

# MCSA LAB

(Routing, DHCP, DNS, IIS, IPSec)

## MỤC LỤC

### **A/ Định tuyến**

I/ Mô tả mô hình và cài đặt dịch vụ định tuyến.

II/ Cấu hình định tuyến tĩnh (Static routing).

III/ Cấu hình định tuyến động.

### **B/ Dịch vụ cấp phát IP (DHCP)**

I/ Mô tả mô hình và cài đặt dịch vụ DHCP.

II/ Cấu hình DHCP.

III/ Thực hiện xin cấp IP từ máy Client.

IV/ Phân biệt sự khác nhau giữa các chế độ server, scope, class, reserved client trong DHCP.

V/ Cấu hình áp dụng chế độ Class trong việc cấu hình thông tin IP trên DHCP Server.

VI/ Cấu hình DHCP Relay Agent.

### **C/ Hệ thống phân giải tên miền (DNS).**

I/ Mô tả mô hình và cài đặt dịch vụ DNS.

II/ Cấu hình dịch vụ DNS.

### **D/ Dịch vụ Web IIS.**

I/ Cài đặt dịch vụ Web IIS.

II/ Cấu hình dịch vụ Web IIS.

### **E/ Dịch vụ mã hóa đường truyền IPSec.**

I/ Mô tả mô hình.

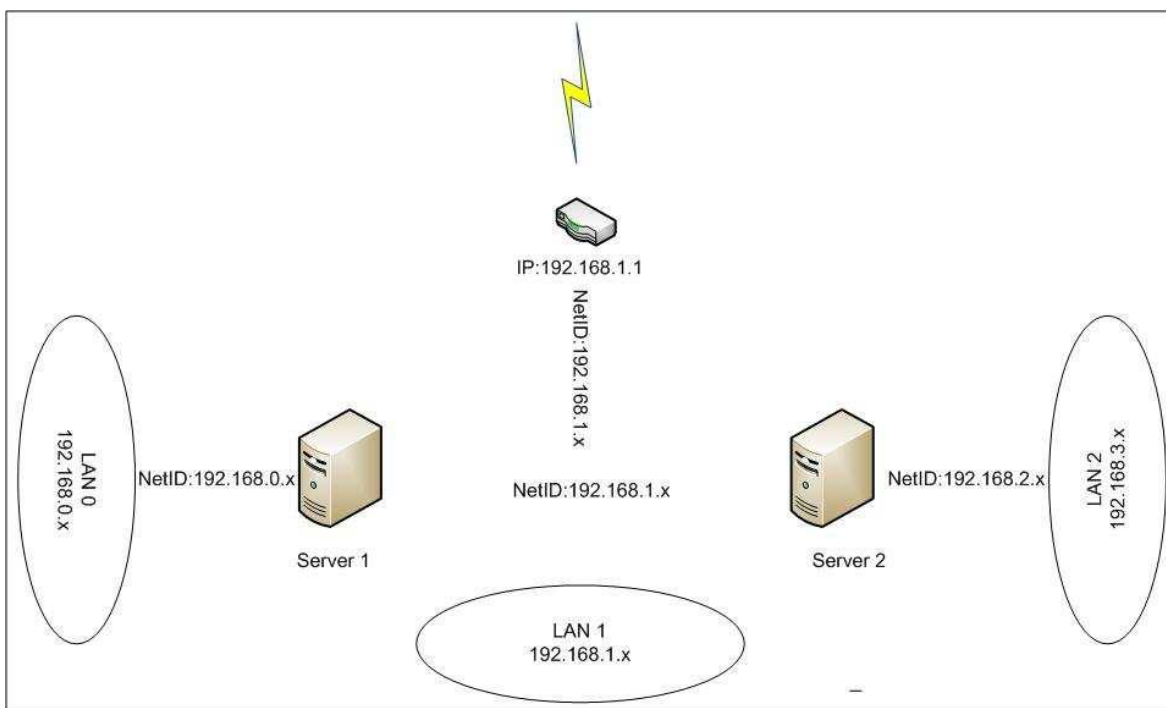
II/ Cấu hình IPSec dùng phương pháp Preshared-key.

# Định tuyến

## I/ Mô tả mô hình và cài đặt dịch vụ định tuyến.

Ở phần này ta thực hiện trên 2 máy Windows Server 2003. Các máy server này đảm nhận chức năng như 2 router mềm để định tuyến đường đi trong hệ thống mạng.

		Card LAN	Card Cross
Server 1	IP	192.168.0.10	192.168.1.10
	SM	255.255.255.0	255.255.255.0
	GW	để trống	để trống
	DNS	để trống	để trống
Server 2	IP	192.168.2.10	192.168.1.11
	SM	255.255.255.0	255.255.255.0
	GW	để trống	để trống
	DNS	để trống	để trống

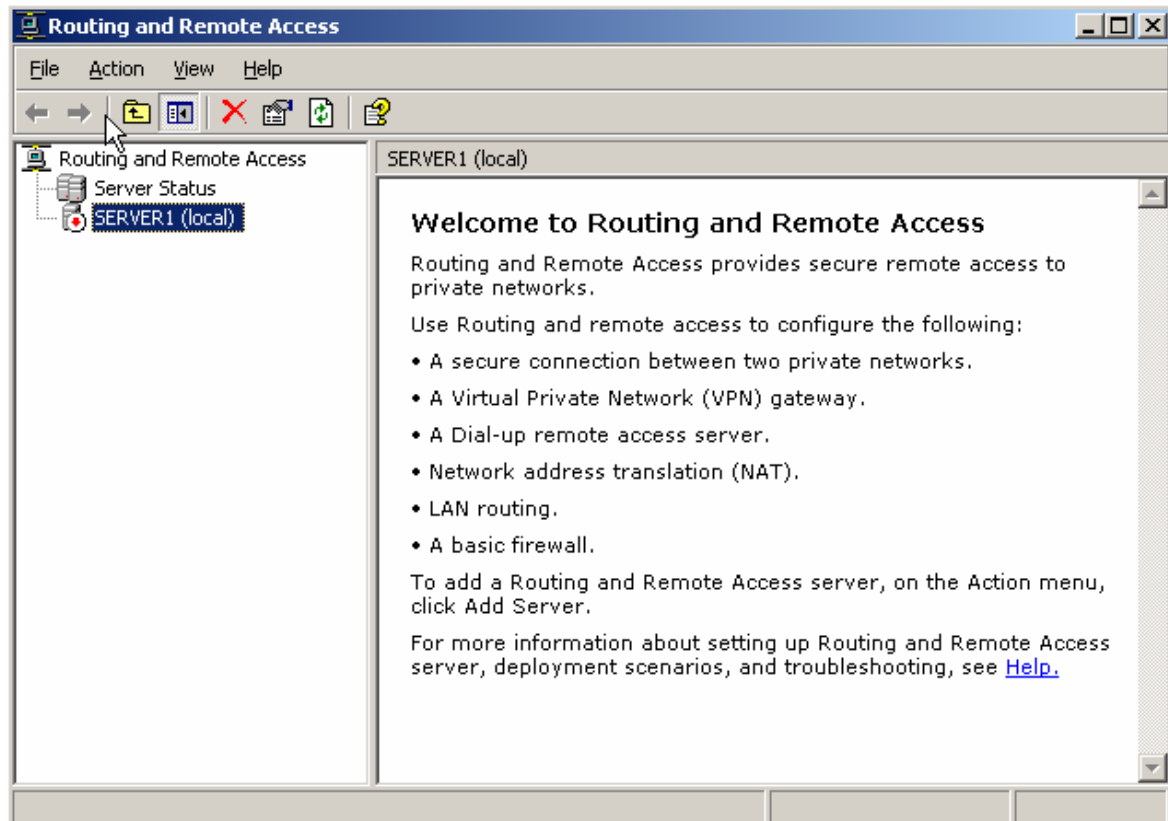


Test: Mặc định các máy client bên LAN 0 không thể liên lạc với các máy client bên LAN 1 nếu chưa có một giải pháp định tuyến nào. Các bạn có thể test bằng lệnh ping.

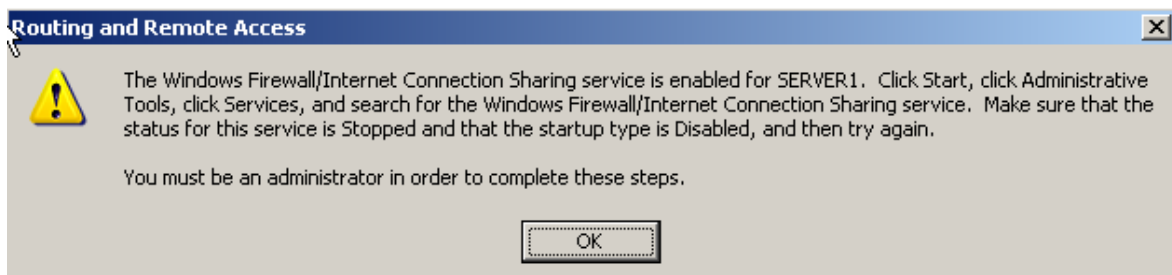
Client bên LAN 0	Client bên LAN 2
IP: 192.168.0.100	IP: 192.168.1.100
SM: 255.255.255.0	SM: 255.255.255.0
<b>GW: 192.168.0.10</b>	<b>GW: 192.168.1.1</b>

## B1/ Cài đặt chức năng LAN Routing and Remote Access trên máy tính Server 1.

Start, chọn **Programs**, chọn **Administrative Tools** và chọn **Routing and Remote Access**. Hoặc các bạn dùng câu lệnh **rrasmgmt.msc** để vào. Chương trình có giao diện như sau:

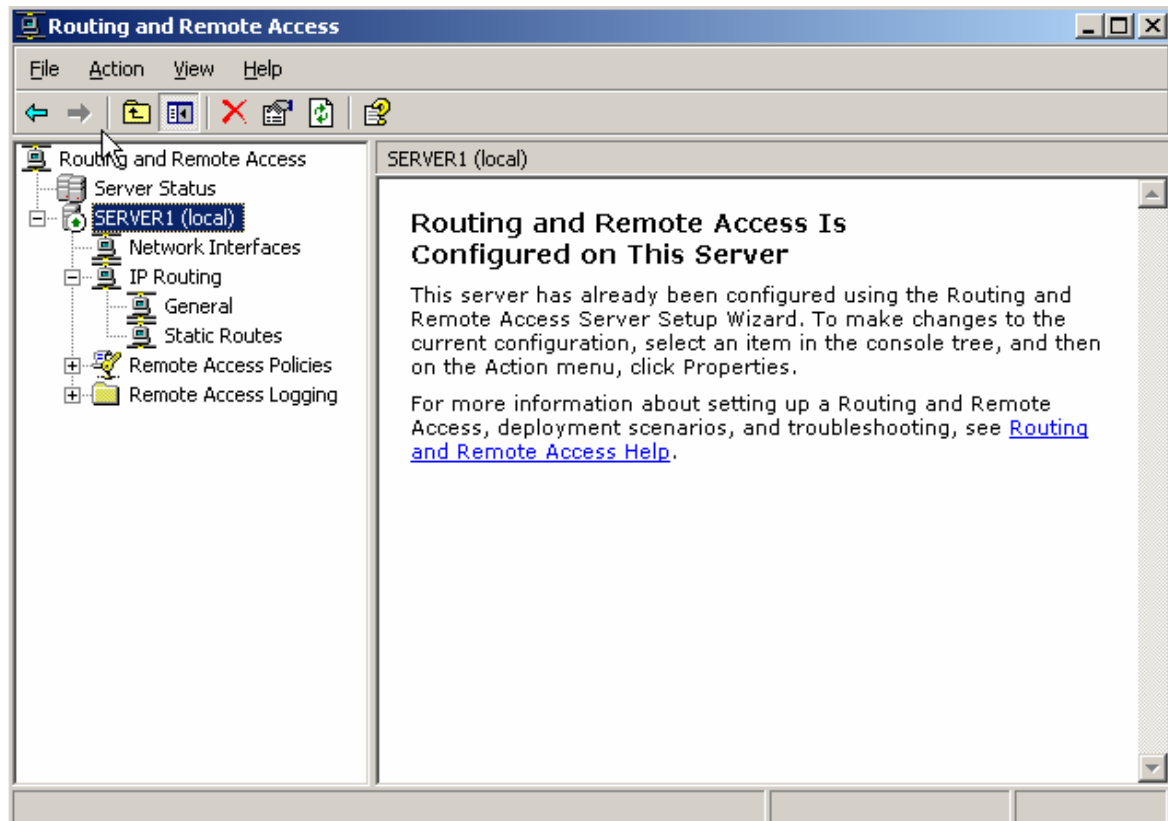


Right click vào tên **Server1** chọn **Configure and Enable Routing and Remote Access**. Nếu các bạn gặp hộp thoại cảnh báo như sau:



Cách khắc phục: Start, chọn **Programs**, chọn **Administrative Tools** và chọn **Services** - tắt và disable dịch vụ **Windows Firewall/Internet Connection Sharing** đi và làm lại bước **Configure and Enable Routing and Remote Access**.

Khi hộp thoại cấu hình xuất hiện bạn thực hiện tiếp các bước sau: click **Next** => chọn **Custom Configuration** - click **Next** => chọn **Lan Routing** – click **Next** => **Finish**. Sau khi cấu hình chính xác sẽ có giao diện như sau:



Kết quả Bước 1: Các client bên LAN 0 có thể tương tác với các client bên LAN 1 mặc dù hai lớp mạng này khác NetID nhau. Test kết quả bằng lệnh ping.

#### B2/ Cài đặt chức năng LAN Routing and Remote Access trên máy tính Server 2.

Các bạn làm tương tự như bên Server 1. Sau khi làm xong nhớ test kiểm tra sự tương tác giữa hai lớp LAN 2 và LAN 1. Nếu tương tác thành công xem như cấu hình đúng!

#### B3/ Cài đặt chức năng định tuyến trên cả hai Server: Server 1 và Server 2.

Chúng ta thấy rằng hiện tại LAN 0 và LAN 1 có thể tương tác với nhau, LAN 2 và LAN 1 có thể tương tác với nhau. Tuy nhiên LAN 0 và LAN 2 không thể tương tác với nhau được! Vì sao? Vì chúng ta chưa có một giải pháp định tuyến nào cho hai lớp mạng này (không có tính chất bắc cầu). Vì thế ta phải thực hiện định tuyến trên cả hai server để hai lớp LAN 0 và LAN 2 có thể tương tác với nhau.

Chúng ta sẽ thực hiện cấu hình cả hai loại định tuyến là : định tuyến tĩnh (static routing) và định tuyến động (dynamic routing).

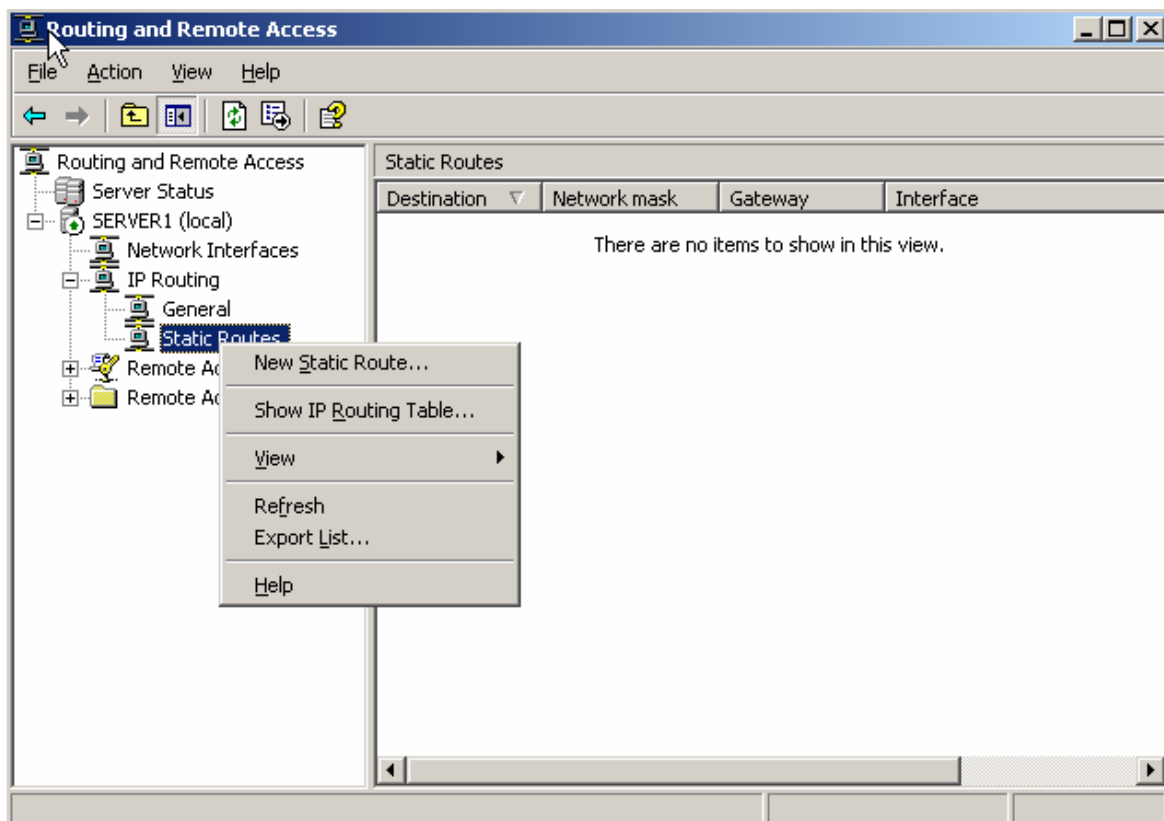
Default route cũng là một dạng của static routing.

Dynamic routing có hai giao thức là OSPF và RIP.

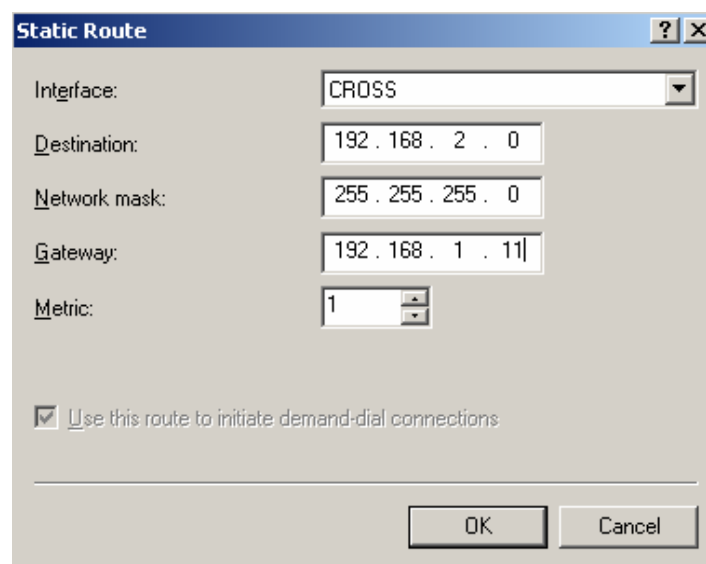
## II/ Cấu hình định tuyến tĩnh (STATIC ROUTING).

Trên Server 1:

Trong cửa sổ Routing and Remote Access, right click vào Static routings.



Cửa sổ cấu hình static routing như sau:



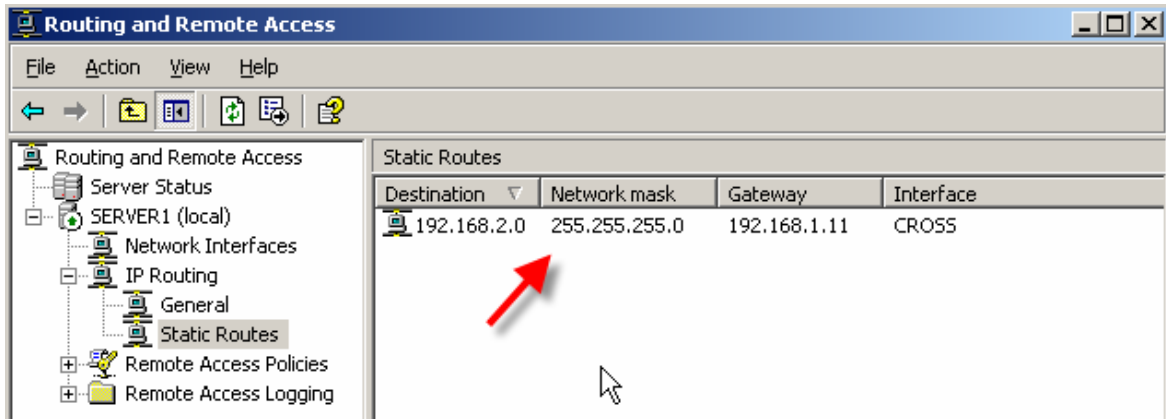
Interface: Chọn card mạng **CROSS**

Destination: Chọn NetID của lớp mạng cần tương tác đến (ở đây lớp mạng 0.x cần tương tác đến lớp mạng 2.x) => **Đánh vào NetID là 192.168.2.0**

Network mask: Mặc định **theo lớp mạng 2.x**

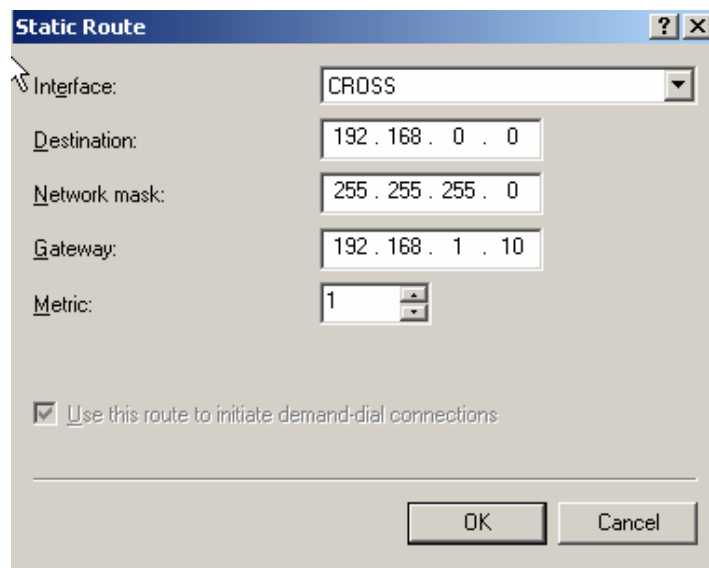
Gateway: **Đánh vào địa chỉ 192.168.1.11** (là địa chỉ IP card CROSS trên Server 2)

Sau khi điền hết thông tin, click **OK** để hoàn tất. Giao diện sau khi định tuyến sẽ như sau:



Trên Server 2:

Các bạn làm tương tự , tuy nhiên thông tin định tuyến sẽ khác. Cụ thể như sau:

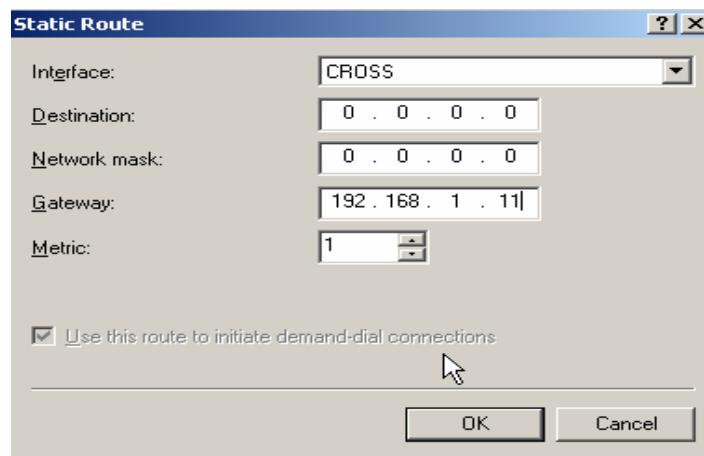


Sau khi định tuyến xong trên cả hai Server, giờ bạn có thể kiểm chứng sự tương tác giữa hai lớp LAN 0 và LAN 2.

Client bên LAN 0	Client bên LAN 2
IP:192.168.0.100	IP: 192.168.2.100
SM: 255.255.255.0	SM: 255.255.255.0
GW: 192.168.0.10	GW: 192.168.2.10

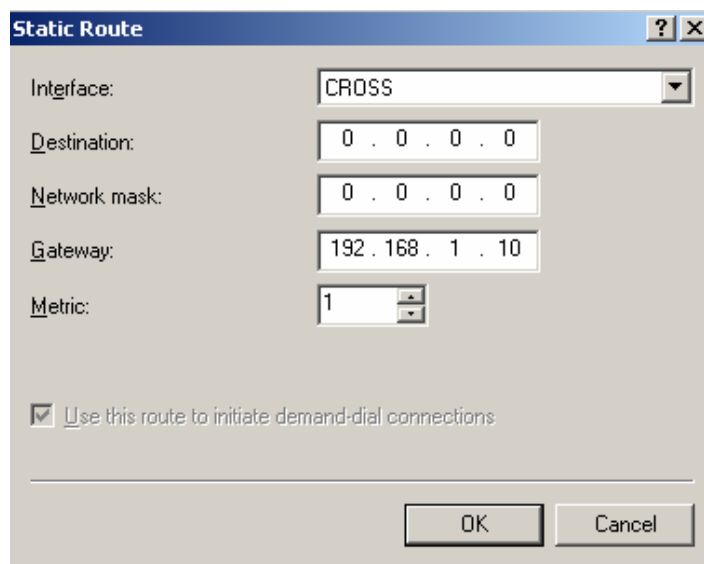
\*Cấu hình định tuyến tĩnh theo phương thức DEFAULT ROUTE.

Các bạn thực hiện tương tự ở static routing, tuy nhiên lúc này thông tin định tuyến sẽ như sau: Trên Server 1.



The image shows a 'Static Route' configuration window. The 'Interface' dropdown is set to 'CROSS'. The 'Destination' field is '0 . 0 . 0 . 0', the 'Network mask' is '0 . 0 . 0 . 0', and the 'Gateway' is '192 . 168 . 1 . 11'. The 'Metric' is set to '1'. There is a checkbox labeled 'Use this route to initiate demand-dial connections' which is checked. At the bottom are 'OK' and 'Cancel' buttons.

Trên Server 2.



The image shows a 'Static Route' configuration window. The 'Interface' dropdown is set to 'CROSS'. The 'Destination' field is '0 . 0 . 0 . 0', the 'Network mask' is '0 . 0 . 0 . 0', and the 'Gateway' is '192 . 168 . 1 . 10'. The 'Metric' is set to '1'. There is a checkbox labeled 'Use this route to initiate demand-dial connections' which is checked. At the bottom are 'OK' and 'Cancel' buttons.

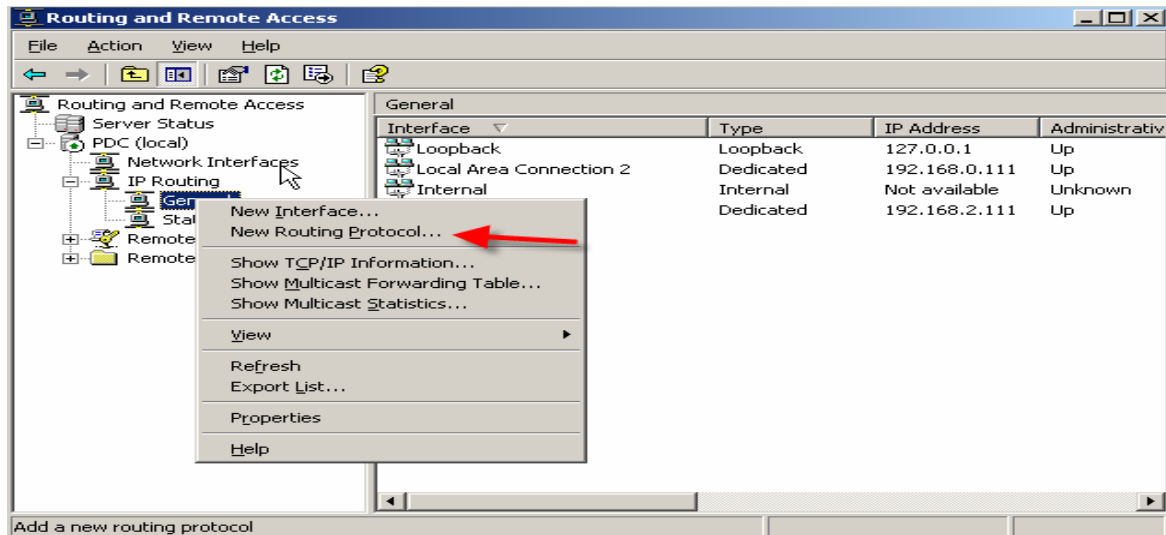
**III/ Cấu hình định tuyến động (DYNAMIC ROUTING).**

Định tuyến động thực hiện tương đối dễ dàng hơn định tuyến tĩnh, vì ưu điểm này nên định tuyến động được thực hiện trên mạng diện rộng. Ở bài Lab này ta thực hiện định tuyến động với hai giao thức là : RIP và OSPF. Cả hai Server 1 và Server 2 đều cấu hình tương tự nhau.

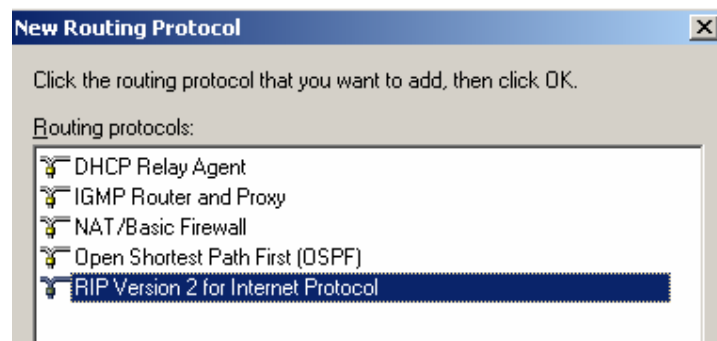
Trường hợp sử dụng giao thức định tuyến RIP.

Ở cửa sổ Routing and Remote Access, right click và dòng General chọn New Routing Protocol



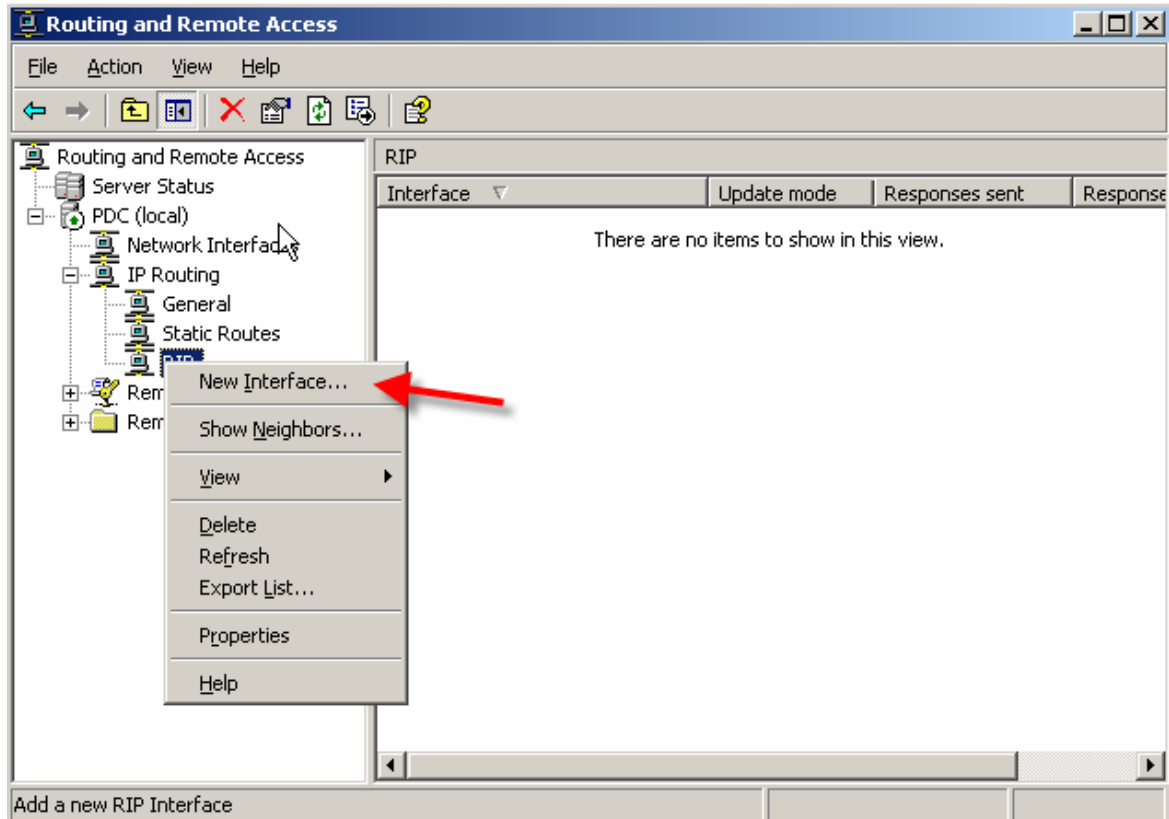


Chọn RIP Version 2 for Internal Protocol =>OK

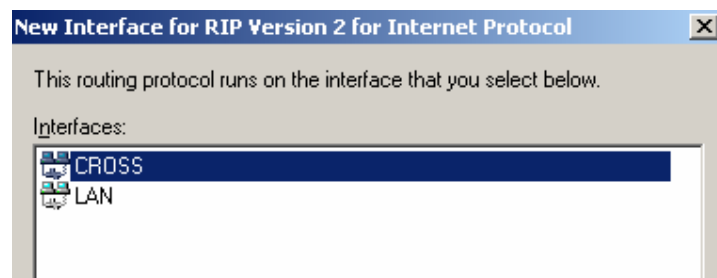


Giao diện cửa sổ Routing and remote access sau khi chọn giao thức định tuyến RIP sẽ có thêm một dòng RIP

Right click và dòng RIP và chọn New Interface.



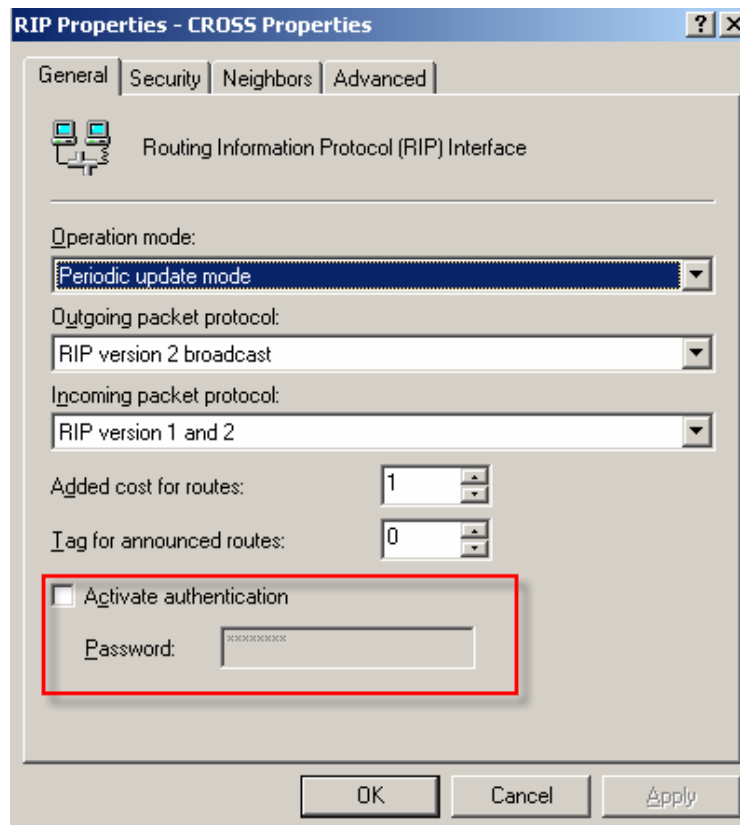
Chọn card CROSS (là interface card giao tiếp giữa các server với nhau) =>OK



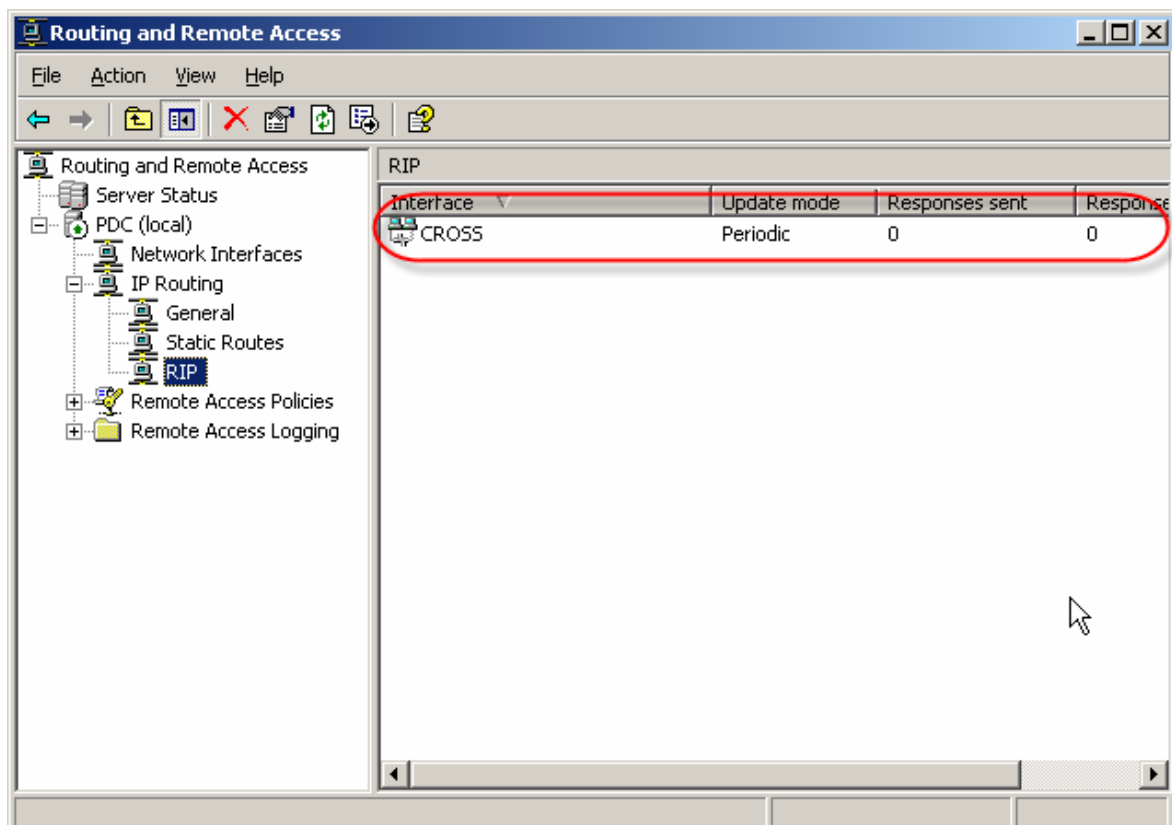
Giao diện của sổ RIP Properties sẽ xuất hiện như sau: Chọn

OK để hoàn tất định tuyến.

\*Lưu ý: Ở tùy chọn Activate authentication, nếu ta sử dụng tùy chọn này thì phải có cùng password trên cả hai server 1 và 2.

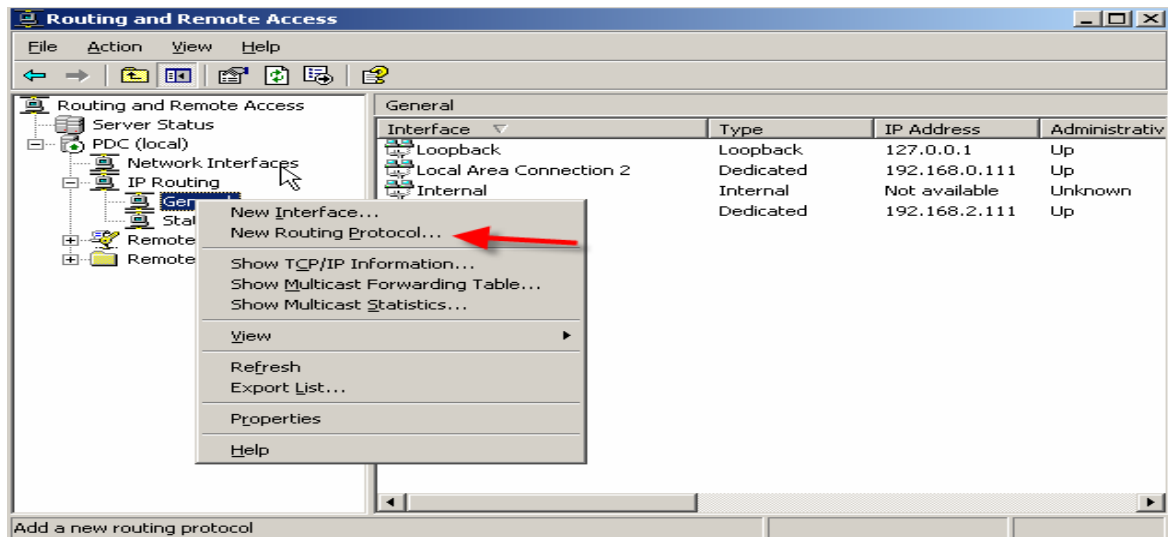


Giao diện của sổ Routing and Remote access sau khi định tuyến với giao thức RIP như sau:

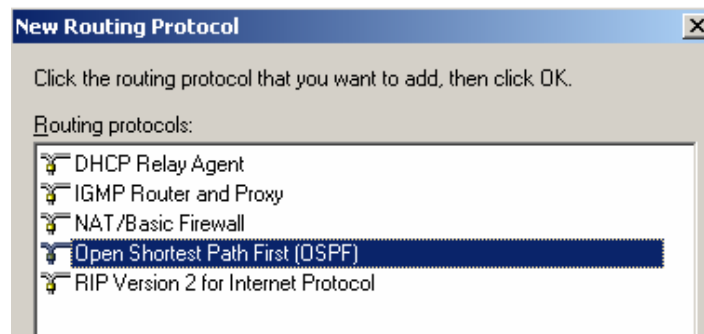


Trường hợp sử dụng giao thức định tuyến OSPF.

Ở cửa sổ Routing and Remote Access, right click và dòng General chọn New Routing Protocol

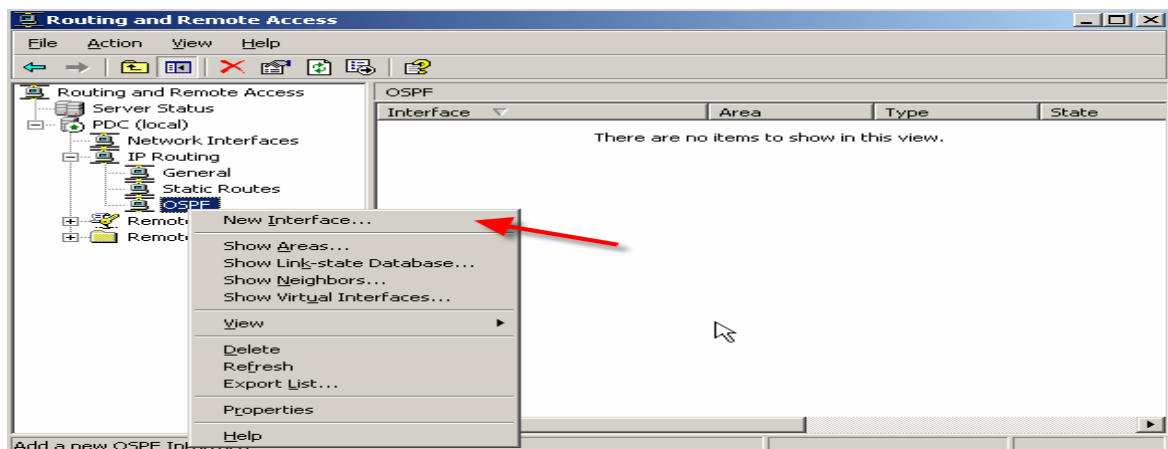


Chọn Open Shortes Path First (OSPF).

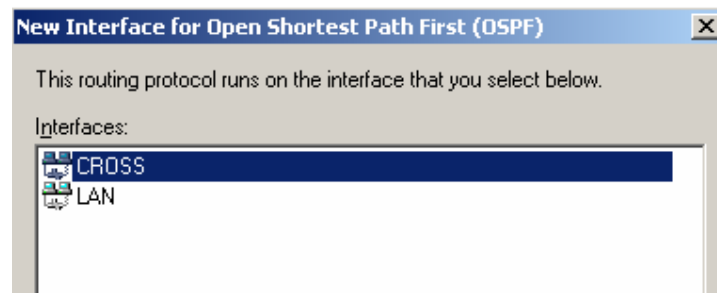


Giao diện cửa sổ Routing and remote access sau khi chọn giao thức định tuyến RIP sẽ có thêm một dòng OSPG

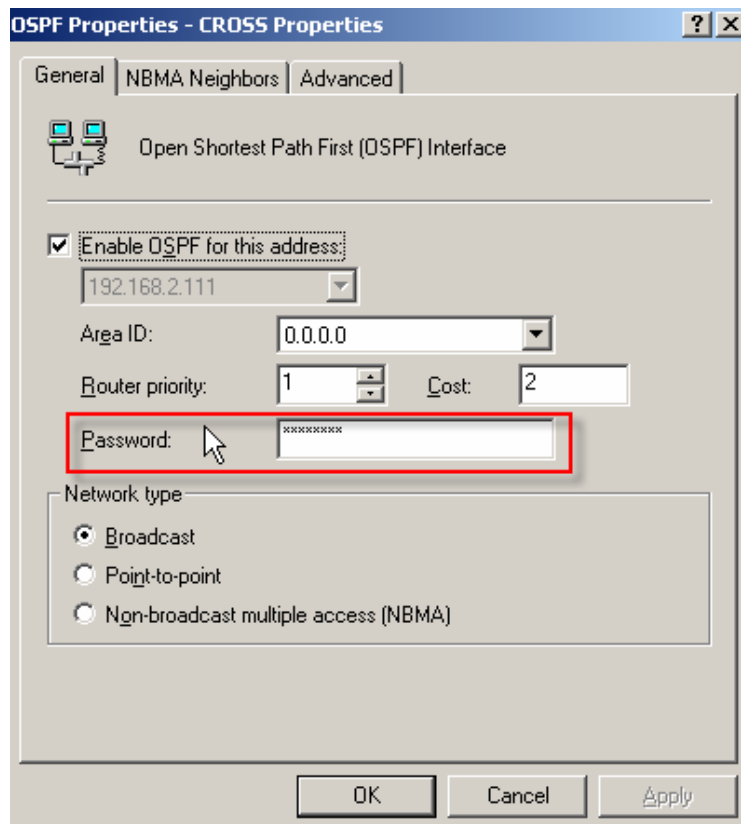
Right click và dòng OSPF và chọn New Interface..



Ở giao thức định tuyến OSPF này, ta lần lượt chọn cả hai card CROSS và LAN.

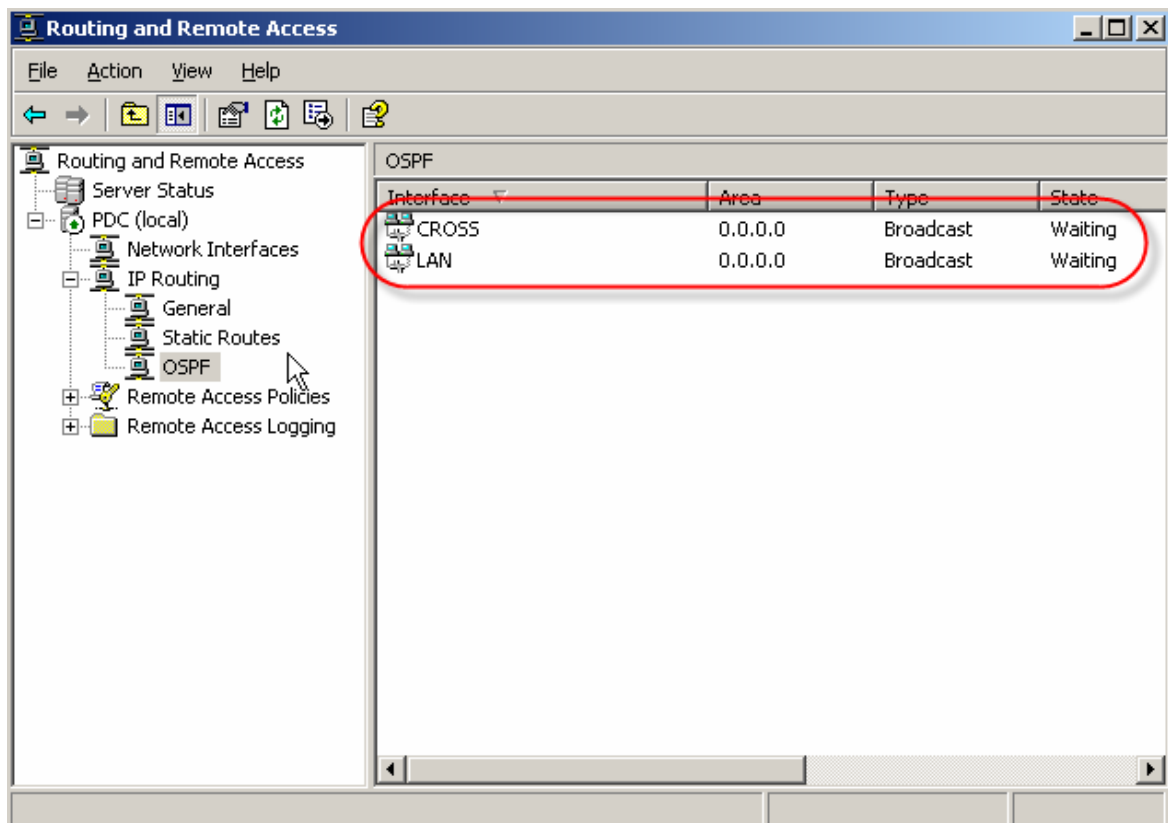


Click OK để hoàn tất định tuyến.



\*Lưu ý: Ở tùy chọn Password, nếu ta sử dụng tùy chọn này thì phải có cùng password trên cả hai server 1 và 2.

Giao diện cửa sổ Routing and Remote access sau khi định tuyến với giao thức OSPF như sau:

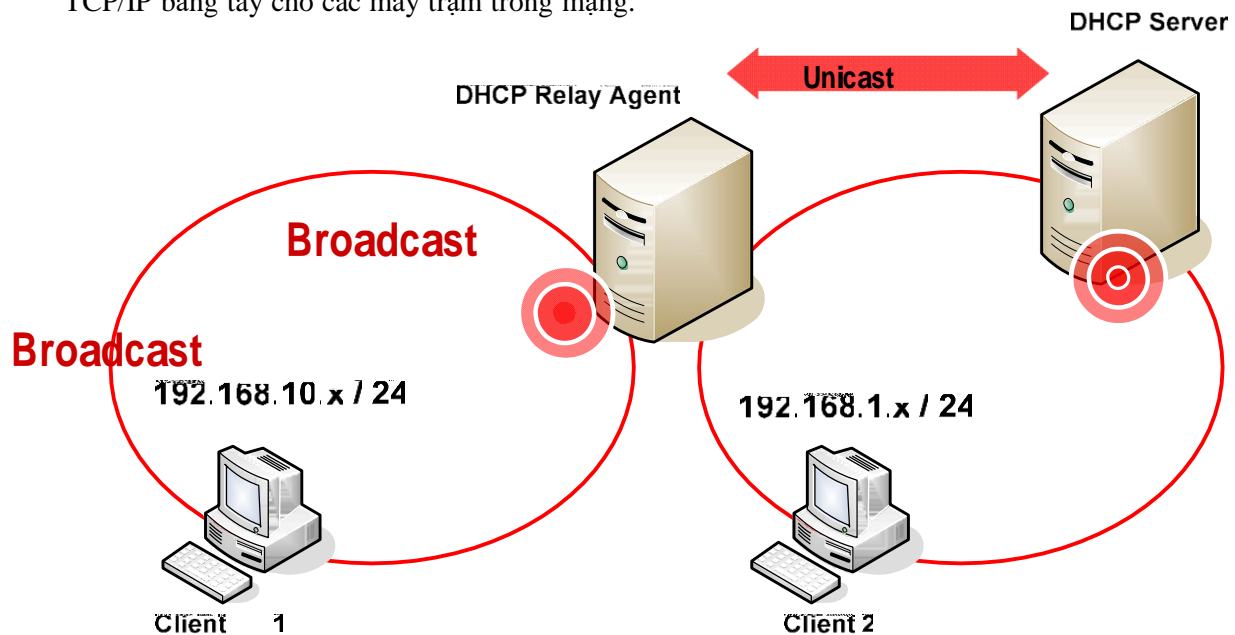


# Dịch vụ cấp phát IP (DHCP)

## I/ Mô tả mô hình và cài đặt dịch vụ DHCP.

Dịch vụ DHCP (Dynamic Host Configuration Protocol) được thiết kế để giảm thời gian cấu hình mạng TCP/IP bằng cách tự động cấp tất cả thông tin cấu hình cần thiết cho DHCP client khi chúng tham gia vào mạng. DHCP tập trung việc quản lý các địa chỉ IP ở máy chủ chạy dịch vụ DHCP.

DHCP làm giảm đáng kể thời gian và những rắc rối có thể phát sinh của việc chỉnh cấu hình TCP/IP bằng tay cho các máy trạm trong mạng.



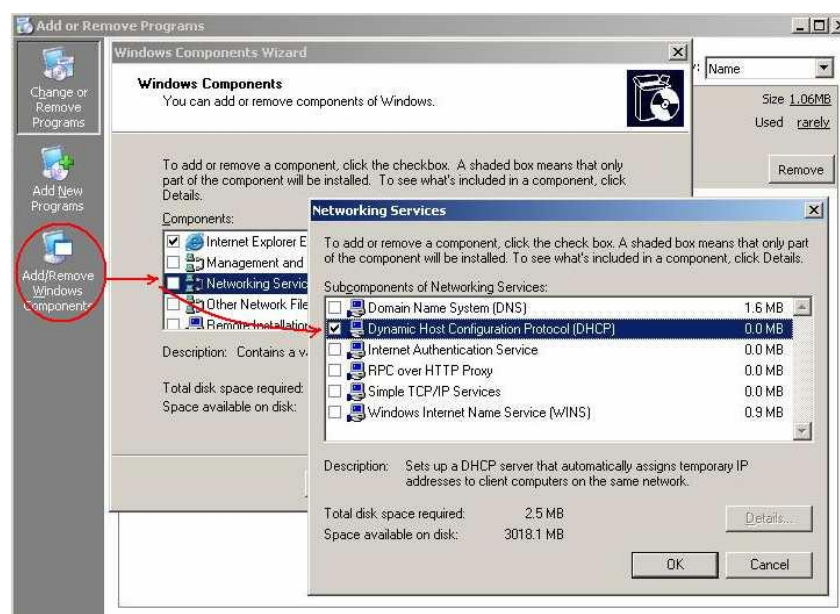
Thông tin cấu hình các máy

		DHCP Server	DHCP Relay	Client 2	Client 1
Card Lan	IP Address	192.168.1.2	192.168.10.10	Obtain IP	Obtain IP
	Subnet Mask	255.255.255.0	255.255.255.0		
	Default Gateway	192.168.1.3	Không có		
	Preferred DNS Server	192.168.1.1	Không có		

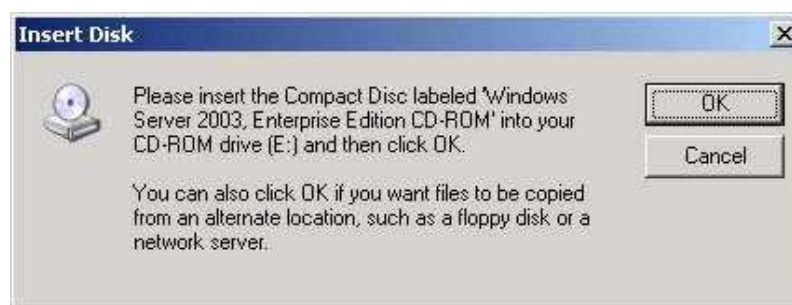
Card Relay	IP Address		192.168.1.3		
	Subnet Mask	Không có	255.255.255.0	Không có	Không có
	Default Gateway		Không có		
	Preferred DNS Server		Không có		

Cài đặt dịch vụ DHCP

1. Vào **Start Settings Control Panel Add or Remove Program**
2. Chọn **Add/Remove Windows Component Networking Services**



3. Nhấn **OK** 2 lần để cài đặt
4. Hệ thống yêu cầu nguồn cài đặt, bạn chỉ đường dẫn đến thư mục I386 trong đĩa cài đặt Windows Server 2003.

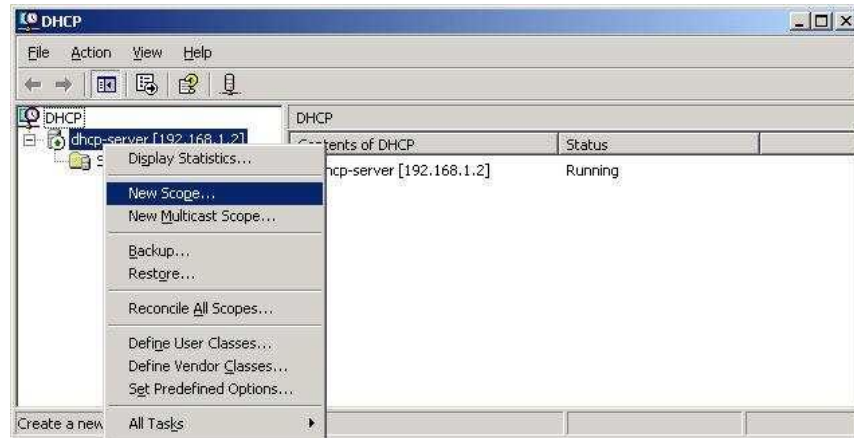


5. Nhấn **Finish** để kết thúc cài đặt

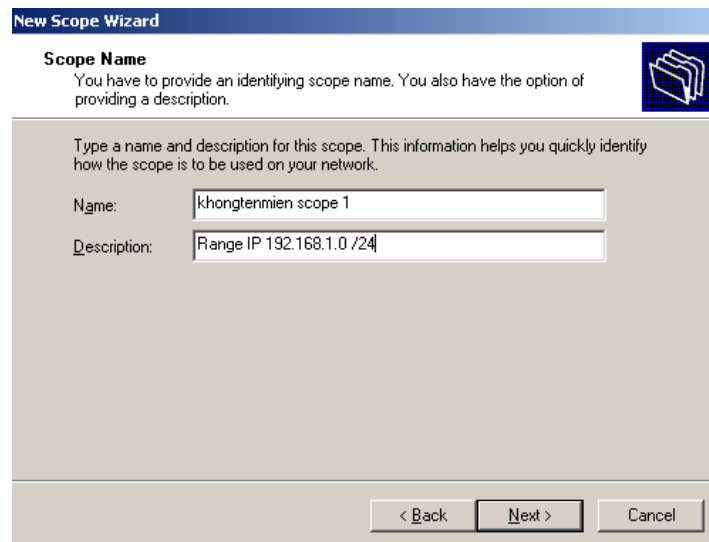


## II/ Cấu hình DHCP Server.

1. Vào **Start**    **Run** gõ lệnh **dhcpgmt.msc**
2. Chuột phải vào DHCP Server    **New Scope**    **Next**



3. Name : là **khongtenmien scope 1**, Description nhập vào **Range IP 192.168.1.0/24**    **Next**



4. Nhập vào Range IP mà bạn muốn cấp cho các máy client    **Next**

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes:

Start IP address: 192.168.1.50

End IP address: 192.168.1.100

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255.255.255.0

< Back Next > Cancel

5. Nhập vào Range IP mà bạn không muốn cấp cho client, nằm trong Range IP phía trên ->  
**Next**

**New Scope Wizard**

**Add Exclusions**  
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

1.1.1.1 2.2.2.2 Add

Excluded address range:

192.168.1.50 to 192.168.1.59 Remove

< Back Next > Cancel

6. Giữ nguyên giá trị mặc định thời gian sử dụng IP khi cấp cho client là 8 ngày

7. Trong Configure DHCP Options chọn **Yes, I want to configure these options now**

**Next**

**New Scope Wizard**

**Configure DHCP Options**

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back   Next >   Cancel

8. Trong Router (Default Gateway) nhập IP Default Gateway, 192.168.1.1

**New Scope Wizard**

**Router (Default Gateway)**

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below:

IP address:

192.168.1.1

Add   Remove   Up   Down

< Back   Next >   Cancel

9. Thông tin Parent domain : **khongtenmien.com**, địa chỉ IP của DNS Server : **192.168.1.1**

**New Scope Wizard**

**Domain Name and DNS Servers**

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: khongtenmien.com

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

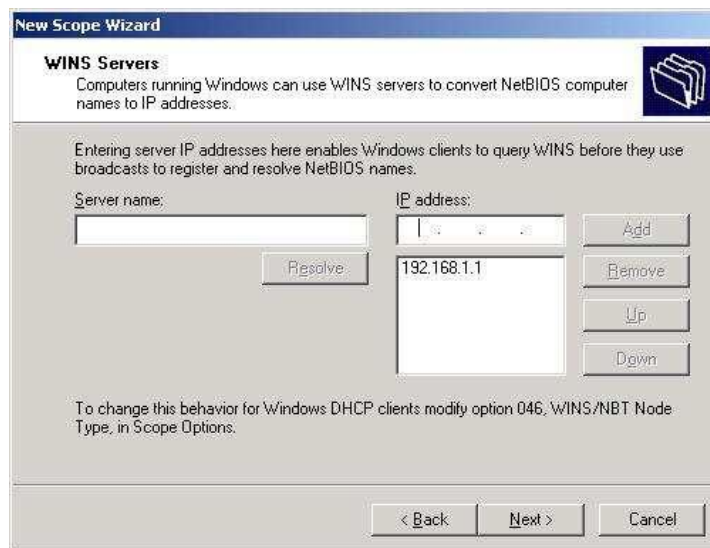
Server name:   IP address:

192.168.1.1

Add   Remove   Up   Down

< Back   Next >   Cancel

10. Cung cấp thông tin địa chỉ IP của WINS Server : 192.168.1.1      nhấn **Next**



The screenshot shows the 'New Scope Wizard' window, specifically the 'WINS Servers' step. The title bar reads 'New Scope Wizard'. Below the title, the section is 'WINS Servers' with a sub-header 'Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.' A descriptive text states: 'Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.' There are two input fields: 'Server name:' and 'IP address:'. The 'IP address:' field contains '192.168.1.1'. To the right of the 'IP address:' field are buttons 'Add', 'Remove', 'Up', and 'Down'. Below the 'IP address:' field is a list box containing '192.168.1.1'. To the left of the list box is a 'Resolve' button. At the bottom of the window are buttons '< Back', 'Next >', and 'Cancel'.

11. Trong Activate Scope chọn **Yes, I want to activate this scope now**      **Next**



The screenshot shows the 'New Scope Wizard' window, specifically the 'Activate Scope' step. The title bar reads 'New Scope Wizard'. Below the title, the section is 'Activate Scope' with a sub-header 'Clients can obtain address leases only if a scope is activated.' A question is asked: 'Do you want to activate this scope now?'. There are two radio button options: 'Yes, I want to activate this scope now' (which is selected) and 'No, I will activate this scope later'. At the bottom of the window are buttons '< Back', 'Next >', and 'Cancel'.

12. Nhấn Finish để hoàn tất cấu hình

### III/ Thực hiện xin cấp IP từ DHCP Server.

1. Properties card LAN, chọn **Obtain an IP address automatically** và **Obtain DNS server address automatically**
2. Vào **Start**    **Run** gõ lệnh **cmd**
3. Trong màn hình command line gõ lệnh **ipconfig /renew** để xin DHCP Server cấp địa chỉ IP
4. Sau đó gõ lệnh **ipconfig /all** để xem thông tin IP nhận được

```
Ethernet adapter Local Area Connection:

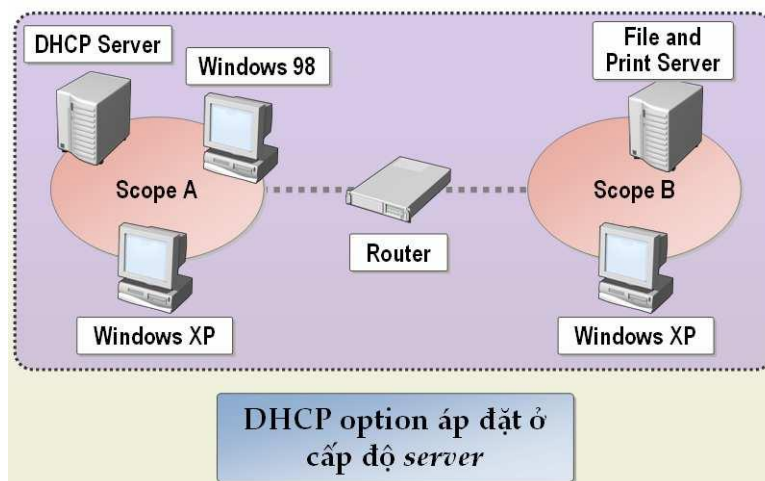
    Connection-specific DNS Suffix  . : khongtenmien.com
    Description . . . . . : VMware Accelerated AMD PCNet Adapter

    Physical Address. . . . . : 00-0C-29-8D-FC-E2
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.111
    DNS Servers . . . . . : 192.168.1.1
    Lease Obtained. . . . . : Friday, December 12, 2008 12:21:51 P
    Lease Expires . . . . . : Saturday, December 20, 2008 12:21:51 PM
```

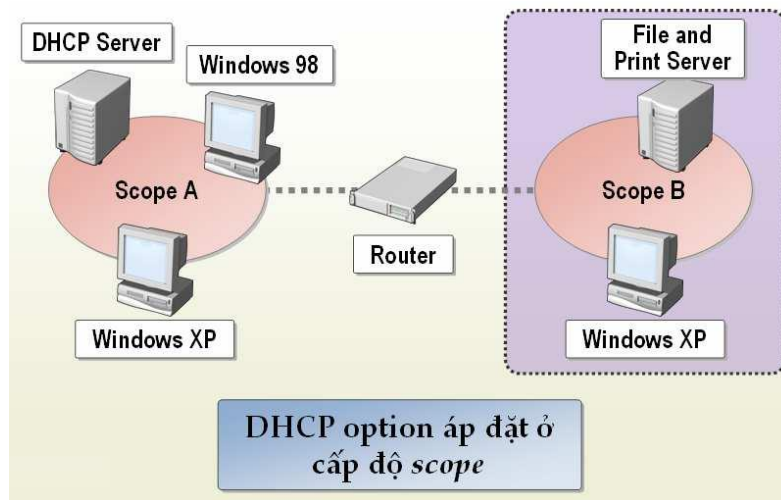
Thông số client nhận được từ DHCP

### IV/ Phân biệt sự khác nhau giữa các chế độ như server, scope, class và reserved client trong dịch vụ DHCP.

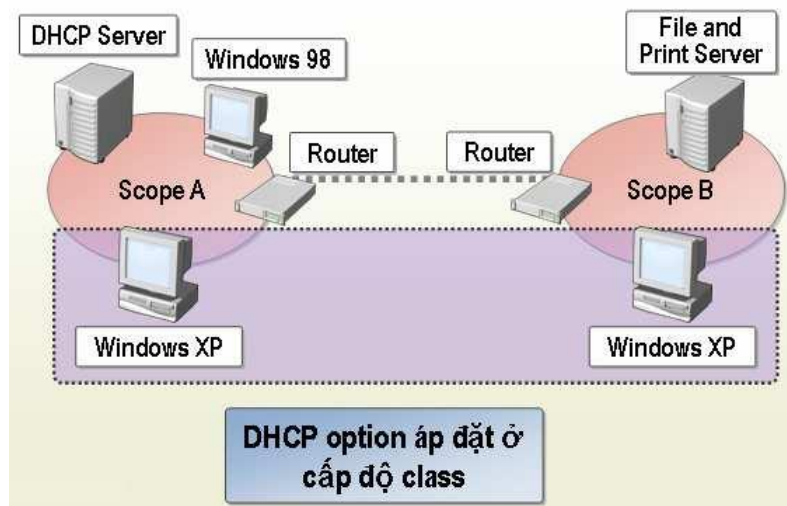
+ **Server level** : các option khai báo ở cấp độ server sẽ được áp đặt tới tất cả các DHCP client của DHCP Server. đây là option có độ ưu tiên thấp nhất.



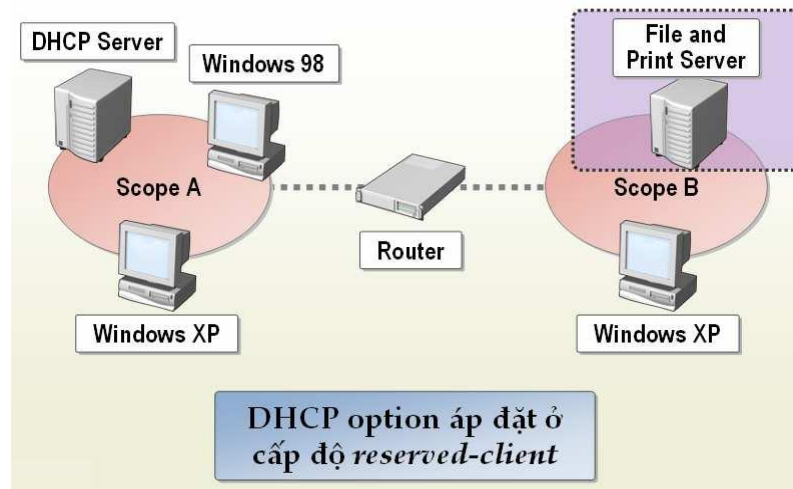
+ **Scope level** : các option khai báo ở cấp độ scope sẽ được áp đặt tới tất cả các DHCP client của riêng scope đó mà thôi, các scope khác sẽ không chịu ảnh hưởng. Đây là option có độ ưu tiên cao hơn option ở cấp độ server level.



+ **Class level** : Các option khai báo ở cấp độ class level sẽ được áp đặt tới những thành viên của class. Độ ưu tiên của các option này cao hơn option ở cấp độ scope level.



+ **Reversed client level** : Các option ở cấp độ này sẽ chỉ được áp đặt đến một DHCP client mà thôi. Đây là option có độ ưu tiên cao nhất. Nó sẽ ghi đè tất cả các option khác nếu có conflict (xung đột level) xảy ra.



#### V/ Cấu hình áp dụng chế độ class trong việc cấu hình thông tin IP trên DHCP Server.

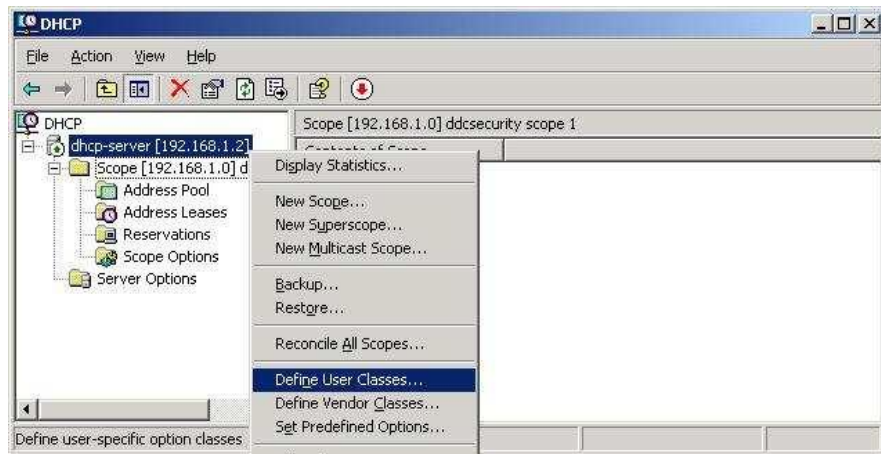
Giả sử một vấn đề đặt ra là trong cùng một scope, chúng ta muốn cho một số máy có thể truy cập Internet và số máy còn lại thì không được truy cập Internet. Vấn đề ở đây là các máy nào không được truy cập Internet thì ta chỉ cần chỉ Default Gateway về một địa chỉ IP nào đó không phải là Default Gateway thật thì các máy đó sẽ tự động không thể truy cập Internet được. Các máy được chỉ đúng Default Gateway thì sẽ truy cập Internet được.

Theo các định nghĩa về các level option ở trên thì để giải quyết vấn đề này ta chỉ có 2 sự lựa chọn đó là Class level và Reversed client level. Nhưng nếu số lượng máy tính trong scope nhiều thì việc sử dụng Reversed client level là việc không khả thi vì bạn phải tiến hành cấu hình rất nhiều lần trên mỗi DHCP client. Ngược lại giải pháp sử dụng Class level thì rất hữu hiệu, chúng ta chỉ cần cấu hình 2 user class khác nhau.

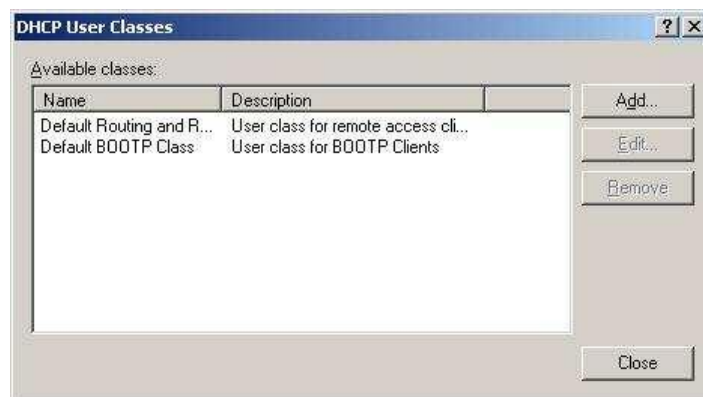
Trong trường hợp này chúng ta sẽ tiến hành định nghĩa 2 user class : **Allow Internet** và **Deny Internet**. Thực hiện các bước sau trên máy DHCP Server để định nghĩa 2 user class này :

1. Chọn **Start** → **Run** gõ lệnh **dhcpcmgmt.msc**
2. Chuột phải vào DHCP Server → **Define User Classes**

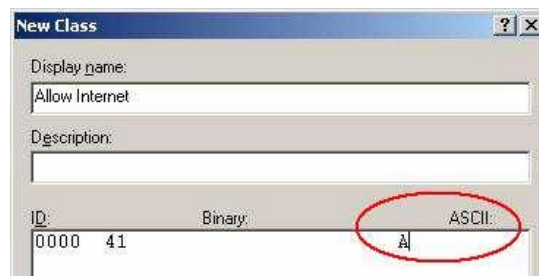




3. Nhấn **Add**

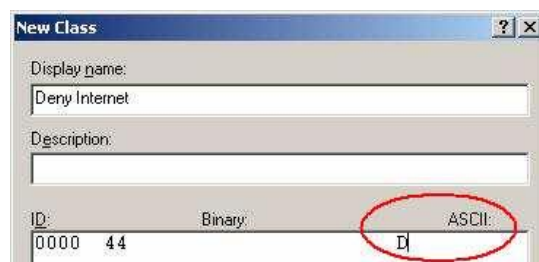


4. Trong Display Name điền vào **Allow Internet** và điền vào cột ASCII giá trị là **A**     **OK**



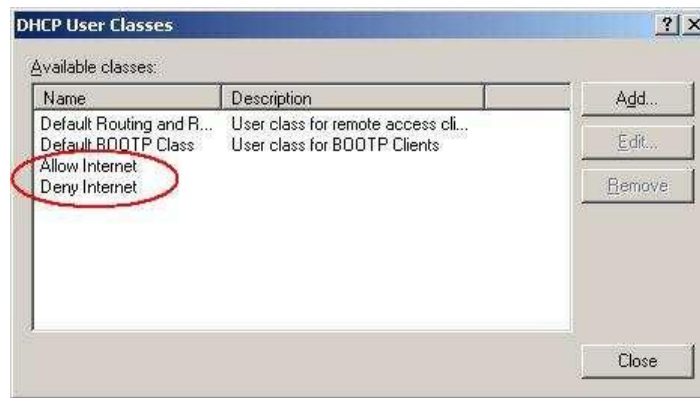
6. Nhấn **Add** để định nghĩa thêm cho nhóm Deny Internet

7. Trong Display Name điền vào **Deny Internet** và điền vào cột ASCII giá trị là **D**     **OK**

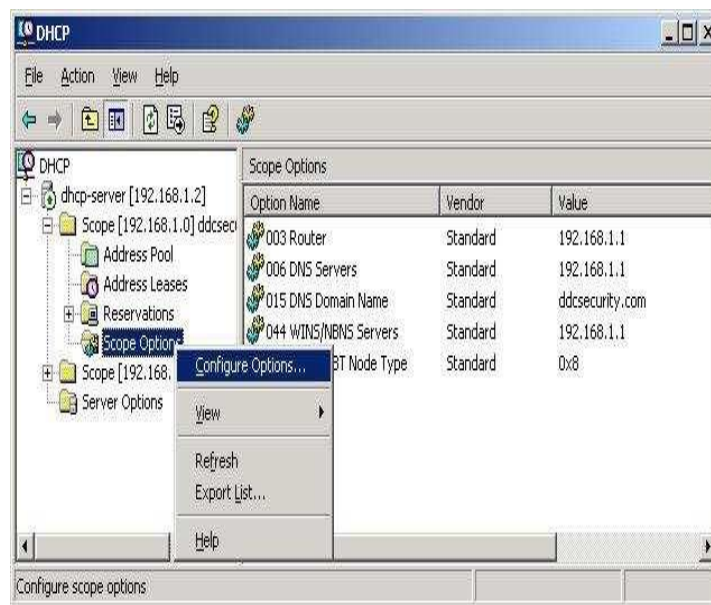


8. Hai user class mà chúng ta vừa định nghĩa đã có trong DHCP User Classes     Nhấn **Close**

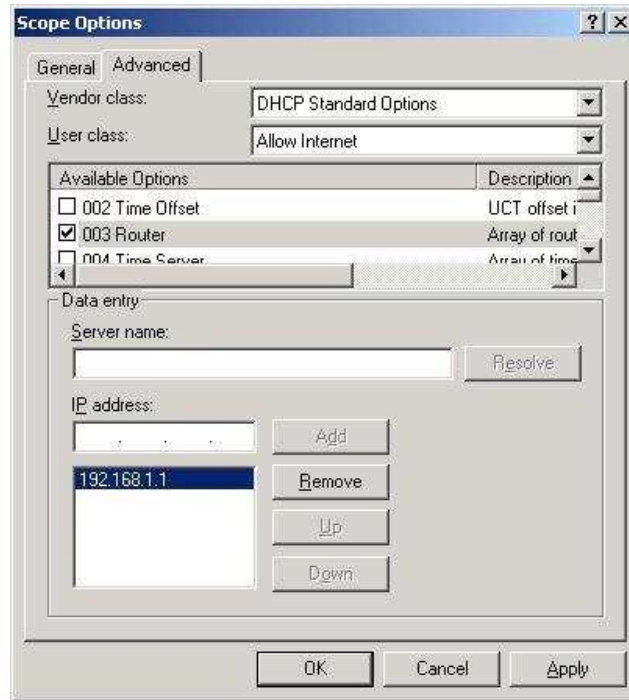




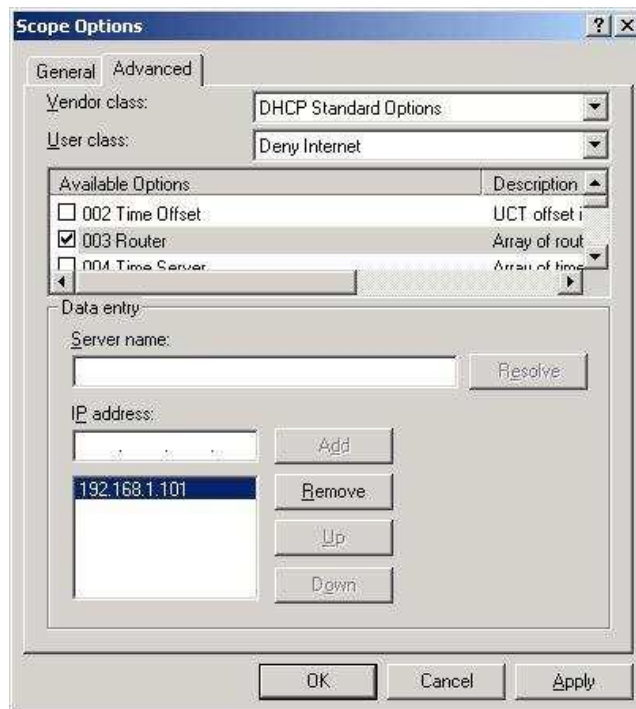
9. Cấu hình Scope Options chọn **Configure Options**



10. Chọn tab **Advanced**, chọn **Allow Internet** trong User class, đánh dấu check vào 003 Router và điền địa chỉ IP đúng của Default Gateway Nhấn **Apply**



11. Chọn tiếp **Deny Internet** trong User class, đánh dấu check vào 003 Router và nhập địa chỉ không phải của Default Gateway    **Nhấn Apply    OK**



### Cấu hình DHCP Client để nhận user class trong class level của DHCP Server

Có nhiều cách để tiến hành nhóm các máy tính vào từng user class thích hợp, Admin có thể tiến hành nhập bằng tay trên từng máy tính DHCP client hoặc triển khai bằng Group Policy thông qua 1 file thực thi và gán xuống cho từng máy client theo chức năng Log on Script.

Trong bài Lab này ta chỉ thực hiện cách nhập bằng tay trên máy Client 2

1. Vào **Start**    **Run** gõ lệnh **cmd**
2. Nhập vào dòng lệnh **ipconfig /setclassid "Card Lan" "Allow Internet"** để đưa client 2 vào nhóm Allow Internet.
3. Trong màn hình command line gõ lệnh **ipconfig /release** để hủy bỏ IP đã thuê.
4. Nhập tiếp dòng lệnh **ipconfig /renew** để xin cấp mới địa chỉ IP
5. Nhập tiếp dòng lệnh **ipconfig /all** để kiểm tra thông tin IP vừa nhận được

```
Windows IP Configuration

Host Name . . . . . : xp
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Card Lan:

Connection-specific DNS Suffix . :
Description . . . . . : Intel 21140-Based PCI Fast Ethernet
Adapter (Generic)
Physical Address. . . . . : 00-03-FF-F2-AD-18
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.60
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.2
DNS Servers . . . . . : 192.168.1.1
Primary WINS Server . . . . . : 192.168.1.1
Lease Obtained. . . . . : Thursday, August 28, 2008 11:49:30 PM
Lease Expires . . . . . : Sunday, August 31, 2008 11:49:30 PM
```

### **VI/ Cấu hình DHCP Relay Agent sử dụng dịch vụ Routing and Remote Access.**

Các DHCP client sử dụng tín hiệu DHCP/BOOTP broadcast để thuê một địa chỉ IP từ DHCP Server. Thông thường, các router được cấu hình để không cho các tín hiệu broadcast đi qua. Nếu không có bất kỳ một cấu hình gì khác, các DHCP Server chỉ cho thuê địa chỉ IP đối với các máy client nằm trong cùng subnet với máy DHCP Server mà thôi.

Trong mô hình Lab này thì DHCP Server chỉ cung cấp IP cho các máy client trong mạng 192.168.1.0/24. Vì vậy, máy Client 1 sẽ không thể nhận địa chỉ IP từ DHCP Server.

Để giải quyết vấn đề này, chúng ta thường sử dụng một trong hai cách sau :

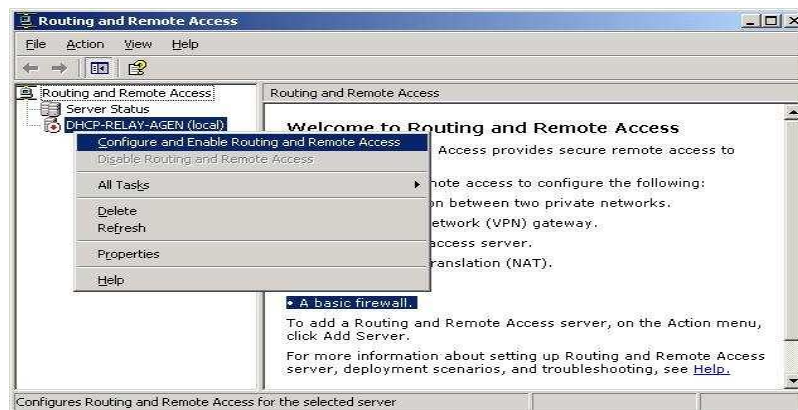
+ Cấu hình router trên máy tính DHCP Relay Agent cho phép các tín hiệu broadcast đi qua để máy tính Client 1 có thể gửi yêu cầu thuê IP đến DHCP Server.

+ Cấu hình một DHCP Relay Agent trên router bằng cách sử dụng dịch vụ Routing and Remote Access. DHCP Relay Agent có thể là một máy tính hoặc một router được cấu hình để lắng nghe các tín hiệu DHCP/BOOTP broadcast từ các DHCP Client và chuyển các tín hiệu này tới các DHCP Server nằm trên một subnet khác.

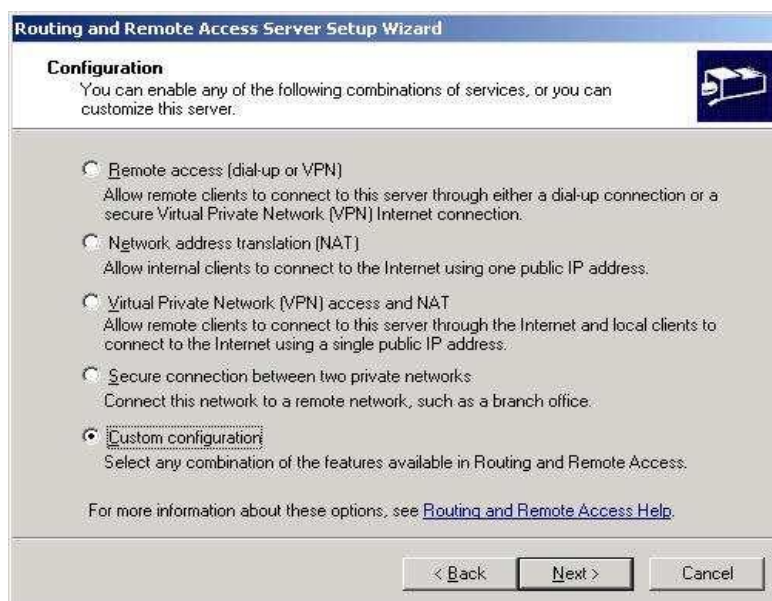
Việc cấu hình router để cho phép các tín hiệu broadcast đi qua không phải là một giải pháp tốt. Cấu hình như vậy sẽ làm giảm băng thông mạng do các tín hiệu broadcast gây ra. Trong thực tế, giải pháp sử dụng một DHCP Relay Agent được ưu thích hơn.

1. Vào **Start**      **Run** gõ lệnh **rrasmgmt.msc**

2. Chuột phải vào Server (local)      **Configure and Enable Routing and Remote Access**



3. Nhấn **Next**      Chọn **Custom configuration**      **Next**



4. Đánh dấu check vào **LAN routing**      **Next**      28



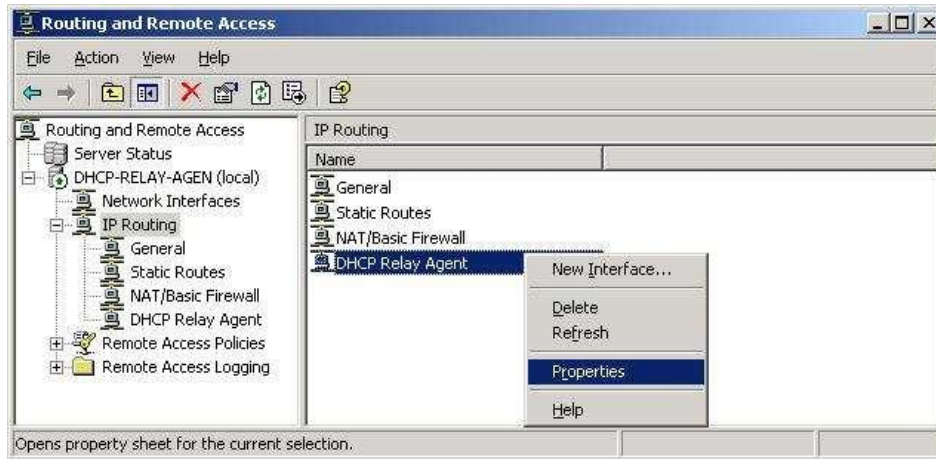
5. Chuột phải vào **General**    Chọn **New Routing Protocol**



6. Chọn **DHCP Relay Agent**    **OK**



7. Chuột phải vào **DHCP Relay Agent** vừa tạo    Chọn **Properties**



8. Tab General, điền địa chỉ IP của DHCP Server vào Server Address là **192.168.1.2** **OK**

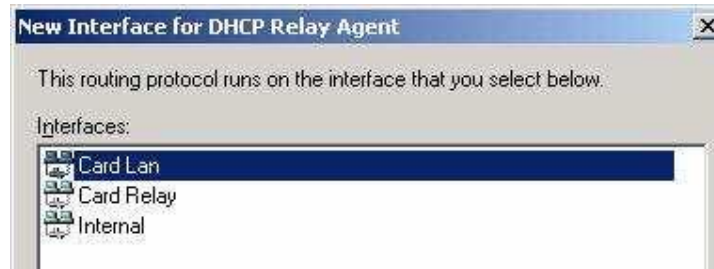


9. Chuột phải vào **DHCP Relay Agent** Chọn **New Interface**

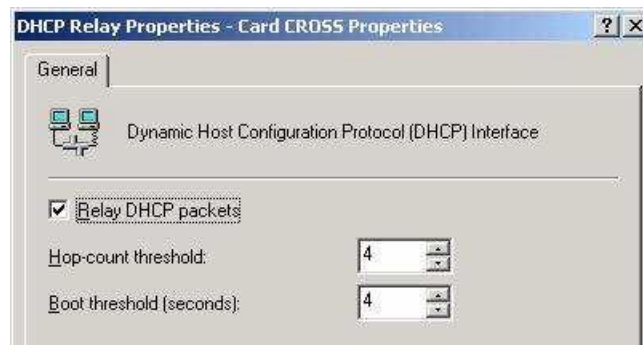


10. Chọn **Card Lan** **OK**





11. đảm bảo rằng dấu check đã được chọn ở **Relay DHCP packets**      **OK**

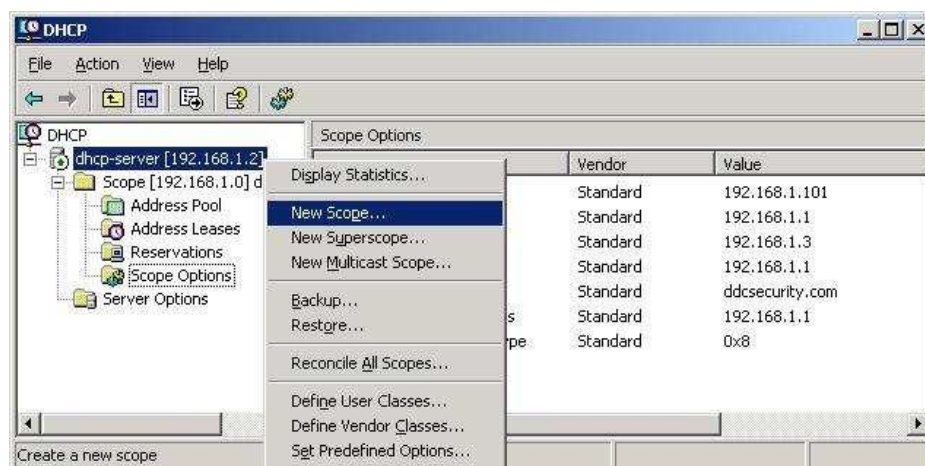


đến đây là chúng ta đã hoàn tất cấu hình DHCP Relay Agent. Việc tiếp theo là cấu hình 1 scope mới cho lớp mạng 192.168.10.0/24

### Cấu hình New Scope cho lớp mạng 192.168.10.0/24 trên DHCP Server

để DHCP Server có thể cấp IP phù hợp cho Client 1 và các máy cùng subnet với Client 1. Chúng ta tiến hành tạo một scope mới trên DHCP Server

1. Vào **Start**      **Run** gõ lệnh **dhcpgmt.msc**
2. Chuột phải vào DHCP Server      Chọn New Scope



3. Điền vào name : **khongtenmien scope 2** và Description là **Range IP 192.168.10.0/24**

**Next**

**New Scope Wizard**

**Scope Name**  
 You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back   Next >   Cancel

3. Trong IP Address, nhập vào Range IP mà bạn muốn cấp cho client      **Next**

**New Scope Wizard**

**IP Address Range**  
 You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes:

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back   Next >   Cancel

4. Trong Add Exclusions, nhập vào Range IP mà bạn không cấp cho client (range này để cấp cho các Server như DNS, WINS, Web, FTP,...)



**New Scope Wizard**

**Add Exclusions**  
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:  End IP address:

Excluded address range:  
192.168.10.150 to 192.168.10.159

< Back Next > Cancel

**New Scope Wizard**

**Configure DHCP Options**  
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back Next > Cancel

7. Trong Router (Default Gateway) nhập địa chỉ IP **192.168.10.10** Next

**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.10.10

< Back Next > Cancel

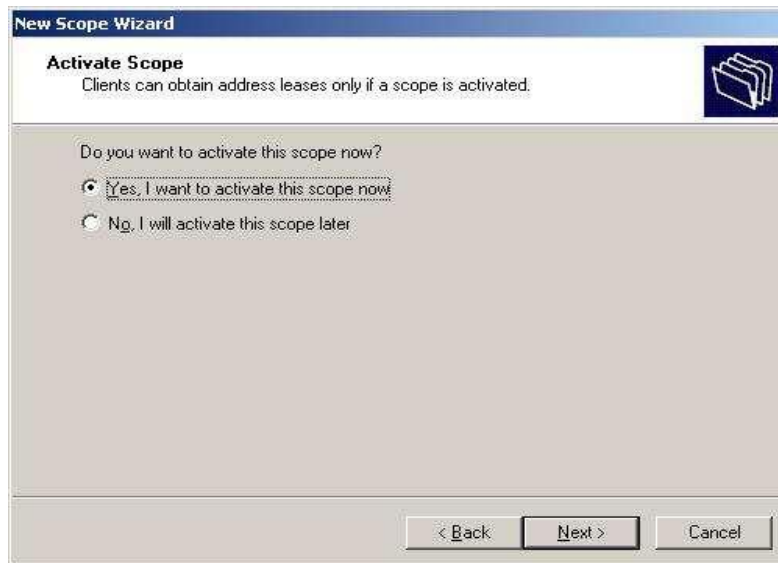
8. Parent domain điền vào **khongtenmien.com**, IP Address nhập vào IP DNS **192.168.1.1**

The screenshot shows the 'New Scope Wizard' window with the title 'Domain Name and DNS Servers'. It includes a description of DNS and a text box for 'Parent domain' containing 'khongtenmien.com'. Below, there are fields for 'Server name' and 'IP address'. The 'IP address' field contains '192.168.1.1'. Buttons for 'Add', 'Remove', 'Up', and 'Down' are present. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

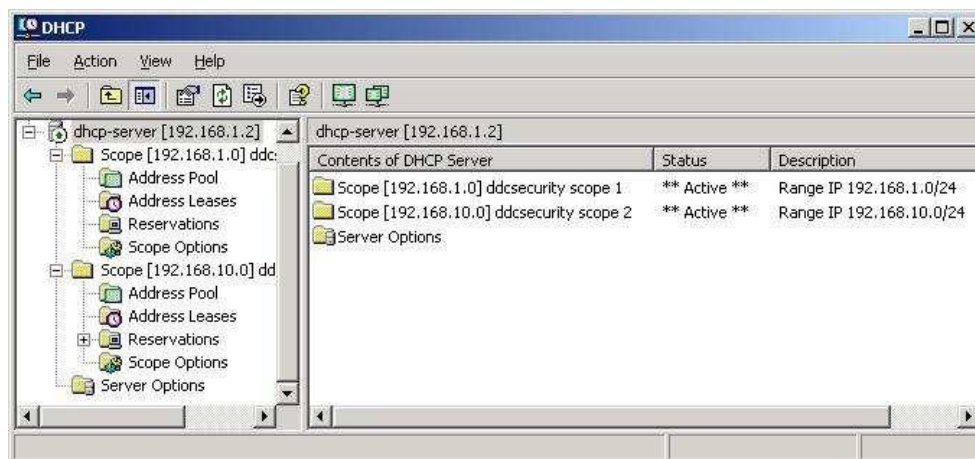
9. Điền IP của WINS Server vào IP Address Nhấn **Add** **Next**

The screenshot shows the 'New Scope Wizard' window with the title 'WINS Servers'. It includes a description of WINS servers and a text box for 'Server name'. Below, there are fields for 'IP address'. The 'IP address' field contains '192.168.1.1'. Buttons for 'Add', 'Remove', 'Up', and 'Down' are present. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

10. Trong Activate Scope chọn **Yes, I want to active this scope now** **Next**



11. Nhấn Finish để kết thúc cài đặt, xem lại trong màn hình của DHCP Server



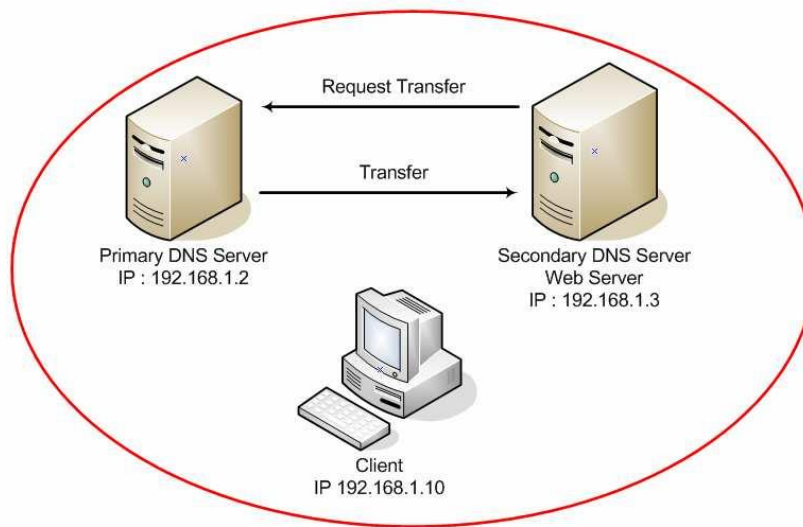
**Cấu hình Client 1 để nhận IP do DHCP Server cung cấp**

1. Properties card mạng Cross, chọn **Obtain an IP address automatically** và **Obtain DNS server address automatically**
2. Vào **Start** Run gõ lệnh **cmd**
3. Trong màn hình command line gõ lệnh **ipconfig /renew** để xin DHCP Server cấp địa chỉ IP
4. Sau đó gõ lệnh **ipconfig /all** để xem thông tin IP nhận được

```
Physical Address. . . . . : 00-03-FF-F2-AD-18
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
IP Address. . . . . : 192.168.10.168
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.10
DHCP Server . . . . . : 192.168.10.10
DNS Servers . . . . . : 192.168.1.1
Primary WINS Server . . . . . : 192.168.1.1
Lease Obtained. . . . . : Thursday, August 28, 2008 9:50:43 PM
Lease Expires . . . . . : Friday, September 05, 2008 9:50:43 PM
```

# Hệ thống phân giải tên miền (Domain Name System)

## I/ Mô tả mô hình và cài đặt dịch vụ DNS.



Thông tin cấu hình các máy

		PC1	PC2	PC3
Card	IP Address	192.168.1.2	192.168.1.3	192.168.1.10
LAN	Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
	Default			
	Gateway	Không có	Không có	Không có
	Preferred DNS Server	192.168.1.2	192.168.1.3	192.168.1.2
	Alternate DNS Server	Không có	Không có	192.168.1.3
	Full computer name	pdc.khongtenmien.com	sdc.khongtenmien.com	Client.khongtenmien.com

Trong mô hình này, chúng ta sử dụng 3 máy. Hai máy là Server 2003 và 1 máy là XP SP2

Client truy cập web site [www.khongtenmien.com](http://www.khongtenmien.com)

DNS Server sẽ phân giải địa chỉ web site thành địa chỉ IP của máy 192.168.1.3.

Máy 192.168.1.3 nhận http request từ Client và trả kết quả về cho máy Client.

## Cài đặt dịch vụ DNS

Có nhiều cách cài đặt dịch vụ DNS trên môi trường Windows như :

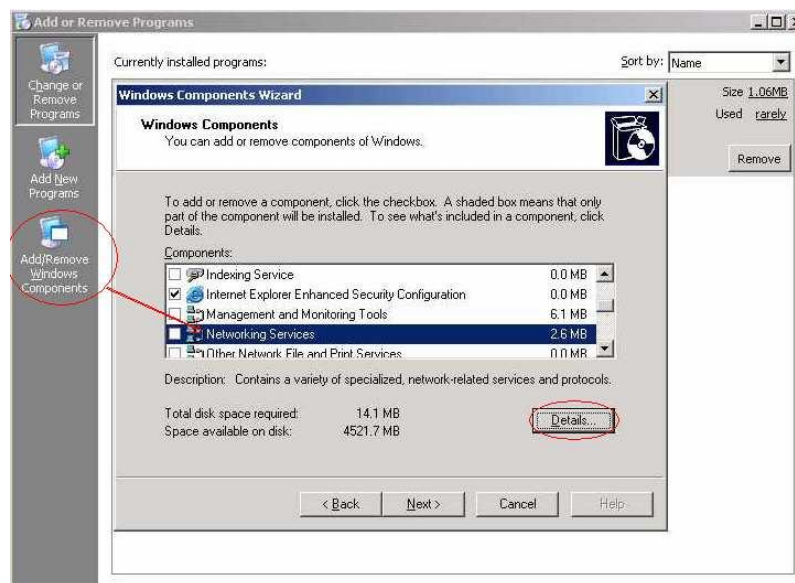
- Cài đặt DNS trên máy stand-alone Windows Server 2003.
- Cài đặt DNS khi ta nâng cấp máy chủ lên Domain Controllers.

Người thực hiện : Domain Admins, Admin Local

1. Chọn **Start    Control Panel    Add/Remove Programs**

2. Chọn **Add or Remove Windows Components**

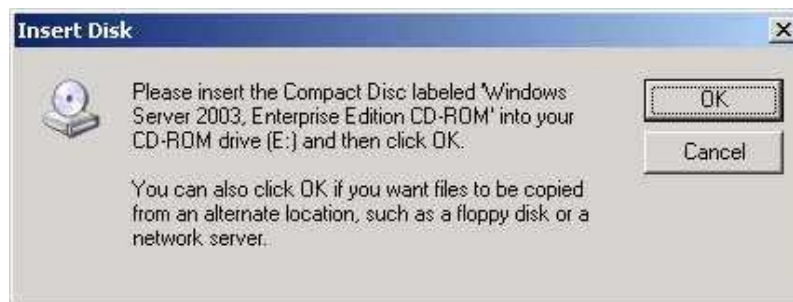
3. Chọn **Networking Services    Nhấn nút Details**



4. Chọn **Domain Name System    OK**



5. Chọn **Next**, lúc này hệ thống sẽ yêu cầu nguồn cài đặt (nằm trong thư mục I386 trong bộ source Windows 2003), chỉ đường dẫn đến thư mục I386. Chọn **OK**



6. Nhấn **Finish** để hoàn tất quá trình cài đặt.

## **II/ Cấu hình dịch vụ DNS.**

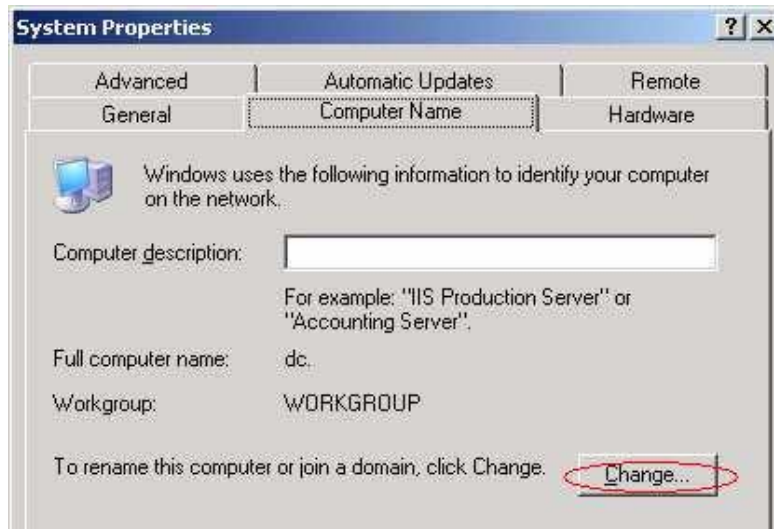
Trước khi cấu hình dịch vụ DNS, chúng ta phải đổi DNS Suffix của DNS Server để tránh trường hợp gặp lỗi về Name Server.

**đổi DNS Suffix :**

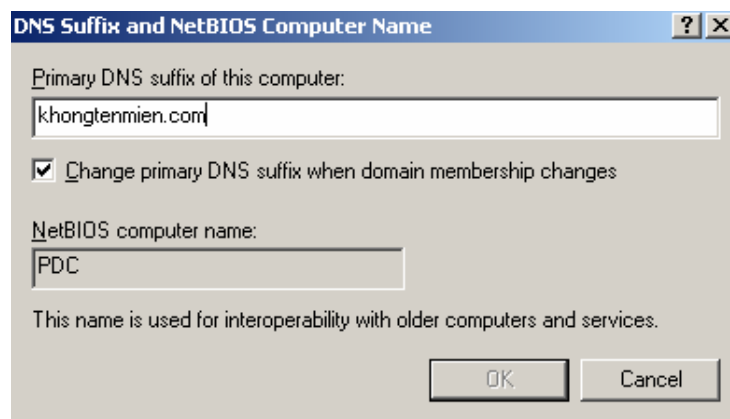
1. Chọn **Start** Chuột phải lên **My Computer** chọn **Properties** (hoặc vào **Start** **Run** gõ lệnh **sysdm.cpl**)



2. Chọn tab **Computer Name**    **Change**    **more**



3. Điền DNS Suffix dưới dạng DNS Name level 2, tên DNS Suffix trùng tên với tên của domain.



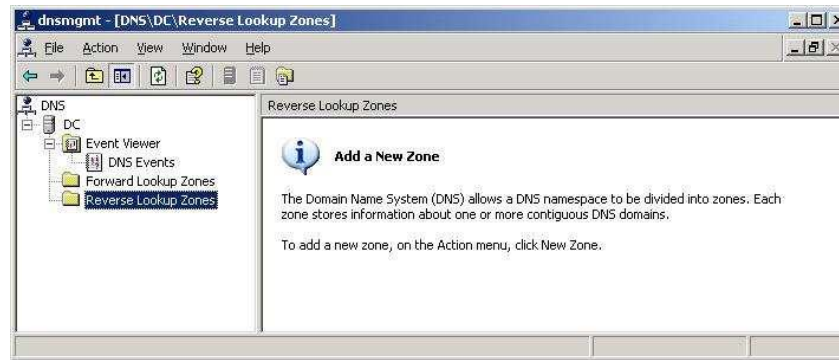
4. Nhấn OK hai lần và khởi động lại máy.

### **Tạo mới Primary Zone**

Primary Zone chứa DNS Zone Database (Zone file) trên Server và toàn quyền trên Zone file đó. Admin có thể thêm hoặc Record vào Zone File trên Primary Zone.



Chọn **Start**    **Administrative Tools**    **DNS** (hoặc vào **Run** gõ lệnh **dnsmgmt.msc**)



- Event Viewer : theo dõi nhật ký của dịch vụ DNS, nơi lưu trữ các thông tin về : cảnh giác (alert), cảnh báo (warnings), lỗi (errors).

- Forward Lookup Zones : chứa các zone thuận của dịch vụ DNS. Zone này được lưu tại DNS Server.

- Reverse Lookup Zones : chứa tất cả các zone nghịch của dịch vụ DNS, zone này cũng được lưu tại DNS Server.

### Tạo Forward Lookup Zone

Forward Lookup Zone dùng để phân giải tên máy (hostname) thành địa chỉ IP.

1. Chuột phải vào **Forward Lookup Zones**    **New Zone**

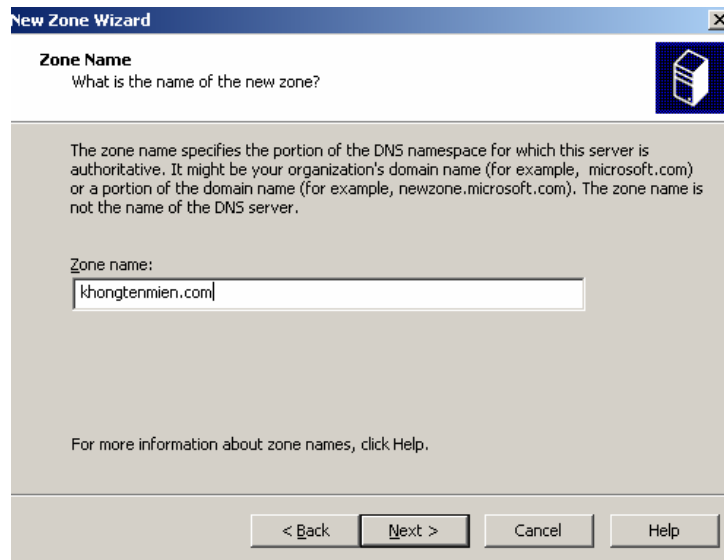


2. Zone type : chọn **Primary Zone**    **Next**

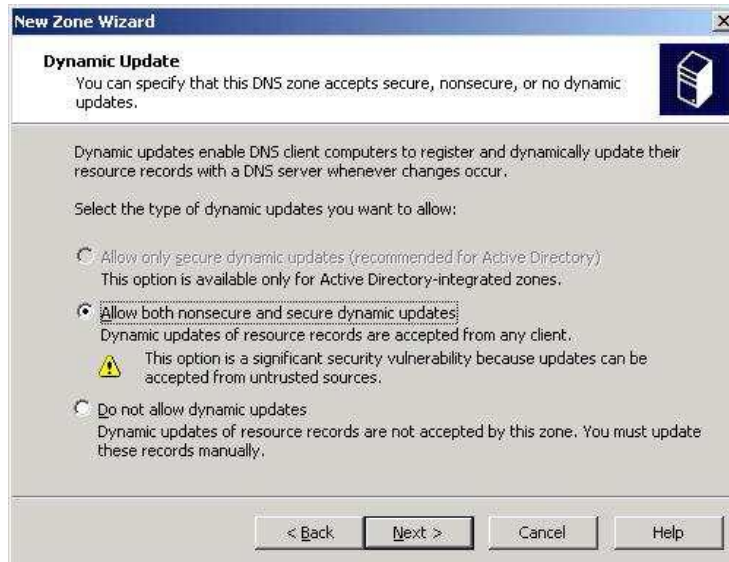




3. Zone name : điền vào tên domain là khongtenmien.com      **Next**      **Next**



4. Chọn **Allow both nonsecure and secure dynamic updates**



5. Nhấn **Finish** để hoàn tất.



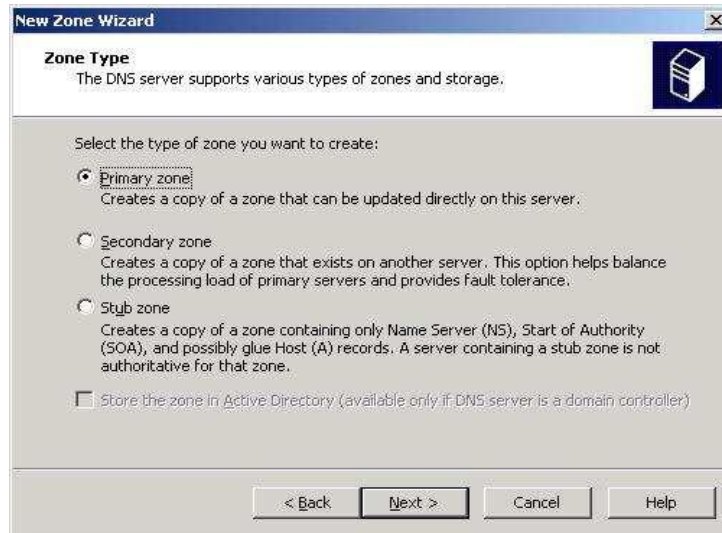
## Tạo Reverse Lookup Zone

Reverse Lookup Zone có cơ chế hoạt động ngược lại với Forward Lookup Zone tức là phân giải địa chỉ IP thành tên máy (hostname).

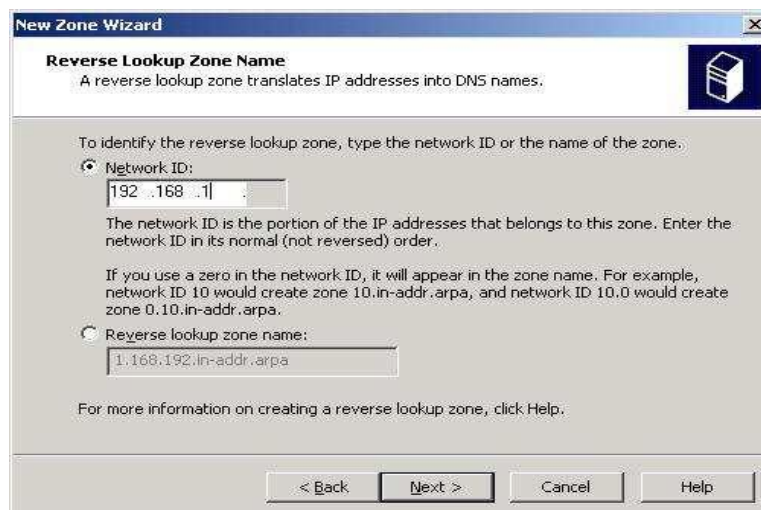
1. Chuột phải vào **Reverse Lookup Zones**      **New Zone**



## 2. Zone type : chọn **Primary Zone**      *Next*



## 3. Zone Name sử dụng Network ID **192.168.1**      *Next*      *Next*



## 4. Allow both nonsecure and secure dynamic updates



5. Nhấn **Finish** để hoàn tất.



Kiểm tra hoạt động của DNS Server

Sau khi đã cấu hình tạo Forward Lookup Zone và Reverse Lookup Zone xong, tiến hành kiểm tra DNS Server bằng cách :

1. Vào **Start**    **Run** gõ lệnh **cmd**.
2. Tại màn hình cmd, gõ lệnh **nslookup**

```

C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 192.169.1.2: Timed out
Default Server: UnKnown
Address: 192.169.1.2

> _

```

*DNS request timed out. timeout*

*was 2 seconds.*

**\*\*\* Can't find server name for address 192.168.1.2: Timed out**

**Default Server: UnKnown**

**Address: 192.168.1.2**

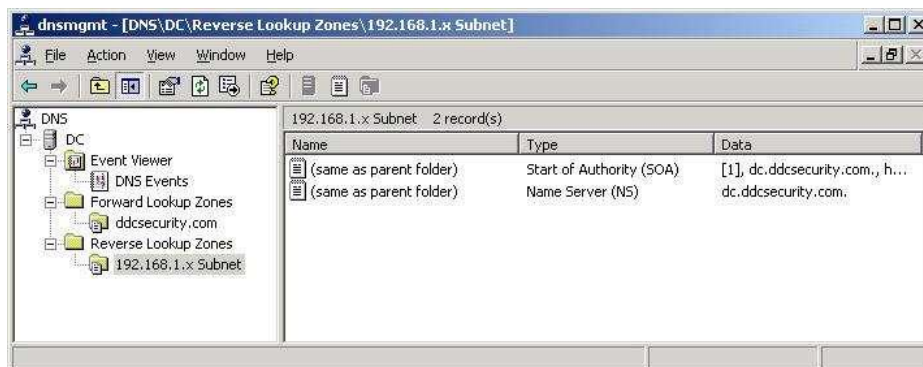
Thông báo trên cho thấy dịch vụ DNS cấu hình chưa đúng. Kiểm tra lại DNS.

3. Kiểm tra tại Forward Lookup Zone :



Ok, Forward Lookup Zone của khongtenmien.com đã có host (A) là pdc với IP 192.168.1.2.

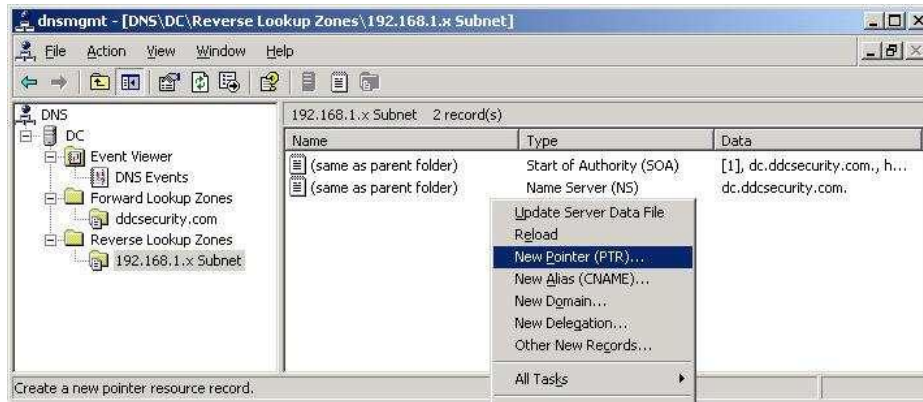
4. Kiểm tra tiếp Reverse Lookup Zone.



Reverse Lookup Zone chưa có Pointer, tạo Pointer để ánh xạ địa chỉ IP là 192.168.1.2 đến tên máy (hostname) là pdc.

### Tạo Pointer

1. Chuột phải vào cửa sổ bên phải của Reverse Lookup Zone    **New Pointer (PTR)**

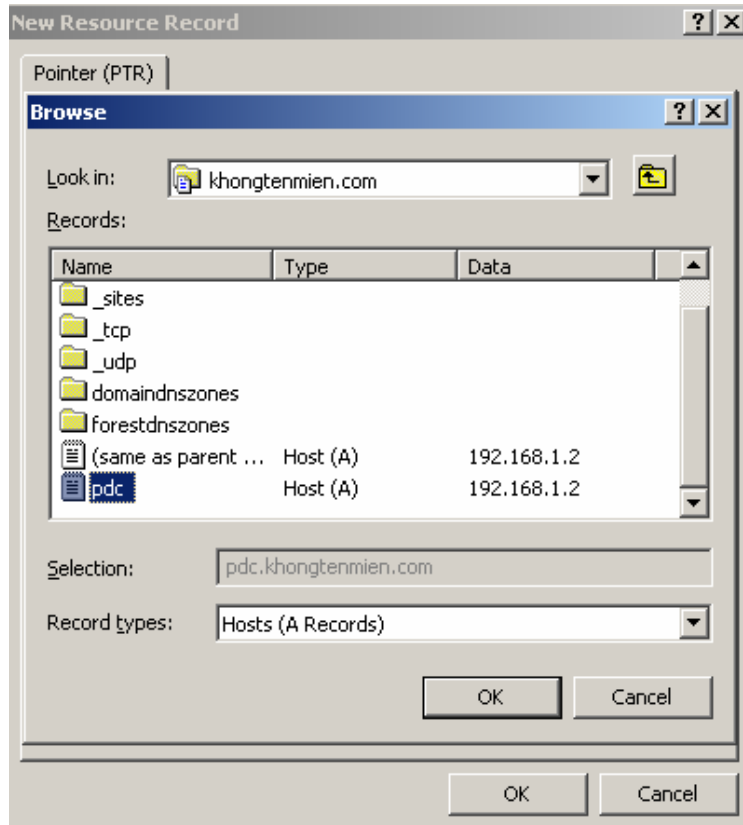


2. Host IP number điền vào là 2      Nhấn nút Browse



3. Double click lần lượt vào DC, Forward Lookup..., khongtenmien.com, dc.





4. Nhấn **OK** để hoàn tất việc tạo Pointer

Kiểm tra lại bằng dòng lệnh nslookup

Chọn **Start** → **Run** → gõ lệnh **cmd**. Sau đó gõ lệnh **nslookup**

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
Default Server:  pdc.khongtenmien.com
Address:  192.168.1.2

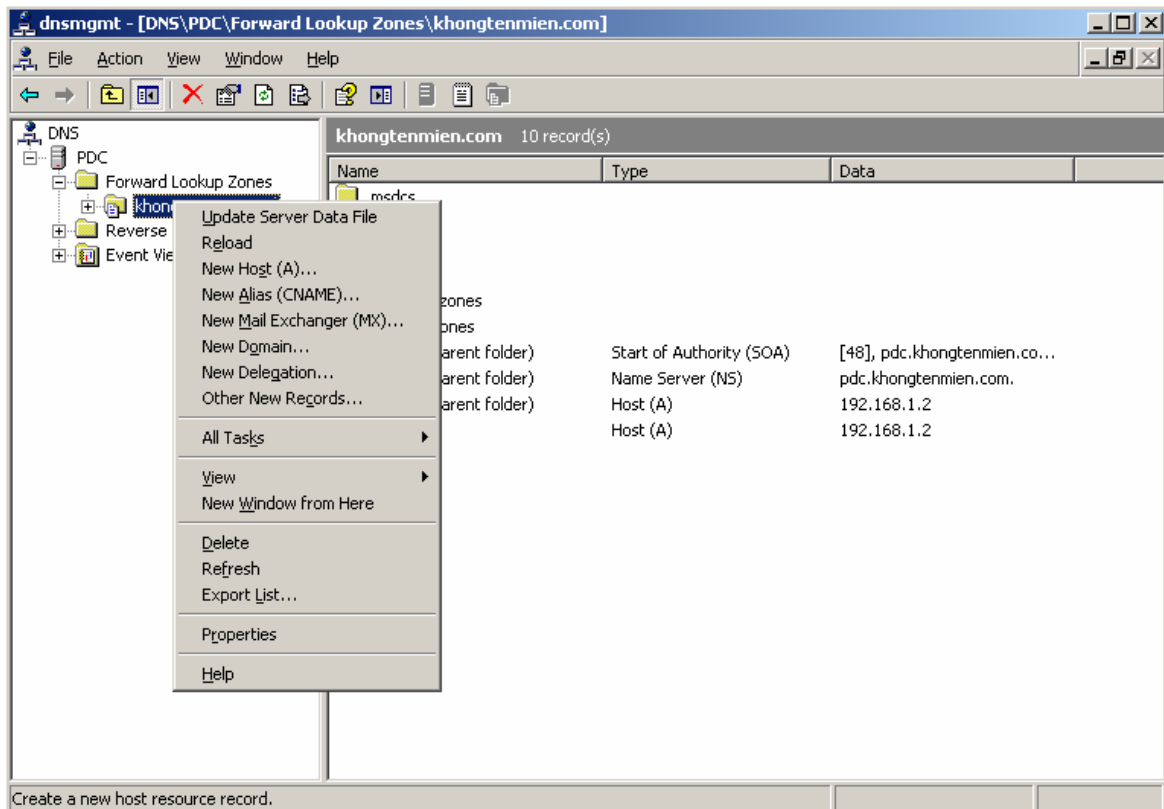
>
```

Như vậy là DNS đã được cấu hình xong.

### Tạo Host (A)

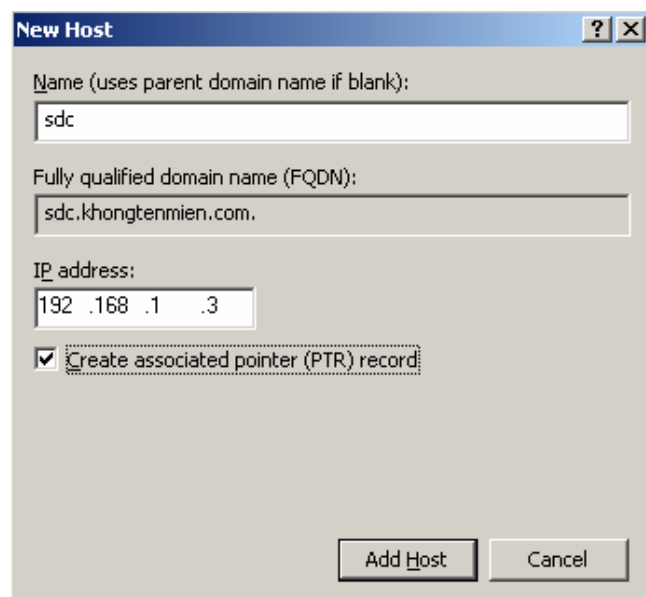
Trong nội bộ LAN, có bao nhiêu máy tính thì sẽ tạo bấy nhiêu Host (A) trên Primary DNS. Trong bài Lab này, ngoài Primary DNS Server chúng ta có thêm 2 máy tính nữa đó là Secondary DNS Server và Client. Do đó ta sẽ tiến hành tạo Host (A) cho cả 2 máy tính này.

1. Chuột phải vào Zone **khongtenmien.com** trong Forward Lookup Zone    **New Host (A)**



2. Điền thông tin như hình bên dưới, nhớ check vào Create associated Pointer (PTR) record để tạo mới Pointer cho Host (A) này. Sau đó nhấn **Add Host**

**\*Lưu ý:** Check dấu “*Create associated pointer (PTR) record*” để DNS server tự tạo Pointer cho phần Reverse Lookup Zone.





3. Thông báo tạo Host (A) cho Secondary DNS Server hoàn tất, nhấn OK để kết thúc



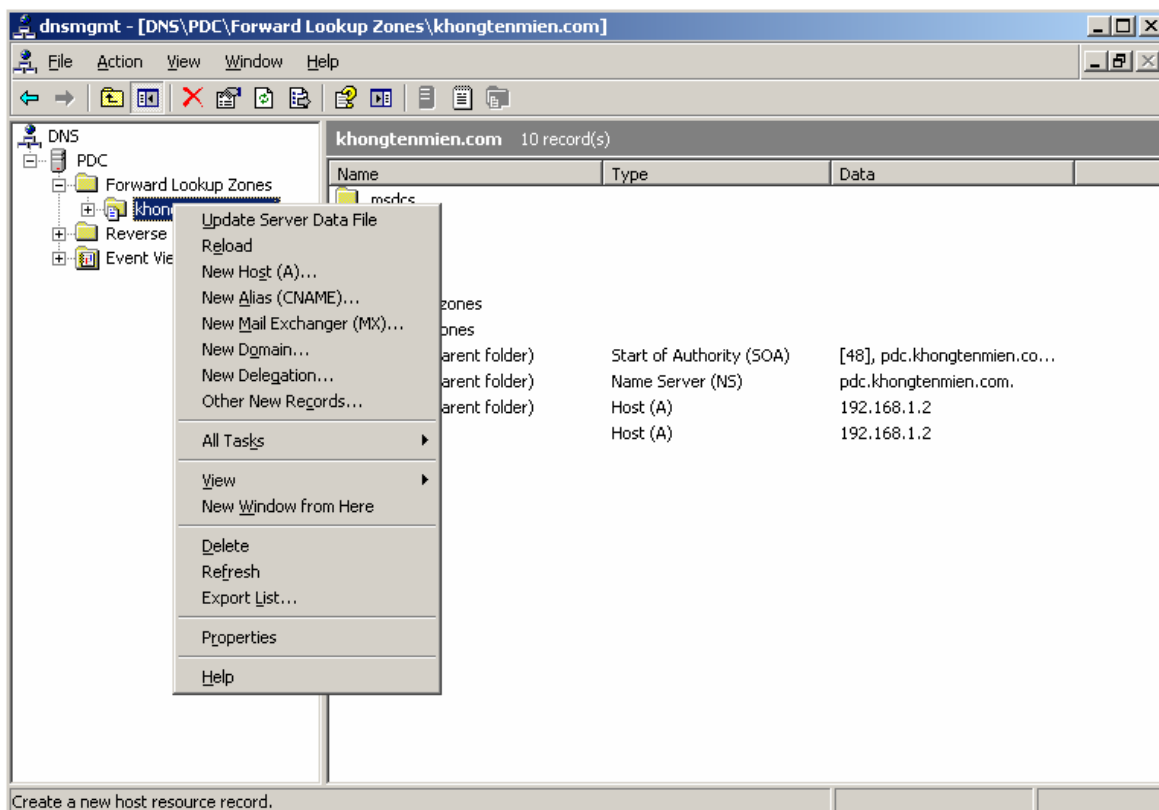
4. Tương tự như vậy tạo Host (A) cho máy Client, hoặc trên máy Client sau khi đã chỉ Preferred DNS về 192.168.1.2. Ta sử dụng dòng lệnh `ipconfig /registerdns` để đăng ký Host (A) và Pointer cho Client trên Primary DNS Server.

**\*Lưu ý:** Nếu ở môi trường domain, máy client join domain thành công thì Host (A) và Pointer sẽ được tự động tạo trên DNS server (đĩ nhiên client phải preferred DNS về DNS server).

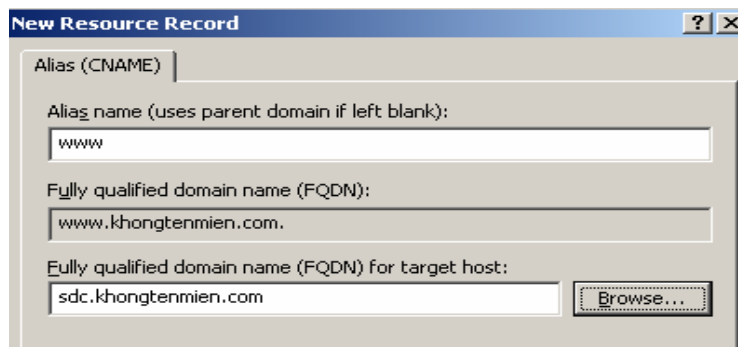
### Tạo Alias (CNAME)

Trong mô hình này do Secondary DNS Name chạy Web Server nên ta cấu hình Alias Name để chỉ [www.khongtenmien.com](http://www.khongtenmien.com) về địa chỉ 192.168.1.3

1. Chuột phải vào khongtenmien.com trong Forward Lookup Zone New Alias (CNAME)



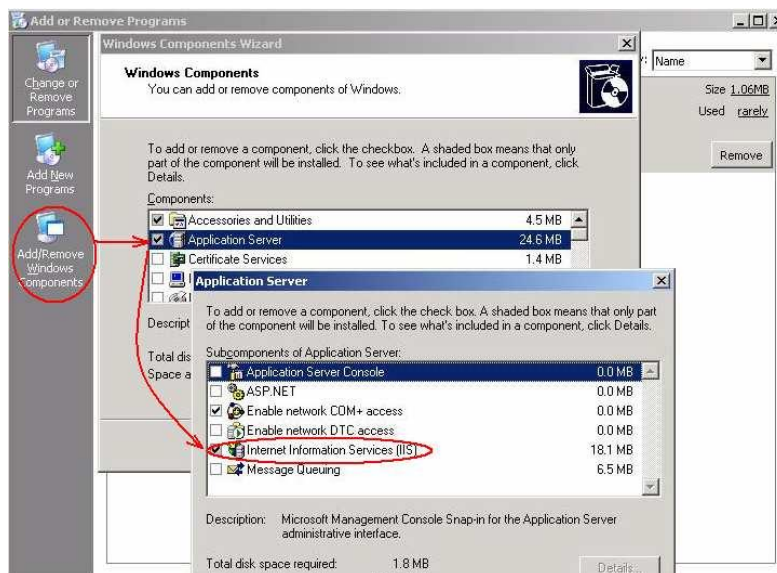
2. Alias Name : điền vào **www**, sau đó nhấn nút Browse và lần lượt double click vào DC, Forward Look..., khongtenmien.com, sdc Nhấn **OK OK**



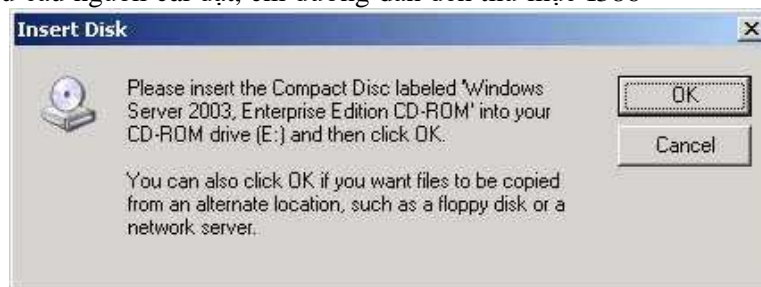
## Dịch vụ WEB

### I/ Cài đặt dịch vụ Web IIS (Internet Information Services).

1. Chọn **Start**    **Control Panel**    **Add/Remove Programs**
2. Chọn **Add or Remove Windows Components**
3. Chọn **Application Server**    Nhấn nút **Details**    Chọn **Internet Information Services (IIS)**



4. Nhấn **OK**    nhấn **Next**
5. Hệ thống yêu cầu nguồn cài đặt, chỉ đường dẫn đến thư mục I386



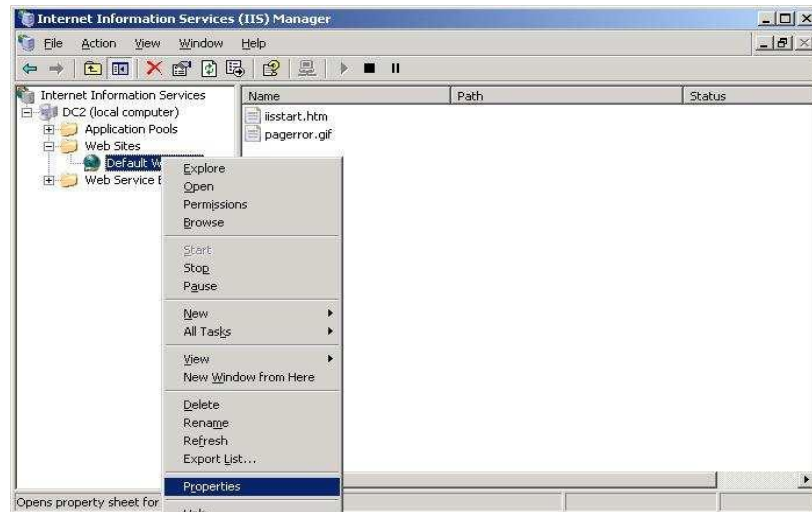
6. Nhấn **Finish** để kết thúc quá trình cài đặt

## II/ Cấu hình dịch vụ Web IIS (Internet Information Services).

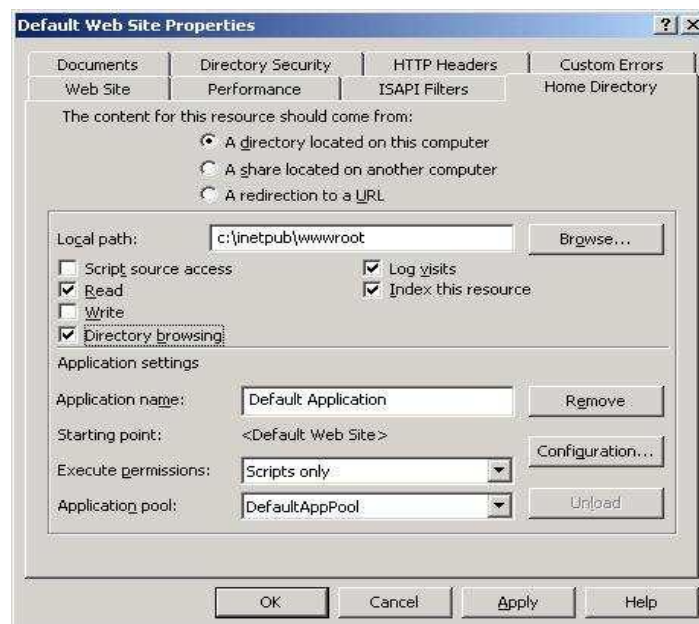
Sau khi cài đặt hoàn tất, để cấu hình ta chọn :

1. Chọn **Start Administrative Tools Information Services (IIS) Manager**

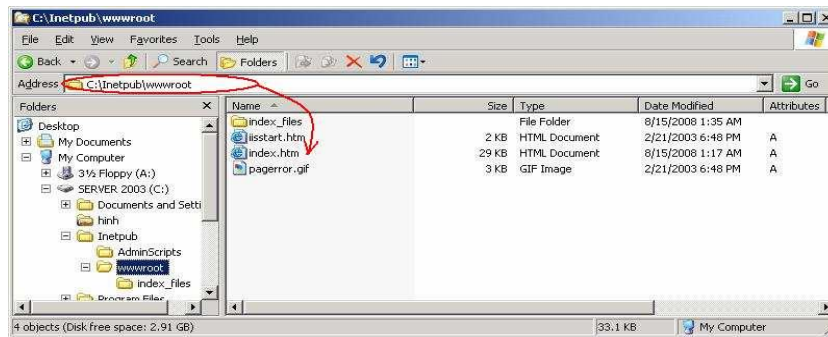
2. Chuột phải vào **Default Website** trong phần Web Sites Chọn **Properties**



3. Ta cần quan tâm đến 2 tab đó là **Documents** và **Home Directory**.



4. Save 1 trang web làm mẫu, sau đó copy vào đường dẫn C:\inetpub\wwwroot. Trong bài Lab này ta lấy trang web mẫu có tên là **index.htm** được save về từ web site [www.khongtenmien.com](http://www.khongtenmien.com)



Kiểm tra kết nối đến Web service vừa cài đặt trên máy Client

1. Cấu hình các thông số địa chỉ IP trên máy Client theo bảng thông tin cấu hình

☐ Obtain an IP address automatically  
☒ Use the following IP address:

IP address: 192 . 168 . 1 . 10  
 Subnet mask: 255 . 255 . 255 . 0  
 Default gateway: . . .

☐ Obtain DNS server address automatically  
☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 2  
 Alternate DNS server: 192 . 168 . 1 . 3

2. Mở Internet Explorer và gõ địa chỉ www.khongtenmien.com



# Dịch vụ mã hóa đường tuyến IPSec

## I/ Mô tả mô hình.

Thông thường, các dữ liệu vận chuyển trong LAN có thể bị các hacker dễ dàng chặn được và hiệu chỉnh bằng một số các công cụ phân tích protocol. Để bảo vệ, chúng ta có thể sử dụng đặc điểm mã hóa dữ liệu trước khi vận chuyển trên mạng bằng cách sử dụng IPSec. Sử dụng IPSec, chúng ta có thể mã hóa tất cả các dữ liệu cho một máy tính client hoặc tất cả các máy tính trong domain tùy thích.

Mỗi một rule trong IPSec Security Policy bao gồm các thành phần:

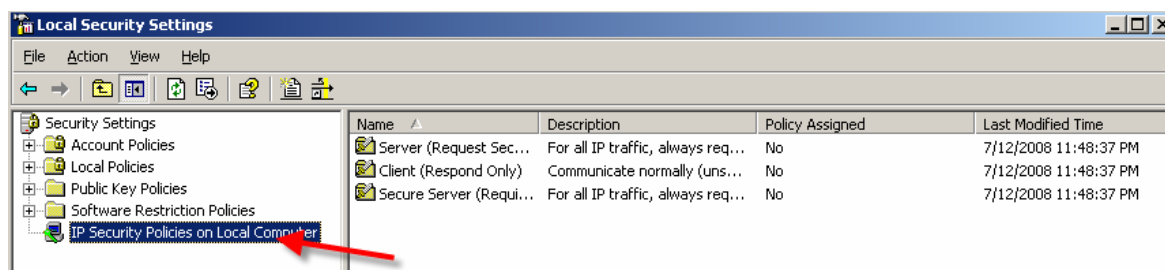
- Bộ lọc - Filter: Xác định kiểu giao thông nào sẽ được áp đặt. VD như HTTP,FTP,Telnet ..v..v..
- Hành động áp đặt - Filter action: Thực hiện hành động nào với kiểu giao thông được áp đặt bộ lọc. VD như cho phép, cấm ..v..v..
- Phương pháp xác thực - authentication: Có 3 phương pháp xác thực được sử dụng trong IPSec là Pre-Shared Key, Keberos, Certificate. Bạn có thể dùng nhiều phương pháp xác thực khác nhau trong cùng 1 rule.

## II/ Cấu hình IPSec giữa hai máy tính sử dụng xác thực bằng pre-shared key.

	Client 1	Client 2
Card LAN	IP: 192.168.1.10 SM: 255.255.255.0	IP: 192.168.1.11 SM: 255.255.255.0

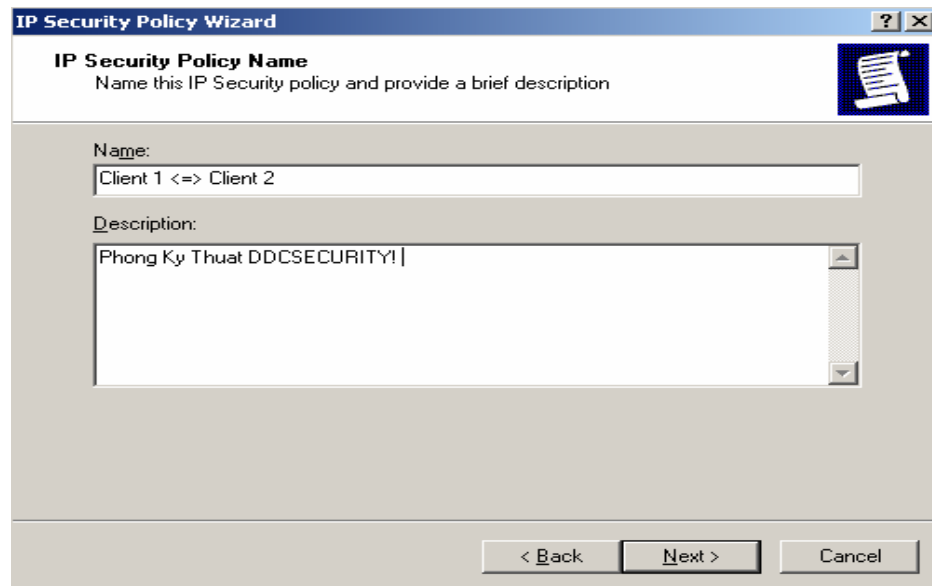
Thực hiện các bước sau trên máy Client 1:

1. Click Start, chọn Programs, chọn Administrative Tools và chọn Local Security Policy.  
Hoặc sử dụng dòng lệnh secpol.msc
2. Trong cửa sổ Local Security Settings, click vào mục IP Security Policies on Local Computer.

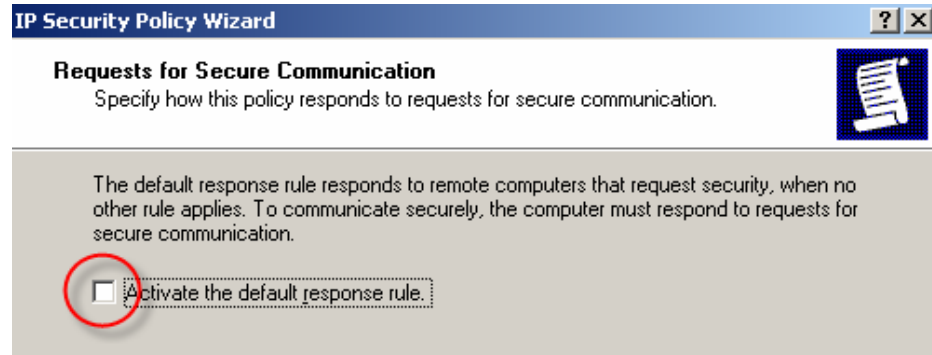


3. Right click vào mục IP Security Policies on Local Computer, click vào mục Create IP Security Policy để tạo ra một chính sách IPSec mới.

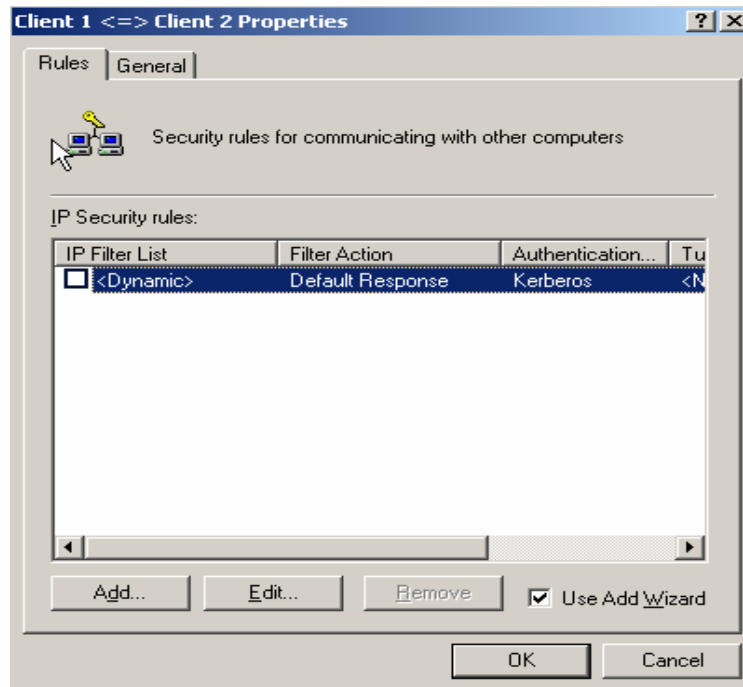
4. Trên hộp thoại IP Security Policy Wizard, trên trang Welcome to the IP Security Policy Wizard, click Next.
5. Trên trang IP Security Policy Name, nhập tên của IPSec policy vào trong hộp Name, click Next.



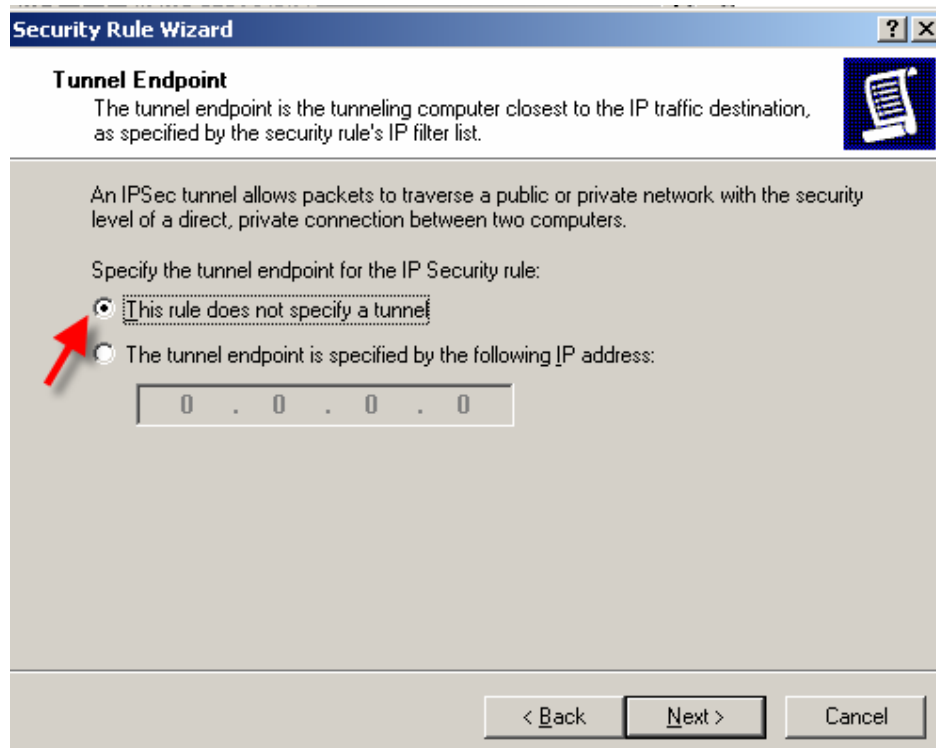
6. Trên trang Requests for Secure Communication, loại bỏ dấu check “Active the default response rule”, click Next.



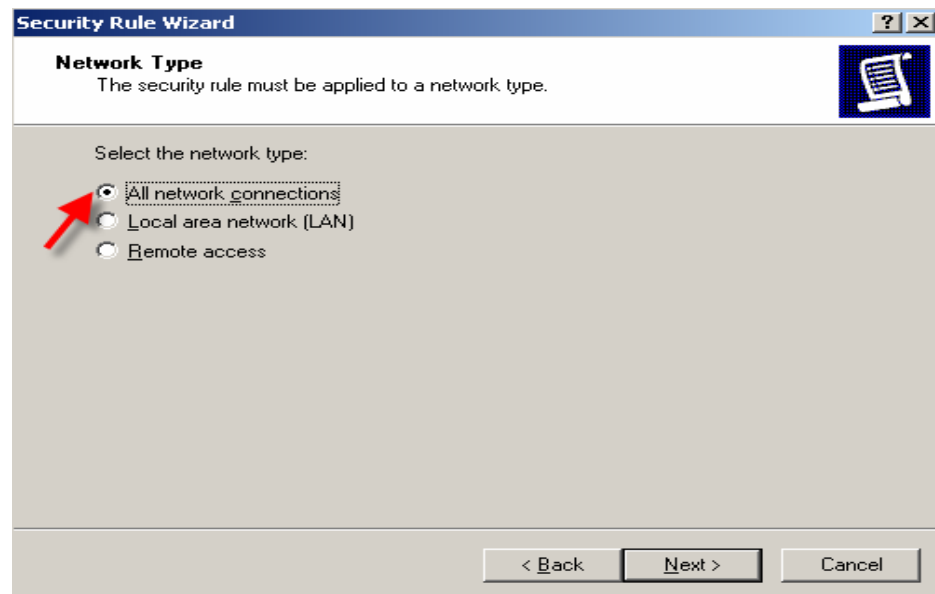
7. Trên trang Completing the Security Policy Wizard, Click Finish. Một hộp thoại xuất hiện như sau.



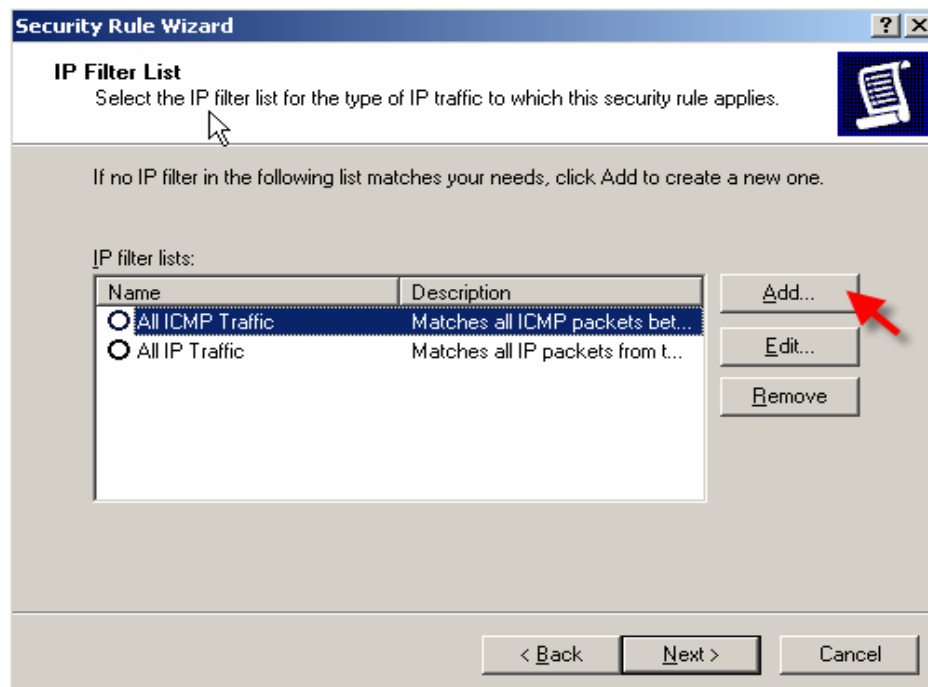
8. Click Add để tạo thêm một rule mới.
9. Trong hộp thoại Security Rule Wizard, trên trang “Welcome to the Create IP Security Rule Wizard” , click Next.



10. Trên trang Tunnel EndPoint, chắc chắn rằng phương án “This rule does not specify a tunnel” được chọn, click Next.

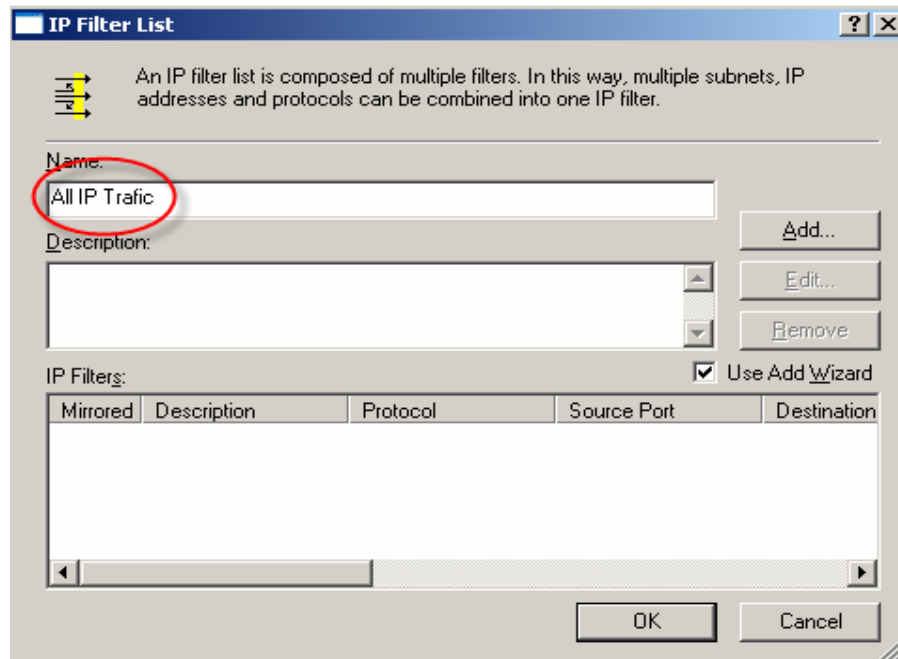


11. Trên trang Network Type, chắc chắn rằng phương án “All network connections” được chọn, click Next.

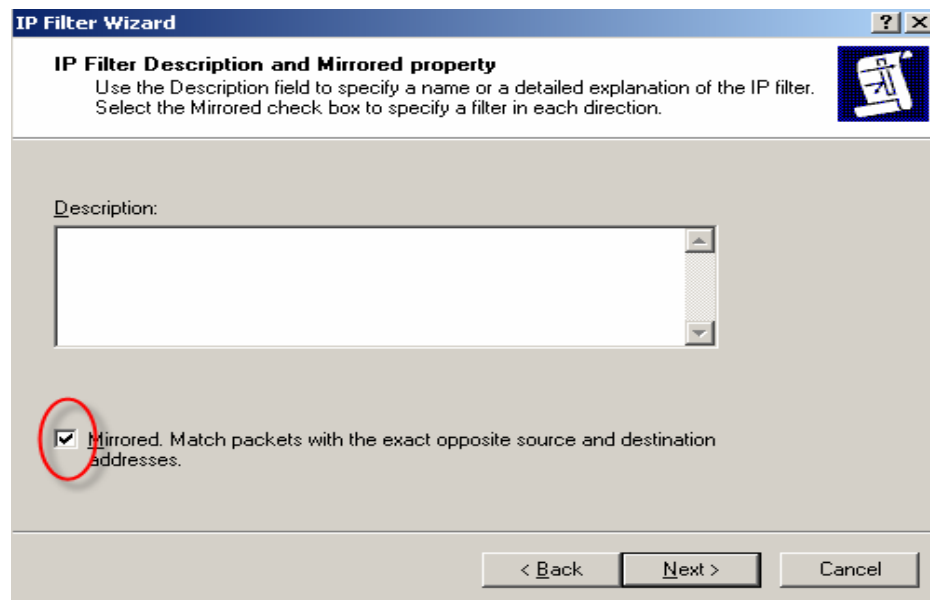


12. Trên trang IP Filter List, click vào nút Add để tạo một IP Filter hoàn toàn mới.

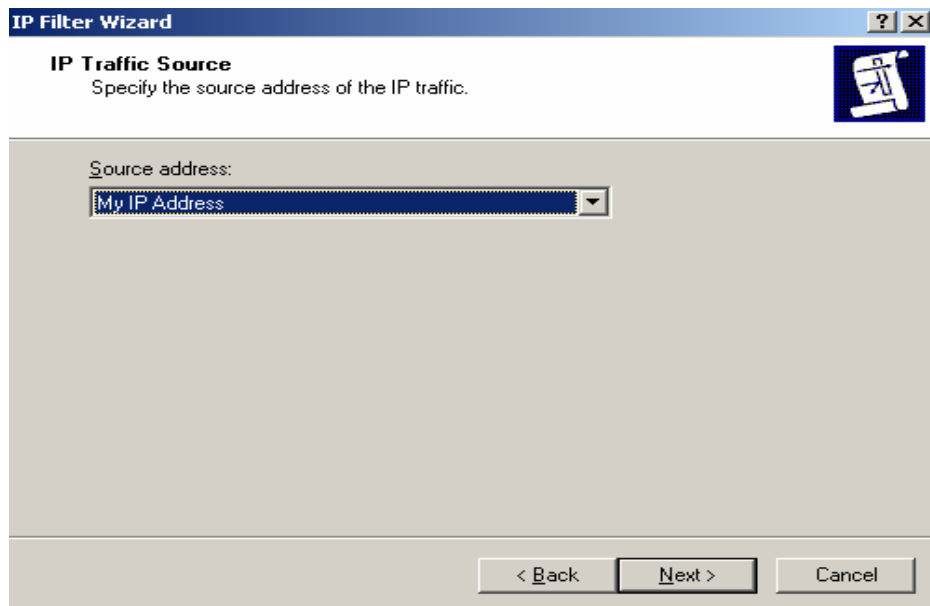




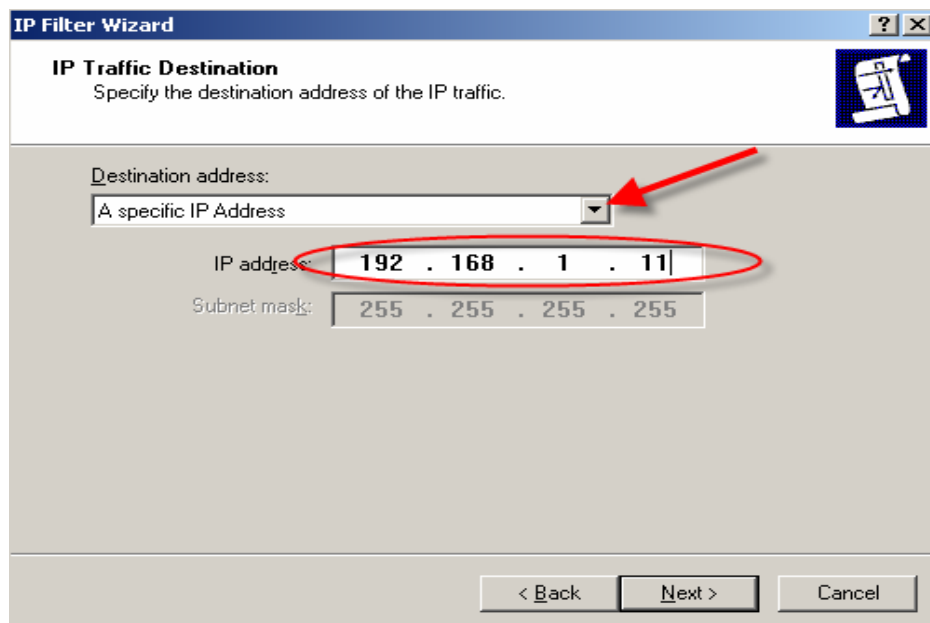
13. Trong hộp thoại IP Filter List, đặt tên “All IP Traffic” vào text Name, click Add.
14. Trong hộp thoại IP Filter Wizard, trên trang Welcome to the IP Filter Wizard, click Next.



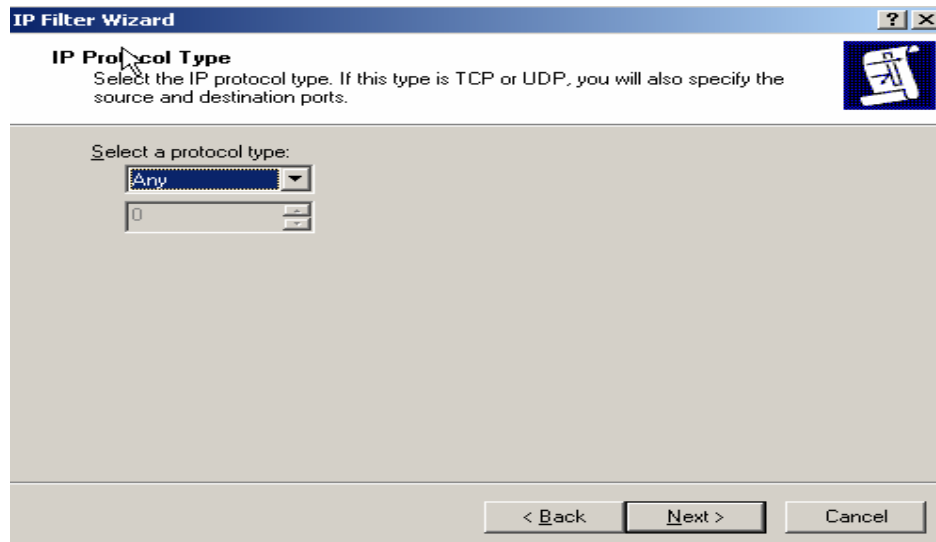
15. đảm bảo check chọn “Mirrored...” . Phương án này đảm bảo sẽ tạo ra một bộ lọc filter hoàn toàn tự động theo chiều ngược lại với chiều bạn đã cấu hình. Ở VD này, chúng ta tạo một filter từ địa chỉ IP của máy Client 1 tới địa chỉ Client 2. Như vậy một filter theo chiều Client 2 đến Client 1 được tự động tạo ra khi tạo check chọn Mirrored.



16. Trên trang IP Traffic Source, chắc chắn trong mục chọn Source address là giá trị “My IP Address”. Điều này thể hiện filter sẽ xem xét các giao thông mạng xuất phát từ máy Client 1 đi ra. Click Next.



17. Trên trang IP Protocol Traffic Destination, trong mục chọn Destination address, lựa chọn phương án “A Specific IP Address”. Nhập địa chỉ IP của máy tính Client 2 vào hộp text IP address (192.168.1.11). Điều này thể hiện filter sẽ xem xét các giao thông xuất phát từ máy tính Client 1 nhưng có đích đến là máy tính Client 2. Click Next.

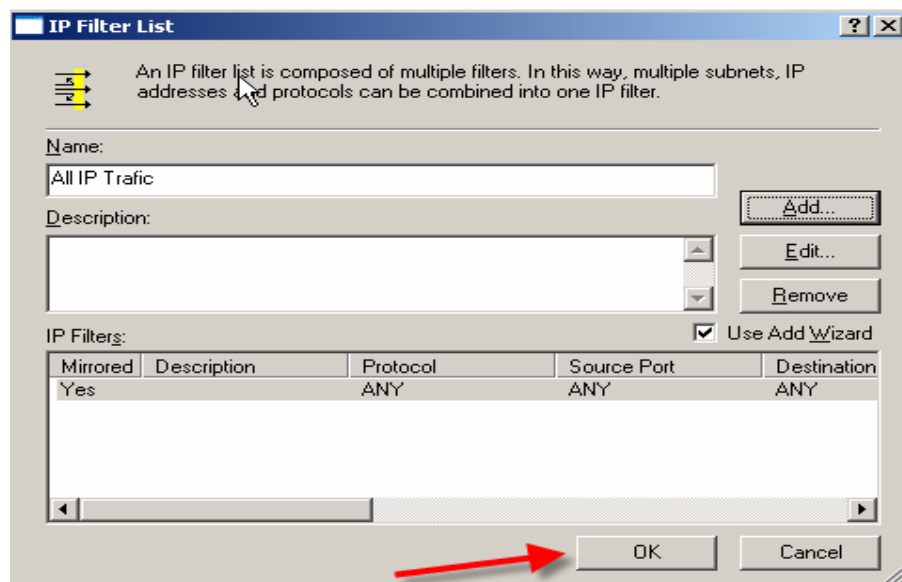


18. Trên trang IP protocol Type, chọn phương án “Any”, click Next.

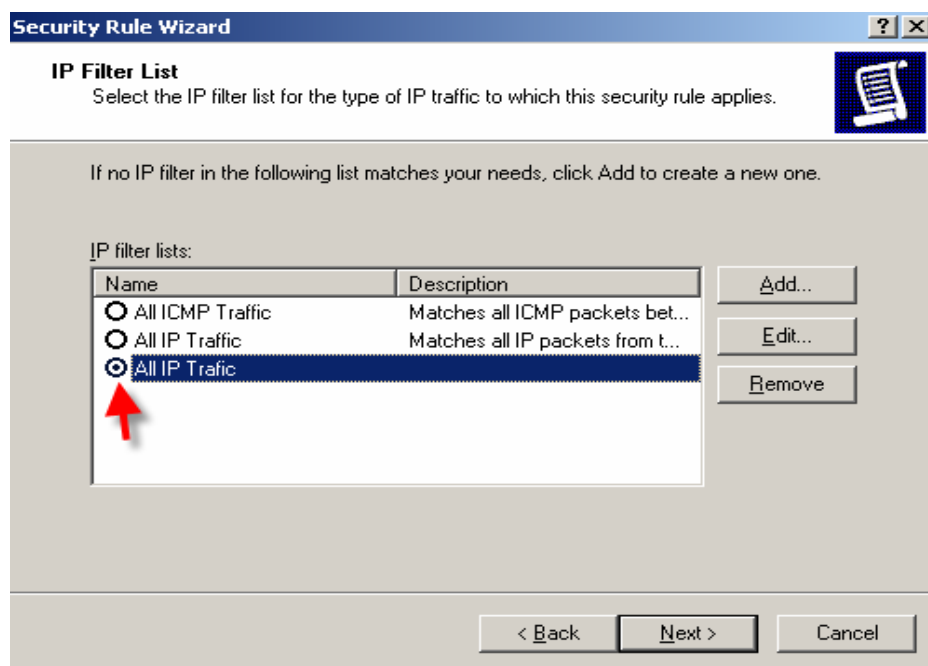
**\*Lưu ý:** Vì trong VD này ta quy định filter là “All IP Traffic” nên phải chọn Any. Nếu như các bạn chỉ muốn áp dụng IPSec cho từng loại dịch vụ riêng biệt, các bạn sẽ xác định cụ thể hơn. VD như HTTP, các bạn phải chọn TCP port 80; FTP, các bạn phải chọn TCP port 21 ..v..v..



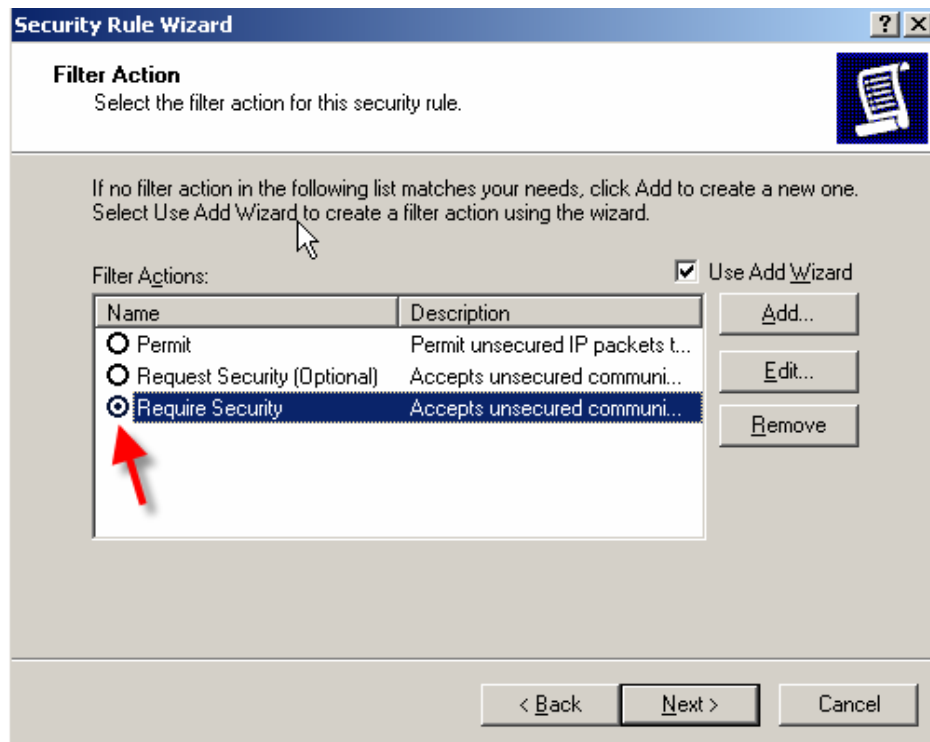
19. Click Finish.



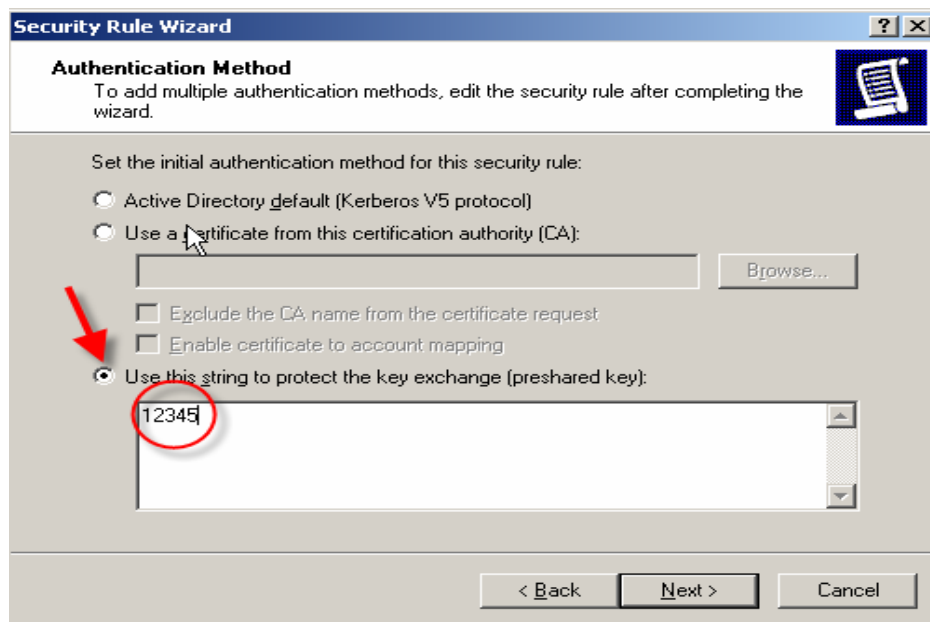
20. Click OK.



21. Trên trang IP Filter List, đánh dấu chọn IP Filter có tên “All IP Traffic” mà ta vừa mới tạo, click Next.



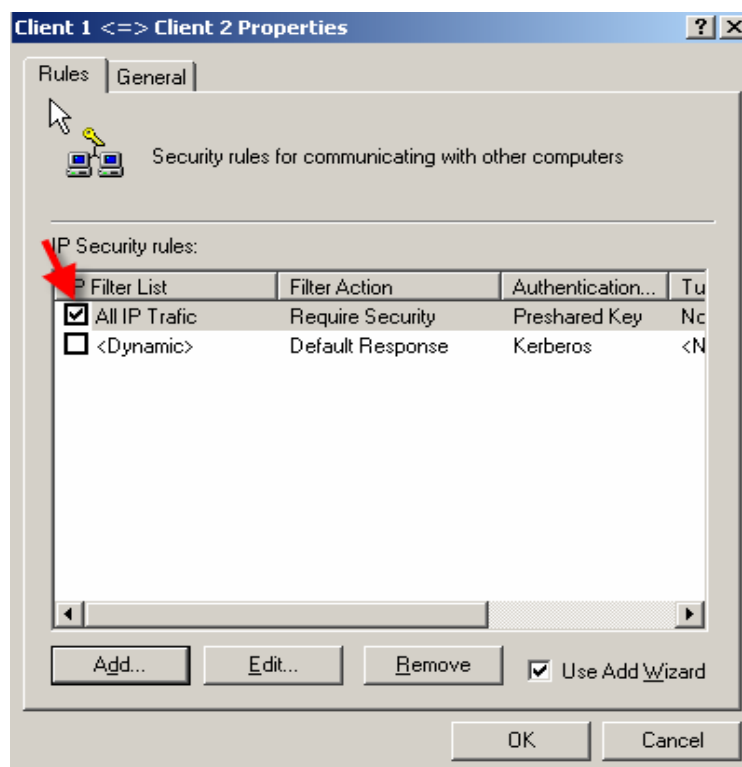
22. Trên trang Filter Action, đánh dấu chọn phương án Require Security trong khung Filter Actions. Phương án này buộc phải thỏa mãn điều kiện IP filter mới thiết lập kết nối. Click Next.



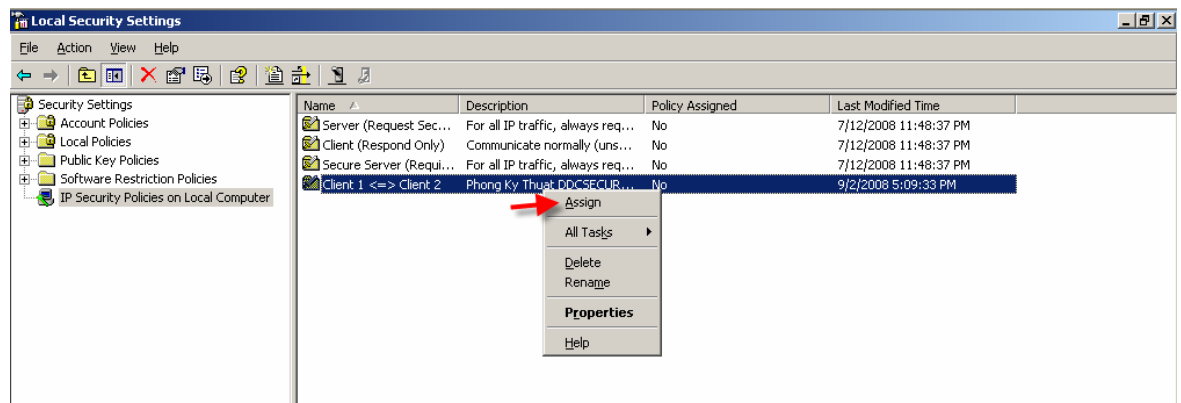
23. Trên trang Authentication Method, chọn phương pháp xác thực là Preshared key, điền chuỗi bảo vệ vào. Click Next.



24. Trên trang Completing the Security Rule Wizard, loại bỏ dấu check “Edit Properties” , click Finish.



25. Trong hộp thoại “Client 1 <=> Client 2” Properties, đảm bảo rule mới vừa tạo được chọn. Click Ok để hoàn tất.
26. Hiện tại chính sách policy này chưa được assign, để assign – right click vào policy mới được tạo và chọn Assign.



## 27. GPUPDATE /FORCE để cập nhật policy.

### Trên máy Client 2:

Thực hiện tương tự các bước như ở Client 1, tuy nhiên trên trang IP Traffic Destination, phần IP address, ta sẽ điền là IP của Client 1 (192.168.1.10). Và đặc biệt phần chuỗi preshared key phải giống như bước cấu hình ở Client 1 (Bước 12345)