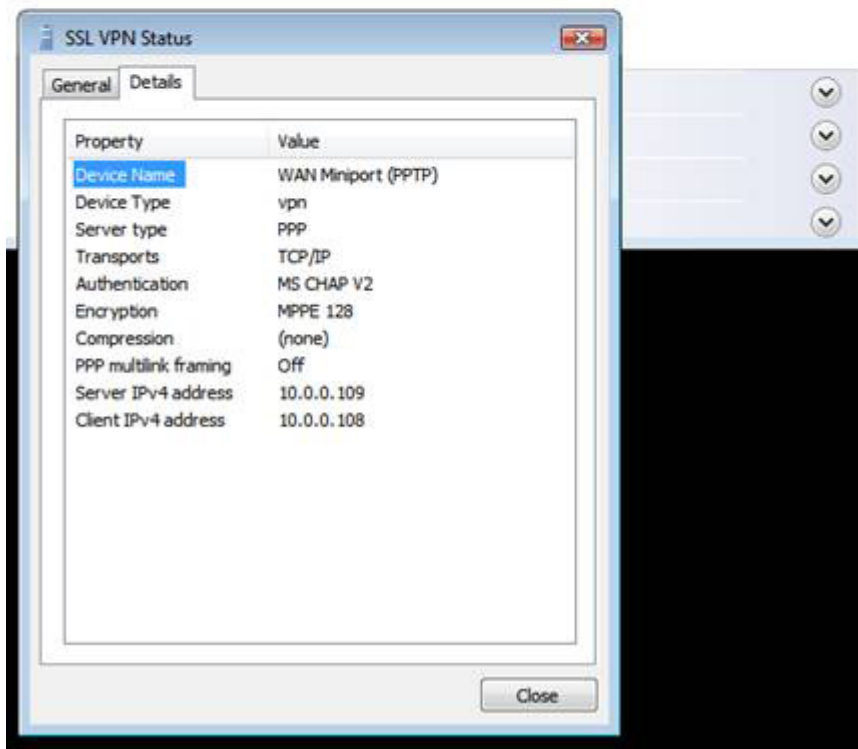
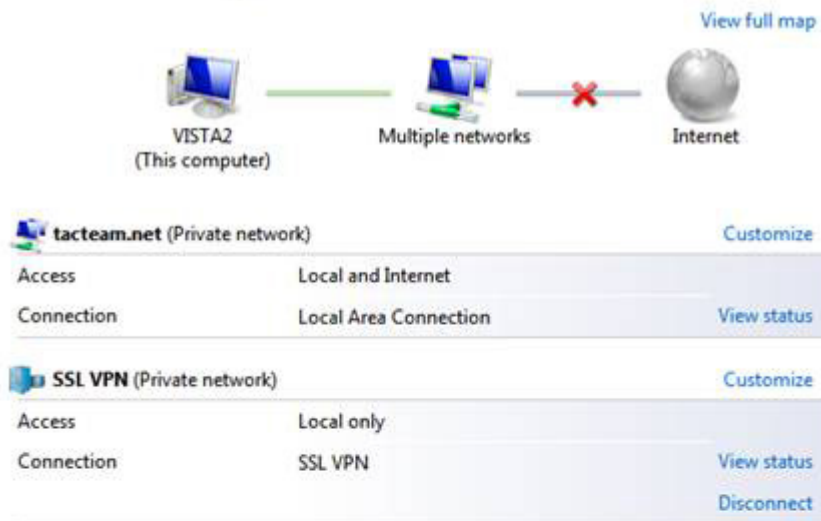
10. Kích **Close** trên cửa sổ **Successfully set network settings**



Hình 14

11. Trong **Network and Sharing Center**, kích vào liên kết **View status** trong phần **SSL VPN**, có thể tham khảo trong hình bên dưới. Bạn sẽ thấy trong hộp thoại **SSL VPN Status** kiểu kết nối VPN này là **PPTP**. Kích **Close** trong hộp thoại **SSL VPN Status**.

## Network and Sharing Center



Hình 15

12. Mở cửa sổ lệnh và **ping** đến domain controller. Trong ví dụ này, địa chỉ IP của domain controller là **10.0.0.2**. Nếu kết nối VPN được thực hiện thành công thì bạn sẽ nhận được một reply của quá trình ping từ domain controller.

```
Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\tshinder>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=31ms TTL=127
Reply from 10.0.0.2: bytes=32 time=3ms TTL=127
Reply from 10.0.0.2: bytes=32 time=2ms TTL=127
Reply from 10.0.0.2: bytes=32 time=3ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 31ms, Average = 9ms

C:\Users\tshinder>_
```

Hình 16

## Cấu hình Windows Server 2008 thành SSL VPN Server truy cập từ xa (Phần 4)

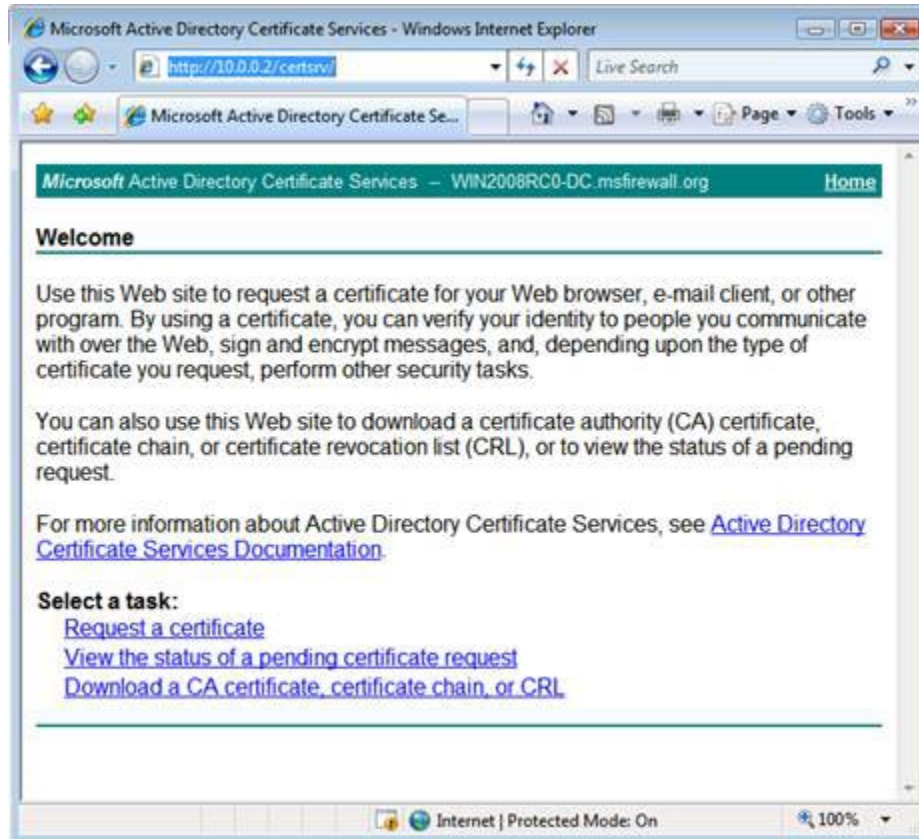
Nguồn : quantrimang.com

*Thomas Shinder*

### Đạt được chứng chỉ CA từ Enterprise CA

Máy khách SSL VPN cần phải tin cậy CA đã phát hành chứng chỉ được sử dụng bởi máy chủ VPN. Để thiết lập sự tin cậy này, chúng ta cần phải cài đặt chứng chỉ CA đã phát hành chứng chỉ của máy chủ VPN. Chúng ta có thể thực hiện điều này bằng việc kết nối đến Web site kết nạp trên CA trên mạng bên trong và cài đặt chứng chỉ trong kho lưu trữ chứng chỉ Trusted Root Certification Authorities của máy khách VPN. Thực hiện các bước dưới đây để có được chứng chỉ từ Web site kết nạp.

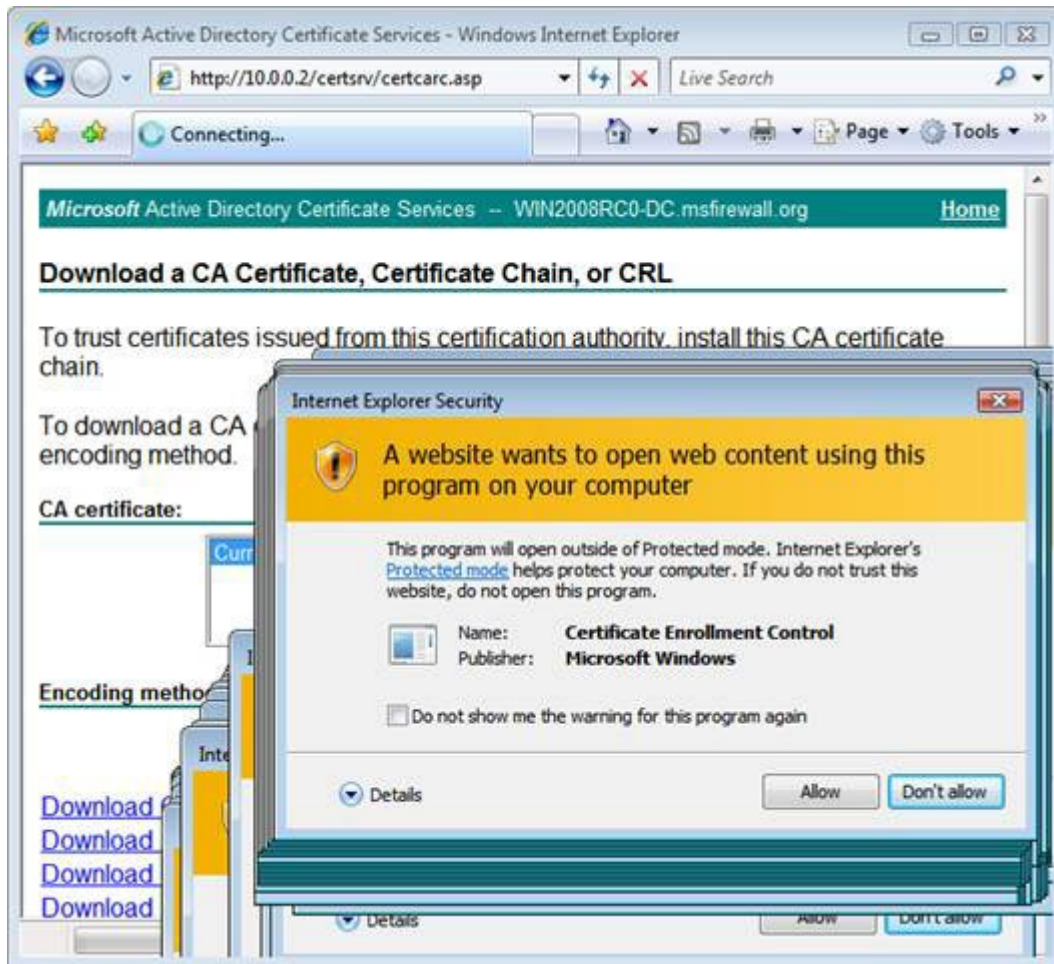
1. Trên máy khách VPN đã được kết nối với máy chủ VPN thông qua liên kết PPTP, nhập vào dòng **http://10.0.0.2/certsrv** trong thanh địa chỉ trong Internet Explorer và nhấn ENTER.
2. Nhập vào tên người dùng và mật khẩu hợp lệ trong hộp thoại cần thiết. Trong ví dụ này, chúng tôi sẽ sử dụng mật khẩu và tên người dùng của tài khoản quản trị viên miền mặc định.
3. Trong cửa sổ Welcome của Web site kết nạp, kích vào liên kết **Download a CA certificate, certificate chain, or CRL**.



Hình 17

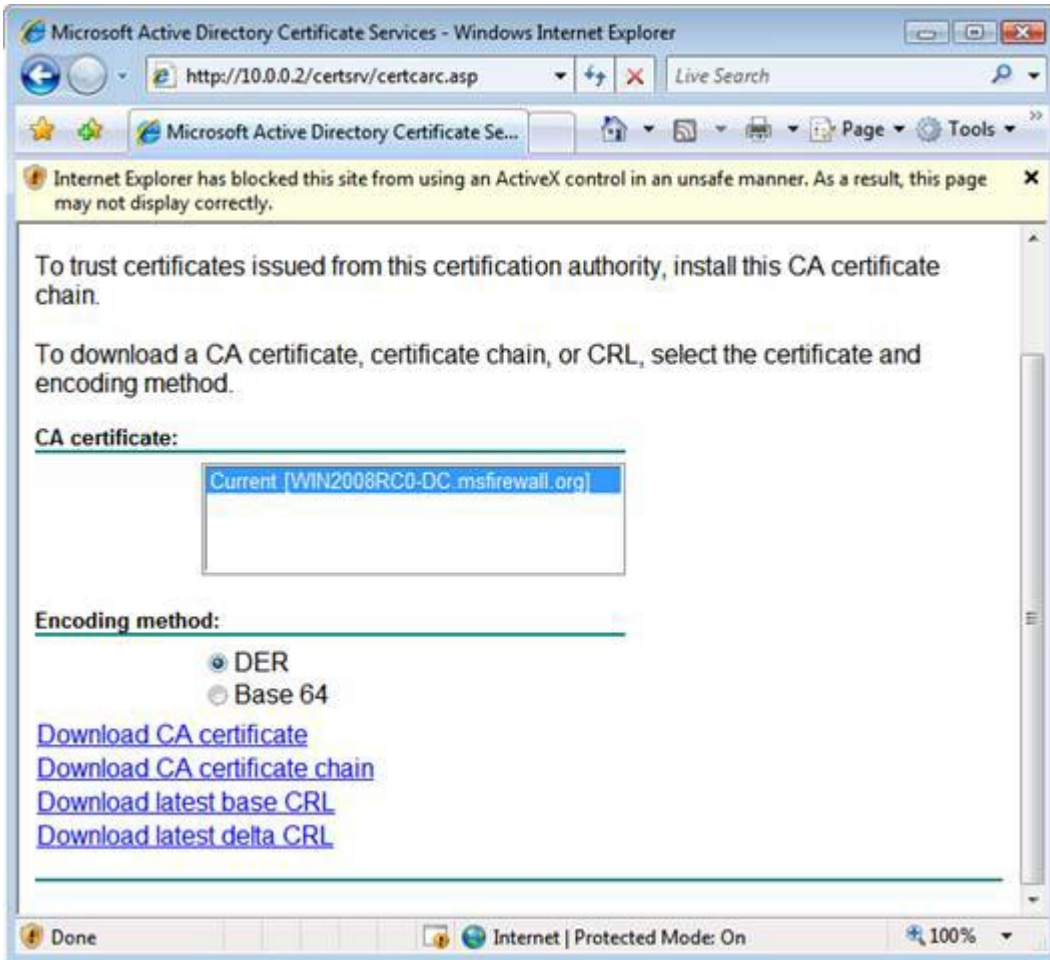
4. Kịch **Allow** trong hộp thoại cảnh báo rằng **A website wants to open web content using this program on your computer**. Sau đó kích **Close** trên hộp thoại **Did you notice the Information bar** nếu nó xuất hiện.





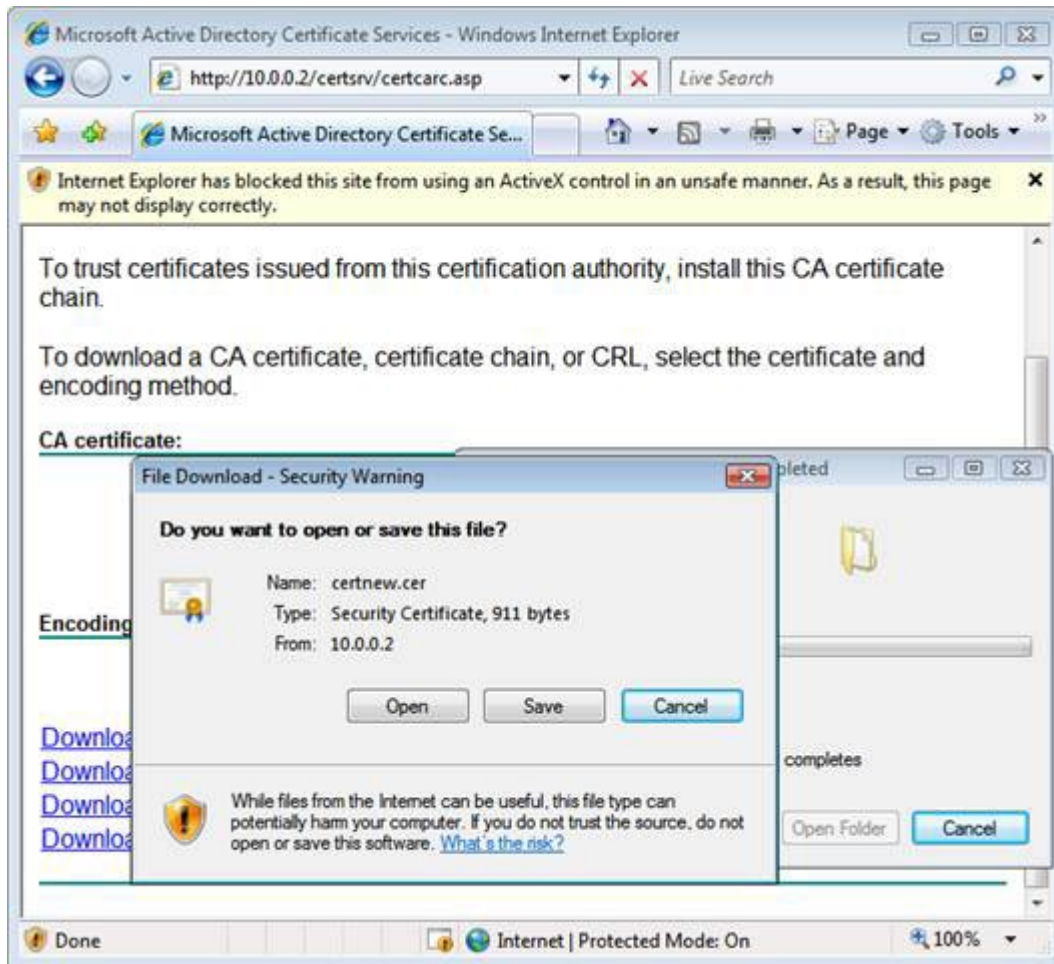
Hình 18

5. Lưu ý rằng các thông tin này cho bạn biết rằng Web site có thể làm việc không đúng, vì ActiveX control bị khóa. Tuy nhiên điều này không phải là một vấn đề, vì chúng tôi sẽ download một chứng chỉ CA và sử dụng Certificates MMC để cài đặt chứng chỉ. Kích vào liên kết **Download CA certificate**.



Hình 19

6. Trong hộp thoại **File Download – Security Warning**, kích nút **Save**. Lưu chứng chỉ vào Desktop.



Hình 20

7. Kích **Close** trong cửa sổ **Download complete**.

8. Đóng Internet Explorer.

Bây giờ chúng ta cần phải cài đặt chứng chỉ CA trong Trusted Root Certification Authorities Certificate Store của máy khách VPN. Thực hiện theo các bước dưới đây để cài đặt chứng chỉ:

1. Kích **Start** và sau đó nhập vào **mmc** trong hộp Search. Nhấn ENTER.

2. Kích **Continue** trong hộp thoại UAC

3. Trong cửa sổ **Console1**, kích menu File và sau đó kích tiếp **Add/Remove Snap-in**.

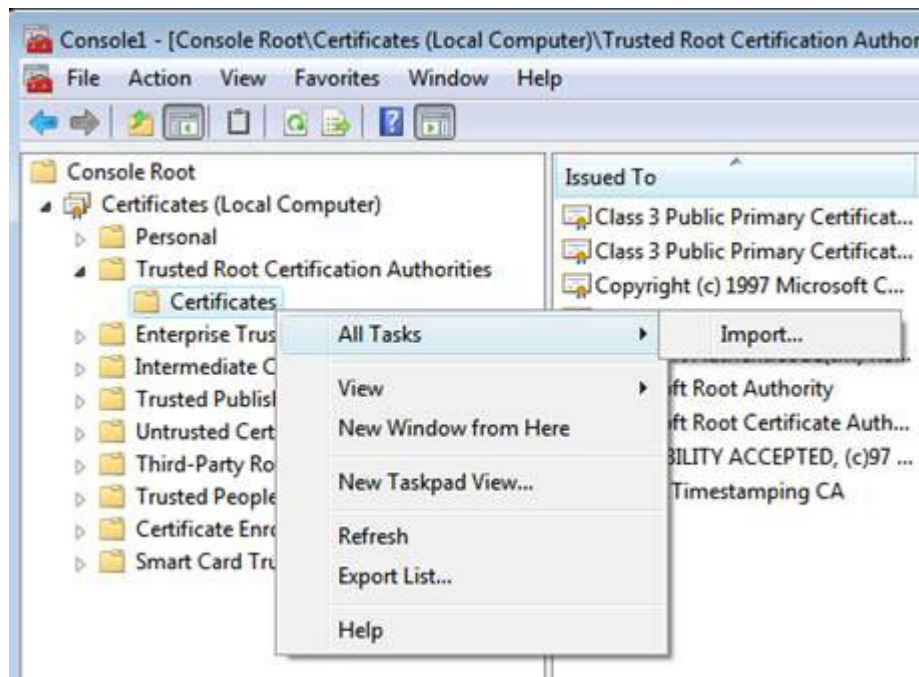
4. Trong hộp thoại **Add or Remove Snap-ins**, kích mục **Certificates** trong danh sách **Available snap-ins** và sau đó kích tiếp **Add**.

5. Trong cửa sổ **Certificates snap-in**, chọn tùy chọn **Computer account** và kích **Finish**.

6. Trong cửa sổ **Select Computer**, chọn tùy chọn **Local computer** và kích **Finish**.

7. Kích **OK** trong hộp thoại **Add or Remove Snap-ins**

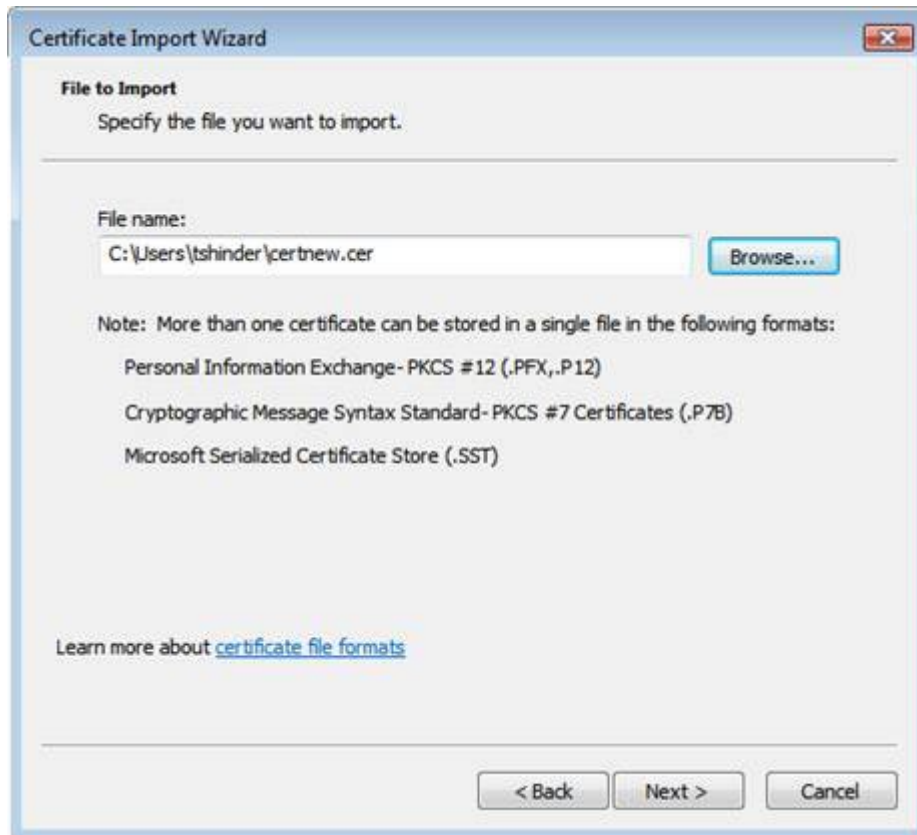
8. Trong phần giao diện điều khiển bên trái, mở nút **Certificates (Local Computer)** và sau đó vào nút **Trusted Root Certification Authorities**. Kích nút **Certificates**. Kích chuột phải vào nút **Certificates**, trở đến **All Tasks** và kích **Import**.



Hình 21

9. Kích **Next** trên cửa sổ **Welcome to the Certificate Import Wizard**

10. Trên cửa sổ **File to Import**, sử dụng nút **Browse** để tìm chứng chỉ, sau đó kích **Next**.



Hình 22

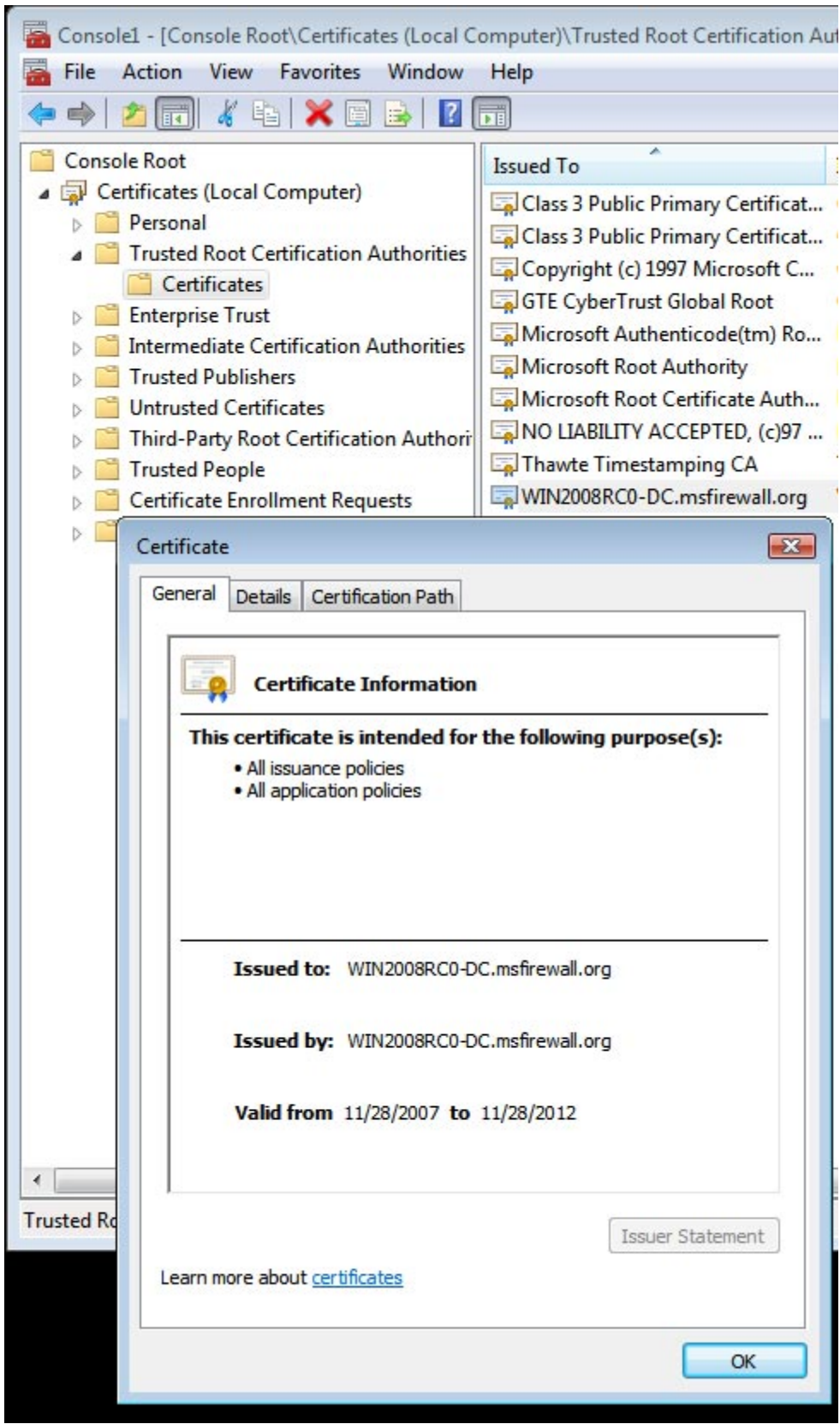
11. Trong cửa sổ **Certificate Store**, xác nhận rằng tùy chọn **Place all certificates in the following store** đã được chọn và kho lưu trữ **Trusted Root Certification Authorities** được liệt kê trong danh sách. Kích **Next**.



Hình 23

12. Kích **Finish** trong cửa sổ **Completing the Certificate Import**.
13. Kích **OK** trong hộp thoại cho bạn biết rằng việc import đã thành công.
14. Chứng chỉ lúc này sẽ xuất hiện trong giao diện điều khiển, bạn có thể thấy như trong hình bên dưới đây.





## Hình 24

15. Đóng giao diện điều khiển MMC.

### **Cấu hình máy khách để sử dụng SSTP và kết nối với máy chủ VPN bằng SSTP**

Lúc này chúng ta cần hủy kết nối đối với kết nối VPN và cấu hình máy khách VPN để có thể sử dụng SSTP cho giao thức VPN của nó. Trong môi trường sản xuất, bạn sẽ không có người dùng thực hiện bước này, lý do là vì bạn sẽ sử dụng Connection Manager Administration Kit để tạo kết nối VPN cho người dùng, điều đó sẽ thiết lập máy khách sử dụng SSTP, hoặc bạn sẽ chỉ cấu hình các cổng SSTP trên máy chủ VPN. Phụ thuộc vào từng môi trường, vì đôi khi bạn muốn người dùng có thể sử dụng PPTP trong lúc bạn đang triển khai các chứng chỉ. Rõ ràng bạn luôn có thể triển khai các chứng chỉ CA ngoài dải thông qua download hoặc email, đó là trong trường hợp bạn không cần cho phép PPTP. Nhưng sau đó, nếu đã có một số máy khách ở mức thấp không có sự hỗ trợ SSTP thì bạn sẽ cần phải cho phép PPTP hoặc L2TP/IPSec, chính vì vậy sẽ không thể vô hiệu hóa tất cả các cổng non-SSTP. Trong trường hợp đó, bạn sẽ phải phụ thuộc vào vấn đề cấu hình thủ công hoặc một gói CMAK mới được nâng cấp.

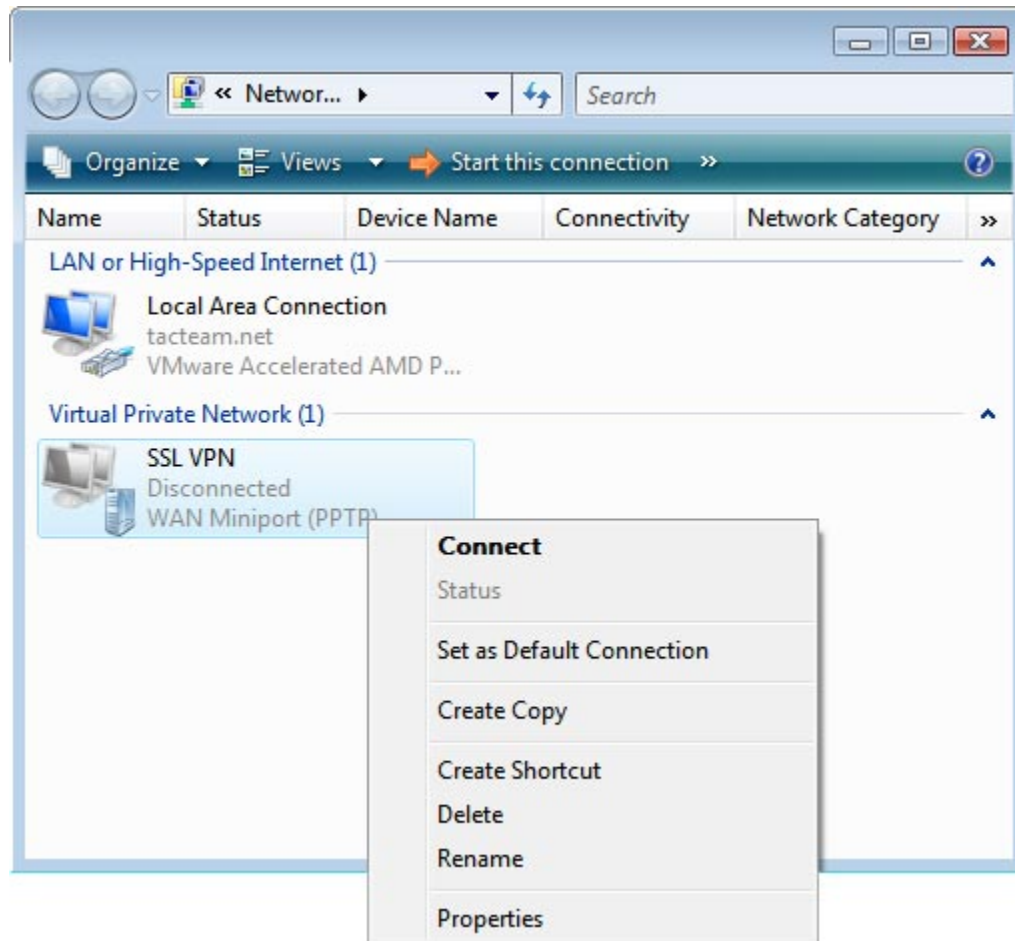
Một cách khác ở đây là đóng lại các bộ nghe SSTP đối với một địa chỉ IP nào đó trong máy chủ RRAS. Trong trường hợp này, bạn có thể tạo một gói CMAK tùy chỉnh để chỉ ra địa chỉ IP trên máy chủ SSL VPN đang nghe các kết nối SSTP đi đến. Các địa chỉ khác trên máy chủ SSTP VPN sẽ nghe các kết nối PPTP hoặc L2TP/IPSec.

Thực hiện các bước sau để hủy kết nối session PPTP và cấu hình kết nối máy khách VPN sử dụng SSTP:

1. Tại máy khách VPN, mở **Network and Sharing Center** như những gì bạn đã thực hiện từ trước.
2. Trong cửa sổ Network and Sharing Center, kích liên kết **Disconnect**, liên kết này nằm dưới liên kết **View Status** mà chúng ta đã sử dụng từ trước.
3. Session SSL VPN sẽ biến mất trong Network and Sharing Center.
4. Trong Network and Sharing Center, kích vào liên kết **Manage network connections**.

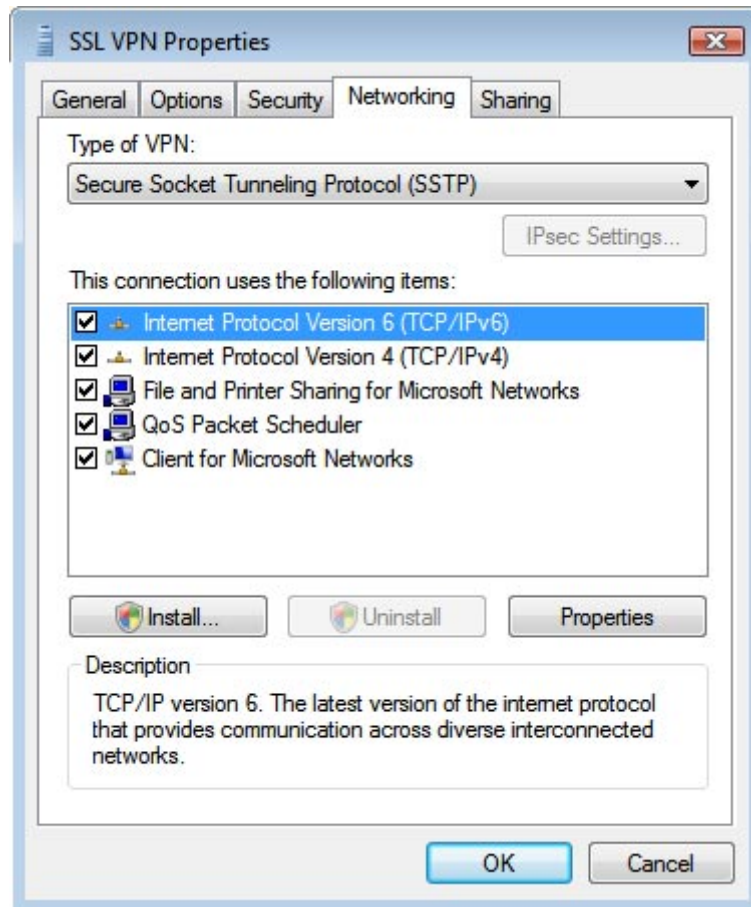


5. Kích chuột phải vào liên kết **SSL VPN** và kích **Properties**.



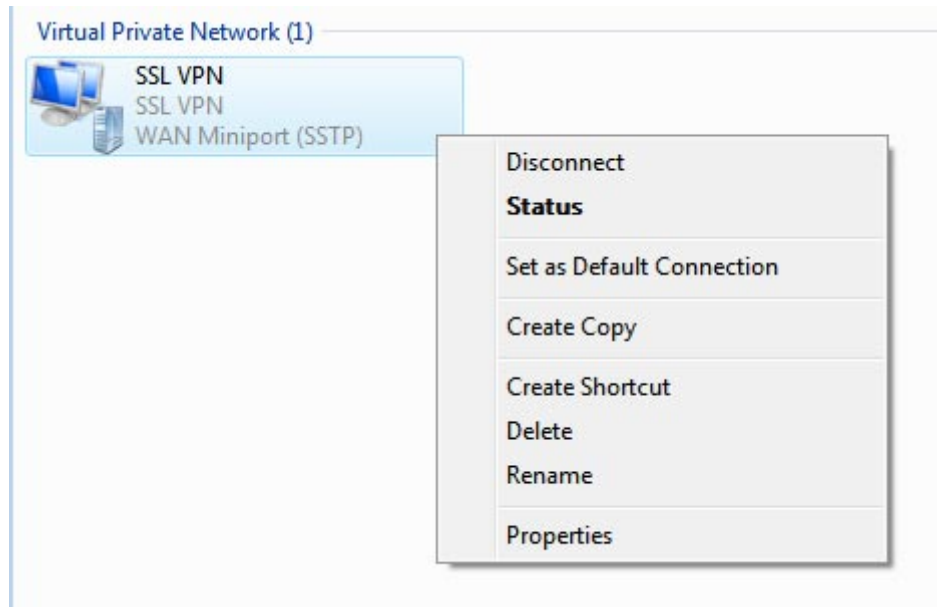
Hình 25

5. Trong hộp thoại **SSL VPN Properties**, kích tab **Networking**. Trong mục chọn **Type of VPN**, kích vào mũi tên xuống và chọn tùy chọn **Secure Socket Tunneling Protocol (SSTP)**, sau đó kích **OK**.



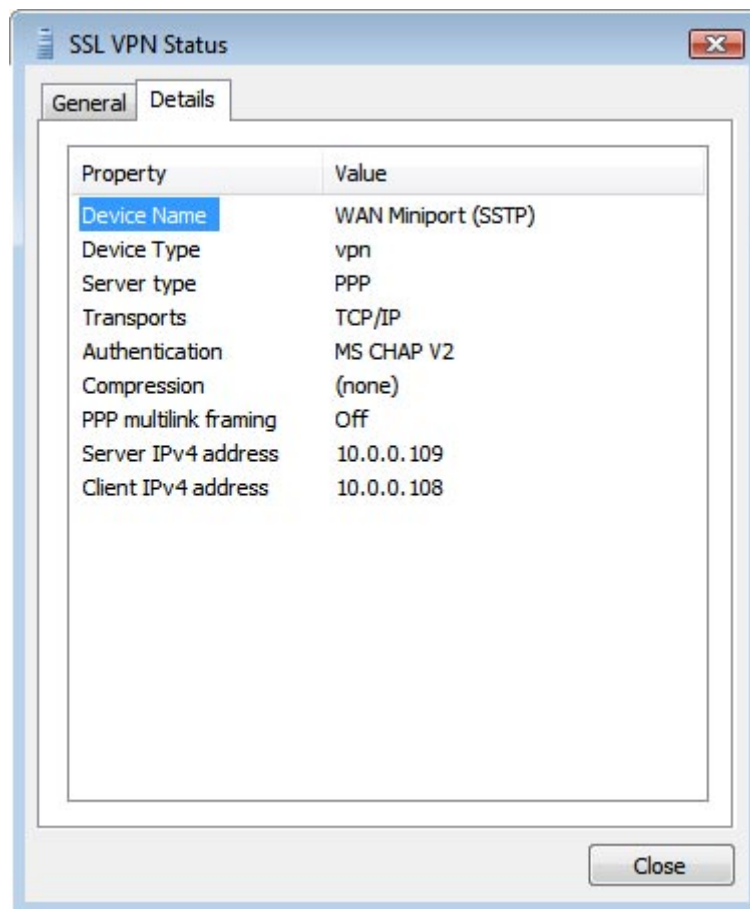
Hình 26

6. Kích đúp vào kết nối **SSL VPN** trong cửa sổ Network Connections
7. Trong hộp thoại **Connect SSL VPN**, kích nút **Connect**.
8. Khi kết nối được hoàn tất, kích chuột phải vào kết nối SSL VPN trong cửa sổ **Network Connections** và sau đó kích **Status**.



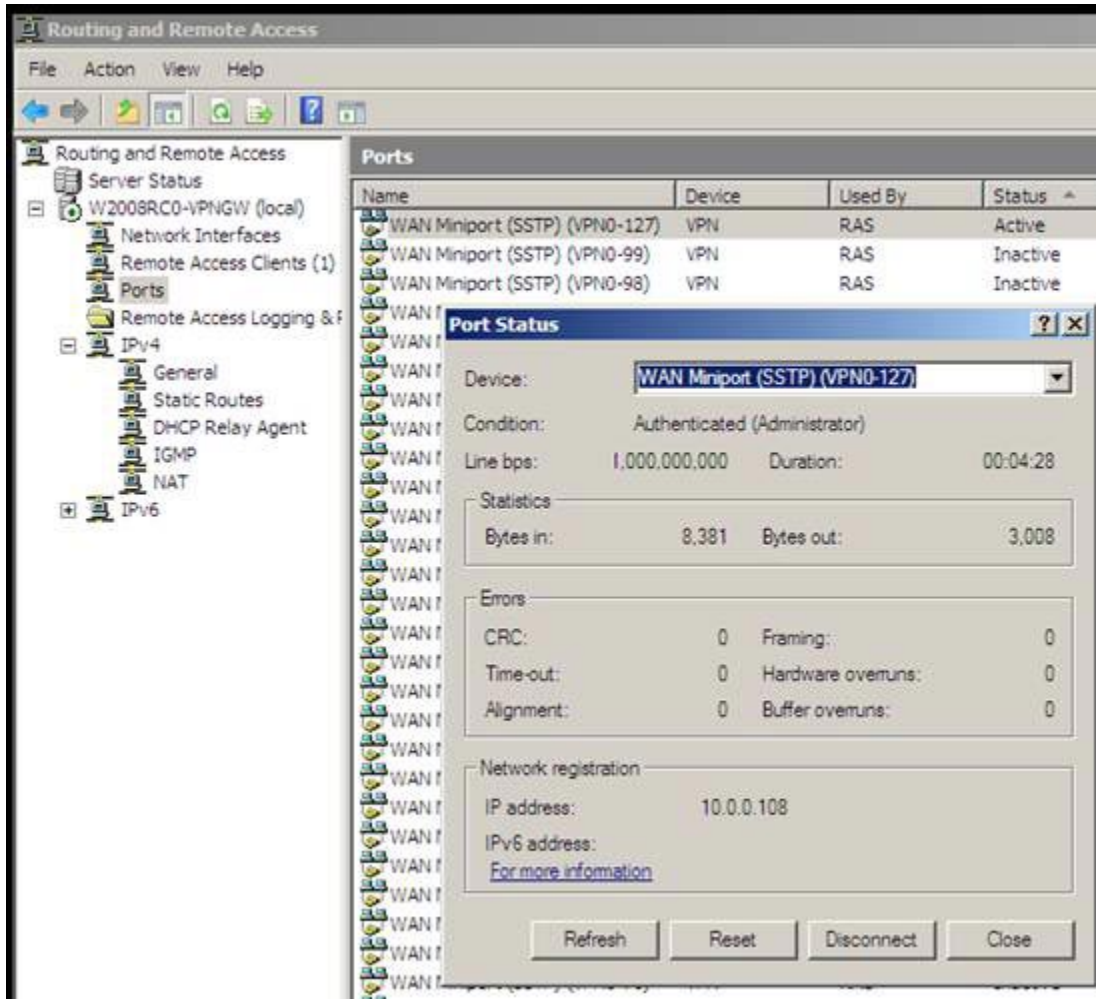
Hình 27

9. Trong hộp thoại **SSL VPN Status**, bạn có thể thấy được một kết nối **SSTP WAN Miniport** đã được thiết lập.



Hình 28

10. Nếu bạn vào máy chủ VPN và mở **Routing and Remote Access Console** thì sẽ nhận thấy rằng một kết nối SSTP đã được thiết lập.



Hình 29

## Kết luận

Trong phần ba này, phần cuối của loạt bài báo về cách kết hợp cùng nhau một máy chủ SSL VPN bằng cách sử dụng Windows Server 2008, chúng tôi đã hoàn tất cấu hình của tài khoản người dùng, CRL Web site, và máy khách SSL VPN. Kết thúc bài chúng tôi đã hoàn tất kết nối SSTP và xác nhận rằng nó đã thành công. Hy vọng bạn sẽ thấy được nhiều thú vị trong loạt bài này.

## Cấu hình Windows Server 2008 thành SSL VPN Server truy cập từ xa (Phần 1)

Nguồn : [quantrimang.com](http://quantrimang.com)

*Thomas Shinder*

**Truy cập từ xa (Remote Access) là một vấn đề rất quan trọng ngày nay. Khi số lượng người cần truy cập thông tin được lưu vào các máy tính gia đình và nơi làm việc tăng thì khả năng truy cập thông tin từ bất kỳ đâu trở thành một vấn đề vô cùng quan trọng. Bạn có thể nói rằng “Tôi sẽ có được thông tin cho bạn khi tôi vào được máy tính của tôi”. Bạn sẽ cần các thông tin đó nếu muốn cạnh tranh trong môi trường doanh nghiệp ngày nay.**

Trước kia, cách truy cập thông tin từ xa trên máy tính được sử dụng thực hiện là sử dụng một kết nối quay số. Các kết nối RAS dial-up làm việc trên các đường điện thoại POTS (Plain Old Telephone Service) thông thường và có tốc độ đạt vào khoảng 56kbps. Tốc độ là một vấn đề lớn đối với các kết nối dial-up RAS, tuy nhiên một vấn đề lớn hơn là chi phí cho các kết nối đối với khoảng cách dài cần có cho việc truy cập.

Với sự lớn mạnh của Internet, các kết nối dial-up RAS dần dần không còn thích đáng. Điều đó là do xuất hiện các mạng riêng ảo (VPN). Các kết nối mạng riêng ảo đã mang đến những kết nối điểm – điểm mà các kết nối quay số đã cung cấp nhưng với giá cả rẻ hơn và tốc độ nhanh hơn nhiều, tốc độ của kết nối mạng riêng ảo có thể nhanh bằng kết nối Internet và chi phí của kết nối hoàn toàn không phụ thuộc vào khoảng cách của đích. Chi phí chỉ phụ thuộc vào kết nối Internet.

### **Mạng riêng ảo (VPN)**

Kết nối mạng riêng ảo cho phép một máy tính có thể thiết lập một kết nối *riêng* và *ảo* đối với một mạng trên Internet. Kết nối là *ảo* bởi khi máy tính thiết lập một kết nối VPN thông qua Internet, máy tính tạo ra các hoạt động kết nối như một nút được nối trực tiếp trong mạng thông qua cáp Ethernet. Người dùng có thể truy cập vào tất cả các tài nguyên có thể, như là được kết nối trực tiếp vào mạng. Mặc dù vậy, trong trường hợp đối với kết nối VPN client đến một máy chủ VPN, kết nối này là một kết nối *ảo* vì không có kết nối Ethernet thực sự đến mạng đích. Kết nối là *riêng* vì các nội dung của luồng dữ liệu chuyển động bên trong kết nối VPN được mã hóa để không ai trên Internet có thể nghe trộm hoặc đọc được các nội dung của dữ liệu truyền thông đang chuyển động trong liên kết VPN.

Windows Servers và các client đã hỗ trợ các kết nối VPN ngay từ những ngày đầu của Windows NT và Windows 95. Các Windows client và server đều hỗ trợ kết nối VPN đến hàng thập kỷ qua, kiểu hỗ trợ VPN ngày càng được phát triển theo thời gian. Windows Vista Service Pack 1 và Windows Server 2008 hiện hỗ trợ đến 3 kiểu kết nối VPN, đó là:

- PPTP
- L2TP/IPSec
- SSTP

PPTP là giao thức kết nối điểm – điểm. PPTP là phương pháp đơn giản nhất mà bạn có thể sử dụng để thiết lập một kết nối VPN, tuy nhiên có một điều không may mắn là nó cũng có độ bảo mật kém nhất. Lý do là bởi các thông tin quan trọng của người dùng không được trao đổi qua một liên kết an toàn. Có thể nói rằng, việc mã hóa của kết nối VPN xảy ra sau khi các thông tin quan trọng được trao đổi. Tuy thông tin quan trọng không được truyền giữa các VPN client và VPN server, nhưng dữ liệu có thể bị tấn công bởi các hacker tinh vi truy cập vào máy chủ VPN và kết nối đến các mạng công ty.

Một giao thức có độ bảo mật tốt hơn đó là L2TP/IPSec. L2TP/IPSec là một phát triển hợp tác giữa Microsoft và Cisco. L2TP/IPSec an toàn hơn PPTP là bởi vì có một IPSec session được thiết lập trước khi các thông tin quan trọng được gửi đi trên dây tín hiệu. Các hacker không thể truy cập vào thông tin quan trọng của người dùng và như vậy không thể đánh cắp hoặc ăn trộm chúng để sử dụng cho các mục đích xấu. Một điểm quan trọng hơn nữa là IPSec cung cấp cơ chế chứng thực giữa các máy tính với nhau, chính vì vậy các máy tính không được tin cậy sẽ không thể kết nối vào L2TP/IPSec VPN gateway. IPSec còn cung cấp sự toàn vẹn dữ liệu, khả năng tin cậy và sự không thoái thác. L2TP hỗ trợ các cơ chế chứng thực PPP và EAP cho người dùng, các cơ chế này cho phép độ bảo mật đạt được mức cao vì cả việc chứng thực người dùng mà các chứng thực máy tính đều được yêu cầu ở đây.

Windows Vista SP1 và Windows Server 2008 hiện hỗ trợ một giao thức VPN mới - Secure Socket Tunneling Protocol hay SSTP. SSTP sử dụng các kết nối HTTP đã được mã hóa SSL để thiết lập một kết nối VPN đến VPN gateway. SSTP là một giao thức rất an toàn vì các thông tin quan trọng của người dùng không được gửi cho tới khi có một “đường hầm” SSL an toàn được thiết lập với VPN gateway. SSTP cũng được biết đến với tư cách là PPP trên SSL, chính vì thế nó cũng có nghĩa là bạn có thể sử dụng các cơ chế chứng thực PPP và EAP để bảo đảm cho các kết nối SSTP được an toàn hơn.

**Riêng tư nhưng không có nghĩa là bảo mật tốt**

Tôi cần phải nhắc nhở các bạn ở đây rằng các kết nối VPN thiên về tính riêng tư hơn là bảo mật. Khi tôi nhận ra rằng sự riêng tư là một thành phần chính của các truyền thông bảo mật, thì sự riêng tư bản thân nó lại không cung cấp sự bảo mật. Các công nghệ VPN cung cấp sự riêng tư về truyền thông trên Internet, việc này ngăn chặn kẻ lạ mặt có thể đọc được nội dung trong khi bạn thực hiện các công việc truyền thông. Công nghệ này cũng cho phép bạn trở nên an toàn vì chỉ người dùng được chứng thực mới có thể kết nối vào mạng thông qua VPN gateway. Tuy vậy sự riêng tư, chứng thực và thẩm định không cung cấp một giải pháp bảo mật toàn diện.

Ví dụ bạn có một nhân viên và bạn muốn công nhận sự truy cập VPN của anh ta. Trong khi các giao thức Windows Server 2008 VPN hỗ trợ chứng thực người dùng EAP, còn bạn quyết định triển khai các thẻ thông minh đến người dùng và sử dụng giao thức L2TP/IPSec VPN. Sự kết hợp của các thẻ thông minh và L2TP/IPSec giúp bạn an toàn hơn khi có chứng thực người dùng và máy tính tốt. Giải pháp thẻ thông minh và L2TP/IPSec làm việc tốt và mọi người đều hài lòng về nó.

Mọi việc đều tốt cho đến một ngày nọ khi một người dùng kết nối vào máy chủ SQL để truy cập các thông tin tiền lương phải trả cho nhân viên và làm lộ thông tin đó đến các nhân viên. Điều gì sẽ xảy ra? Liệu kết nối VPN có bảo mật trong trường hợp này? Chúng ta có thể khẳng định nó bảo mật trong một khía cạnh nào đó xét về tính riêng tư, chứng thực và thẩm định, nhưng có một thứ mà nó không cung cấp đó là kiểm soát sự truy cập, đây lại là khía cạnh quan trọng nhất đối với việc bảo mật máy tính.

Để giải pháp VPN là an toàn đích thực, bạn cần bảo đảm cho VPN gateway có thể thực hiện được việc kiểm soát truy cập dựa trên các người dùng hay nhóm để có thể thi hành sự truy cập đặc quyền tối thiểu đối với người dùng. Các VPN gateway tiên tiến và firewall như ISA Firewall đều có thể thực hiện được nhu cầu này đối với các kết nối VPN. Thêm vào đó các tường lửa tiên tiến như ISA Firewall còn có thể thực hiện việc kiểm tra lớp ứng dụng và gói đã được thẩm định về tình trạng an toàn trên các kết nối VPN client.

Mặc dù Windows Server 2008 VPN không cung cấp vấn đề kiểm soát truy cập user/group nhưng có một số cách mà bạn có thể thực thi kiểm soát truy cập trên bản thân các máy chủ dữ liệu nếu không muốn mất tiền để chi phí cho tường lửa ưu việt và VPN gateway. Trong bài này, chúng tôi chỉ tập trung vào thành phần máy chủ VPN.

### **Tại sao lại cần có giao thức VPN mới?**

Microsoft đã có hai giao thức VPN cho phép người dùng có thể kết nối đến mạng

công ty, vậy tại sao lại phải giới thiệu thêm giao thức thứ ba? SSTP là một tuyệt vời đối với người dùng VPN vì SSTP không có các vấn đề với tường lửa và thiết bị NAT mà PPTP và L2TP/IPSec vẫn bị mắc phải. Để PPTP làm việc thông qua thiết bị NAT thì thiết bị này cần phải hỗ trợ PPTP thông qua một PPTP “NAT editor”. Nếu không có NAT editor cho PPTP trên thiết bị NAT thì các kết nối PPTP sẽ bị thất bại.

L2TP/IPSec cũng có các vấn đề với các thiết bị NAT và tường lửa vì tường lửa cần có L2TP port UDP 1701 open outbound, IPSec IKE port, UDP 500 open outbound, và IPSec NAT traversal port, UDP 4500 open outbound (L2TP port được yêu cầu khi sử dụng NAT-T). Hầu hết các tường lửa tại những nơi công cộng như khách sạn, trung tâm hội thảo, nhà hàng và các địa điểm khác chỉ cho phép một số cổng nhỏ open outbound, như HTTP, TCP port 80 và HTTPS (SSL), TCP port 443. Nếu bạn cần hỗ trợ cho các giao thức khác với HTTP và SSL khi rời văn phòng thì bạn đang rất mạo hiểm.

Ngược lại, các kết nối SSTP VPN tạo một đường hầm trên SSL bằng TCP port 443. Khi tất cả các tường lửa và thiết bị NAT có TCP port 443 mở, bạn sẽ có thể sử dụng SSTP bất cứ nơi đâu. Điều này đã đơn giản tuyệt vời cho cuộc sống đối với các nhân viên “trên đường”, những người thực sự cần sử dụng các kết nối VPN đến văn phòng để làm việc và nó cũng làm cho cuộc sống trở lên dễ dàng hơn rất nhiều đối với các quản trị viên công ty, những người cần hỗ trợ cho các nhân viên trên đường, cũng như cả những nhân viên trợ giúp tại các nhà cung cấp dịch vụ, những người cung cấp truy cập Internet cho khách sạn, hội thảo và các địa điểm công cộng khác.

## **Quá trình kết nối SSTP**

Giới thiệu dưới đây là cách tiến trình kết nối SSTP làm việc thế nào:

1. SSTP VPN client thiết lập một kết nối TCP với SSTP VPN gateway giữa một cổng nguồn TCP ngẫu nhiên trên SSTP VPN client và TCP port 443 trên SSTP VPN gateway.
2. SSTP VPN client gửi một thông báo SSL Client-Hello, thông báo này chỉ thị rằng SSTP VPN client muốn thiết lập một SSL session với SSTP VPN gateway.
3. SSTP VPN gateway gửi một chứng chỉ máy tính của nó đến SSTP VPN client.
4. SSTP VPN client hợp lệ hóa chứng chỉ này bằng cách kiểm tra kho lưu trữ các chứng chỉ thẩm định chứng chỉ gốc tin cậy của nó để xem chứng chỉ CA có được đặt trong kho lưu trữ đó không. Sau đó SSTP VPN client xác định phương pháp mã hóa cho SSL session, tạo khóa SSL session và mã hóa nó với



khóa công của SSTP VPN gateway, và sau đó gửi biểu mẫu đã mã hóa của khóa SSL session đến SSTP VPN gateway.

5. SSTP VPN gateway giải mã khóa SSL session đã mã hóa bằng một khóa riêng của nó. Tất cả truyền thông sau này giữa SSTP VPN client và SSTP VPN gateway đều được mã hóa bằng phương pháp mã hóa đã được dàn xếp và khóa SSL session.

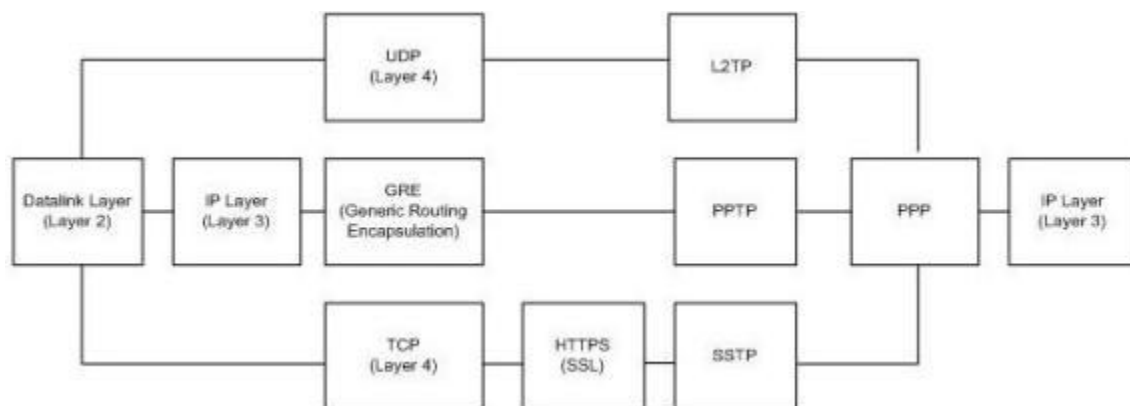
6. SSTP VPN client gửi một thông báo thỉnh cầu HTTP trên SSL (HTTPS) đến SSTP VPN gateway.

7. SSTP VPN client thương lượng một đường hầm SSTP với SSTP VPN gateway.

8. SSTP VPN client thương lượng kết nối PPP với máy chủ SSTP. Sự thương lượng này gồm có việc thẩm định các chứng chỉ của người dùng bằng phương pháp chứng thực PPP chuẩn (hoặc thậm chí là chứng thực EAP) và cấu hình các thiết lập cho lưu lượng Internet Protocol version 4 (IPv4) hoặc Internet Protocol version 6 (IPv6).

9. Lúc này SSTP VPN client bắt đầu gửi lưu lượng IPv4 hoặc IPv6 trên liên kết PPP.

Nếu là người quan tâm đến các đặc điểm của kiến trúc giao thức VPN, thì các bạn có thể xem trong hình bên dưới. Chú ý rằng SSTP có thêm một header so với hai giao thức VPN trước đó. Điều này là vì sự đóng gói HTTPS bổ sung vào SSTP header. L2TP và PPTP không có các header lớp ứng dụng trong việc đóng gói truyền thông.



Hình 1

Chúng ta sẽ sử dụng một ví dụ mạng ba máy tính đơn giản để thể hiện cách SSTP làm việc như thế nào. Các tên và đặc điểm của ba máy tính ở đây là:

**Vista:**

Vista Business Edition  
Vista Service Pack 1  
Thành viên không thuộc miền

**W2008RC0-VPNGW:**

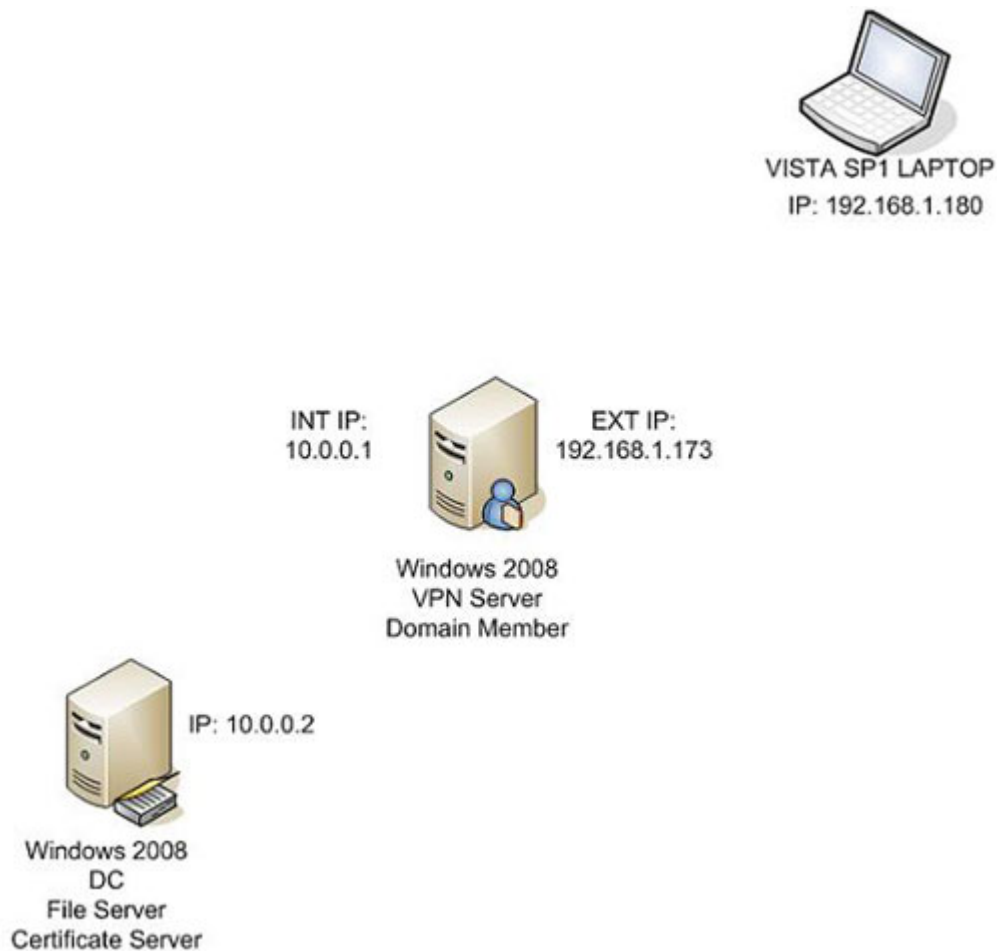
Windows Server 2008 Enterprise Edition  
Hai NICs – Internal và External  
Thành viên miền

**WIN2008RC-DC:**

Windows Server 2008 Enterprise Edition  
Domain Controller of MSFIREWALL.ORG domain  
DHCP Server  
DNS Server  
Certificate Server (Enterprise CA)

Lưu ý rằng bạn phải sử dụng Vista Service Pack 1 cho VPN client. Tuy đã có những tranh luận trước đây về Windows XP Service Pack 3 trong việc hỗ trợ SSTP, nhưng điều này không quan trọng. Gần đây chúng tôi đã cài đặt phiên bản ứng viên “candidate” cho Windows XP Service Pack 3 trên các máy tính thử nghiệm và đã phát hiện không có gì về hỗ trợ SSTP. Đây quả thực là một điều đáng tiếc vì có rất nhiều laptop hiện đang cài đặt Windows XP và hầu hết đều có ý kiến cho rằng Vista chạy quá chậm đối với các laptop. Có lẽ các vấn đề về hiệu ứng của Vista sẽ được sửa đổi trong bản Vista Service Pack 1.

Cấu hình mức cao của mạng ví dụ có thể thấy ngay trong hình bên dưới.



Hình 2

## Kết luận

Trong bài này, chúng tôi đã giới thiệu cho các bạn một chút lịch sử về các truyền thông truy cập từ xa đối với các mạng máy tính. Sau đó chúng tôi đã giới thiệu đến các giao thức VPN chủ yếu được hỗ trợ trong Windows Server và client, giới thiệu một số vấn đề bảo mật đối với các giao thức VPN trước đó. Giới thiệu cách SSTP giải quyết các vấn đề đó như thế nào với hai kiểu giao thức trước đó là PPTP và L2TP/IPSec. Cuối cùng chúng tôi cũng đưa ra một mạng ví dụ đơn giản sẽ được sử dụng trong bài tiếp theo để giới thiệu thêm về giải pháp SSTP VPN client và server đơn giản bằng Windows Server 2008 và Windows Vista Service Pack 1.

Quản lý và tùy biến cấu hình Windows

**Với thiết kế đơn giản cùng các chức năng quản lý tùy biến rõ ràng và đầy đủ, WinASO EasyTweak 3.0 thật sự là công cụ hiệu quả mà người dùng nên lựa chọn để làm chủ hệ điều hành Windows.**

Giao diện sử dụng chính của WET 3.0 gồm 4 nhóm chức năng chính

1. Customize Computer: tùy biến hệ thống

\* **Start Menu and Taskbar**: bao gồm các chức năng chính như điều chỉnh các thành phần - tốc độ hiệu ứng và giao diện hiển thị trên menu Start hay thanh TaskBar (hỗ trợ kể cả Windows 7), cách hiển thị trong các mục thành

Tham khảo và tải bản WET3.0 mới nhất về dùng thử với dung lượng 5.87MB [tại đây](#).

phần chủ chốt trên hệ điều hành (My Documents, thùng rác, Control Panel...), hiệu ứng trong suốt của menu Start và thanh TaskBar.

Giao  
diện sử  
dụng của  
WinASO  
Easy  
Tweak

Lưu ý: Tùy biến xong chức năng nhấp Save để đồng ý với các xác lập.

\* **Control Panel:** gồm các xác lập cần thiết cho bảng trung tâm điều khiển Control Panel (ẩn hiện các thành phần tùy ý, che dấu hay vô hiệu hóa khả năng

sử dụng Control Panel), vô hiệu hóa việc sử dụng  
Add/Remove Programs...

Tùy  
chọn  
thiết  
lập ở  
Control  
Panel

\* **Windows Explorer:** các tùy chọn tinh chỉnh cần thiết cho Explorer như ẩn/hiện các thành phần hay phân vùng (ổ đĩa) hệ thống, chức năng tùy biến tập tin thư mục **Folder Options**, đặc biệt chức năng **Automatic Complete** giúp kích hoạt hay vô hiệu hóa việc sử dụng tự điền các mẫu danh sách tự động khi

xử lý nội dung văn bản trên các chương trình chuyên dụng.

Tự  
động  
gợi ý  
nội  
dung  
khi  
điền  
thông  
tin

\* **Desktop:** các tùy biến cao cấp phân quyền sử dụng Desktop cho người dùng như ẩn hiện các icon, đổi tên thùng rác, không cho thay đổi xác lập trên desktop...

\* **System:** tùy biến hệ thống như hiện thông báo khi dung lượng đĩa cứng xuống thấp, cách thể hiện Font chữ trong Context menu, vô hiệu hóa sử dụng Registry...

## 2. System Maintain: bảo dưỡng hệ thống

\* **StartUp Manager:** quản lý hiệu quả các tiến trình khởi động cùng lúc với Windows.

\* **Task Manager:** quản lý các tiến trình chạy nền trên Windows.

\* **System Information:** cung cấp đầy đủ thông tin chi tiết về hệ thống – các thiết bị phần cứng kết nối trên máy để từ đó giúp bạn có thể phát hiện và khắc phục kịp thời các sự cố phát sinh tiềm ẩn về phần cứng.



tin chi  
tiết phần  
cứng

### 3. Internet Explorer Setting: thiết lập trình duyệt

\* **IE Appearance:** bao gồm các xác lập về phong cách hiển thị của trình duyệt IE như thay đổi nội dung thanh TitleBar, vô hiệu hóa Internet Options, ngăn việc download dữ liệu – lưu – xem mã nguồn, cũng như các chế độ ActiveX nguy hiểm...)

Thiết  
lập  
cho  
trình  
duyet

## IE

\* **IE Favorites:** thiết lập và theo dõi các địa chỉ trang web thường truy cập.

\* **IE History Manager:** quản lý và theo dõi trực tiếp lịch sử các URL thường xuyên truy cập (các địa chỉ này sẽ không bị mất đi khi sử dụng chức năng Clean History trên IE).

\* **IE Security Setting:** thêm một số tùy biến bảo mật cần thiết khác cho việc quản lý sử dụng IE chặt chẽ hơn (không cho hiển thị các video clip, không chạy âm thanh, không sao lưu mật khẩu vào bộ nhớ đệm, ngăn sử dụng một số tính năng trên hộp thoại **Internet Options** và một số tinh chỉnh phụ khác....)

4. Advanced Tools: tùy biến nâng cao

\* **Program Restrictor:** chức năng giúp phân quyền ngăn không cho sử dụng một số trình ứng dụng tùy ý nào đó (nhấp nút **Select Programs** để đưa vào các

ứng dụng cần khóa, nhấp Save để đồng ý với các xác lập).

## Hình

### 6

\* **Windows Optimizer:** với thuật toán thông minh tự động dò tìm và đưa ra các thông số thích hợp nhất cho hệ thống của bạn, tự động sửa lỗi hệ thống, thanh lý các thư viện động *DLL* dư thừa do quá trình cài đặt và gỡ bỏ ứng dụng, xử lý tối ưu bộ nhớ ảo - bộ nhớ Cache nhằm cải thiện và tăng tốc tối đa hệ thống máy tính.

\* **Connection Optimizer:** bao gồm các thông tin và gợi ý cần thiết cho sự chọn lựa tốt nhất cho kết nối mạng trên hệ thống của bạn.

\* **CD/DVD Setting:** gồm các xác lập về chế độ chơi multimedia trên hệ thống (vô hiệu hóa chế độ *autorun* của CDROM, xác lập ứng dụng mặc định chơi Audio - Video trên hệ thống).

Hình

7

Với sự toàn diện về tính năng và giao diện sử dụng đơn giản thuận tiện đây thật sự là một công cụ tùy biến và làm chủ Windows cho người dùng máy tính.

## Cài đặt và cấu hình DHCP Server trong Windows Server 2008

Việc đặt ra câu hỏi: "Làm thế nào để cài đặt và cấu hình DHCP server trong môi trường Windows Server 2008 nhằm mục đích cung cấp địa chỉ IP, cũng như các thông tin về DNS Server cho một giới hạn người dùng của mình" thực tế không khó giải quyết. Bởi với bài viết hướng dẫn sau đây, bạn hoàn toàn có thể tự mình tạo nên sự bất ngờ.



### Giới thiệu

Dynamic Host Configuration Protocol (DHCP) bản chất là một dịch vụ cơ sở hạ tầng có trên bất kì một hệ thống mạng nào nhằm cung cấp địa chỉ IP và thông tin DNS server tới các "PC client" hay một số

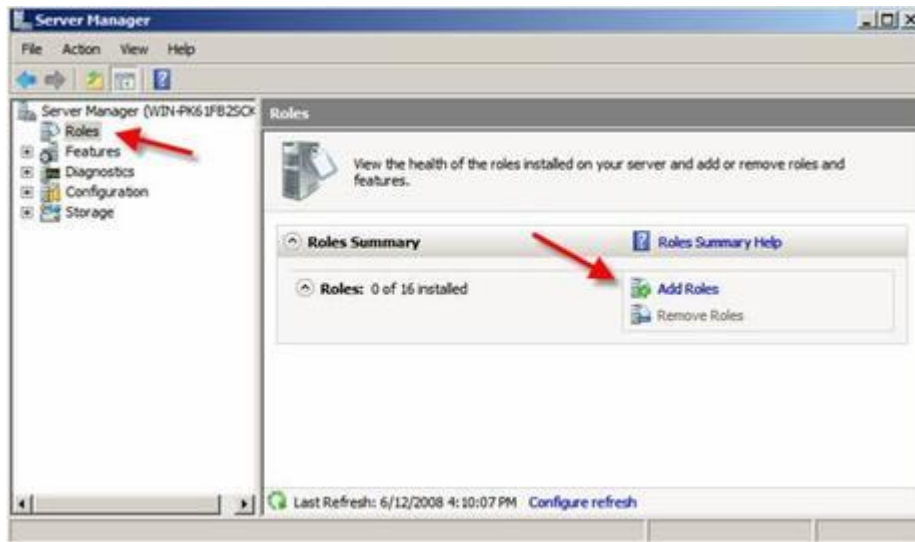
thiết bị khác. DHCP được sử dụng để giúp bạn không phải ấn định địa chỉ IP tĩnh cho tất cả các thiết bị có trong hệ thống mạng của mình và giúp bạn quản lý mọi vấn đề mà địa chỉ IP tĩnh có thể tạo ra. Qua từng thời kì, DHCP ngày càng phát triển để có thể thích hợp trong từng dịch vụ mạng mới giống như "Windows Health Service" hay "Network Access Protection (NAP)". Tuy nhiên, trước khi bạn có thể sử dụng nó để tìm kiếm các tiện ích thú vị mà DHCP mang lại cho mình, trước hết bạn cần cài đặt và cấu hình các đặc tính cơ bản. Sau đây, hãy xem hướng dẫn và tiến hành những gì bạn cần làm.

### **Cài đặt "Windows Server 2008 DHCP Server"**

Việc cài đặt "Windows Server 2008 DHCP Server" thực tế là việc dễ dàng. Các bạn cũng biết rằng DHCP Server hiện tại "đóng vai trò" là Windows Server 2008 - tức không phải là thành phần windows như nó ở trong quá khứ.

Do đó, để làm được điều chúng ta đang nói ở đây , bạn cần có hệ thống "Windows Server 2008" đã được cài đặt và cấu hình cùng với một địa chỉ IP tĩnh. Bên cạnh đó bạn còn cần biết phạm vi địa chỉ IP cho mạng của bạn, vì nhờ vào nó bạn sẽ kiểm soát được các "PC client", địa chỉ IP DNS Server hay các cổng vào mặc định. Bổ sung thêm một điều nữa, bạn cũng cần phải có một dự án cho tất cả các mạng lưới liên quan, những phạm vi nào bạn muốn xác định, hay liệt kê tạo ra những sự loại trừ nhất định. Vì có đầy đủ như thế, bạn mới làm thỏa mãn nhu cầu của chính mình.

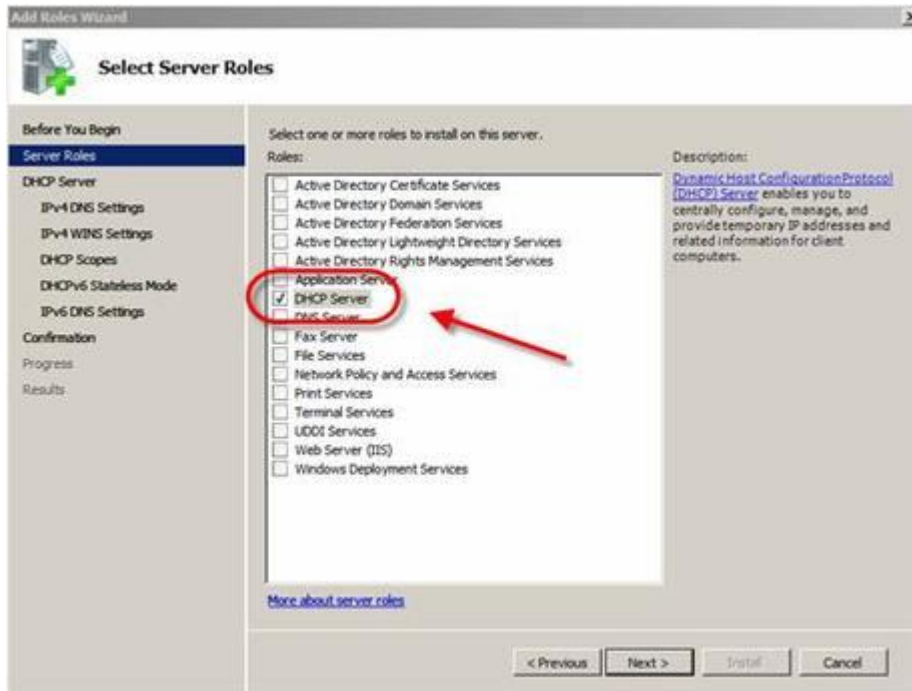
Bắt đầu quá trình cài đặt DHCP, bạn có thể click **Add Roles** từ cửa sổ **Initial Configuration Tasks** hay từ **Server Manager à Roles à Add Roles**



**HÌNH 1:** Thêm mới một Role trong Windows Server 2008

Khi bạn **Add Roles Wizard**, bạn có thể click **Next** hiển thị trên màn hình trong cửa sổ cài đặt sau. Tiếp theo, bạn chọn **DHCP Server Role** mà bạn muốn thêm vào và click **Next**





## HÌNH 2: Chọn DHCP Server Role

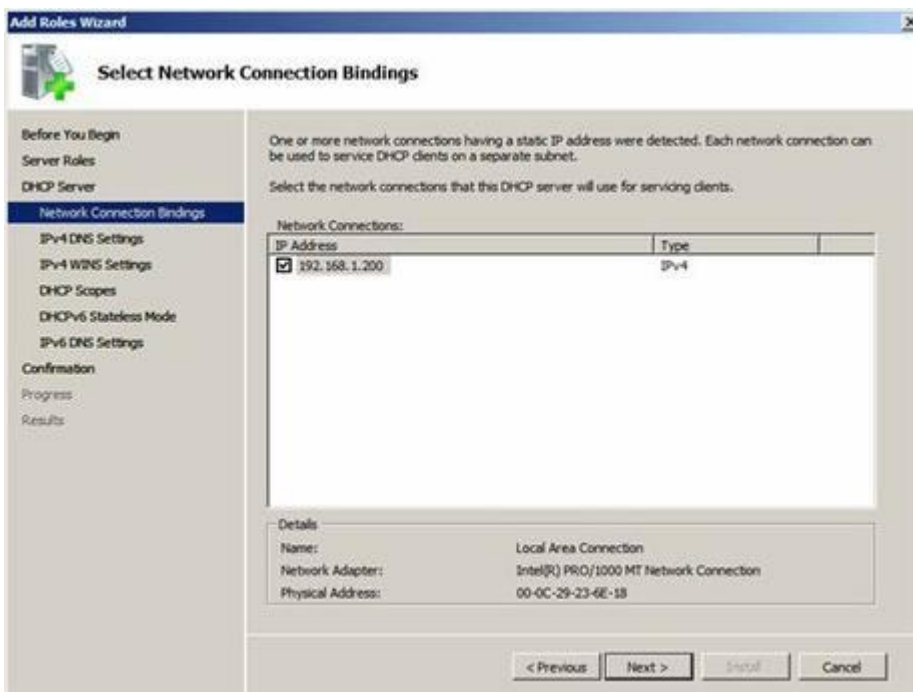
Nếu bạn không có một địa chỉ IP tĩnh để gán cho server của mình, bạn sẽ nhận được một thông báo rằng bạn sẽ không thể tiếp tục tiến hành quá trình cài đặt DHCP với một địa chỉ IP động. Do đó, đến điểm này, bạn sẽ bắt đầu cập nhật thông tin cho IP mạng bao gồm: thông tin về phạm vi và thông tin về DNS. Nếu bạn chỉ muốn cài đặt server DHCP với không một cấu hình nào cho bộ chỉ báo hay các thiết đặt cần

có, bạn có thể chỉ click Next mà không cần bạn tâm  
gì đến các câu hỏi có được trong tiến trình cài đặt.

Trên một phương diện khác, bạn có thể tùy chọn cấu  
hình Server DHCP của mình ở phần cài đặt này.

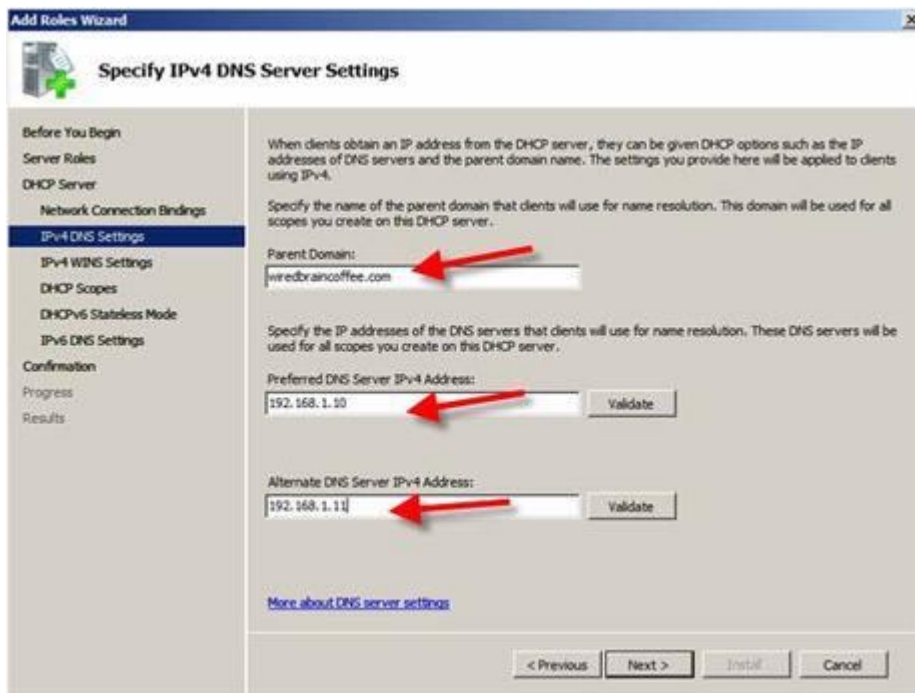
Trong trường hợp của tôi (tức chủ bài viết gốc), tôi  
nắm bắt thời cơ này để cấu hình một vài thiết đặt cơ  
bản cho IP và cấu hình phạm vi DHCP của tôi trước.

Hiện tôi đang hiển thị mạng liên kết kết nối của tôi và  
được đề nghị phải xác minh nó.



### HÌNH 3: Network connection binding

Ở trên có nói tới một đề nghị từ "wizard", và nội dung của nó là: "Giao diện bạn muốn cung cấp trên dịch vụ DHCP là gì?". Không biết các bạn như nào, nhưng ở đây tôi chọn mặc định và đã click Next. Tiếp theo, tôi cũng đã nhập vào **Parent Domain, Primary DNS Server, and Alternate DNS Server** của tôi (như bạn thấy bên dưới) và click **Next**

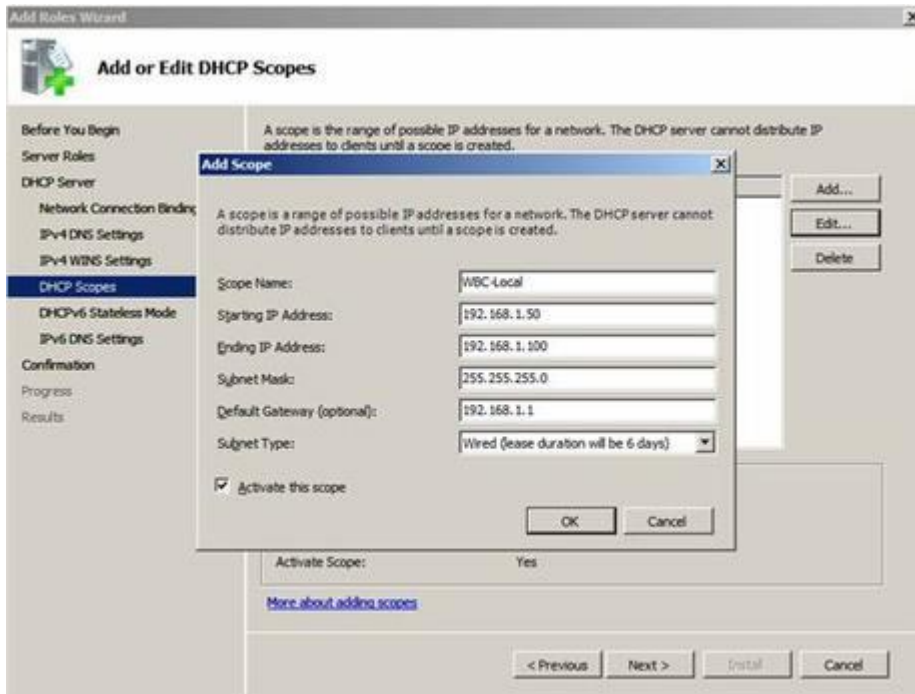


### HÌNH 4: Nhập tên domain và thông tin DNS

Tôi đã chọn NOT để sử dụng WINS trên mạng của tôi và đã click Next.

Sau đó, tôi đã điều chỉnh cấu hình phạm vi một DHCP cho Server DHCP mới, Tôi cũng đã chọn cấu hình phạm vi một địa chỉ IP của 192.168.1.50-100 theo 25+ PC Client trên giới hạn mạng của tôi. Để làm được điều này, tôi đã click Add để thêm vào một phạm vi mới.

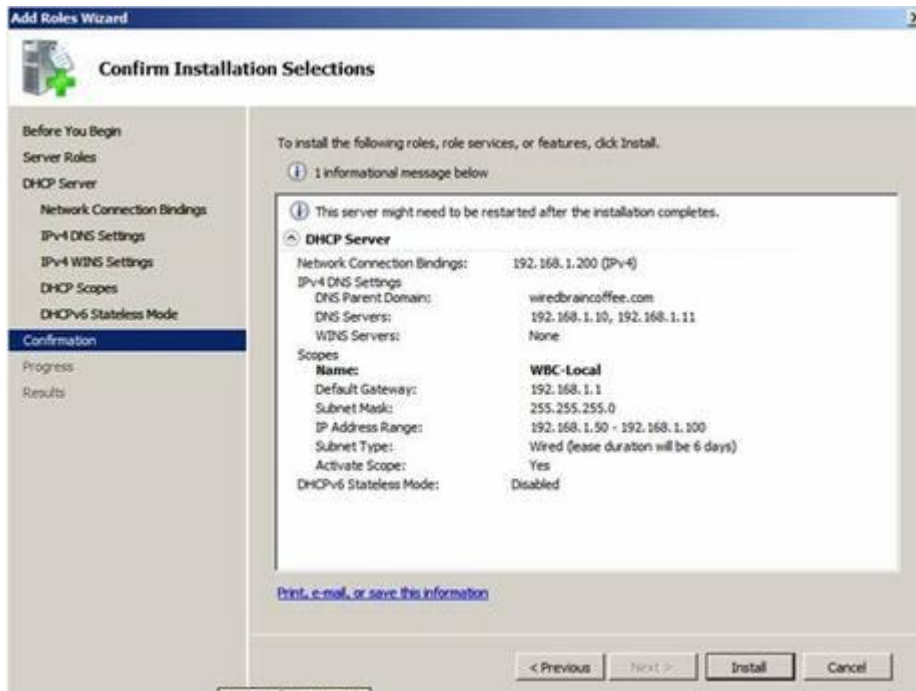
Như các bạn thấy bên dưới, tôi đã viết lại tên Scope **WBC-Local**, cấu hình **starting** và **ending IP addresses** thành 192.168.1.50-192.168.1.100, **subnet mask** thành 255.255.255.0, **default gateway** thành 192.168.1.1, **type of subnet** và **activated** phạm vi này.



## HÌNH 5: Thêm mới một DHCP Scope

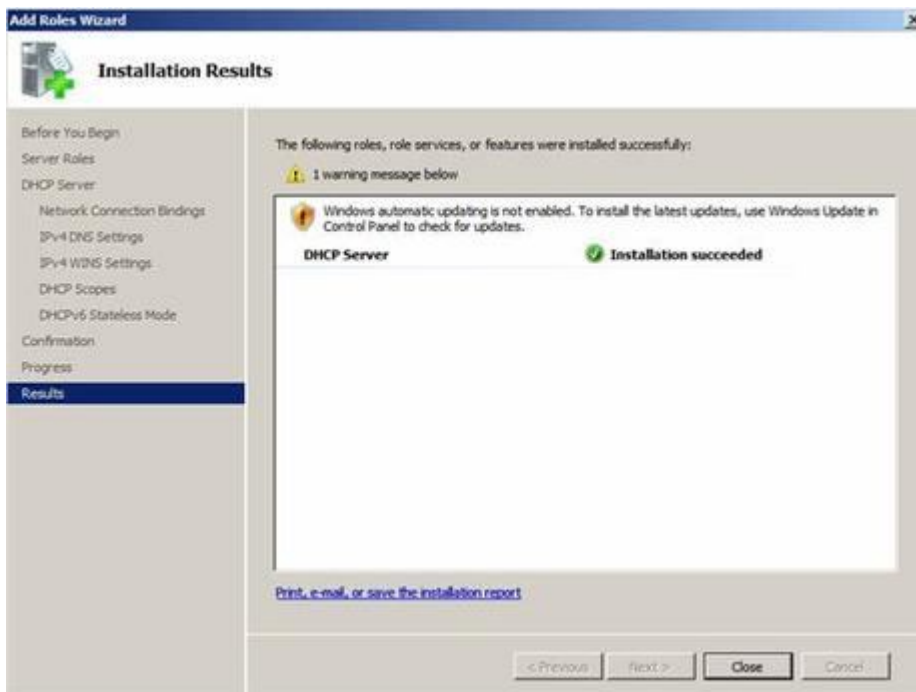
Quay trở lại màn hình Add Scope, tôi đã click Next và thêm vào đó một "new scope" ( một DHCP Server đã được cài đặt).

Tôi chọn Disable DHCPv6 stateless mode cho server này và đã click Next. Sau đó, tôi đã cấu hình DHCP Installation Selections của tôi (minh họa theo hình ảnh dưới) và đã click **Install**.



## HÌNH 6: Confirm Installation Selections

Sau chỉ một vài giây, DHCP Server đã được cài đặt và tôi nhìn thấy thành quả của tôi như hình dưới đây



## **HÌNH 7: Windows Server 2008 DHCP Server**

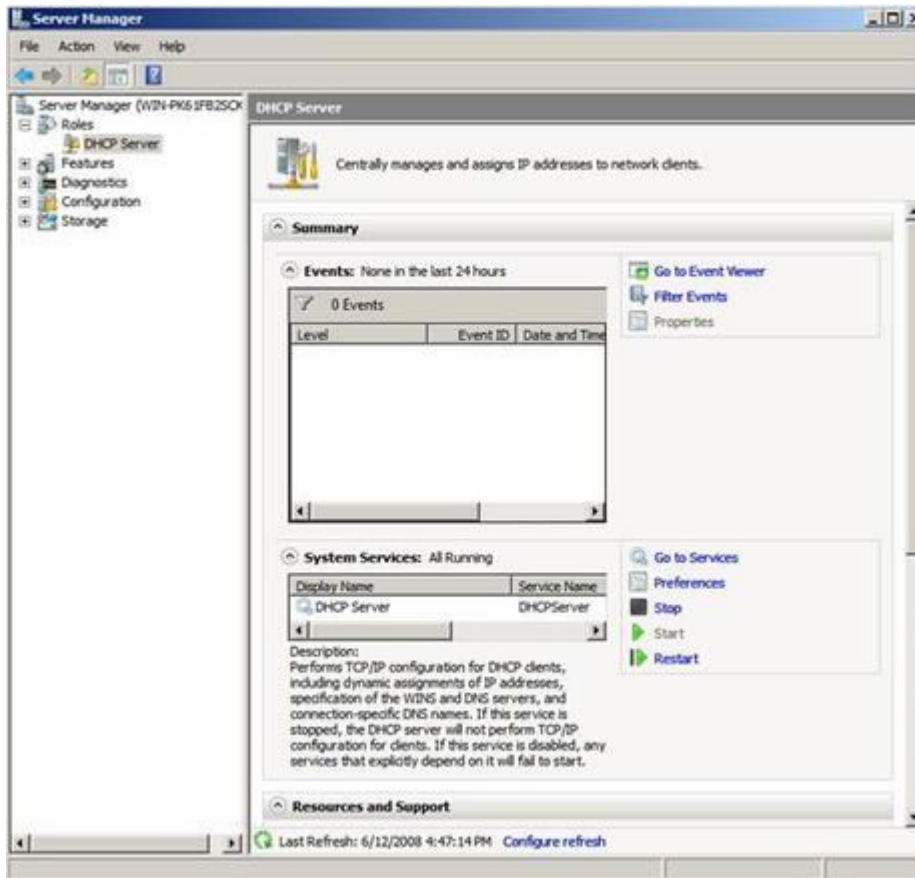
Installation đã được cài đặt thành công

Tôi đã click Close để đóng lại cửa sổ cài đặt, sau đó chúng ta hãy chuyển sang mục làm thế nào để có thể quản lí được DHCP Server mới này.

### **Làm thế nào để quản lí Windows Server 2008**

#### **DHCP Server mới của bạn ?**

Tương tự như quá trình cài đặt, việc quản lí Windows Server 2008 DHCP Server cũng thật dễ dàng. Hãy quay trở lại Windows Server 2008 **Server Manager**, bên dưới **Roles**, tôi đã click lên mục mới là **DHCP Server**.



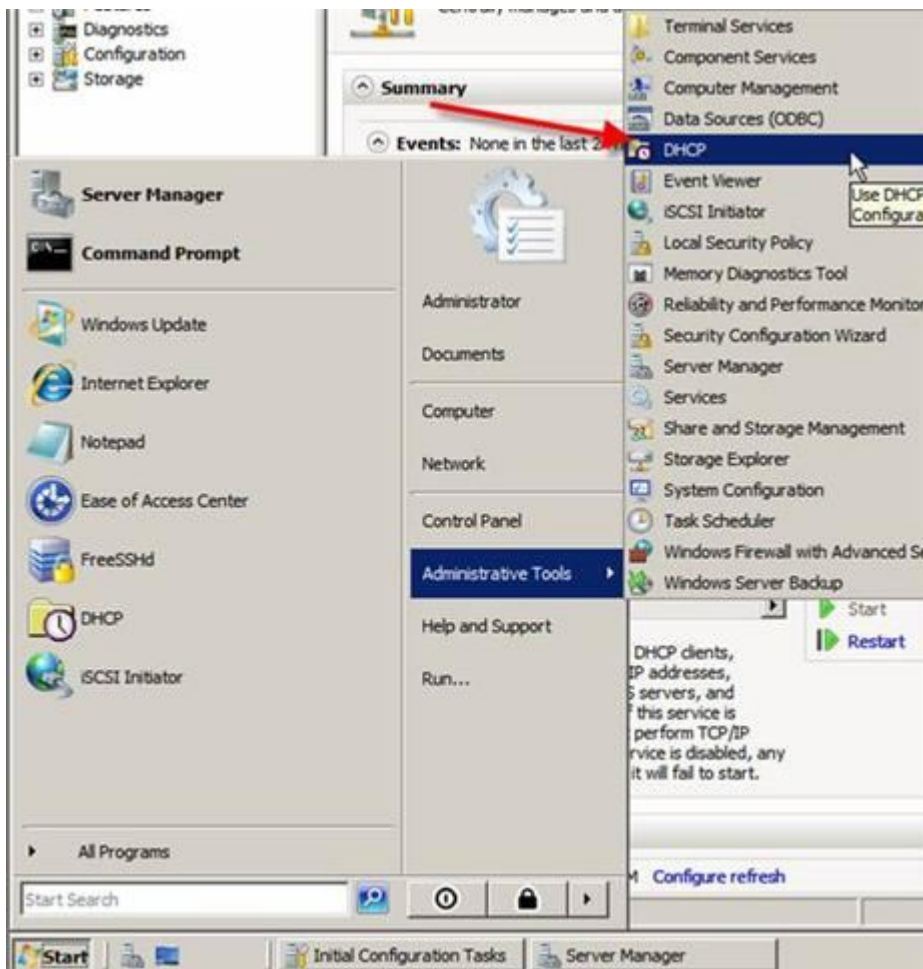
## HÌNH 8: DHCP Server management trong Server Manager

Trong khi tôi không thể quản lý được những phạm vi của DHCP Server và các client tại đây, cái mà tôi có thể làm là quản lý các sự kiện, dịch vụ và những tài nguyên liên quan đến sự cài đặt DHCP Server. Như vậy, đây là một vị trí tốt để đi đến việc kiểm tra trạng



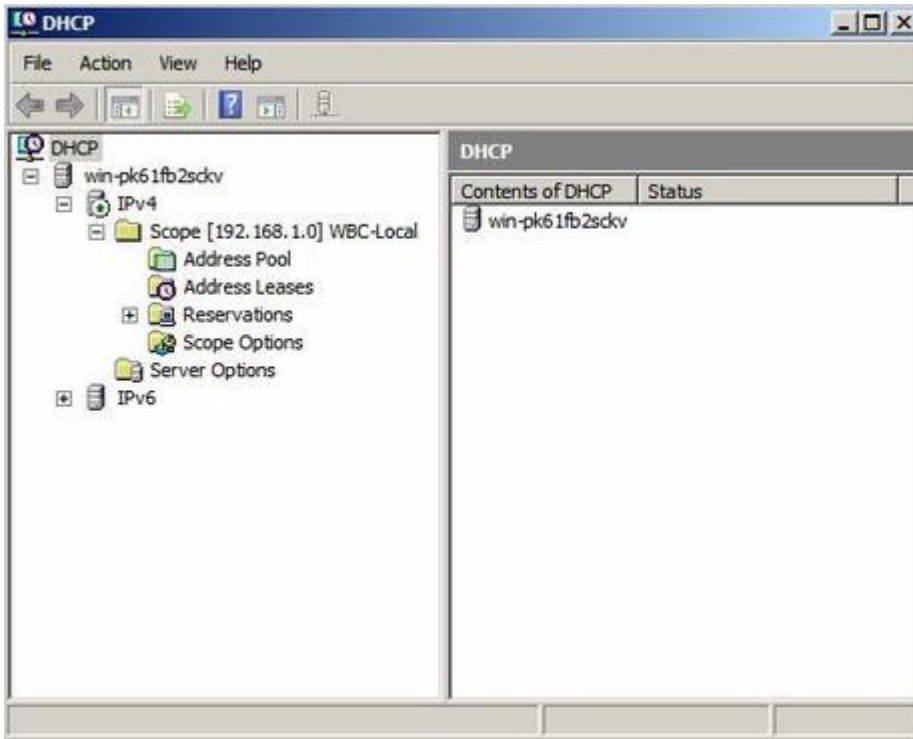
thái của DHCP Server và những biến cố gì đã xảy ra xung quanh nó.

Tuy nhiên, để thật sự định hình DHCP Server và quan sát những gì client đã thu được từ địa chỉ IP, tôi cần phải tiến tới DHCP Server MMC. Để làm được điều này, tôi sẽ **Start à Administrative Tools à DHCP Server**, như đây:



## HÌNH 9: Starting the DHCP Server MMC

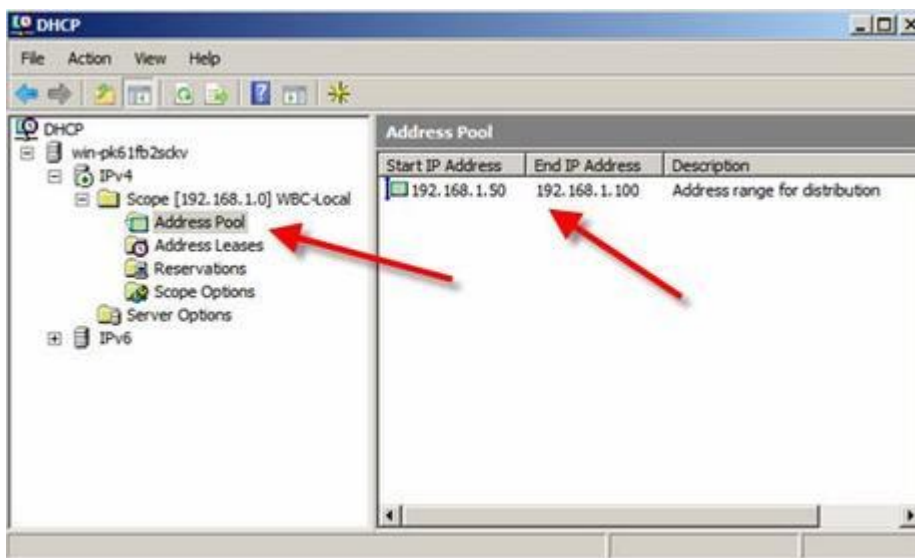
Khi mở rộng ngoài, MMC đưa ra rất nhiều các đặc tính. Và đây là những gì chúng ta thấy được từ nó:



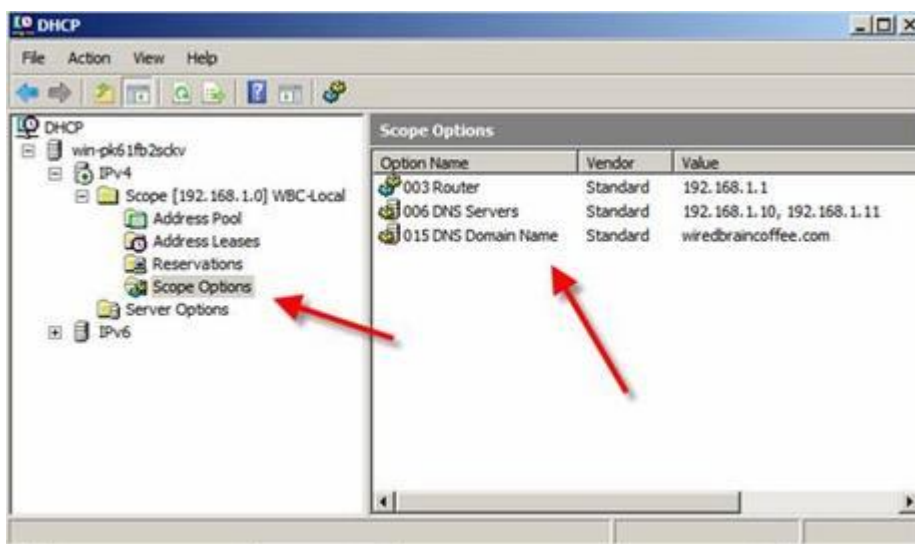
## HÌNH 10: Windows Server 2008 DHCP Server MMC

DHCP Server MMC đưa ra IPv4 & IPv6 DHCP Server bao gồm tất cả thông tin về scopes, pools, leases, reservations, scope options, và server options.

Nếu tôi đi sâu vào pool address và các tùy chọn scope, tôi có thể nhìn thấy các cấu hình mà tôi đã thiết lập khi đồng cài đặt DHCP Server. Phạm vi địa chỉ IP là ở đó, và vì thế DNS Server và các cổng vào là mặc định.



**HÌNH 11:** DHCP Server Address Pool



## **HÌNH 12: DHCP Server Scope Options**

Chúng ta sẽ không thể biết được những gì làm trên có thành công hay không ngay sau khi thiết lập xong, vì thế chúng ta cần kiểm tra tính khả thi của nó. Và sau đây, là hướng dẫn các bạn kiểm tra sự hoạt động.

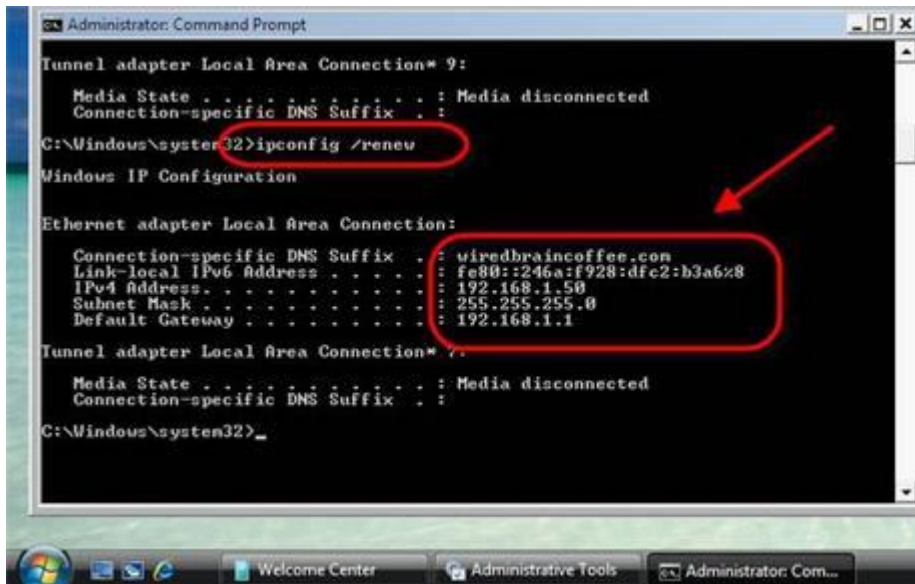
### **Làm thế nào để kiểm tra Windows Server 2008 DHCP Server của chúng ta ?**

Để kiểm tra, tôi cần có một Windows Vista PC Client trên cùng hệ thống mạng hiện tại như Windows Server 2008 DHCP server. Để an toàn, tôi không có thiết bị khác trên hệ thống mạng này.

Tôi gõ **IPCONFIG /RELEASE** sau đó là

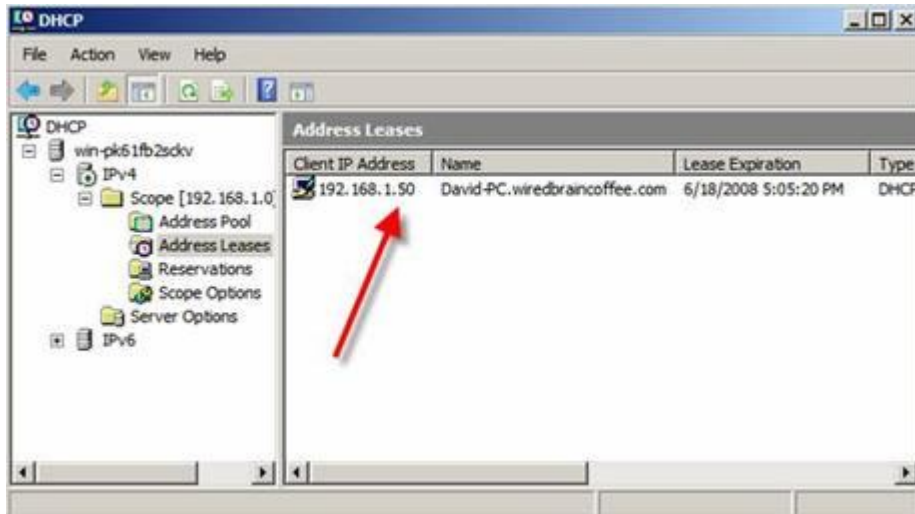
**IPCONFIG /RENEW** và kiểm tra rằng tôi đã nhận được một địa chỉ IP từ DHCP server mới này chưa.

Bạn có thể xem hình dưới đây



**HÌNH 13:** Vista client đã nhận địa chỉ IP từ DHCP Server mới

Ở đây, tôi đồng thời tiến đến Windows 2008 Server của tôi và xác nhận Vista client mới đã được đưa vào danh sách đóng vai trò như một client trên DHCP Server. Thực tế hãy kiểm tra bằng hình ảnh bạn được nhìn thấy dưới đây:



**Cuối cùng:** Win 2008 DHCP Server có Vista client được liệt kê trong Address Leases

Với điều này, tôi biết rằng tôi đã cấu hình thành công.

## Lời kết

Qua bài này, bạn đã học được cách làm thế nào để cài đặt và cấu hình DHCP Server trong Windows Server 2008. Xuyên suốt tiến trình, bạn đã học được DHCP Server là gì, nó có thể giúp gì cho bạn, làm sao để cài đặt nó, làm sao để quản lý server này và làm thế nào để cấu hình các thiết đặt đặc trưng cho DHCP Server cũng như DHCP Server scopes.

Cuối cùng, chúng tôi đã kiểm tra và tất cả đã được vận hành một cách nhịp nhàng, Chúc bạn may mắn khi bạn bắt tay vào cấu hình Windows Server 2008 DHCP Server! của chính bạn.

## Cách cài đặt và cấu hình Windows Server 2008

Cùng với sự kiện ra mắt phiên bản Windows Microsoft Server 2008 sắp tới, bài này sẽ cung cấp cho bạn thấy một đặc tính của hệ điều hành mới đáng được quan tâm này. Trong bản Windows Server 2008 có tùy chọn thực hiện cài đặt Windows Server Core cung cấp cho bạn tập hợp các công cụ nhỏ nhất để chạy trên Windows.

Bạn được cung cấp một nhân và dòng lệnh để quản lý máy chủ. Đây là những cái thiết yếu cơ bản nhất cho phép cấu hình gọn Windows. Kiểu cài đặt này rất hoàn hảo đối với một trung tâm dữ liệu.

### Cài đặt

Trong lần đầu tiên chạy cài đặt Windows Server 2008, bạn có 2 tùy chọn cài đặt là:

- Windows Server 2008 Enterprise (Full Installation) (Cài đặt đầy đủ)
- Windows Server 2008 Enterprise (Server Core Installation) (Cài đặt Server Core)

Thực hiện theo 8 bước như trong các hình vẽ dưới đây để thực hiện cài đặt Windows Server Core.

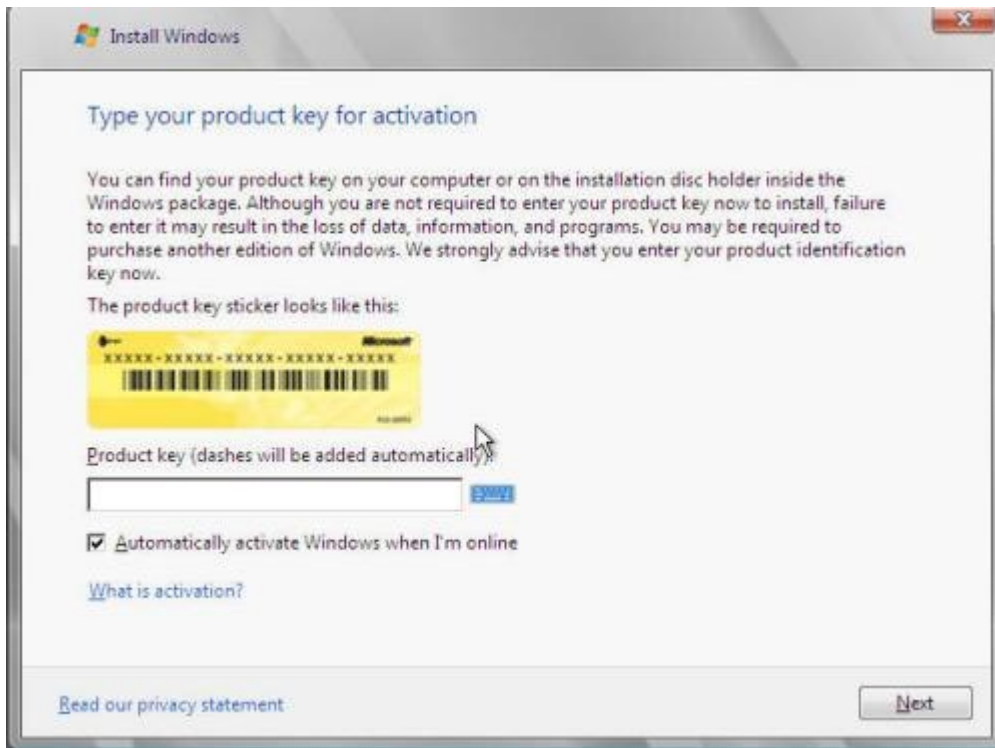


Hình A

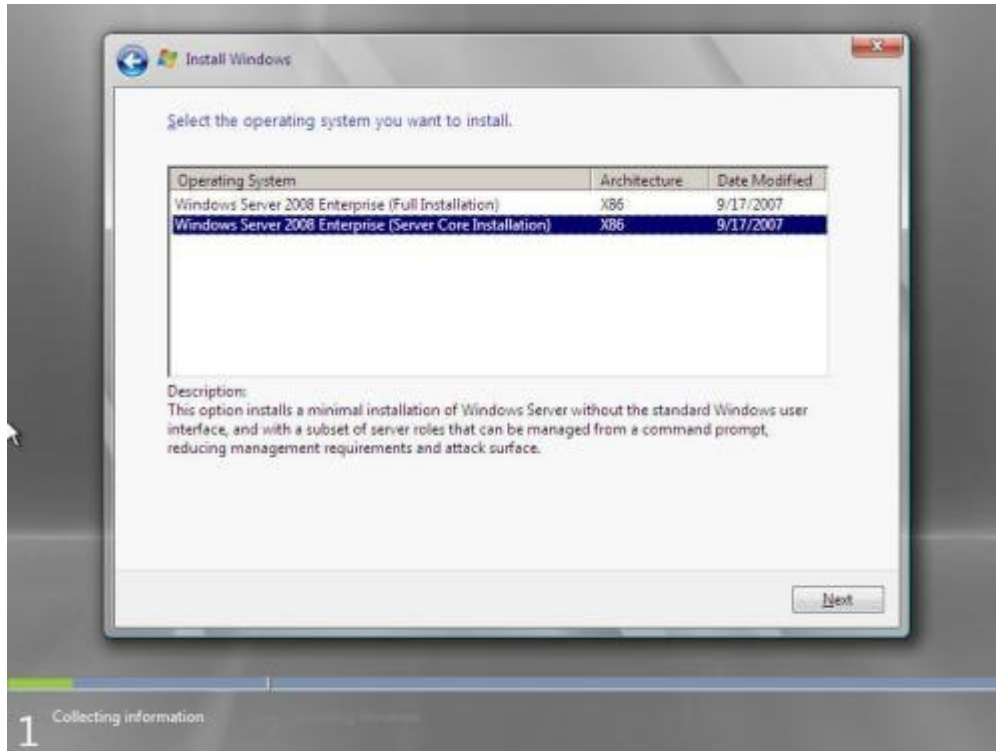




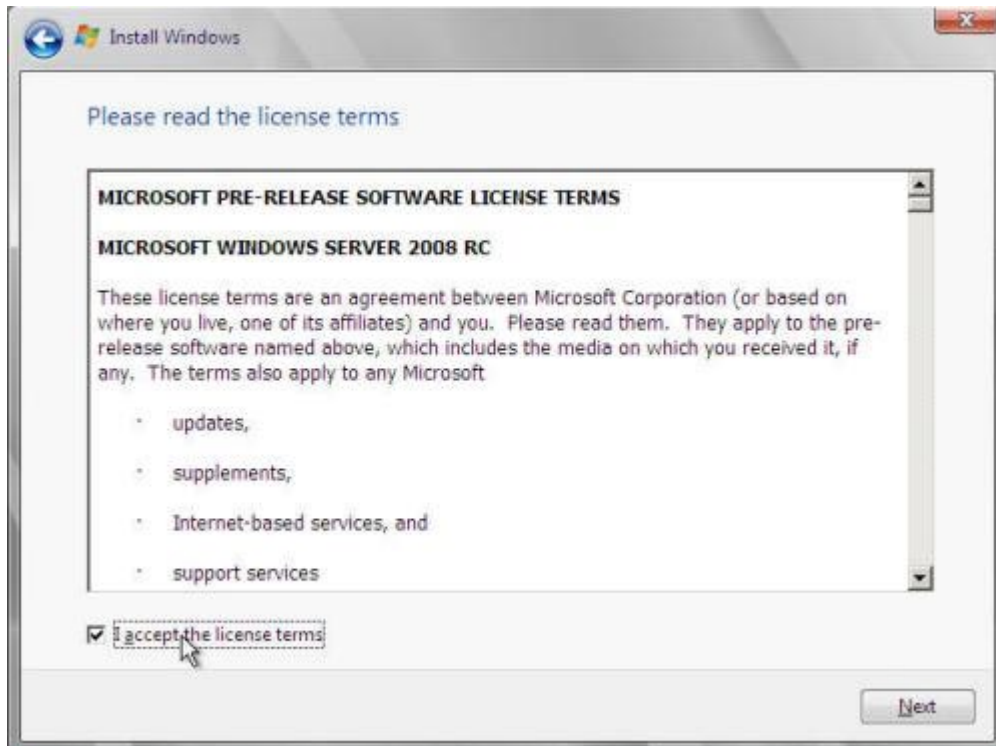
Hinh B



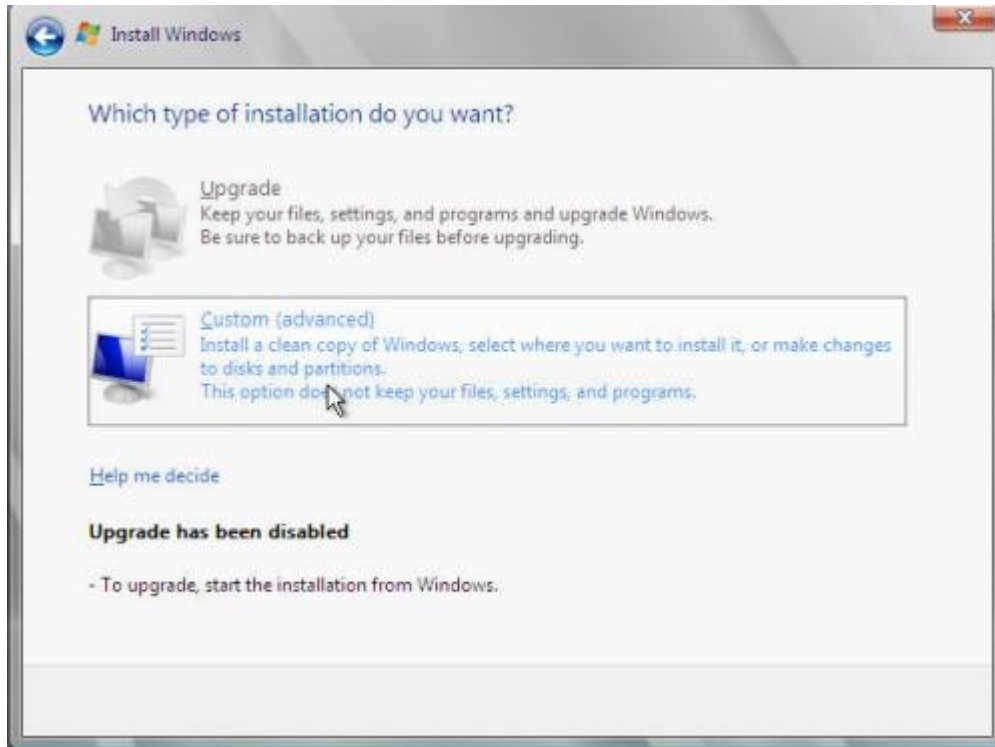
Hinh C



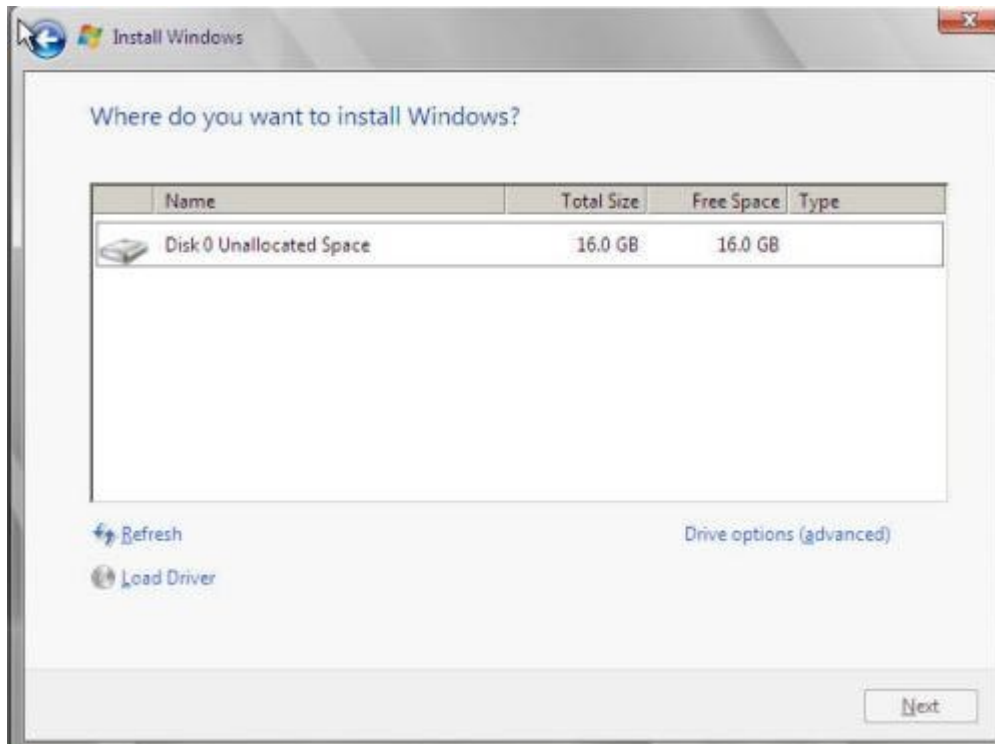
Hình D



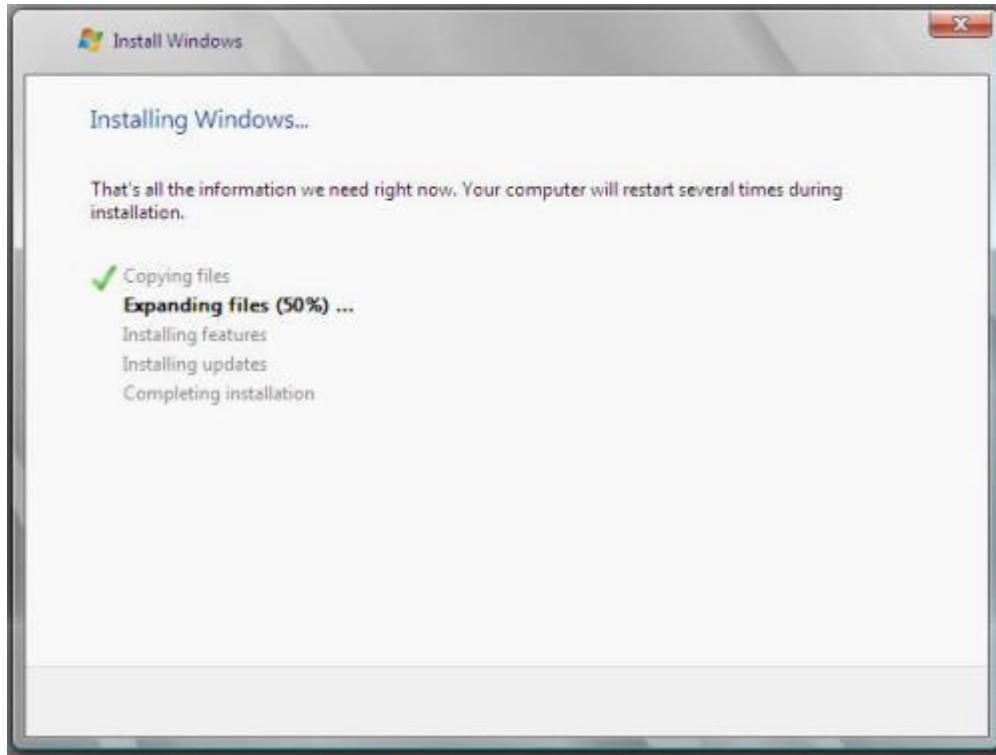
Hình E



Hình F

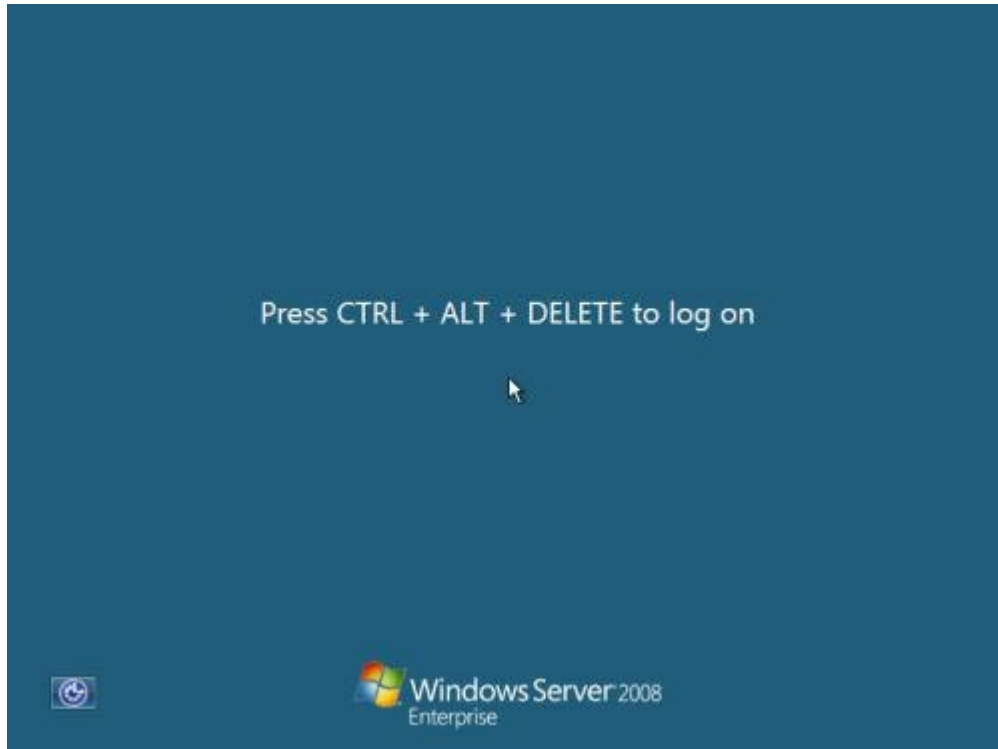


Hình G



Hình H

Sau khi cài đặt, cửa sổ màn hình chính xuất hiện và bạn đã sẵn sàng để đăng nhập như trong Hình I. Tên đăng nhập duy nhất là Administrator và mật khẩu để trống (Hình J). Bạn được yêu cầu thay đổi mật khẩu và thiết lập một mật khẩu Administrator trong lần đăng nhập đầu tiên.



Hình I

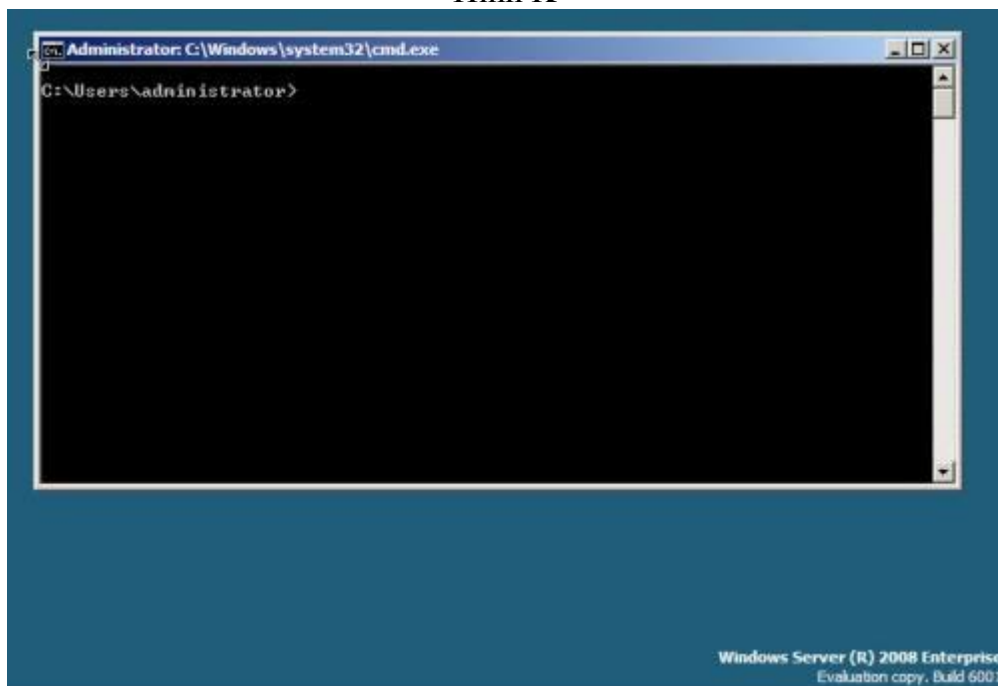


Hình J

Sau khi đăng nhập (Hình K), bạn đã sẵn sàng để cấu hình ngày, giờ và vùng thời gian. Tại dòng lệnh nhập: `controltime date.cpl` và thiết lập các tùy chọn phù hợp (Hình L).

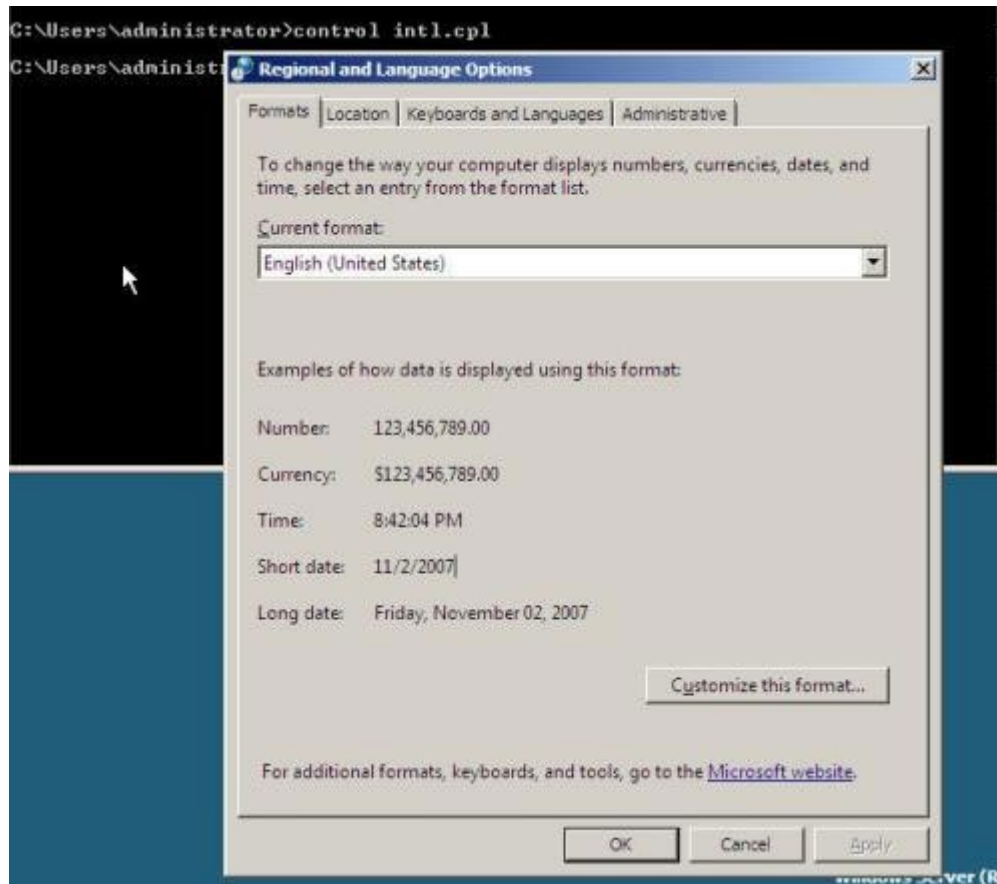


Hình K



Hình L

Nếu bạn cần cấu hình và thay đổi các thiết lập bàn phím, hãy nhập lệnh sau: control intl.cpl (Hình M).



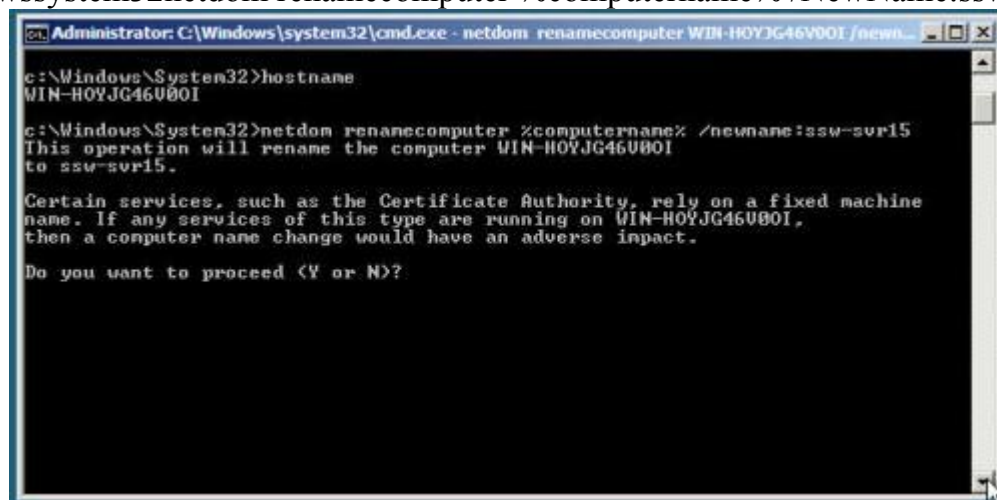
Hình M

Hãy di chuyển và thay đổi tên máy chủ, tên mặc định là một nhóm các kí tự và số ngẫu nhiên. Bạn có thể xem tên máy chủ hiện tại bằng cách nhập lệnh sau:

```
c:\windows\system32>hostname
```

Hãy đổi tên máy chủ là ssw-svr15 bằng cách thực hiện dòng lệnh dưới đây:

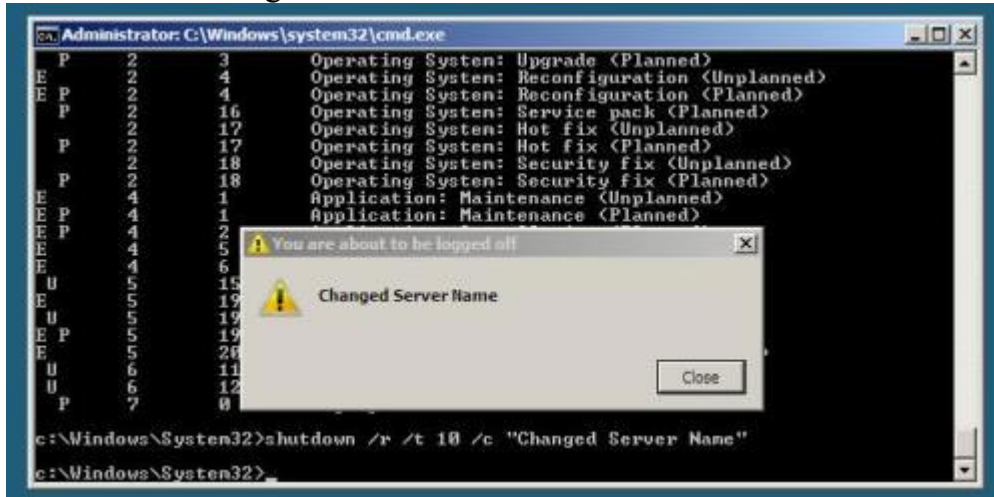
```
c:\windows\system32>netdom renamecomputer %computername% /NewName:ssw-svr15
```



Hình N

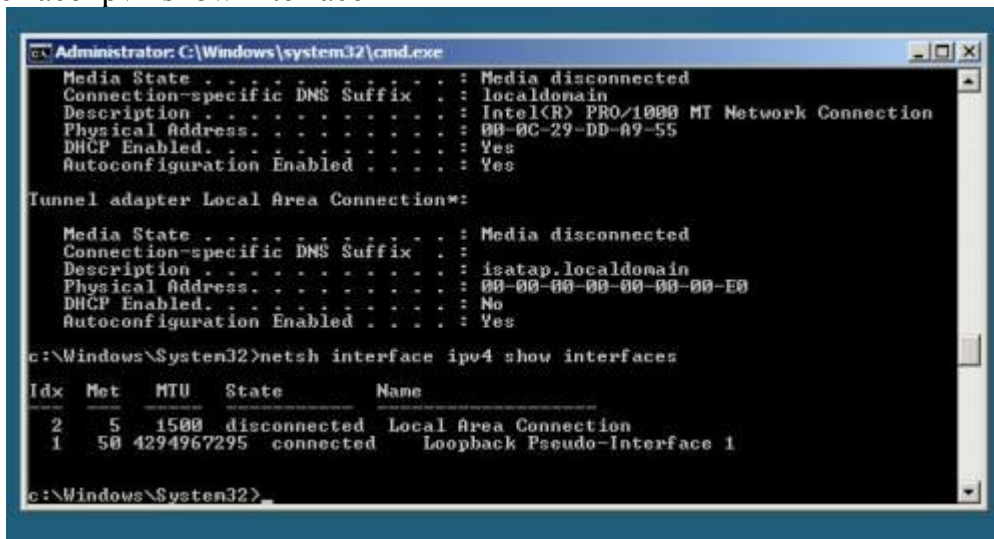
Sau khi chọn để xử lý, thao tác được thực hiện thành công. Bạn cần phải khởi động lại máy chủ bằng lệnh shutdown. Cú pháp là:  
shutdown /?

Sau khi xem lại cú pháp (Hình N) nhập lệnh sau: shutdown /r (chuyển đổi giữa tắt và khởi động lại máy tính) /t 10 (Đợi 10 giây để tắt và khởi động lại) /c "Changed Server Name" (thêm ghi chú với độ dài tối đa là 512 kí tự). Toàn bộ cú pháp như sau:  
shutdown /r /T 10 /C "Changed Server Name"



Hình O

Bây giờ hãy cấu hình mạng để chúng ta có thể đưa máy chủ vào một miền. Để biết được bạn phải cấu hình giao diện nào, (Hình P) hãy nhập:  
netsh interface ipv4 show interface



Hình P

Local Area Connection có một giá trị chỉ mục của 2. Hãy tiến hành và cấu hình configure TCP/IP cho kết nối. (Hình Q) Nhập lệnh sau để thiết lập thông tin TCP/IP:  
netsh interface ipv4 set address name="2" source=static address=192.168.1.199  
mask=255.255.255.0 gateway=192.168.1.1



```

Administrator: C:\Windows\system32\cmd.exe
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection*:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : isatap.localdomain
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

c:\Windows\System32>netsh interface ipv4 show interfaces

Idx Met  MTU  State      Name
-----
  2   5  1500  disconnected Local Area Connection
  1   50 4294967295  connected  Loopback Pseudo-Interface 1

c:\Windows\System32>netsh interface ipv4 set address name="2" source=static address=192.168.1.199 mask=255.255.255.0 gateway=192.168.1.1

c:\Windows\System32>

```

Hình Q

Thực hiện theo ví dụ sau để cấu hình DNS (Hình R):

netsh interface ipv4 add dnsserver name="2" address=192.168.1.1 index=1

```

Administrator: C:\Windows\system32\cmd.exe

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : isatap.localdomain
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

c:\Windows\System32>netsh interface ipv4 show interfaces

Idx Met  MTU  State      Name
-----
  2   5  1500  disconnected Local Area Connection
  1   50 4294967295  connected  Loopback Pseudo-Interface 1

c:\Windows\System32>netsh interface ipv4 set address name="2" source=static address=192.168.1.199 mask=255.255.255.0 gateway=192.168.1.1

c:\Windows\System32>netsh interface ipv4 add dnsserver name="2" address=192.168.1.110 index=1

c:\Windows\System32>

```

Hình R

Nếu nhập ipconfig /all, bạn sẽ xem thêm được thông tin mới (Hình S).

```
Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MI Network Connection
Physical Address. . . . . : 00-0C-29-DD-A9-55
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3497:10fa:d848:bf7b%2<Preferred>
IPv4 Address. . . . . : 192.168.1.199<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.110
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection*:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : isatap.localdomain
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

c:\Windows\System32>
```

Hình S

Hãy đưa nó vào một miền! Để thực hiện chức năng này, chúng ta sẽ sử dụng câu lệnh netdom.exe. (Hình T) Cú pháp như sau:

netdom join ssw-svr15 /domain:watchtower /user:Administrator /passwordD



assword01  
Chú ý: Không quên khởi động lại máy chủ, sử dụng lệnh:  
shutdown /r /T 10 /C "Added to domain"

```
Administrator: C:\Windows\system32\cmd.exe

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.110
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection*:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\administrator>hostname
ssw-svr15

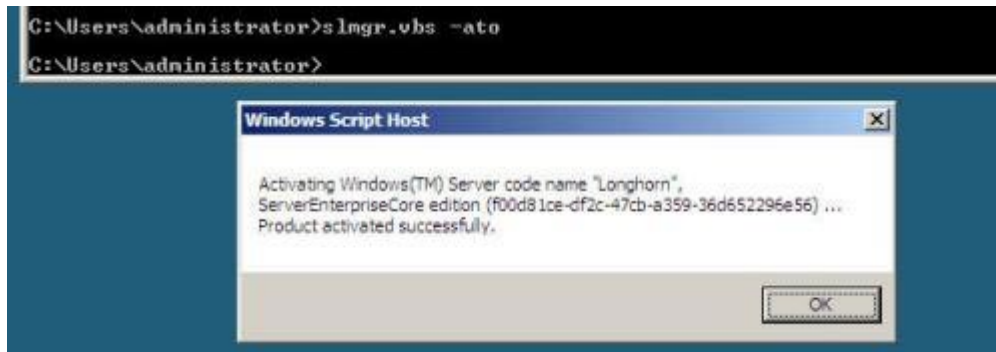
C:\Users\administrator>netdom join ssw-svr15 /domain:watchtower /user:Administrator /passwordd:Password01
The computer needs to be restarted in order to complete the operation.

The command completed successfully.

C:\Users\administrator>
```

Hình T

Bước cuối cùng, bạn đừng quên kích hoạt máy chủ (Hình U) bằng lệnh sau:  
slmgr.vbs -ato



Hình U

*Theo quantrimang*

## CÀI ĐẶT VÀ CẤU HÌNH WINDOWS 2003

### Chuẩn bị

Trong mô hình này tôi chọn cài đặt HĐH Windows Server 2003 và Windows XP. Trước khi bắt tay vào việc bạn cần chuẩn bị :

- 2 máy tính có cấu hình phù hợp, một làm máy chủ và một làm máy trạm có nối mạng với nhau.
- 02 bộ đĩa cài đặt cho 02 HĐH này.

### Trình tự thực hiện

Trình tự thực hiện cài đặt các HĐH như sau:

Máy chủ

- Cài đặt HĐH Windows Server 2003
- Cài đặt dịch vụ DHCP

Máy trạm

- Cài đặt HĐH Windows XP
- Cài đặt các ứng dụng (tùy theo nhu cầu sử dụng của bạn)

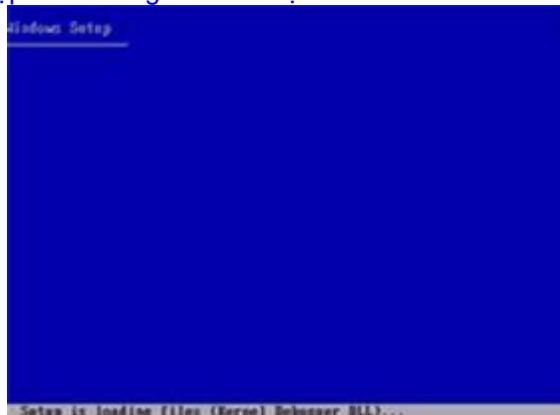
### cài đặt Hệ điều hành

Thiết lập trong BIOS Setup để máy tính khởi động đầu tiên từ CDROM. Đưa đĩa cài đặt Windows Server 2003 vào ổ CDROM, cho máy tính khởi động lại, máy tính sẽ tự động khởi động chương trình cài đặt từ đĩa cài đặt trong ổ CDROM.

#### **Giai đoạn 01:**

Chương trình cài đặt kiểm tra cấu hình máy tính và bắt đầu cài đặt HĐH ở chế độ text (text mode):

- Chương trình cài đặt lần lượt nạp chương trình thực thi, các phần mềm hỗ trợ, các trình điều khiển thiết bị, các tập tin chương trình cài đặt.



- Cửa sổ lựa chọn cài đặt: Nhấn Enter để cài đặt Windows, R để sửa chữa phiên bản đã cài đặt, F3 để hủy bỏ việc cài đặt



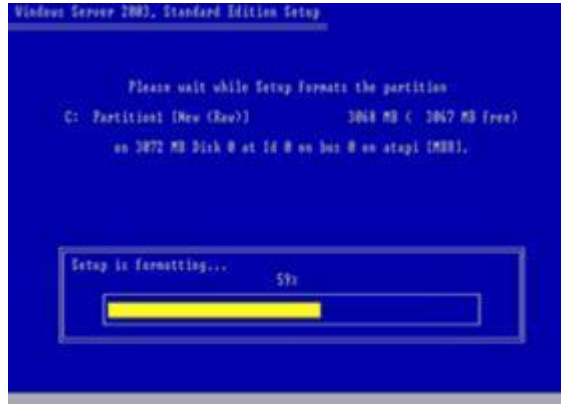
- Chọn không gian đĩa cài đặt: Tại hộp sáng, nhấn Enter để chọn toàn bộ vùng đĩa hoặc nhấn C để chia vùng đĩa này thành nhiều phân vùng nhỏ hơn



- Một phân vùng mới đã được tạo và đòi hỏi phải được định dạng. Chọn mục thứ 3 để định dạng sử dụng hệ thống file NTFS



- Chương trình cài đặt đang định dạng



- Sau khi định dạng xong, chương trình kiểm tra lỗi vật lý ổ cứng và chép các tập tin cần thiết vào ổ cứng



### Giai đoạn 02:

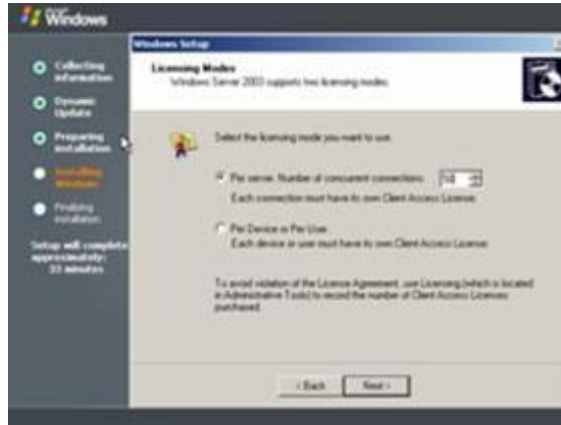
Computer sẽ tự Restart. Chương trình sẽ bắt đầu tiến trình cài đặt dưới giao diện đồ họa, ở giai đoạn này ta lần lượt đi theo các bước hướng dẫn và cung cấp thêm vài thông tin cần thiết cho trình cài đặt

- Click Next trên trang Regional and Language Options
- Trên trang Personalize Your Software, điền Tên và Tổ chức của Bạn  
Ví dụ: **Name: Server 2003**  
**Organization: Tin 05**

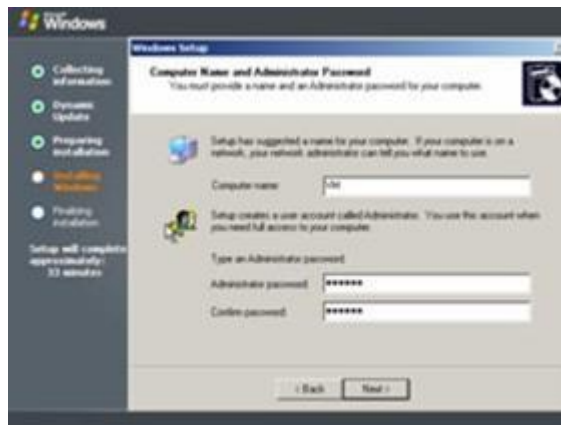
- Trên trang *Product Key* điền vào 25 chữ số của Product Key mà bạn có và click Next.



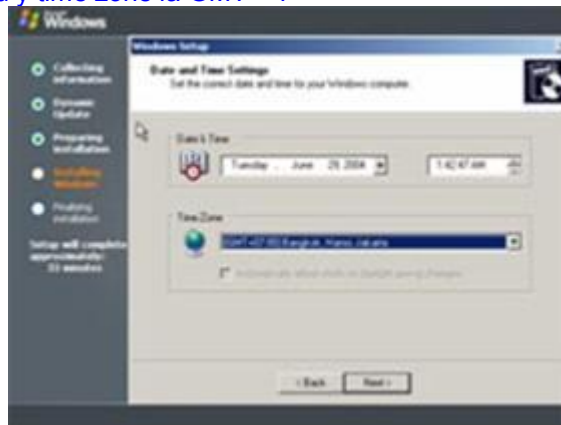
- Trên trang *Licensing Modes* chọn đúng option được áp dụng cho version Windows Server 2003 mà bạn cài đặt. Nếu cài đặt Licence ở chế độ Per server licensing, hãy đưa vào số connections mà bạn đã có License. Click Next



- Trên trang *Computer Name* và *Administrator Password* điền tên của Computer ví dụ Server2003, tên này được điền vào Computer Name text box. Điền tiếp vào mục Administrator password và xác nhận lại password tại mục Confirm password (ghi nhớ lại password administrator cẩn thận, nếu không thì bạn cũng không thể log-on vào Server cho các hoạt động tiếp theo). Click Next.



- Trên trang *Date and Time Settings* xác lập chính xác Ngày, giờ và múi giờ Việt Nam (nếu các bạn ở Việt Nam), lưu ý time zone là GMT + 7



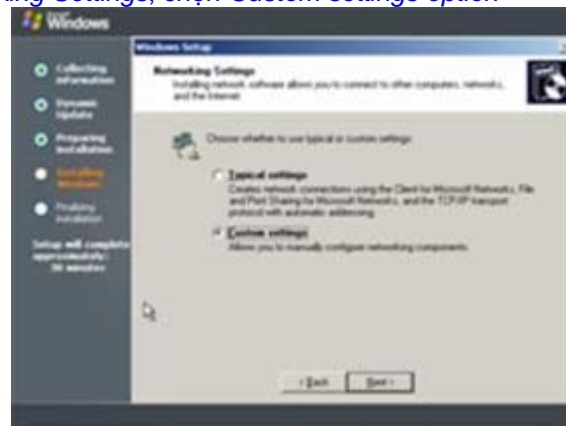
Click Next.

**Cài đặt các thành phần mạng**





- Trên trang *Networking Settings*, chọn *Custom settings option*



- Trên trang *Network Components*, chọn *Internet Protocol (TCP/IP)* entry trong *Components* và click *Properties*.

Trong *Internet Protocol (TCP/IP) Properties dialog box*, xác lập các thông số sau:

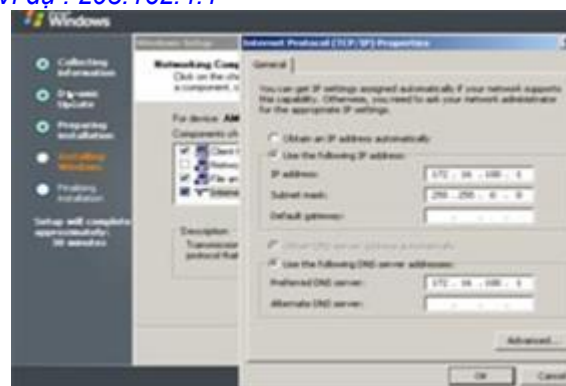
**IP address: 10.0.0.2.**

**Subnet mask: 255.255.255.0.**

**Default gateway: 10.0.0.1**

(chú ý *Default Gateway 10.0.0.1* này cũng là *IP address* của *Card Ethernet* của *Router ADSL*).

**Preferred DNS server: 10.0.0.2** và **Additional DNS server** là địa chỉ mà *ISP* đã cung cấp cho *ADSL Router*, ví dụ : **203.162.4.1**



Click *OK* trong *Advanced TCP/IP Settings dialog box*.

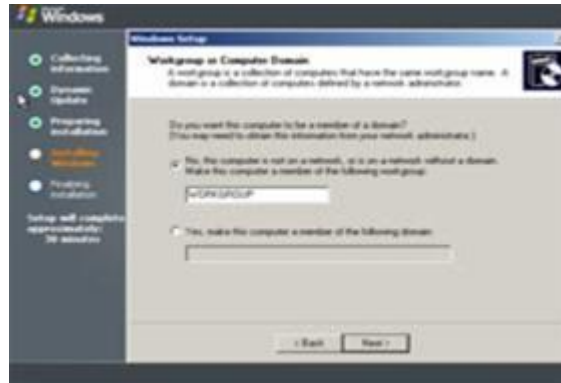
Click *OK* trong *Internet Protocol (TCP/IP) Properties dialog box*.

Click *Next* trên trang *Networking Components*.

- Chấp nhận lựa chọn mặc định môi trường *Network* là *Workgroup* (chúng ta sẽ tạo môi



trường Domain sau, thăng cấp (promote) máy này trở thành một Domain controller và cũng là thành viên của Domain. Click Next.



- Tiến trình cài đặt được tiếp tục và khi Finish, Computer sẽ tự khởi động lại



Log-on lần đầu tiên vào Windows Server 2003 dùng password mà chúng ta đã tạo cho tài khoản Administrator trong quá trình Setup.

Xuất hiện đầu tiên trên màn hình là trang *Manage Your Server*, bạn nên check vào "Don't display this page at logon checkbox" và đóng cửa sổ Window lại.



#### Một vài thủ thuật

##### Tắt manage your sever

Mỗi khi khởi động vào Windows Server 2003, Windows sẽ tự chạy chương trình có tên là Manage Your Server (hoặc bạn có thể vào **Control Panel-> Administrative Tools-> Manage Your Server**).

Bạn hãy đánh dấu chọn vào hộp chọn **"Don't display this page at logon"** ở góc trái dưới của cửa sổ chương trình và lần khởi động sau Windows sẽ không chạy chương trình này nữa.

#### ☛ **Tự động đăng nhập vào Windows**

Nhấn chuột vào nút Start thanh tác vụ, chọn Run, trong khung Open bạn gõ **"control userpasswords2"** và nhấn Enter, cửa sổ User Accounts sẽ xuất hiện.

Nhấn Add và nhập các thông số cần thiết như tên truy cập tên đầy đủ, nhấn Next để nhập password, và nhấn Next tiếp để chọn quyền đăng nhập, bạn chọn **Others: Administrator** (tuỳ vào quyền truy cập cho phép người sử dụng).

Nhấn Finish để kết thúc. Sau khi tạo xong tên sử dụng, bạn hãy nhấn chuột vào tên sử dụng mà bạn vừa tạo, di chuyển chuột đến hộp chọn có tên **"Users must enter a user name and password to use this computer"** và bỏ đánh dấu chọn.

Nhấn OK để kết thúc.

Nếu bạn thực hiện đúng, Windows sẽ yêu cầu bạn nhập password thêm một lần nữa.

Bây giờ bạn hãy thoát ra (logoff) và đăng nhập (logon) trở lại với tên sử dụng mà bạn vừa tạo. Khi khởi động lại Windows sẽ vào ngay màn hình chính mà không yêu cầu bạn phải nhập username hay password.

Để làm cho Windows Server 2003 không hiển thị hộp thoại yêu cầu nhấn CTRL+ALT+DEL để đăng nhập, bạn vào **Control Panel-> Administrative Tools-> Local Security Policy** duyệt đến **Local Policies-> Security Options**, bạn tìm dòng **"Interactive logon: Do not require CTRL+ALT+DEL"** (dòng 24), nhấp đúp vào nó và chọn Enable. Nhấn OK. Đóng các cửa sổ lại và khởi động lại máy

#### ☛ **Loại bỏ tính năng "Shutdown event tracker"**

Mỗi khi tắt máy hay khởi động máy lại, Windows Server 2003 sẽ hiển thị bảng **"Shutdown Event Tracker"** để bạn xác định nguyên nhân tắt máy hay khởi động lại rồi Windows mới thực hiện. Việc này khá mất thời gian.

Để loại bỏ tính năng này, bạn chọn **Start-> Run**, trong khung Open bạn gõ **"gpedit.msc"**, chương trình Group Policy Editor xuất hiện, ở khung bên trái bạn vào **Computer Configuration-> Administrative Templates-> System**; ở khung bên phải bạn tìm dòng **"Display Shutdown Event Tracker"** (dòng 15), click chuột phải vào nó và chọn **Properties**, trong hộp thoại **Display Shutdown Event Tracker** bạn chọn **Disable** và nhấn OK

**Nhóm 1 - Lớp SP TIN 05**

## Cài đặt và cấu hình Windows Server 2008 DHCP Server - Đã đăng: 14/9/2008 lúc 23:49

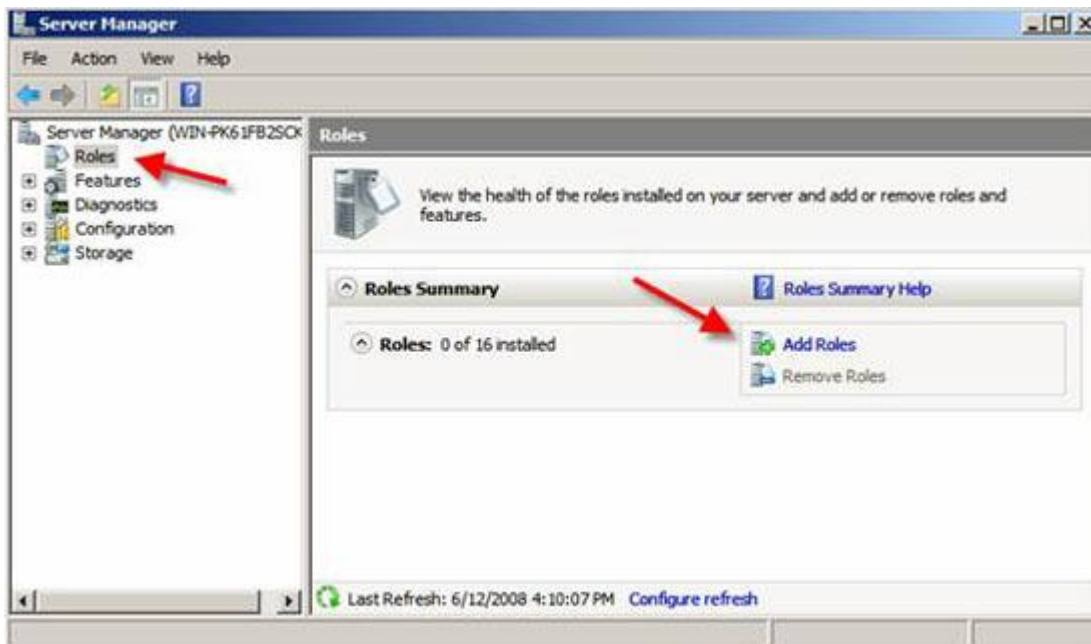
*Dynamic Host Configuration Protocol (DHCP) là một dịch vụ cơ sở hạ tầng lõi trên các mạng, cung cấp các thông tin định địa chỉ IP và máy chủ DNS cho các máy khách cũng như các thiết bị khác. DHCP được sử dụng để bạn không phải gán tĩnh tại các địa chỉ IP cho mỗi thiết bị trên mạng bên cạnh đó còn quản lý các vấn đề của việc định địa chỉ IP động tạo ra. Càng ngày, DHCP càng được mở rộng để thích hợp với các dịch vụ mạng mới như indows Health Service và Network Access Protection (NAP). Mặc dù vậy, trước khi có thể sử dụng các dịch vụ tiên tiến của nó, bạn cần sử phải cài đặt và cấu hình một số vấn đề cơ bản. Đó chính là nội dung chúng tôi sẽ giới thiệu trong bài.*

### Cài đặt Windows Server 2008 DHCP Server

Việc cài đặt Windows Server 2008 DHCP Server hoàn toàn dễ dàng. DHCP Server hiện là một "role" của Windows Server 2008 – chứ không phải là một thành phần riêng biệt như trước kia.

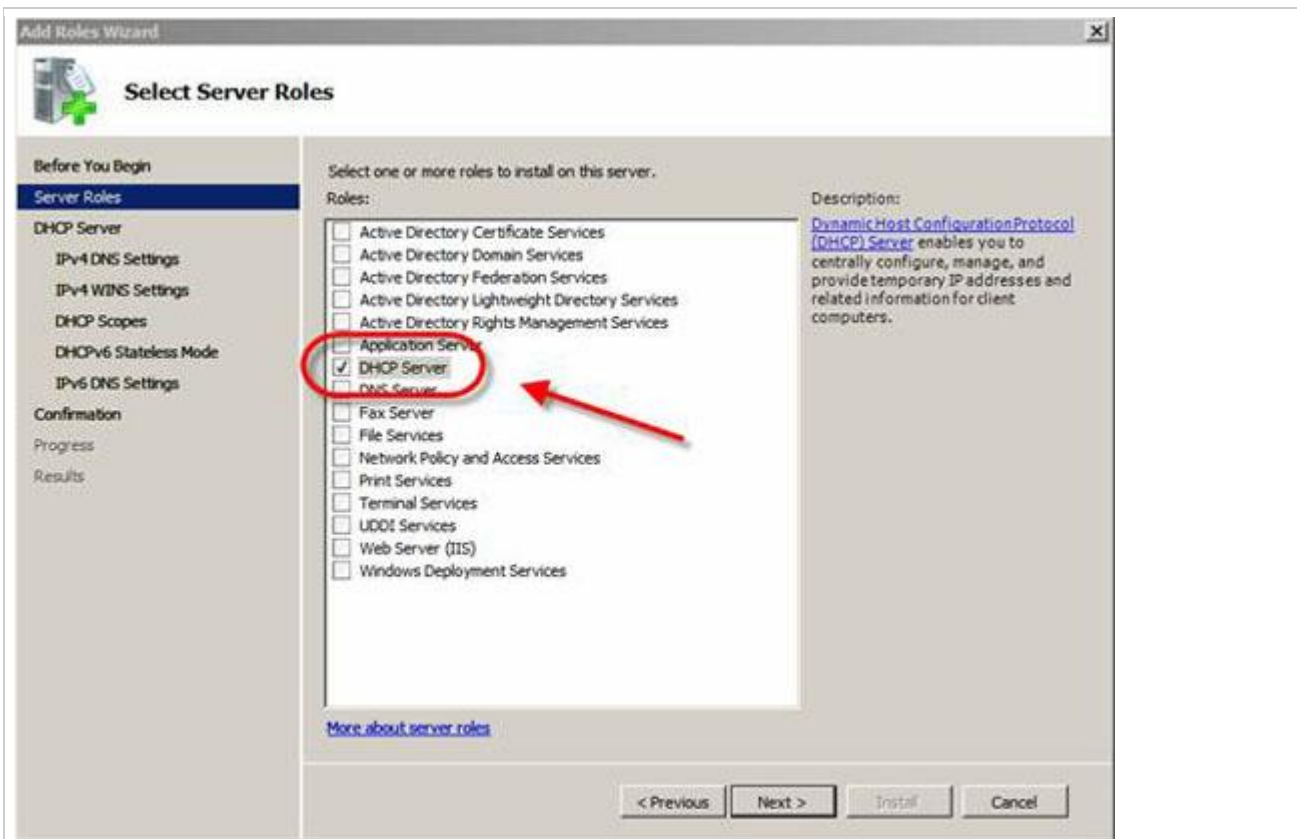
Để cài đặt Windows Server 2008 DHCP Server, bạn cần một hệ thống Windows Server 2008 đã được cài đặt và được cấu hình với địa chỉ IP tĩnh. Cần biết dải địa chỉ IP mạng của mình, dải địa chỉ IP mà bạn muốn sử dụng cho các máy khách, các địa chỉ IP của máy chủ DNS và cổng mặc định. Thêm vào đó, bạn cũng lập kế hoạch cho tất cả các subnet có liên quan, phạm vi mà bạn sẽ định nghĩa và những ngăn chặn nào cần tạo ra.

Để bắt đầu quá trình cài đặt DHCP, bạn có thể kích vào **Add Roles** từ cửa sổ **Initial Configuration Tasks** hoặc từ **Server Manager > Roles > Add Roles**.



Khi **Add Roles Wizard** xuất hiện, bạn hãy kích **Next** trên màn hình đó.

Tiếp đến, chọn thành phần muốn bổ sung, **DHCP Server Role**, sau đó kích **Next**.



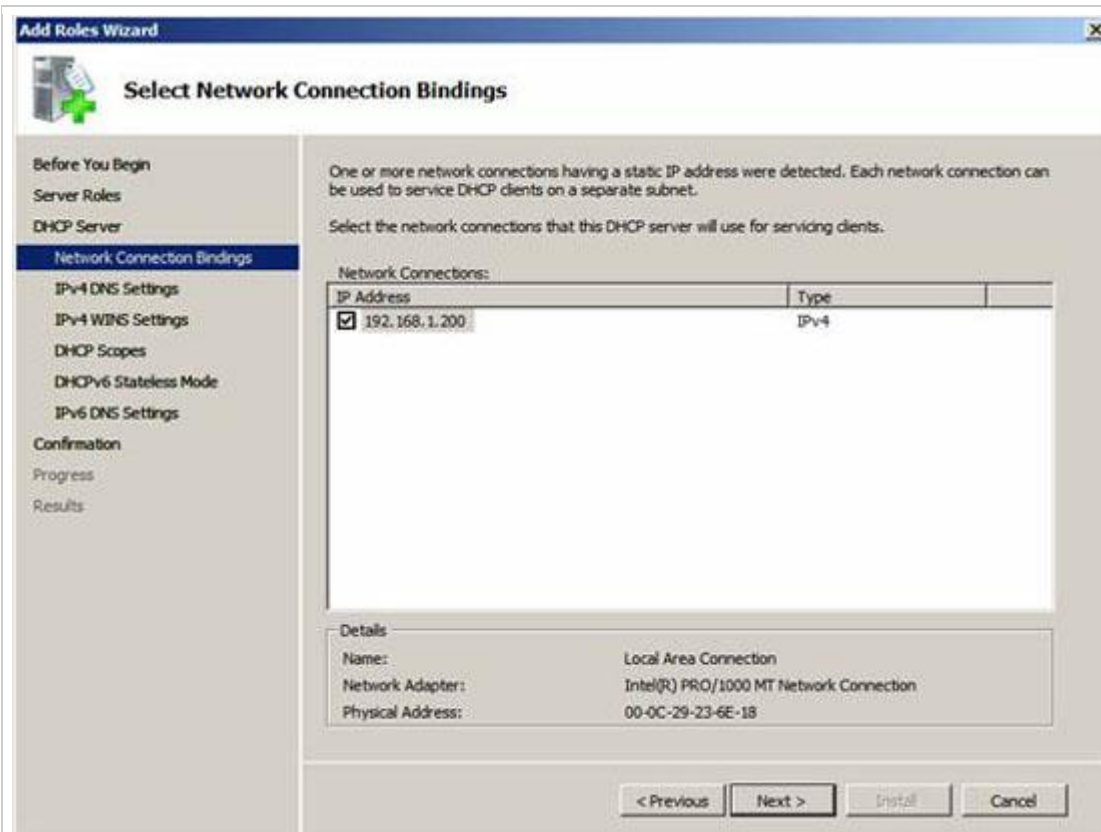
Nếu không có địa chỉ IP tĩnh được gán trên máy chủ thì bạn sẽ gặp một cảnh báo, cảnh báo này thông báo cho bạn biết rằng bạn không nên cài đặt DHCP với một địa chỉ IP động.

Ở đây, bạn sẽ được nhắc nhở về các thông tin IP mạng, thông tin về phạm vi và các thông tin DNS. Nếu chỉ cài đặt DHCP server mà không cần cấu hình các phạm vi và các thiết lập, bạn chỉ cần kích **Next** xuyên suốt các chất vấn trong quá trình cài đặt.

Mặt khác, bạn cũng có thể cấu hình tùy chọn DHCP Server trong suốt giao đoạn này của quá trình cài đặt.

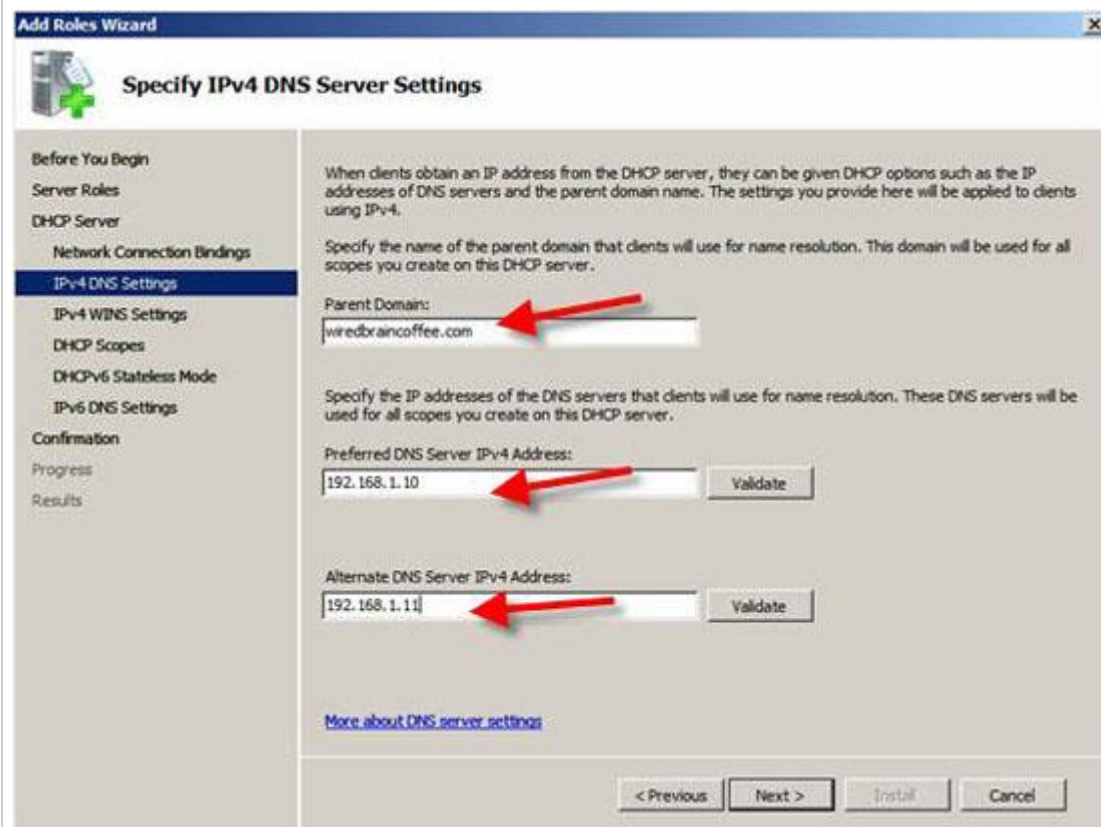
Trong trường hợp của chúng tôi, chúng tôi đã chọn để cấu hình một số thiết lập IP cơ bản và cấu hình DHCP Scope đầu tiên.

Chúng tôi đã thể hiện sự giàng buộc kết nối mạng của mình và đã được yêu cầu thẩm định nó, giống như bên dưới:



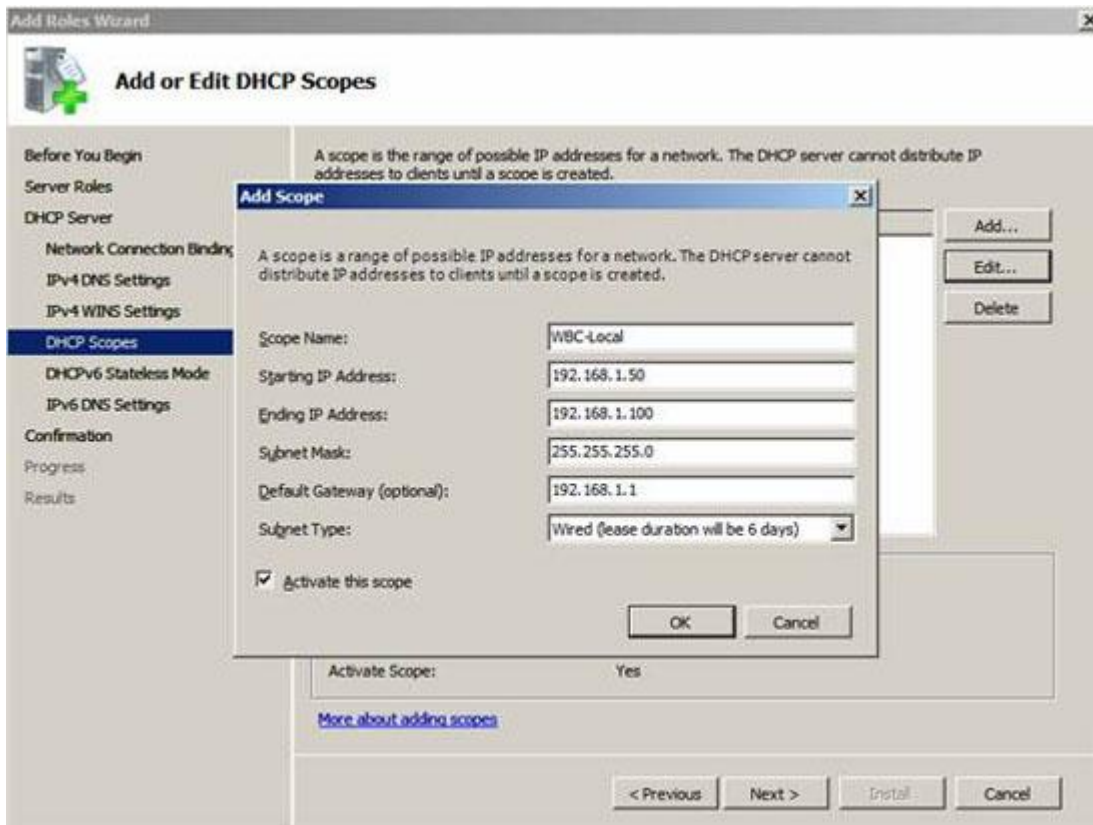
Những gì wizard này hỏi là, "what interface do you want to provide DHCP services on?" tạm được dịch là "giao diện bạn muốn cung cấp cho các dịch vụ DHCP là gì?" Chúng tôi đã chọn mặc định và kích **Next**.

Tiếp đến, nhập vào **Parent Domain**, **Primary DNS Server**, và **Alternate DNS Server** (xem hình bên dưới) và kích **Next**.



Chúng tôi đã lựa chọn NOT để sử dụng WINS trên mạng của mình và kích **Next**.

Sau đó chúng ta sẽ được tăng cấp để cấu hình DHCP scope cho DHCP Server mới. Chọn cấu hình dải địa chỉ IP là 192.168.1.50-100 cho hơn 25 máy khách trên mạng nội bộ của chúng tôi. Để thực hiện điều đó, bạn cần kích **Add** để bổ sung thêm một phạm vi mới. Như những gì bạn có thể thấy trong hình bên dưới, chúng tôi đã đặt tên Scope **WBC-Local**, đã cấu hình địa chỉ IP bắt đầu và kết thúc là 192.168.1.50-192.168.1.100, **subnet mask** là 255.255.255.0, **default gateway** là 192.168.1.1, **kiểu subnet** (chạy dây), và **activated** the scope.

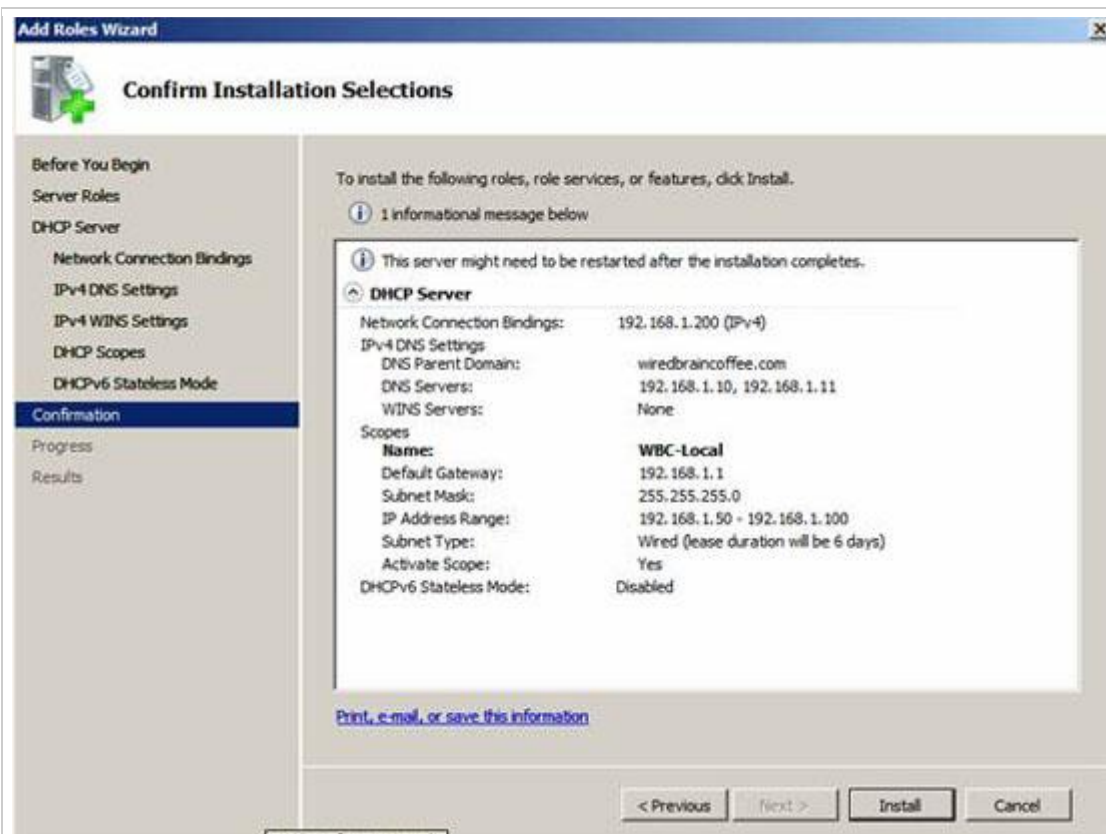


Quay trở lại màn hình Add Scope, chúng ta kích Next để bổ sung thêm một phạm vi mới (khi DHCP Server được cài đặt).

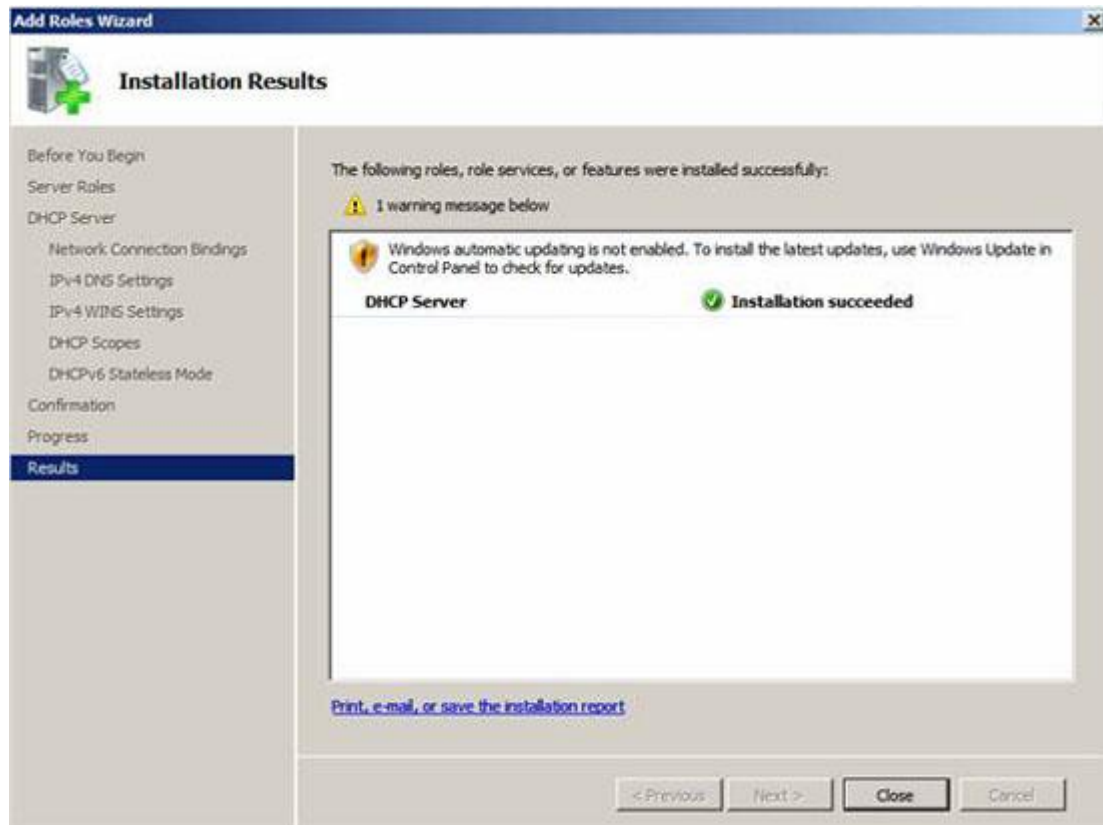
Chọn **Disable DHCPv6 stateless mode** cho máy chủ này và kích **Next**.

Sau đó xác nhận DHCP Installation Selections của mình (trên màn hình bên dưới) và kích **Install**.





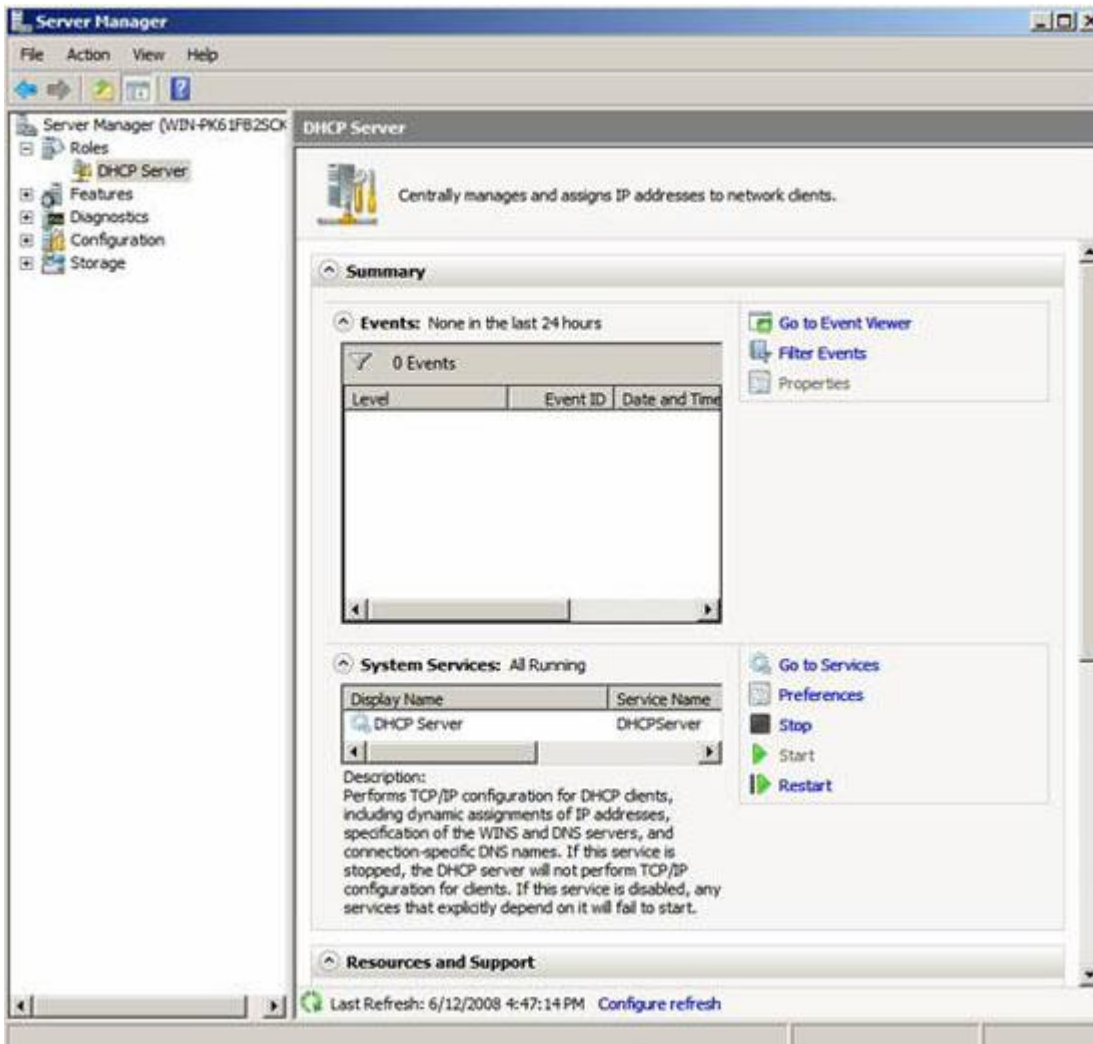
Sau đó một vài giây, DHCP Server sẽ được cài đặt và chúng ta sẽ thấy một cửa sổ xuất hiện như hình bên dưới:



Kích **Close** để đóng cửa sổ cài đặt, sau đó chúng ta hãy chuyển sang cách quản lý DHCP Server.

## Quản lý Windows Server 2008 DHCP Server mới

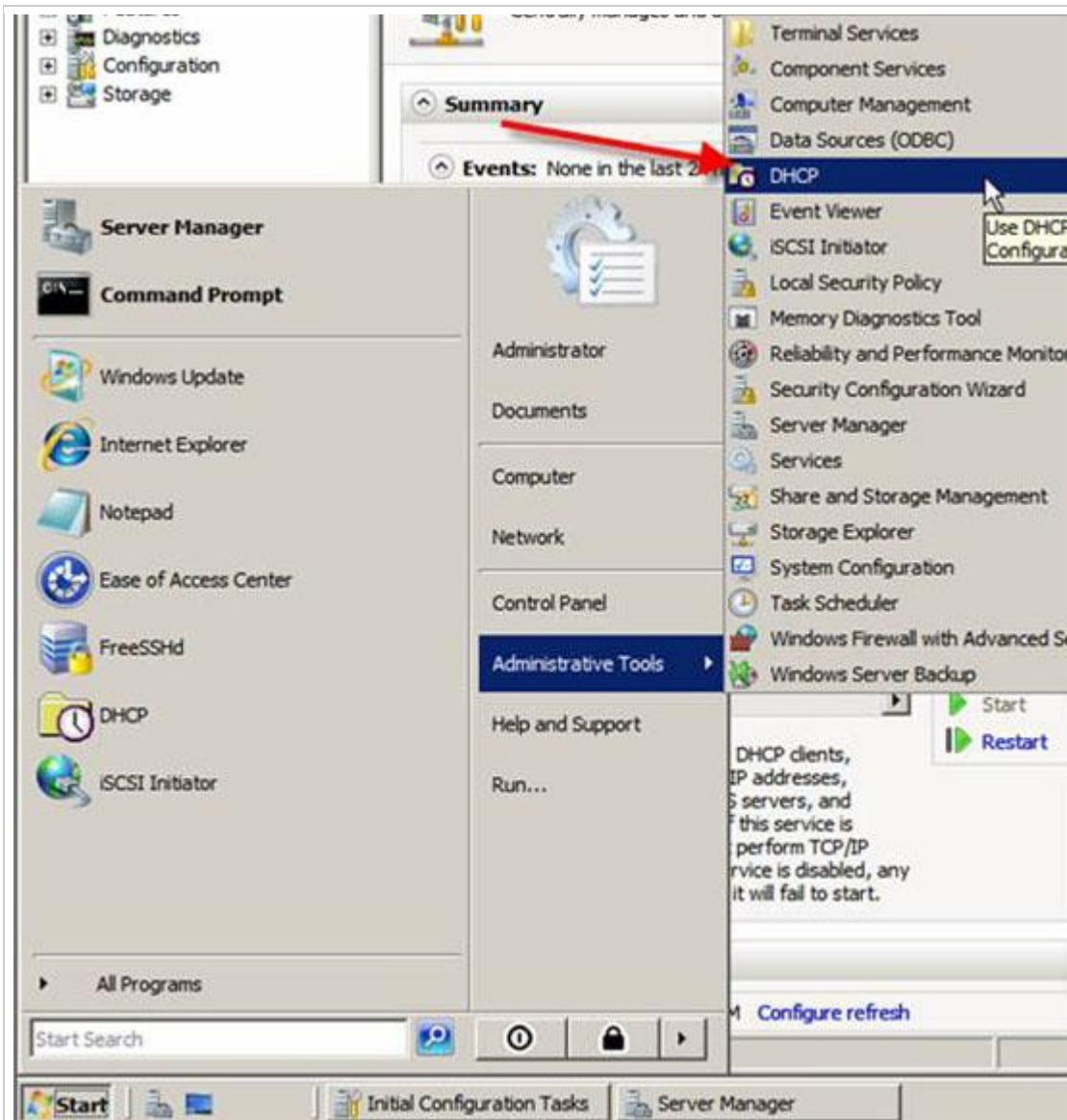
Giống như cài đặt, việc quản lý Windows Server 2008 DHCP Server cũng rất đơn giản. Quay trở lại với Windows Server 2008 **Server Manager**, trong **Roles**, kích vào entry **DHCP Server**.



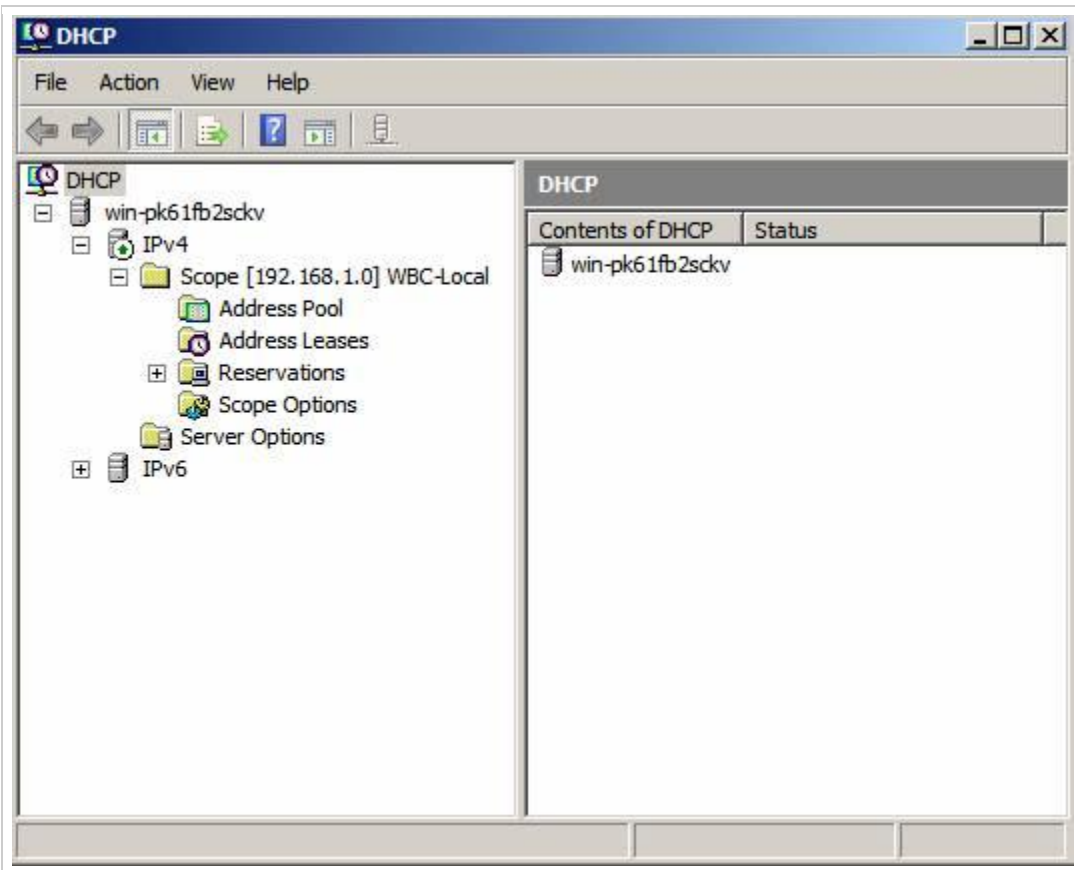
Do không thể quản lý các phạm vi DHCP Server và các máy khách tại đây nên những gì chúng ta có thể thực hiện là quản lý những sự kiện, dịch vụ và tài nguyên gì có liên quan đến cài đặt DHCP Server. Chính vì vậy, đây là nơi tốt để kiểm tra trạng thái của DHCP Server và những sự kiện gì đã xảy ra xung quanh nó.

Mặc dù vậy, để cấu hình DHCP Server và xem xem những máy khách nào đã thu được các địa chỉ IP, chúng ta cần vào DHCP Server MMC. Thực hiện điều đó, bạn cần vào **Start > Administrative Tools > DHCP Server**, giống như dưới đây:



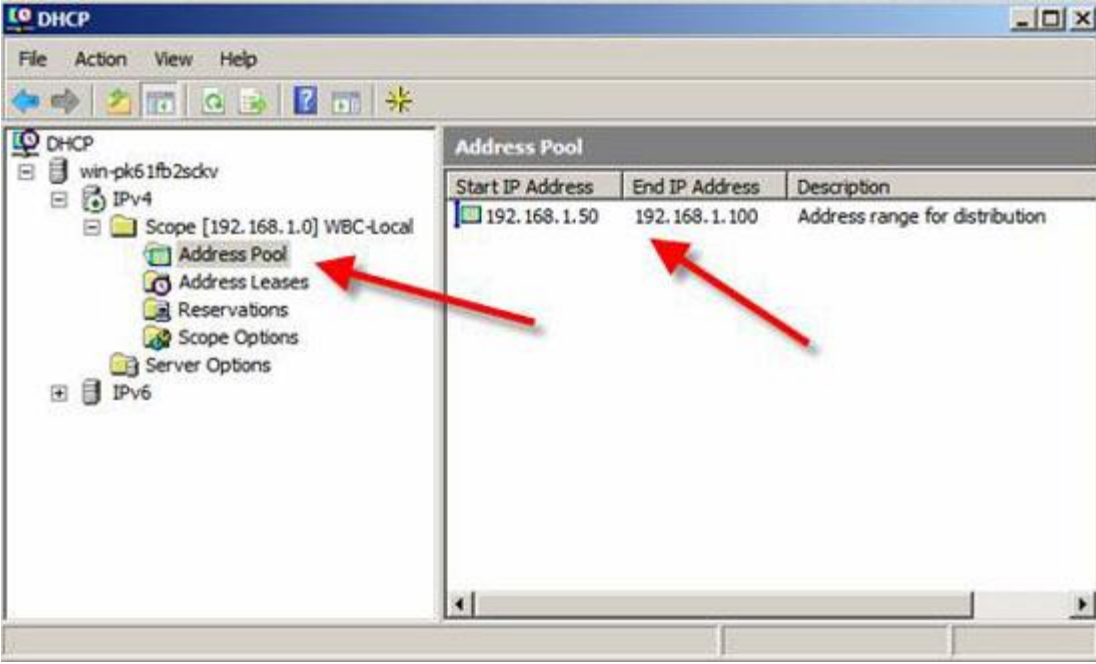


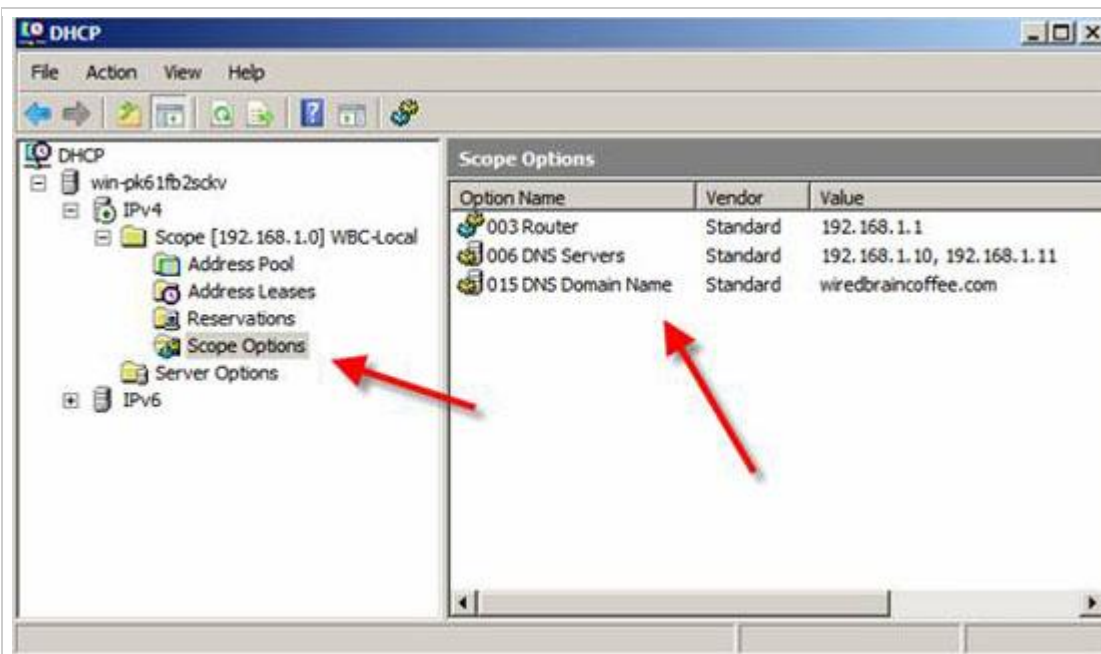
Khi khởi chạy, MMC sẽ cung cấp rất nhiều tính năng. Đây là những gì khi MMC xuất hiện:



DHCP Server MMC cung cấp các thông tin IPv4 & IPv6 DHCP Server gồm tất cả scope, pool, lease, reservation, scope options và server option.

Nếu vào address pool và scope options, chúng có thể thấy cấu hình mình đã tạo khi cài đặt DHCP Server. Dải địa chỉ IP nằm ở đây và DNS Server & gateway mặc định cũng vậy.



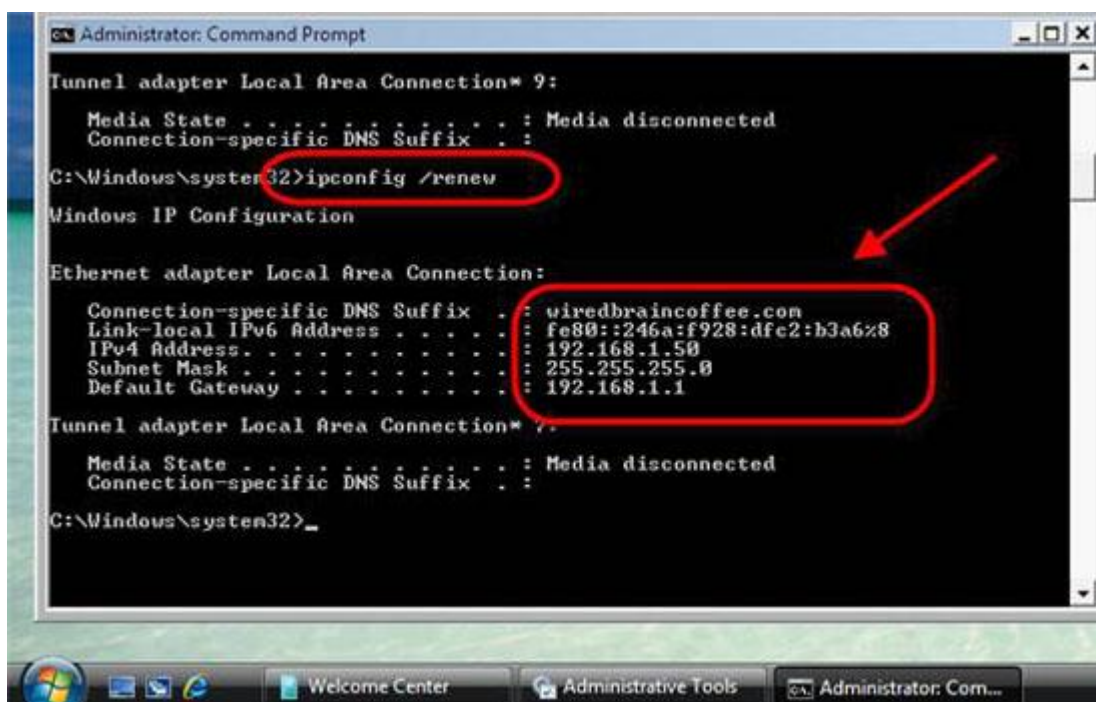


Vậy bằng cách nào chúng ta biết được các cấu hình có làm việc hay không? Để biết được điều đó, chúng ta phải thực hiện một bài test.

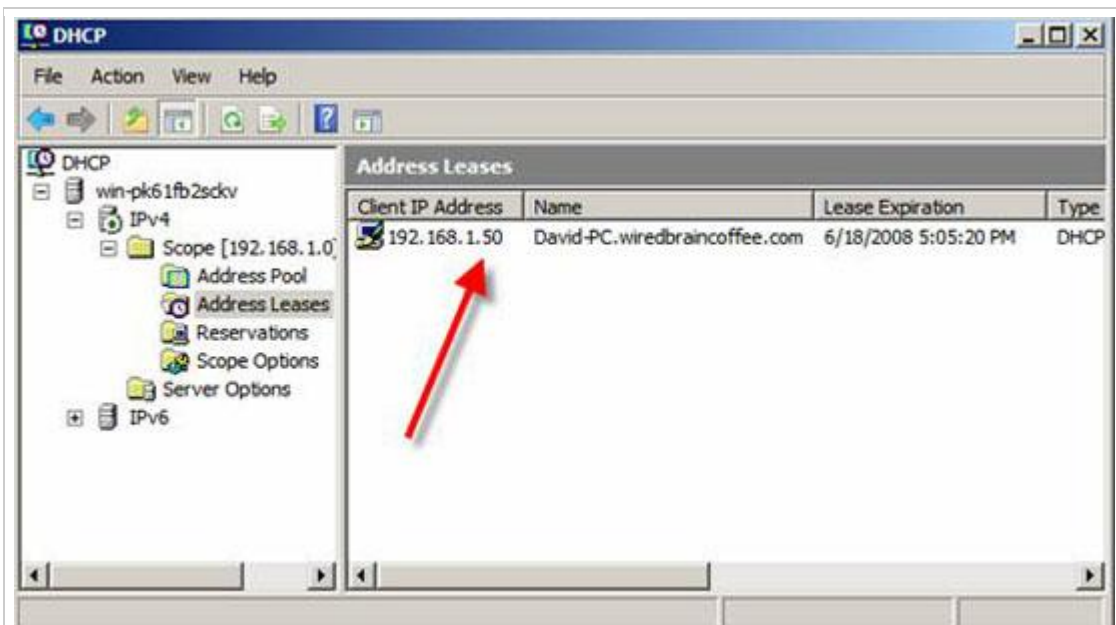
### Cách test Windows Server 2008 DHCP Server

Để test thử, chúng tôi có một máy khách Windows Vista trên cùng đoạn mạng với Windows Server 2008 DHCP server. Với mục đích an toàn, chúng tôi không cho thêm thiết bị khác vào đoạn mạng này.

Sử dụng lệnh **IPCONFIG /RELEASE** và sau đó là **IPCONFIG /RENEW**, chúng tôi thẩm định rằng mình đã nhận một địa chỉ IP từ một máy chủ DHCP mới, xem hình bên dưới:




Vào Windows 2008 Server vào thẩm định Vista client mới đã được liệt kê với tư cách máy khách trong máy chủ DHCP.



Với những thể hiện đó, chúng ta sẽ biết được rằng nhiệm vụ cấu hình của mình đã xong và cấu hình các thiết lập đã làm việc tốt!

### **Kết luận**

Trong bài viết này, chúng tôi đã giới thiệu cho các bạn về cách cài đặt và cấu hình DHCP Server trong Windows Server 2008. Trong suốt quá trình cài đặt, chúng tôi đã giới thiệu cho các bạn về DHCP Server là gì, cách nó có thể giúp bạn cũng như cách cài đặt và quản lý nó và máy chủ, cách cấu hình các thiết lập cụ thể của DHCP server giống như DHCP Server scopes. Phần cuối, chúng tôi đã test thử cấu hình đã được thực hiện như trong bài và nó đã làm việc hoàn hảo.



# **Cấu hình Window Mail**

## **kết nối với Gmail**

Tiếp theo chuỗi bài viết về cách cấu hình Window Mail kết nối với các nhà cung cấp e-mail khác nhau, hôm nay chúng tôi sẽ hướng dẫn từng bước cách cấu hình Window Mail kết nối với tài khoản Gmail. Như các bạn đã biết, Gmail là tài khoản email hỗ trợ POP3 miễn phí. Tuy nhiên để sử dụng đặc tính này bạn cần phải kích hoạt nó tại giao diện web Gmail.

### Cách kích hoạt POP3 trong Gmail

Trước khi bắt đầu hãy kiểm tra tài khoản Gmail của bạn POP3 đã được kích hoạt hay chưa. Để thực hiện hãy đăng nhập vào tài khoản Gmail và chọn *Settings* -> *Forwarding and POP/IMAP*



Chọn một trong hai tùy chọn sau để kích hoạt dịch vụ POP3: *Enable POP for all mail*, hoặc *Enable POP for mail that arrives from now on*.

1. Status: **POP is enabled** for all mail that has arrived since Oct 31

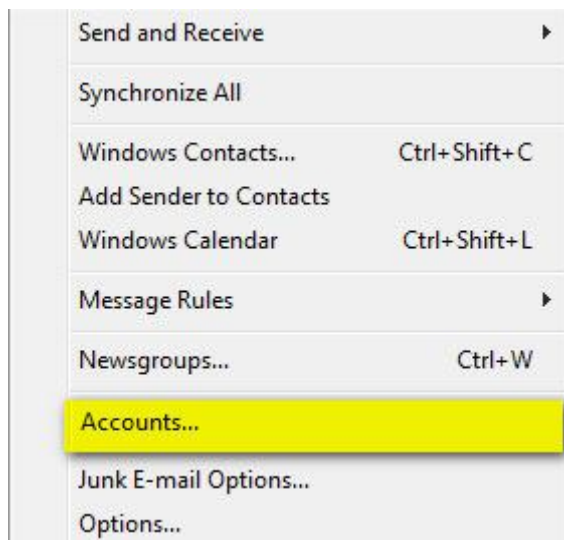
- Enable POP for **all mail** (even mail that's already been downloaded)
- Enable POP for **mail that arrives from now on**
- Disable POP

2. When messages are accessed with POP

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)  
[Configuration instructions](#)

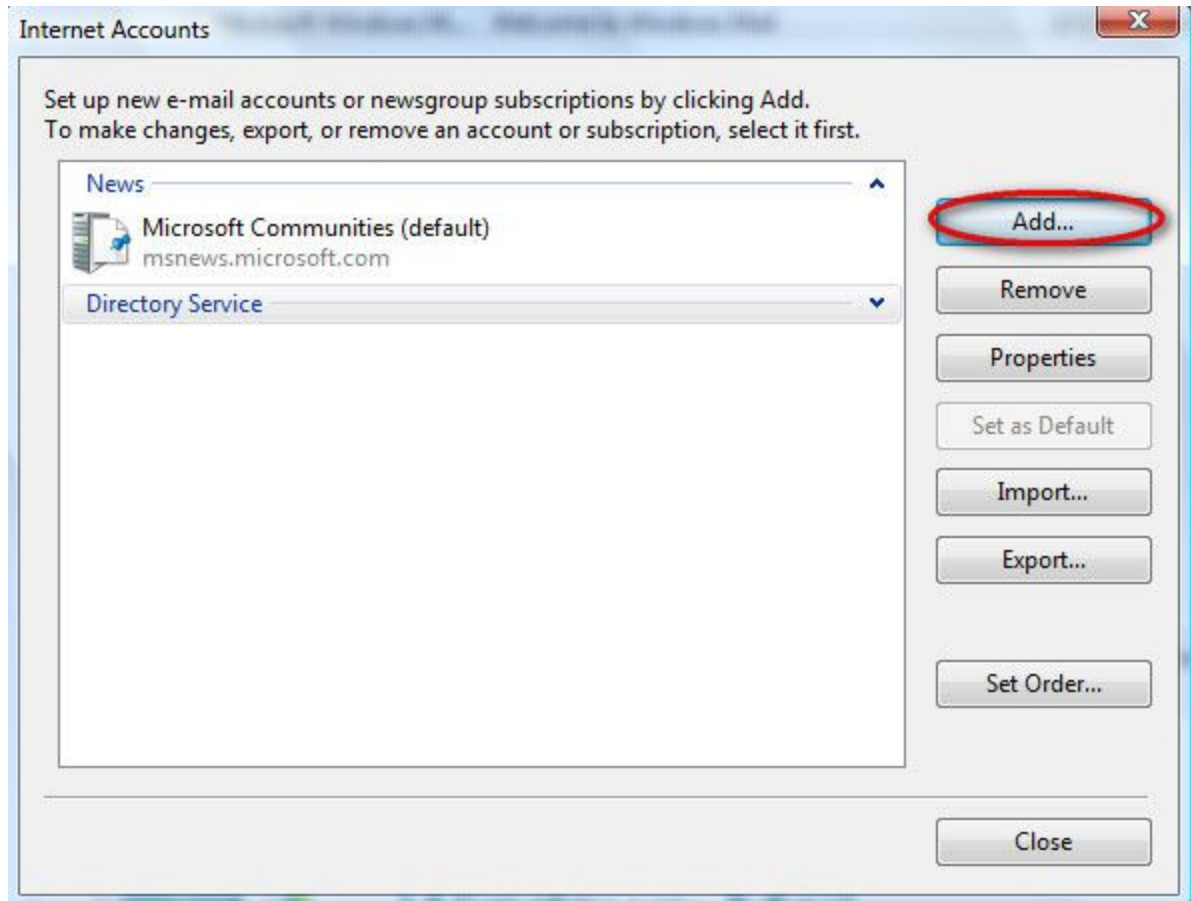
## Cách cấu hình Window Mail

Khởi động Window Mail vào **Tools** rồi ấn nút **Accounts** như hình dưới đây.



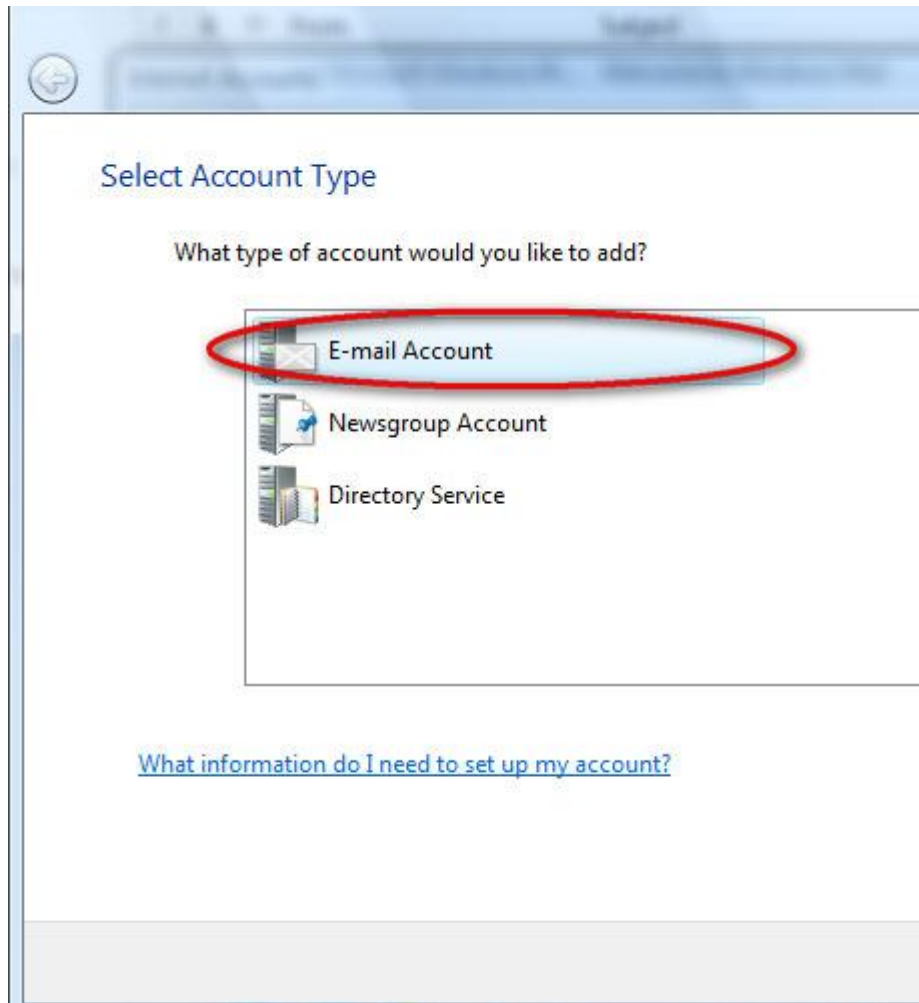
Sau đó kích nút **Add**.



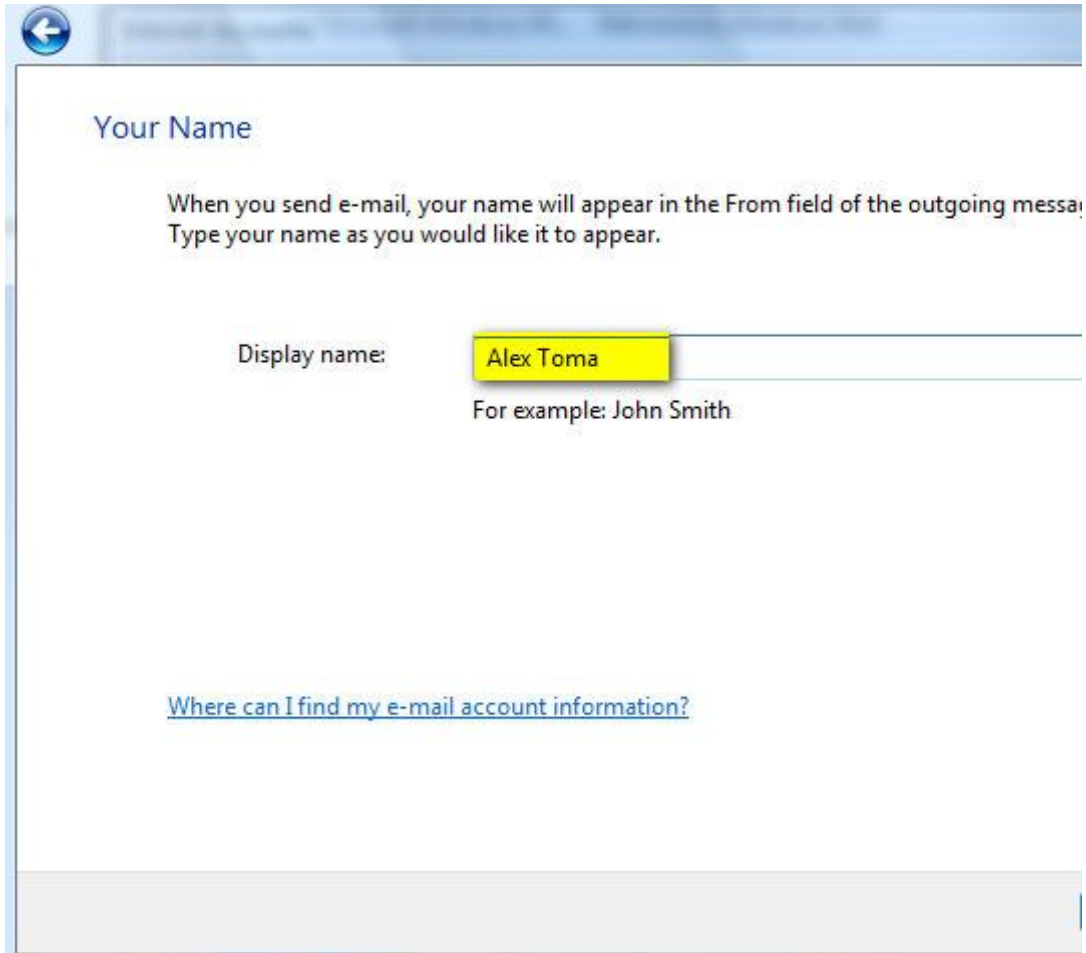


Chọn tùy chọn *E-mail Account* và kích *Next*.





Chọn tên và điền tên hiển thị sẽ xuất hiện trong thư bạn gửi đi rồi  
kích *Next* để chuyển sang cửa sổ tiếp theo.



The screenshot shows a window titled "Your Name" with a back arrow icon in the top-left corner. Below the title, there is a paragraph of text: "When you send e-mail, your name will appear in the From field of the outgoing message. Type your name as you would like it to appear." Below this text is a label "Display name:" followed by a text input field containing "Alex Toma". Below the input field is a small example text: "For example: John Smith". At the bottom of the window, there is a blue hyperlink: "[Where can I find my e-mail account information?](#)".

Bạn được yêu cầu điền địa chỉ e-mail. Hãy điền và kích *Next*.

Internet E-mail Address

Your e-mail address is the address other people use to send e-mail me

E-mail address:

For example: someone@microsoft.com

[Where can I find my e-mail account information?](#)

Trong cửa sổ tiếp theo bạn sẽ phải thiết lập máy chủ e-mail.

Tại *Incoming e-mail server* chọn POP3 và tại *Incoming & Outgoing server* nhập tên như hình bên dưới và kiểm tra tùy chọn *Outgoing server requires authentication*. Khi thực hiện xong kích *Next*.

Set up e-mail servers

Incoming e-mail server type:  
POP3

Incoming mail (POP3 or IMAP) server:  
pop.gmail.com

Outgoing e-mail server (SMTP) name:  
smtp.gmail.com

Outgoing server requires authentication

[Where can I find my e-mail server information?](#)

Next

Nhập địa chỉ e-mail và mật khẩu tại cửa sổ **Internet Mail Logon**. Để dễ dàng sử dụng hãy chọn **Remember password** và kích **Next**.

Internet Mail Logon

Type the account name and password your Internet service provider has given you.

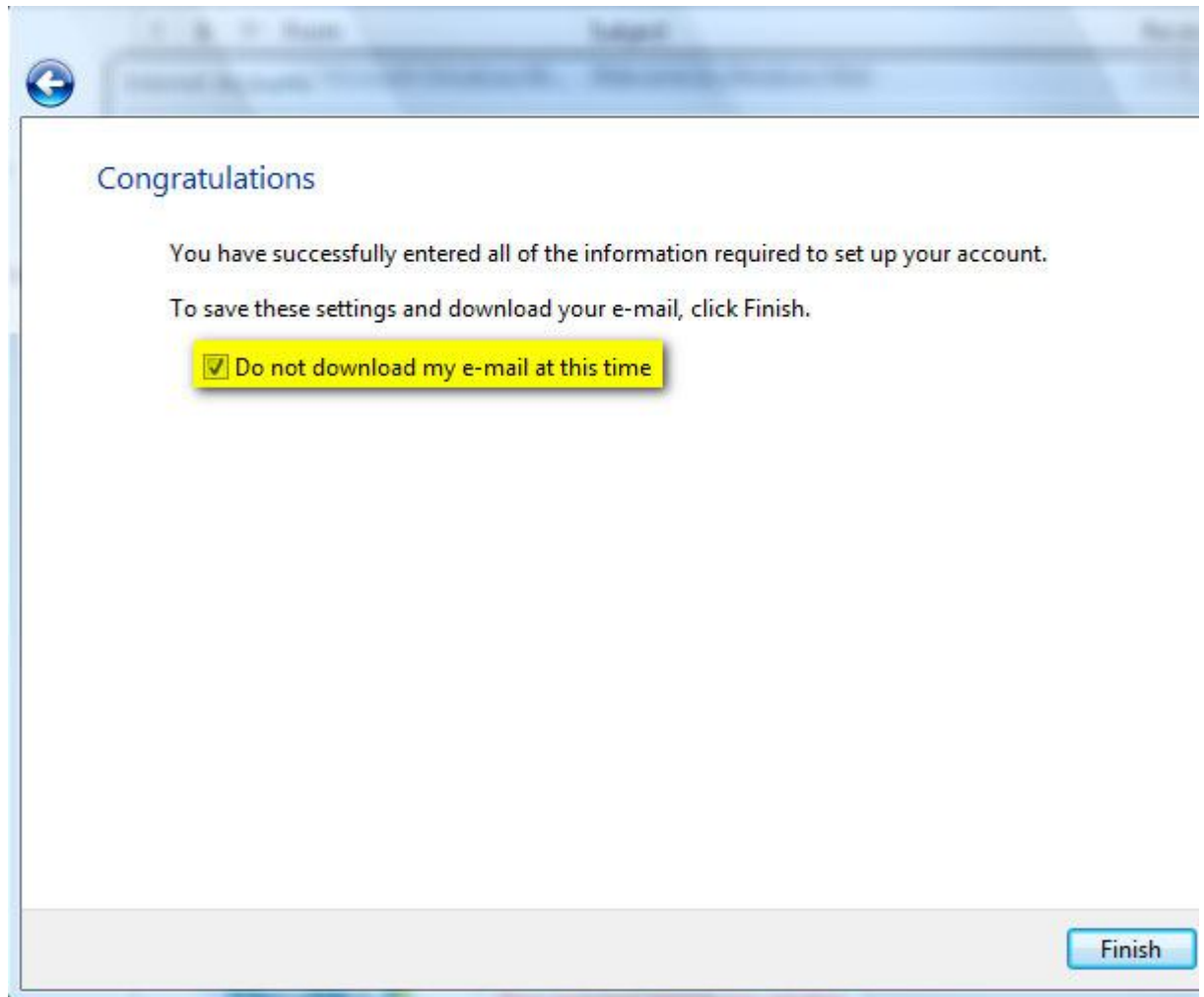
E-mail username:

Password:

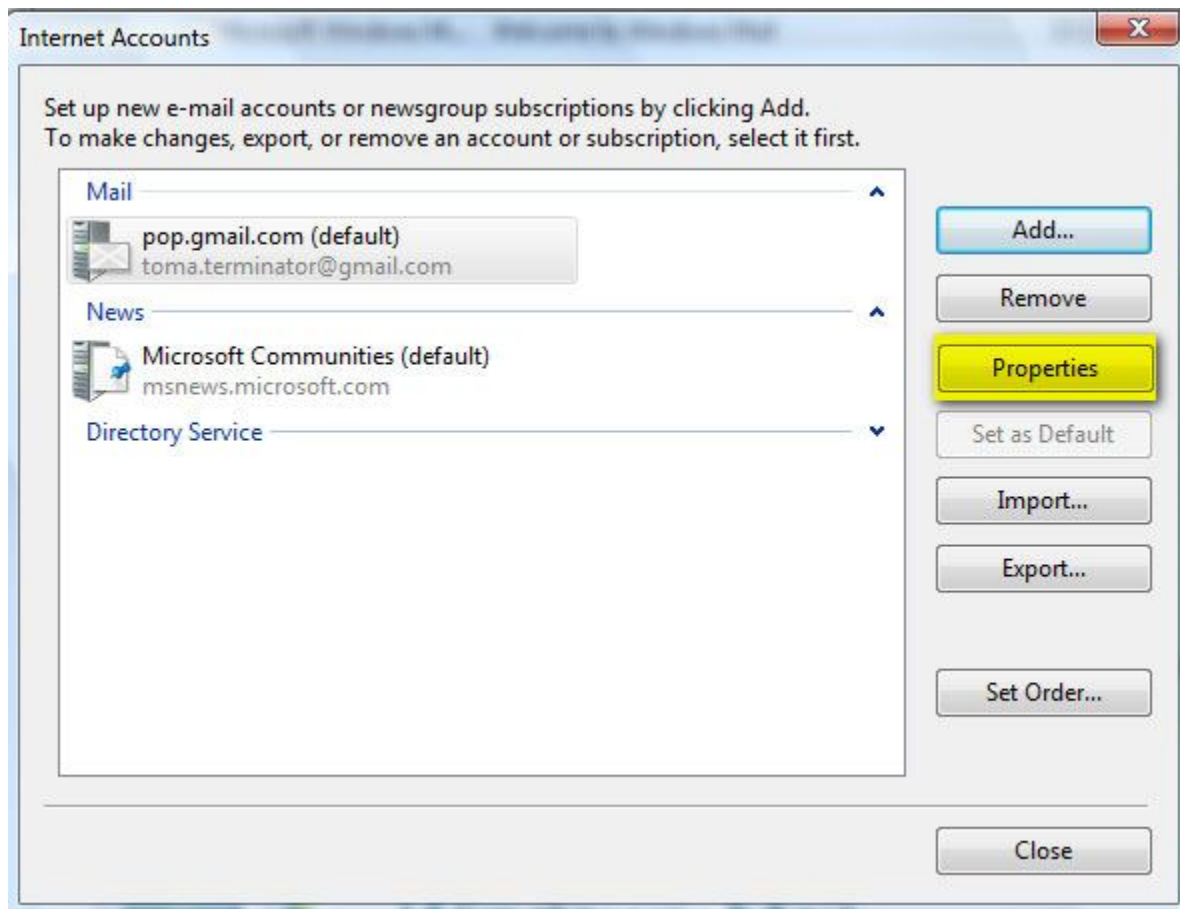
Remember password

Next

Tới đây công việc của bạn gần như đã được hoàn thành. Kích chọn ***Do not download my e-mail at this time*** rồi kích nút ***Finish***.



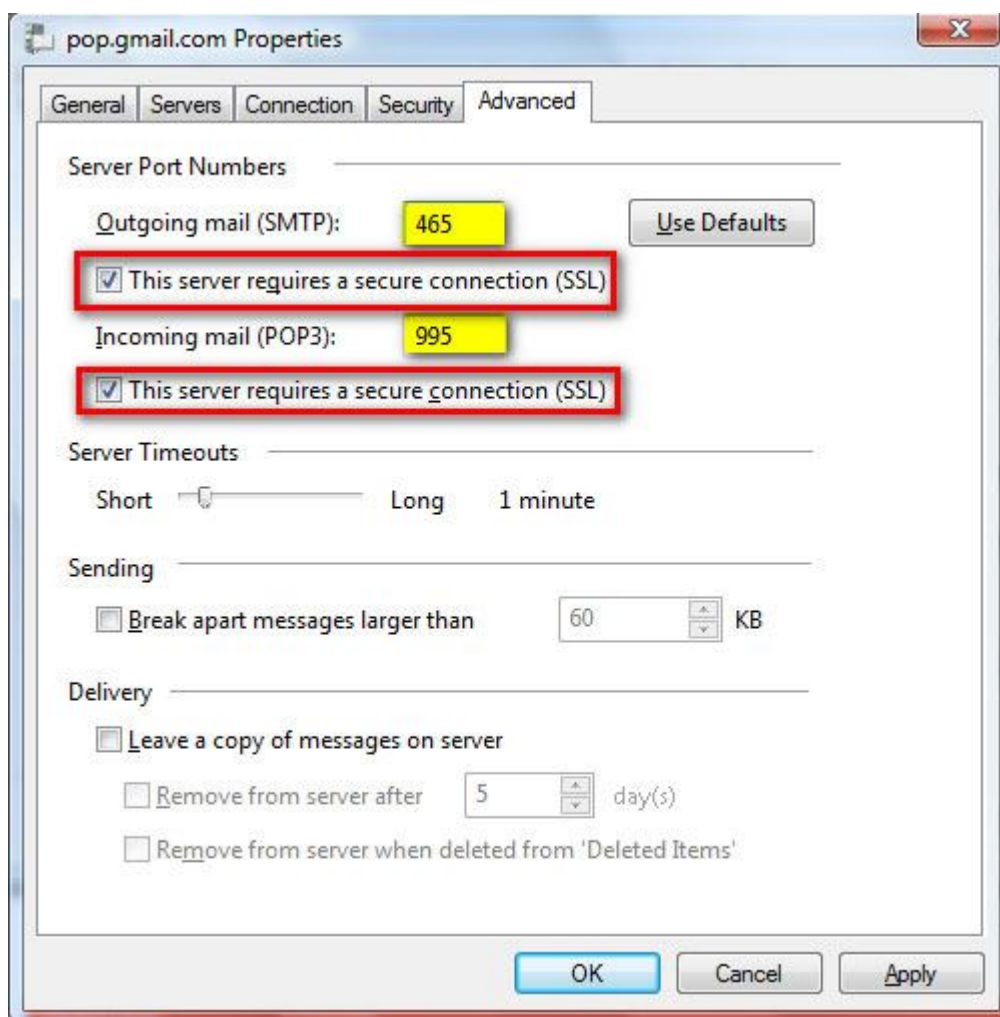
Cửa sổ **Internet Accounts** được mở ra. Hãy chọn tài khoản Gmail của bạn rồi kích **Properties**.



Tại thẻ *Advance* bạn nhập cổng **465** cho **SMTP** và cổng **995** cho **POP3**. Chú ý kích chọn "*This server requires a secure connection (SSL)*" cho cả POP3 và SMTP.

Nếu muốn thư của bạn lưu trên máy chủ Gmail thì đừng quên kích chọn *Leave a copy of messages on server*. Nếu không chọn tùy chọn này thì khi thư của bạn được tải về nó sẽ tự động bị xóa khỏi Gmail.

Sau khi đã hoàn thành, kích **OK**.



Window Mail giờ đây đã được cấu hình kết nối với tài khoản Gmail của bạn. Hãy nhấn nút **Send/Receive** để bắt đầu gửi và nhận thư.