

## BÀI THỰC HÀNH 13

### VPN (VIRTUAL PRIVATE NETWORK)

#### GIỚI THIỆU

- VPN hay còn được gọi là **Mạng riêng ảo** (*Virtual Private Network*)
- VPN là một mạng riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các địa điểm hoặc người sử dụng từ xa với một mạng LAN ở trụ sở trung tâm. Thay vì dùng kết nối thật khá phức tạp như đường dây thuê bao số, VPN tạo ra các liên kết ảo được truyền qua Internet giữa mạng riêng của một tổ chức với địa điểm hoặc người sử dụng ở xa.
- Có hai loại phổ biến hiện nay là VPN truy cập từ xa (Remote-Access ) và VPN điểm-nối-điểm (site-to-site)
- PPTP (**Point-to-Point Tunneling Protocol**) là Protocol dùng tạo kết nối VPN, tạo đường hầm điểm nối điểm sử dụng port 1723. Một giao thức cho phép tạo ra một đường truyền dữ liệu bảo mật của data từ một client đến một private enterprise server bằng cách tạo một VPN thông qua các mạng truyền dữ liệu dựa trên TCP/IP. PPTP có khả năng hỗ trợ on-demand, nhiều giao thức, mạng VPN trên các mạng public, như Internet.

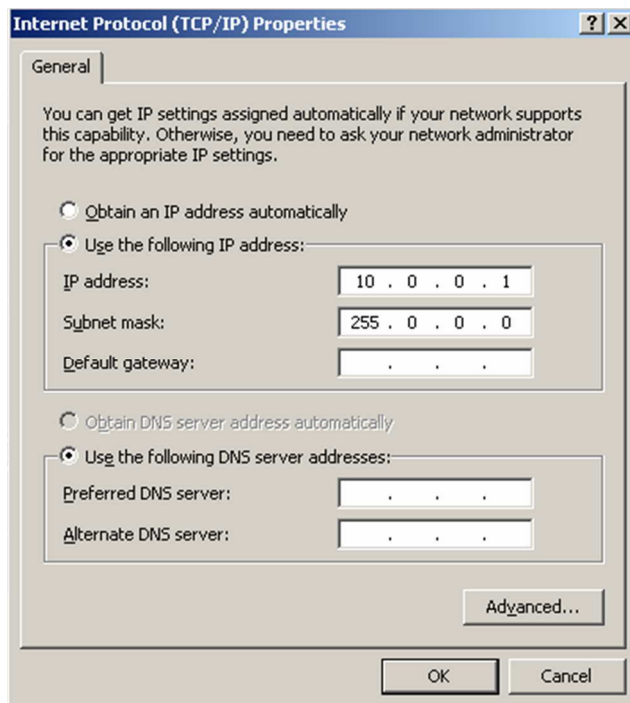
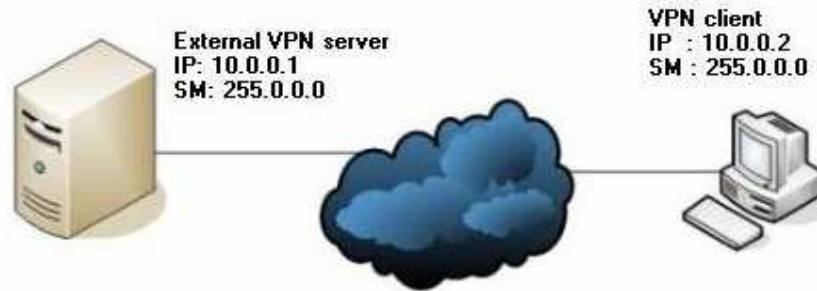
#### Lợi ích khi sử dụng :

- Giải pháp VPN (Virtual Private Network) được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn nên tiết kiệm được được chi phí và thời gian.
- Một mạng VPN điển hình bao gồm mạng LAN chính tại trụ sở (Văn phòng chính), các mạng LAN khác tại những văn phòng từ xa, các điểm kết nối (như 'Văn phòng' tại gia) hoặc người sử dụng (Nhân viên di động) truy cập đến từ bên ngoài

# Bài 1

## Mô Hình Triển Khai:

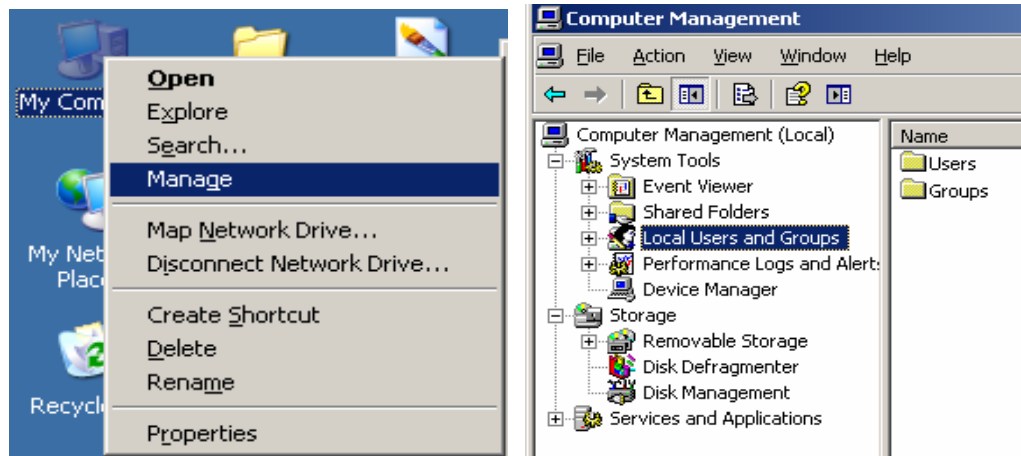
### VPN Client to Site



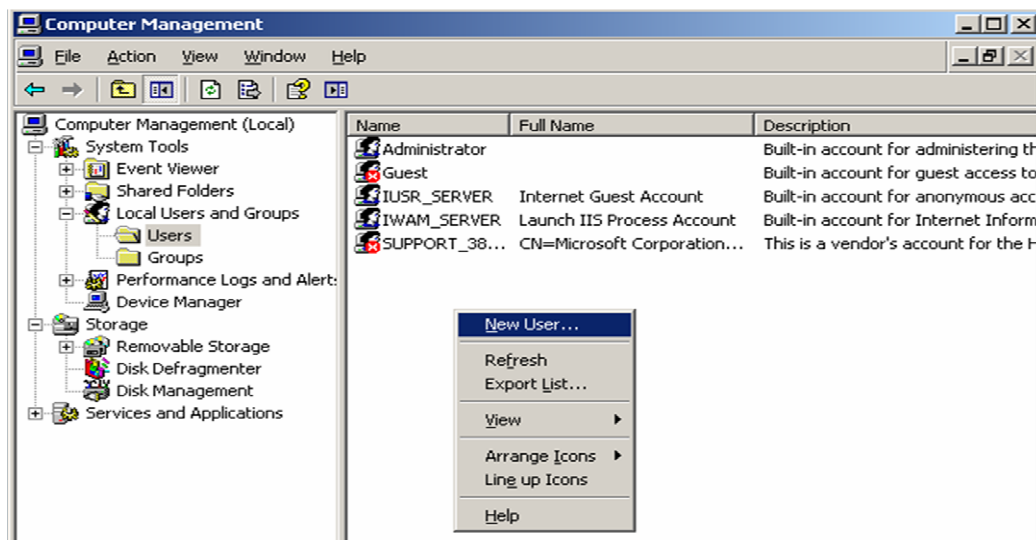
Thiết lập địa chỉ IP cho server như sau:

- **Start → Settings**
- **Network Connection**
- **Local Area Connection**
- Thiết lập địa chỉ IP nhý hình vẽ trên.

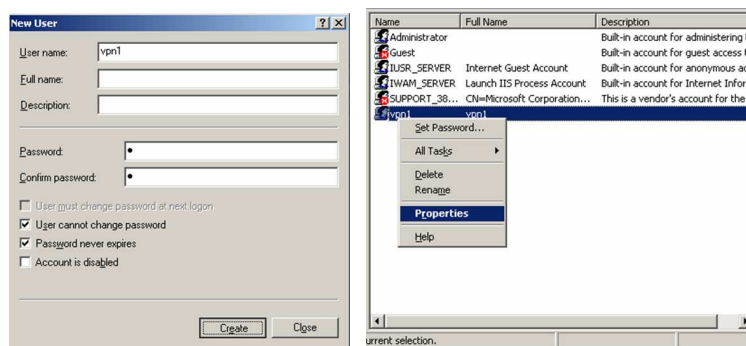
## Bài thực hành số 13



Right click **My Computer** chọn **Manage** chọn **Local Users and Groups**

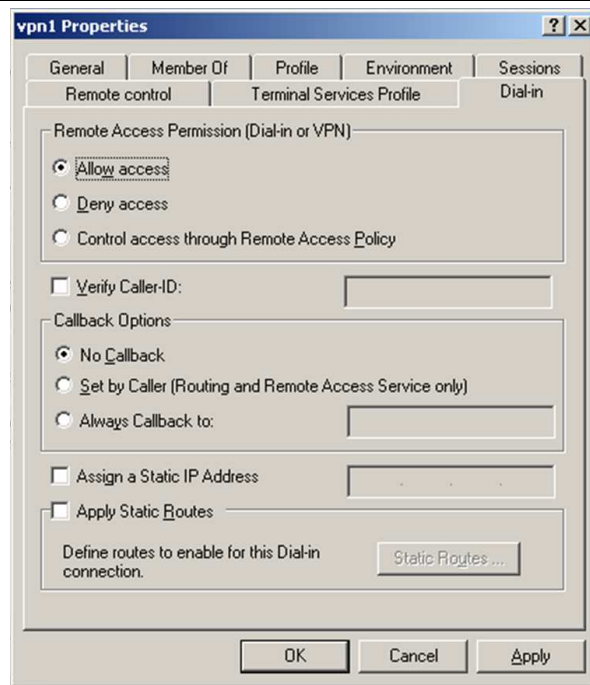


Right click chọn **New user(Tạo 1 users mới )**

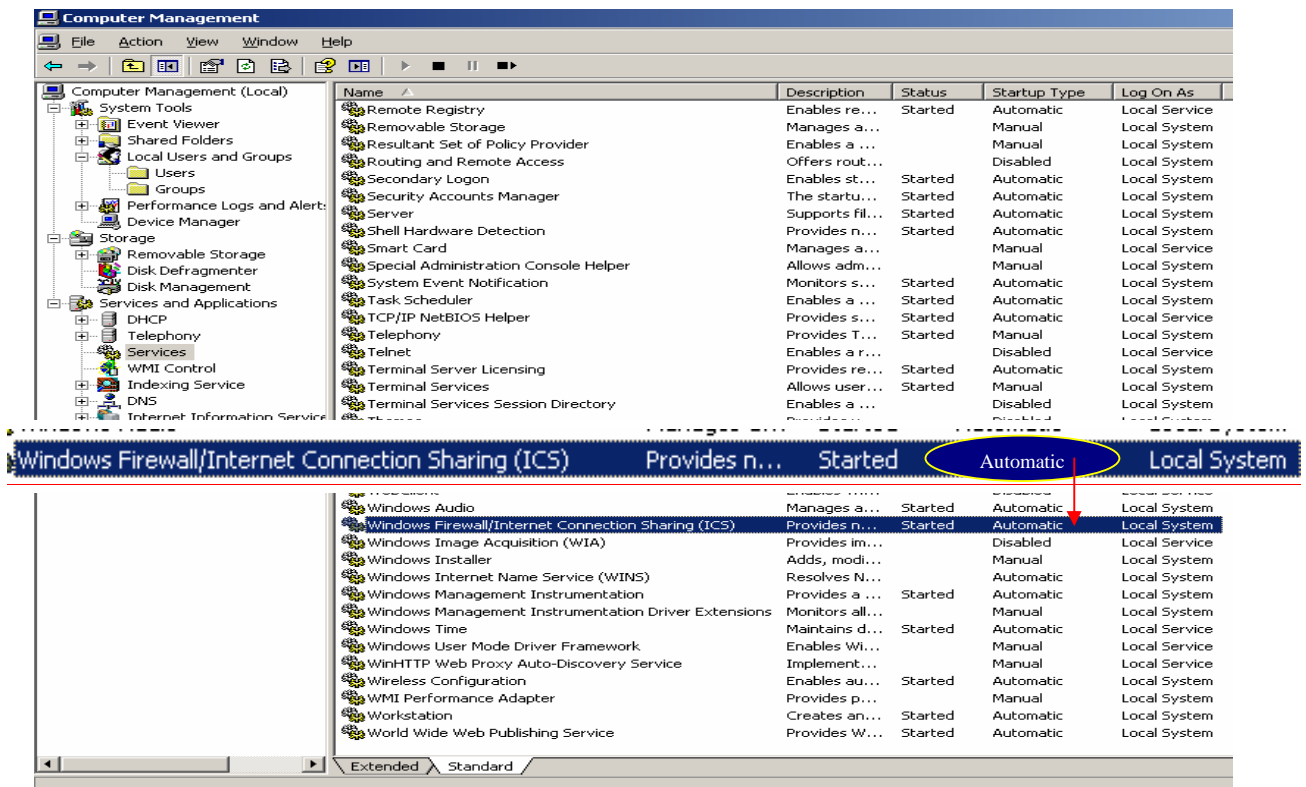


- + Đặt tên Users name : **vpn1**, password : **1**,
- + Check vào 2 ô :
  - ✓ **Use cannot change password** và ✓ **password never expires**
- + Sau đó rightclick vào tên users vừa tạo chọn **Properties**

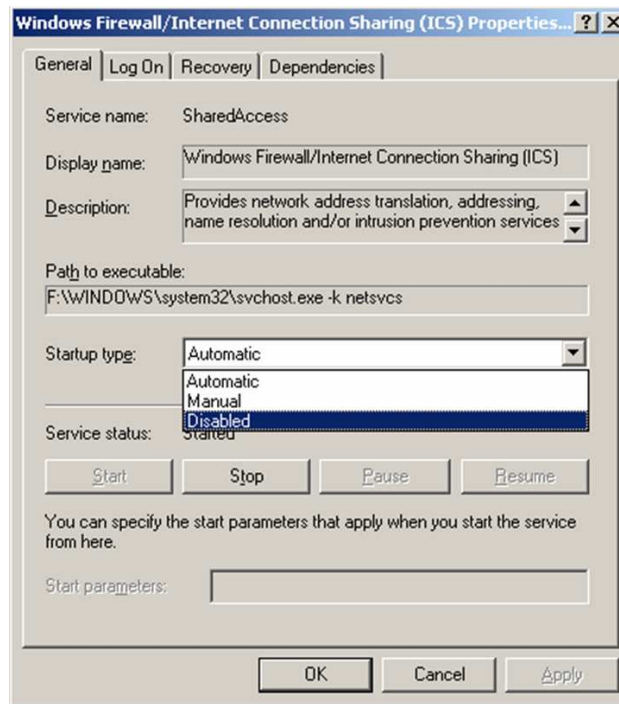
## Bài thực hành số 13



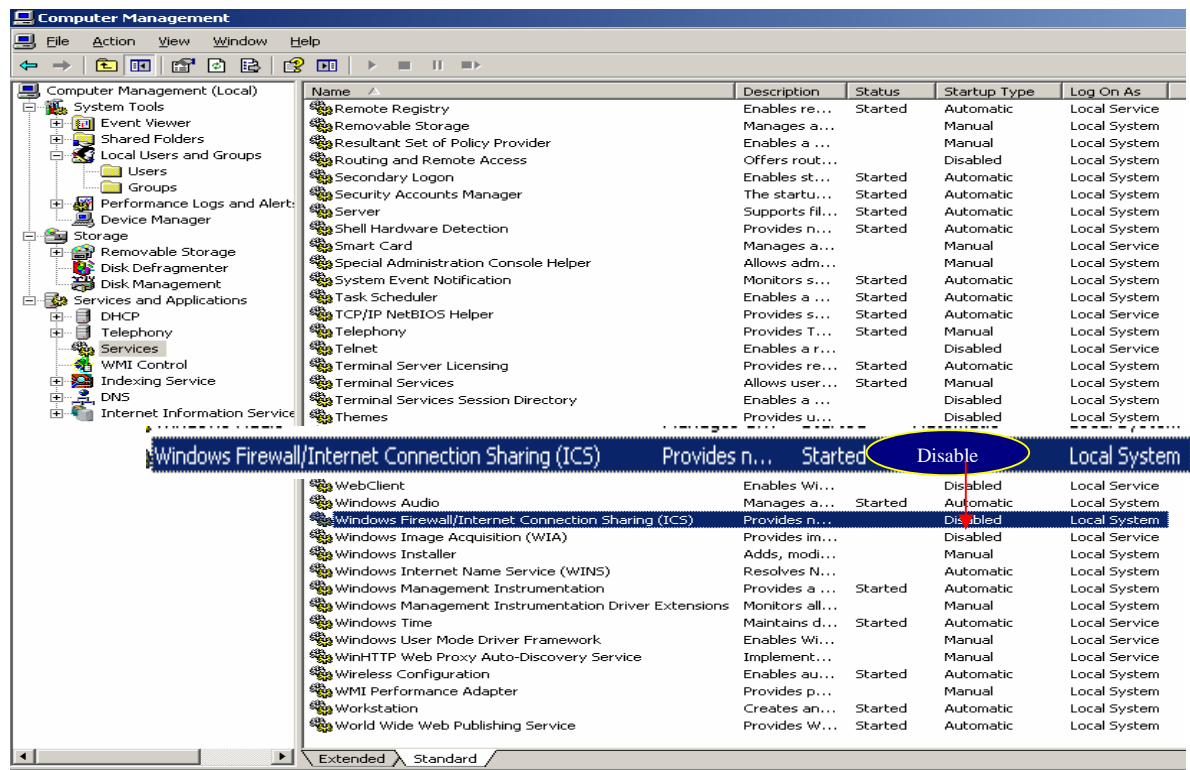
→ **Dial-in** chọn **Allow Access**  
 Trong phần **CallBack Options**  
 chọn **No Callback**



Right click **MyComputer** → **Manage**  
 Tại **Computer management** → **Services** → **Windows Firewall / Internet Connection Sharing(ICS)** và tắt chế độ tường lửa(Disable)

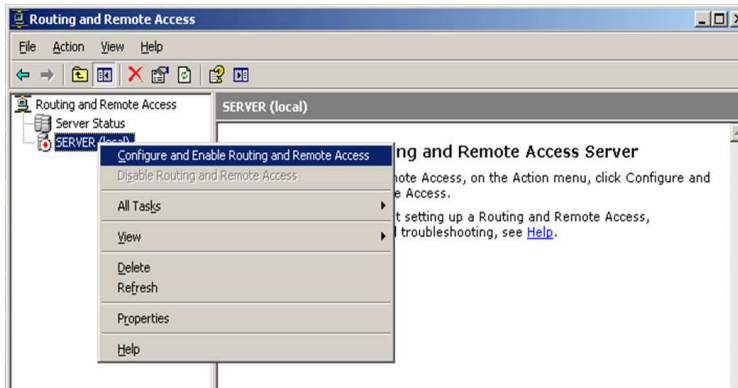


Tại thẻ **General** trong phần **Startup type** ta chọn **Disabled**

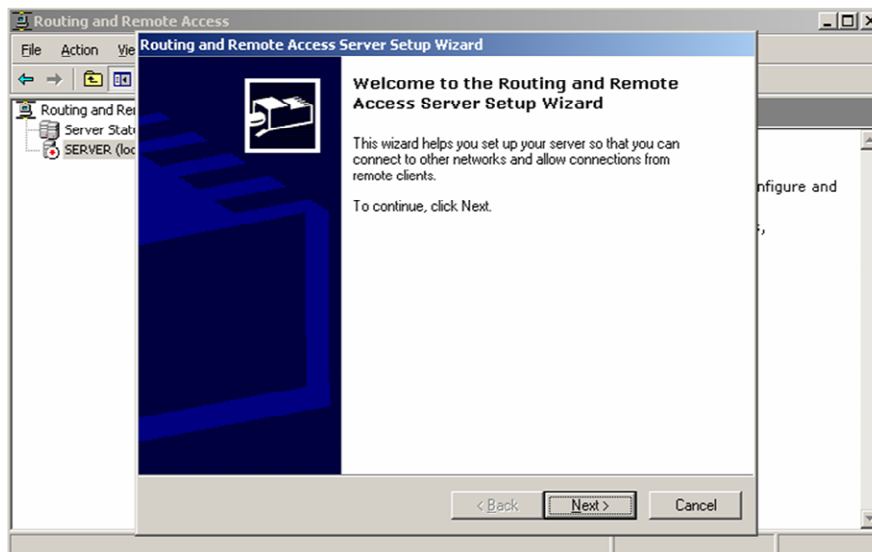


Tường lửa đã được **Disable**

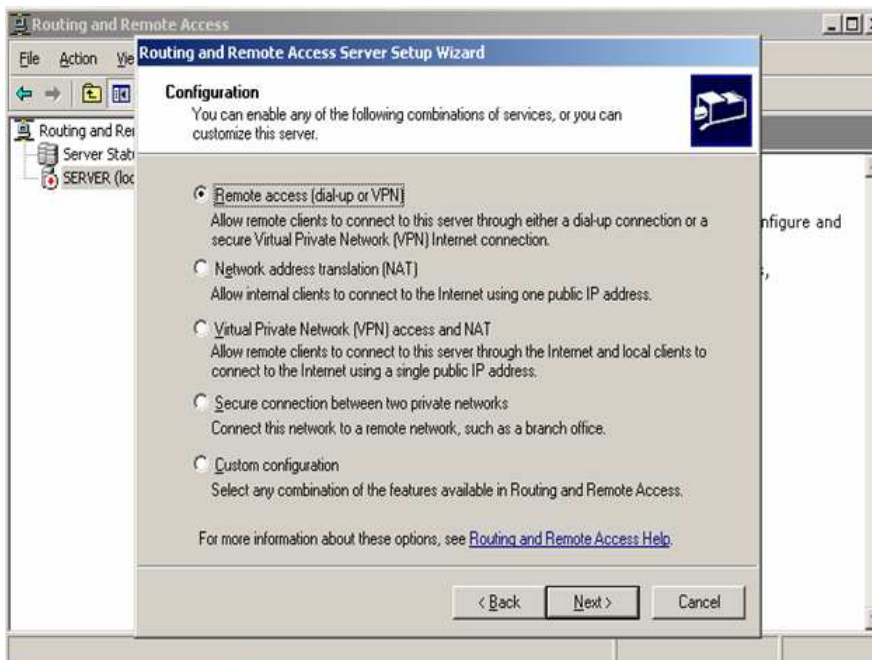
## Bài thực hành số 13



- Start
- Programs
- Administrative Tools
- Routing and Remote Access



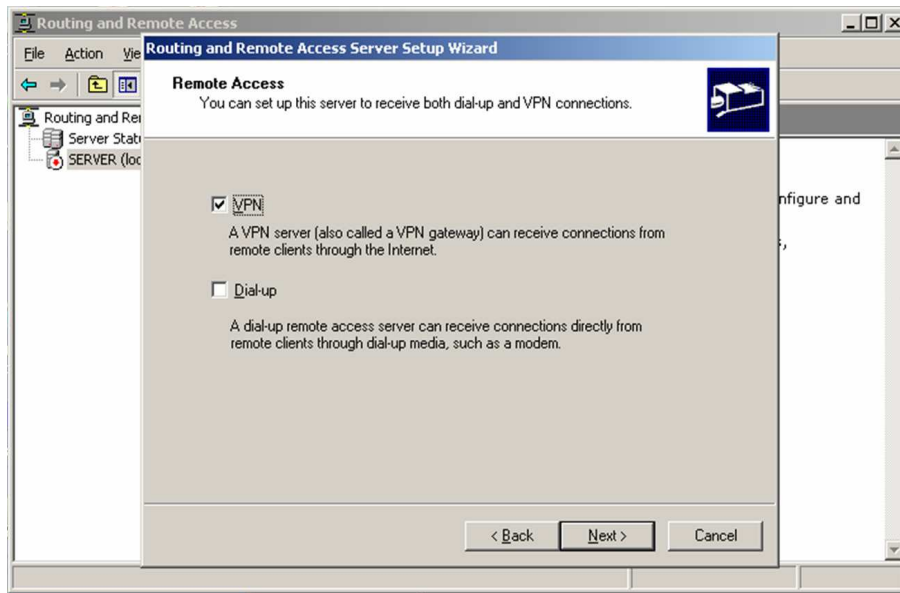
Tạo VPN



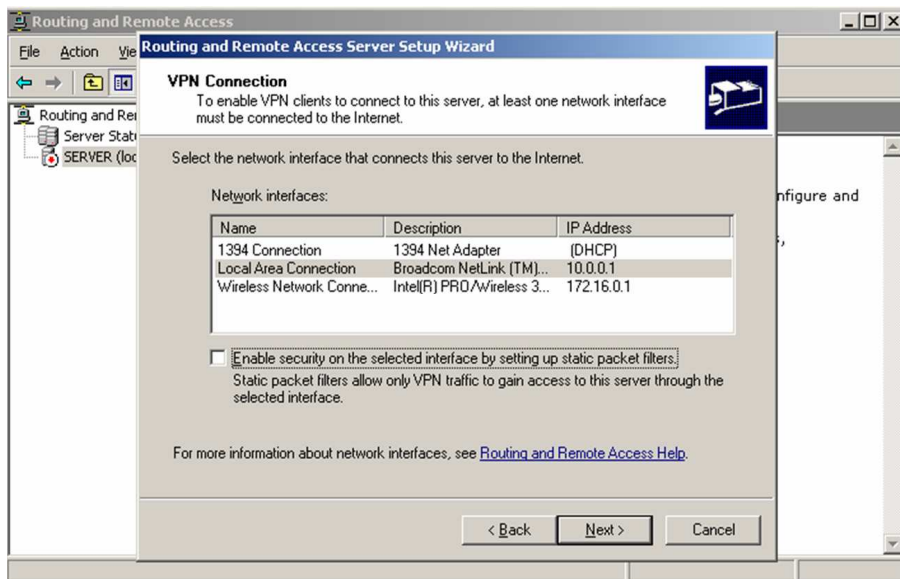
Chọn  
Remote access  
(dial-up or VPN)



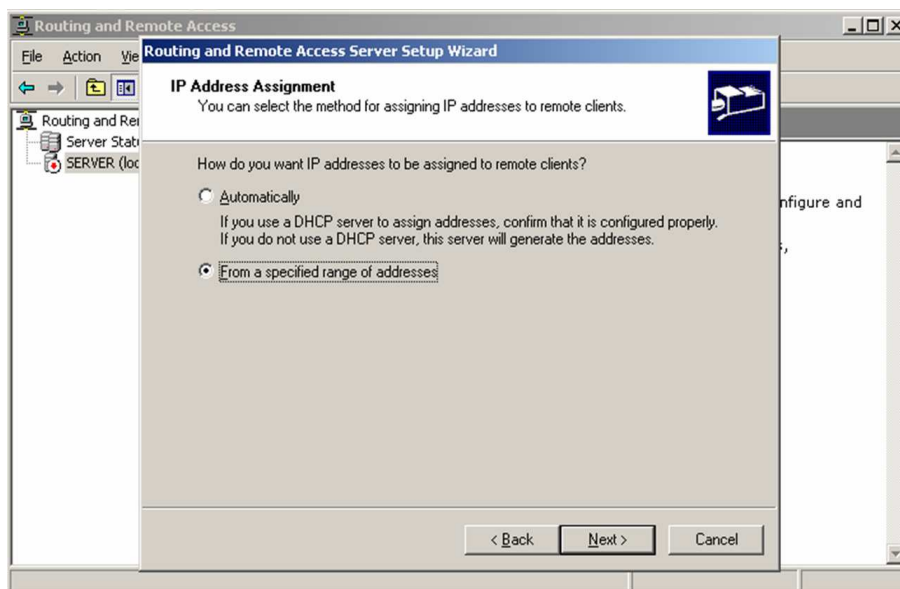
## Bài thực hành số 13



Check VPN

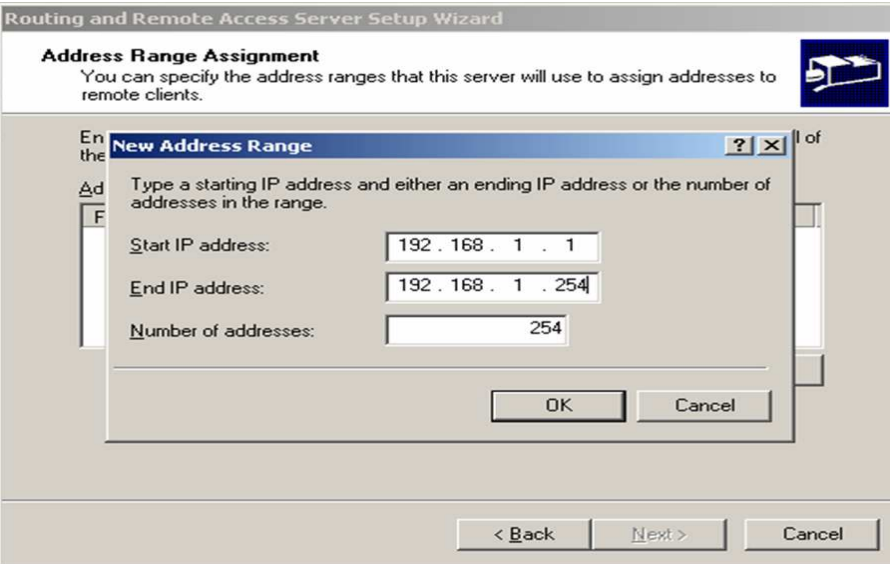


Chọn  
Local Area  
Connection



Chọn From a  
specified range of  
addresses

## Bài thực hành số 13



**Address Range Assignment**  
You can specify the address ranges that this server will use to assign addresses to remote clients.

**New Address Range**

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192.168.1.1

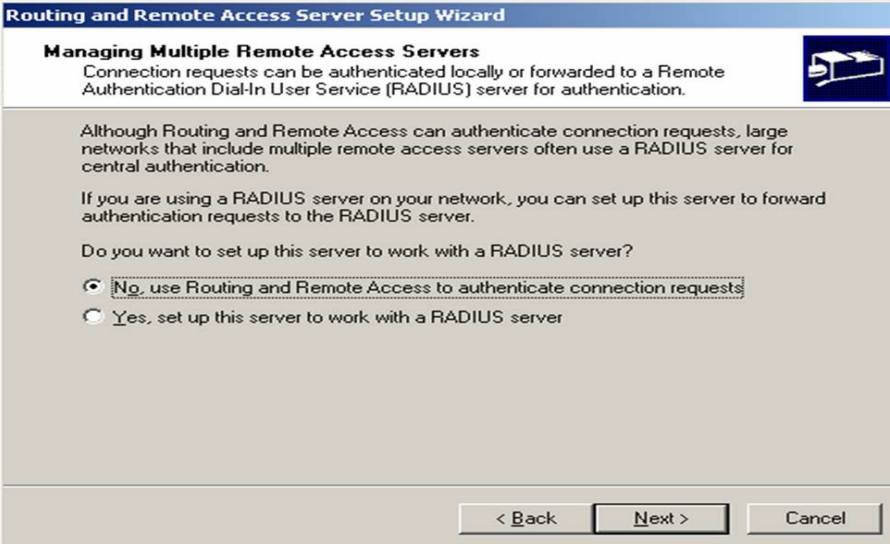
End IP address: 192.168.1.254

Number of addresses: 254

OK Cancel

< Back Next > Cancel

New range:  
thiết lập địa chỉ  
bắt đầu và địa  
chỉ cuối theo  
hình trên



**Managing Multiple Remote Access Servers**  
Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

☒ No, use Routing and Remote Access to authenticate connection requests

☐ Yes, set up this server to work with a RADIUS server

< Back Next > Cancel

Chọn  
No, use Routing and  
Remote Access to  
authenticate  
connection requests



**Completing the Routing and Remote Access Server Setup Wizard**

You have successfully completed the Routing and Remote Access Server Setup Wizard.

Summary:

VPN clients connect to the following public interface:  
Local Area Connection

VPN clients are assigned the following network for  
addressing: Wireless Network Connection.

Client connections are accepted and authenticated  
using: remote access policies for this server.

Before clients can connect, user accounts must be added  
locally or through Active Directory. For more information about  
user accounts, see [Routing and Remote Access Help](#).

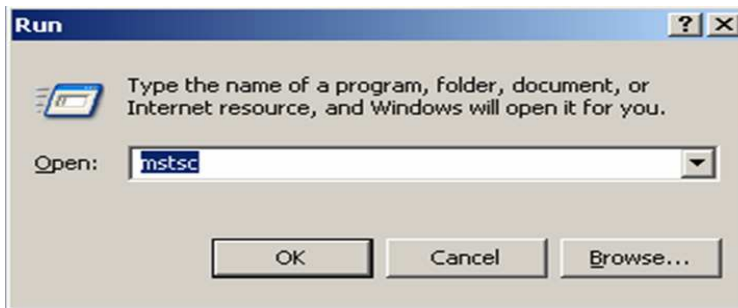
To close this wizard, click Finish.

< Back Finish Cancel

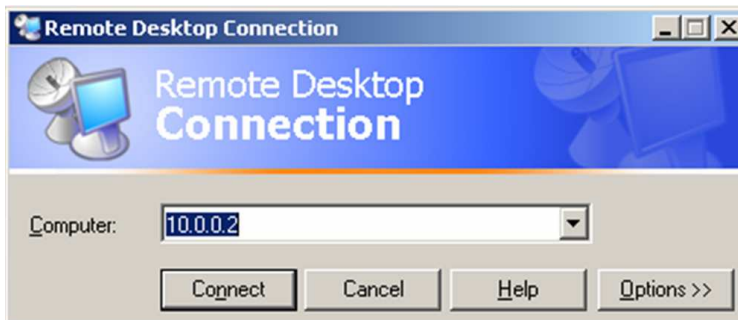
Finish



## Bài thực hành số 13



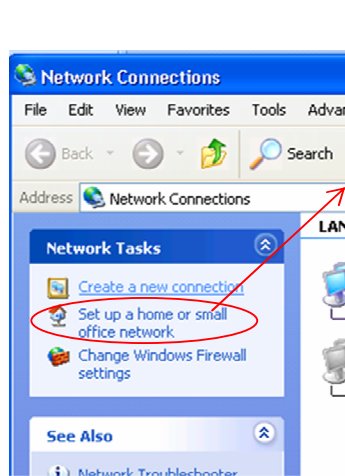
- Start
- Run nhập mstsc



Thực hiện **Remote Desktop Connection**. Tại Computer gõ ip: **10.0.0.2**

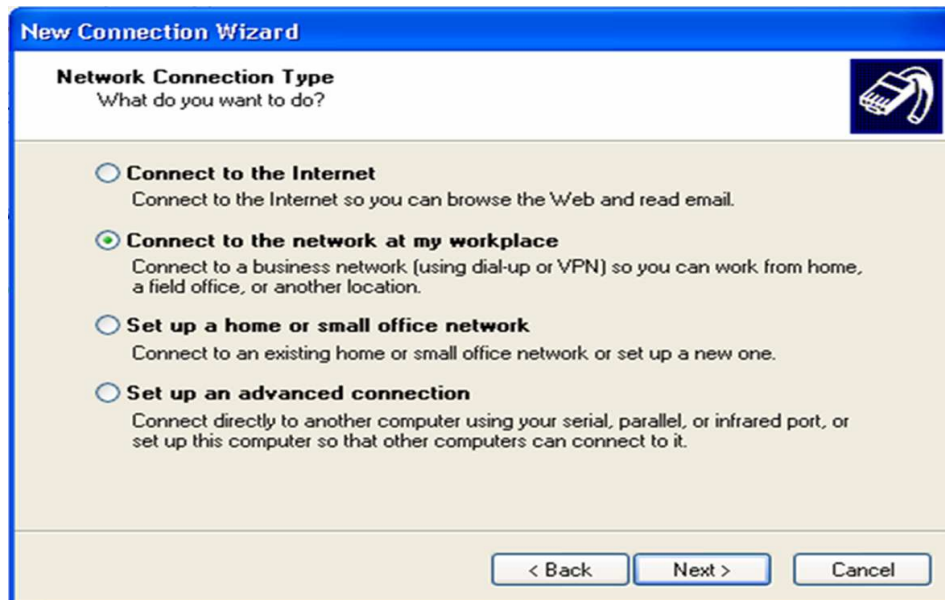


Màn hình đăng nhập vào máy client sau khi thực hiện Remote



Máy Client đã thực hiện remote thành công

→ Start  
→ Setting  
→ Network Connection



Chọn  
Connect to the network at my workplace

**New Connection Wizard**

**Network Connection**  
How do you want to connect to the network at your workplace?

Create the following connection:

☐ **Dial-up connection**  
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

☒ **Virtual Private Network connection**  
Connect to the network using a virtual private network (VPN) connection over the Internet.

**Chọn  
Virtual Private Network  
connection**

< Back   Next >   Cancel

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

SilverLight

For example, you could type the name of your workplace or the name of a server you will connect to.

**Tại Company name  
Đặt tên SilverLight**

< Back   Next >   Cancel

**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1 ):

10.0.0.1

**Tiếp theo ta đặt địa chỉ  
10.0.0.1( kết nối tới server)**

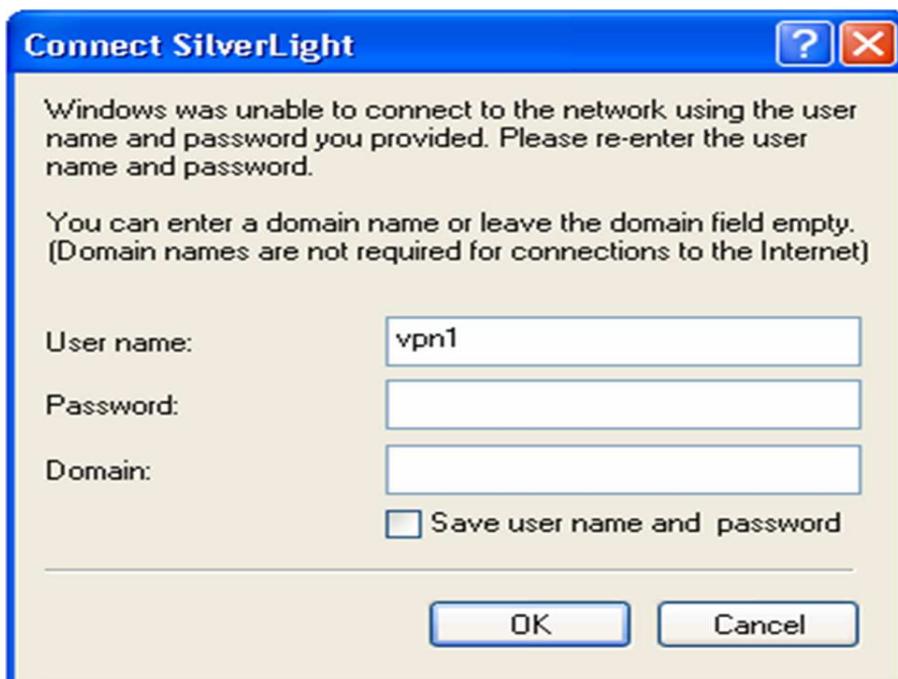
< Back   Next >   Cancel



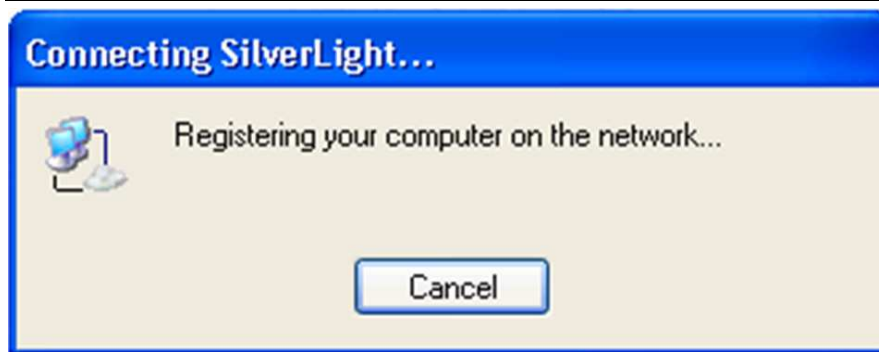
Nhấn **Finish**



Click Connect



User name : **vpn1**  
password : **1**  
→ OK

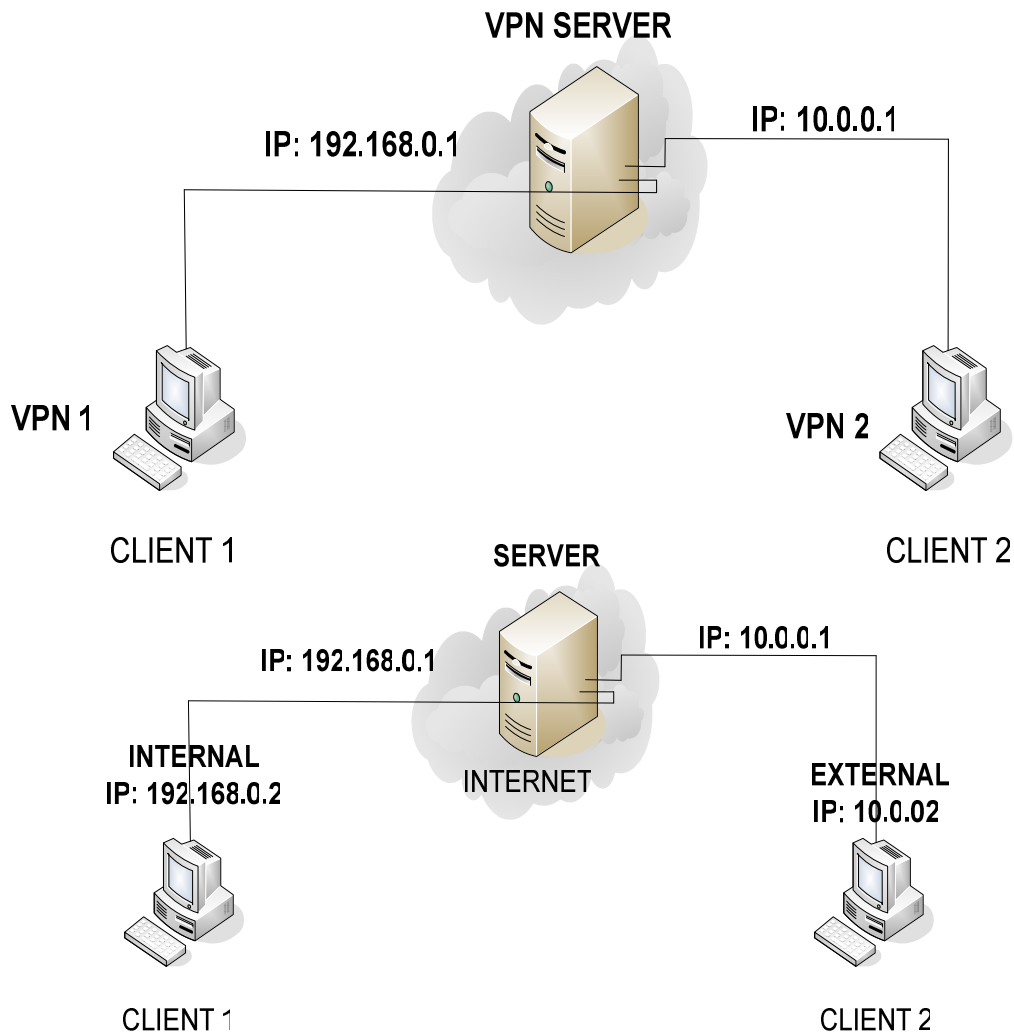


**Đang đăng kí đến vpn1**

---

BÀI 2

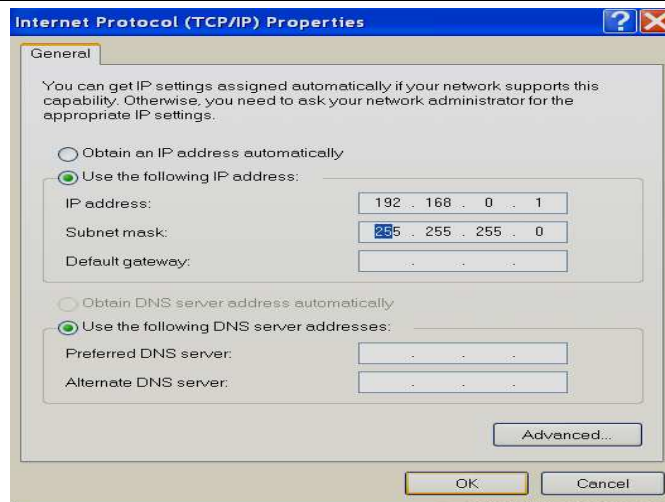
# VPN KẾT HỢP VỚI LAN ROUTING



## 1. Cài đặt và cấu hình trên Server

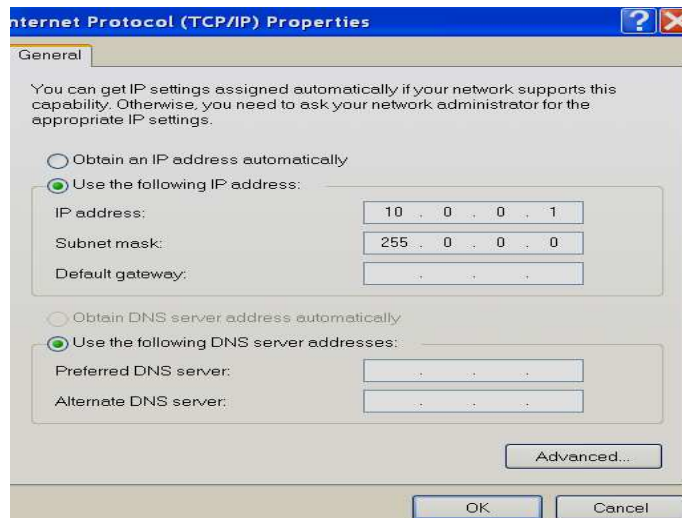
- Cấu hình địa chỉ IP
  - Thực hiện tương tự như cấu hình địa chỉ IP cho máy DC, lần lượt thiết đặt địa chỉ IP cho các card mạng trong và ngoài như sau
    - o Card mạng trong (INTERNAL) :





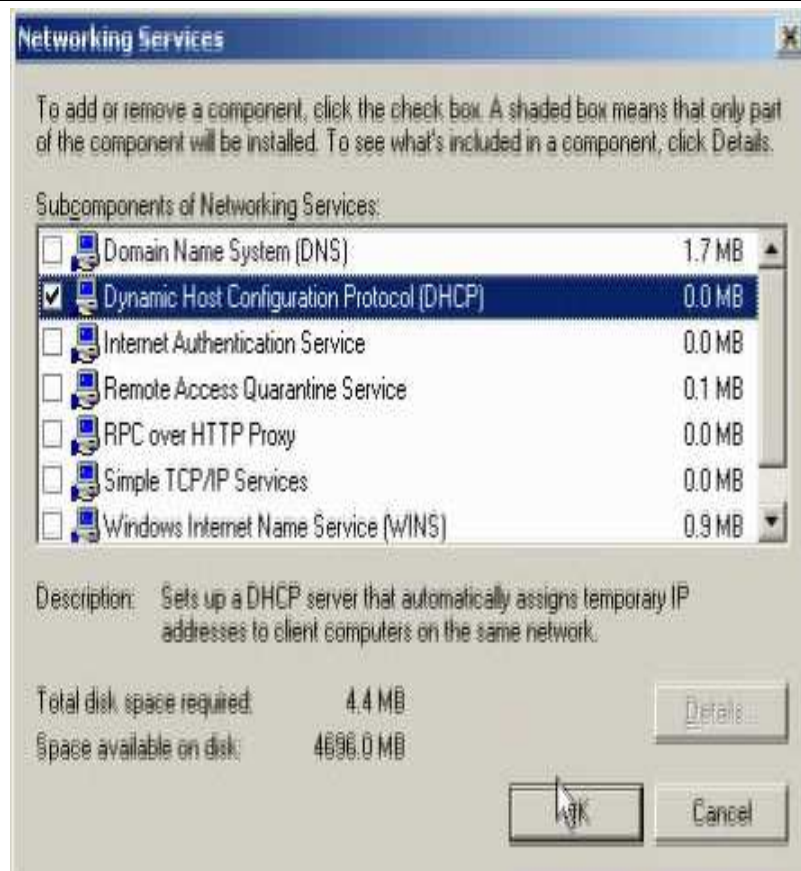
**Hình 1- thiết lập IP cho Card INTERNAL**

o Card mạng ngoài(EXTERNAL)



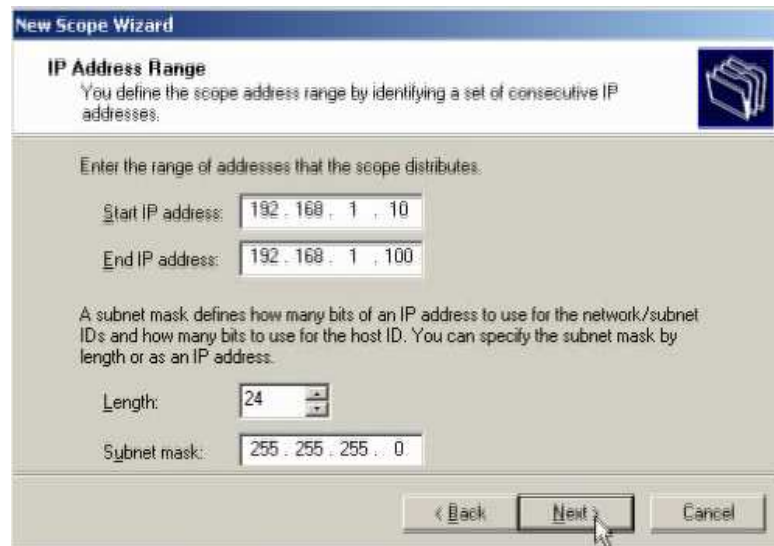
**Thiết lập IP cho EXTERNAL**

- Cài đặt Dynamic Host Configuration Protocol (DHCP)
  - Vào Start→Control Panel→ Add or Remove Programs.
  - Chọn Add/Remove Windows Components.
  - Click chọn Networking Service→Detail.
  - Chọn Dynamic Host Configuration Protocol (DHCP).



Hình 2- Cài đặt DHCP

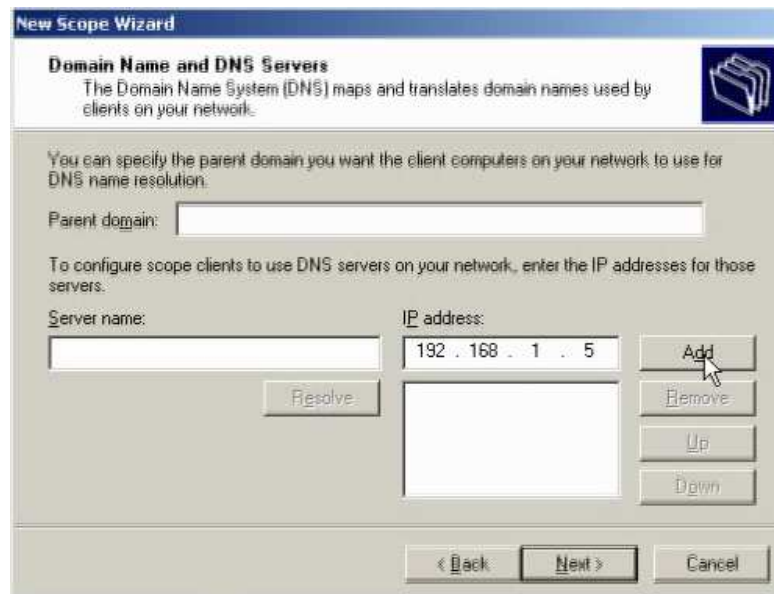
- Click OK→Next→Finish.
- Cấu hình Dynamic Host Configuration Protocol (DHCP)
- Vào Start→Administrative Tools→DHCP
- Tạo Scope cấp phát IP cho mạng trong
- Right-click server[192.168.1.2]→New Scope→Next
- Nhập tên của Scope→Next
- Nhập IP bắt đầu và IP kết thúc của Scop



The screenshot shows the 'New Scope Wizard' window, specifically the 'IP Address Range' step. The title bar reads 'New Scope Wizard'. Below the title, the section is 'IP Address Range' with a subtext: 'You define the scope address range by identifying a set of consecutive IP addresses.' There is a folder icon in the top right. The main area says 'Enter the range of addresses that the scope distributes.' It has two input fields: 'Start IP address:' with the value '192 . 168 . 1 . 10' and 'End IP address:' with the value '192 . 168 . 1 . 100'. Below these, it explains: '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.' There are two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

### IP Scope

- Click Next liên tiếp cho đến khi xuất hiện cửa sổ sau
- Nhập IP của mạng sẽ được cấp IP → Add → Next
- Nhập IP của máy DC → Add → Next



The screenshot shows the 'New Scope Wizard' window, specifically the 'Domain Name and DNS Servers' step. The title bar reads 'New Scope Wizard'. Below the title, the section is 'Domain Name and DNS Servers' with a subtext: 'The Domain Name System (DNS) maps and translates domain names used by clients on your network.' There is a folder icon in the top right. The main area says: 'You can specify the parent domain you want the client computers on your network to use for DNS name resolution.' It has a text box labeled 'Parent domain:'. Below that, it says: 'To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.' There are two input fields: 'Server name:' and 'IP address:'. The 'IP address:' field has the value '192 . 168 . 1 . 5'. To the right of the 'IP address:' field are four buttons: 'Add', 'Remove', 'Up', and 'Down'. A mouse cursor is pointing at the 'Add' button. Below the 'Server name:' and 'IP address:' fields is a 'Resolve' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Click Next → Next → Finish

- Tạo Scope cấp phát IP cho mạng ngoài

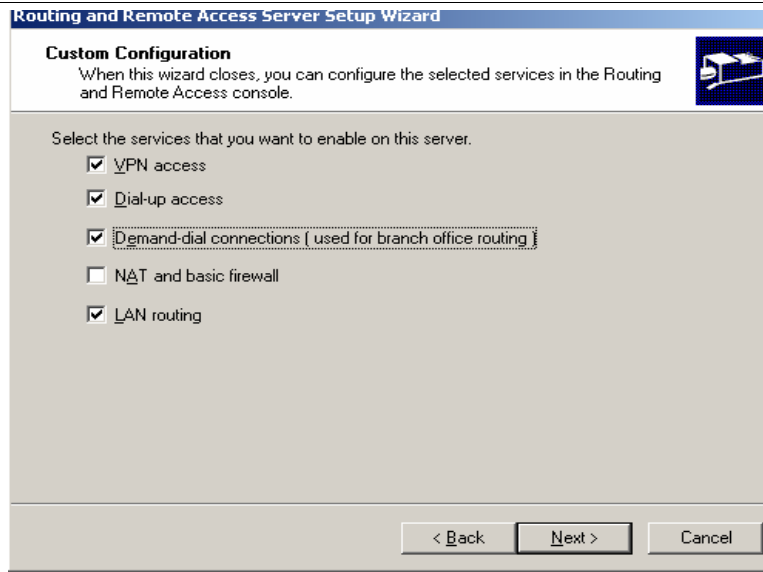
Thực hiện tương tự như tạo Scope cấp phát IP cho mạng trong nhưng chỉ nhập IP bắt đầu và IP kết thúc của Scope, các phần còn lại để trống. Khoảng IP của Scope này là từ 10.0.0.100→10.0.0.200

- Cấu hình RRAS
  - Vào Start→Administrative Tools→Routing and Remote Access
  - Right-click lên biểu tượng có dấu mũi tên đỏ→Configure and Enable Routing and Remote Access→Next
  - Chọn Custom Configuration →Next

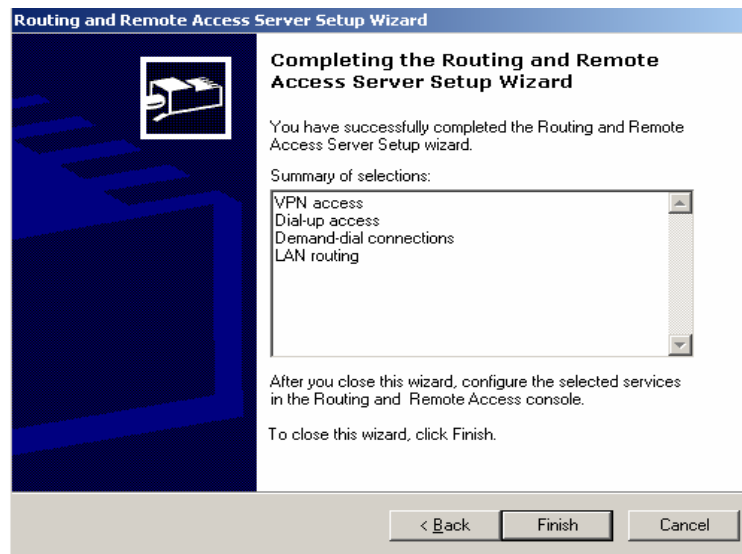


### Chọn loại hình Configuration

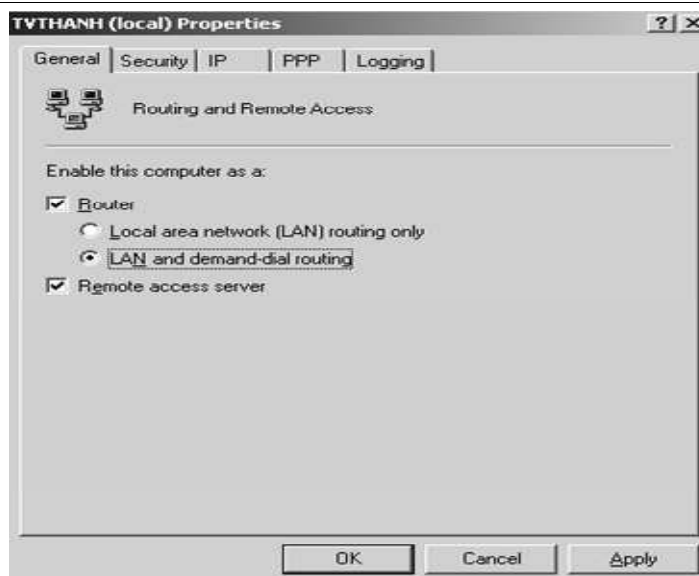
- Tiếp theo đánh tên công ty (tên miền muốn truy cập nếu công ty đó có tên miền) vào ô Company name
- Sau đó là đánh địa chỉ IP của nơi muốn truy cập tới. Nếu là truy cập trong mạng nội bộ thì chúng ta đánh địa chỉ của server ở đây.
- Chọn VPN access ,Dial-up access, LAN routing.



- Hộp thoại thông báo ,chọn finish để khởi động dịch vụ

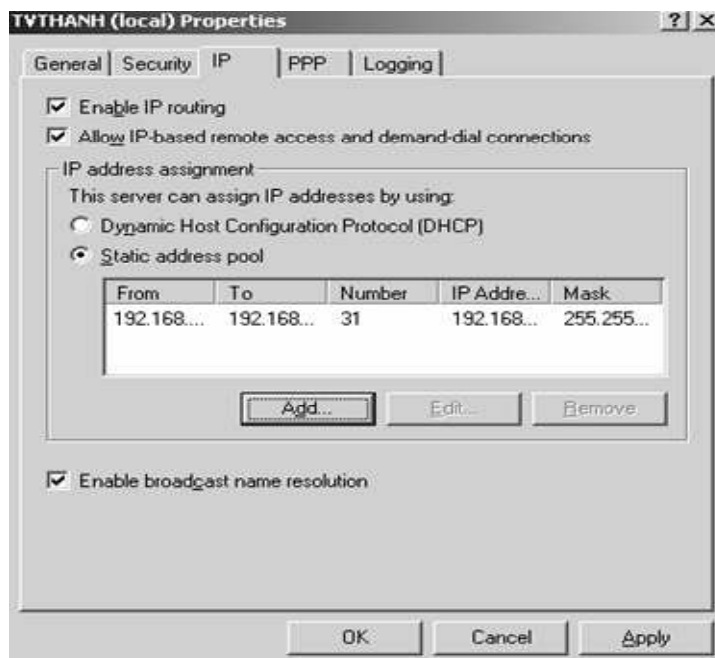


- Sau khi thực hiện xong, bắt đầu cấu hình để Server .
- Nhấn phải chuột lên biểu tượng **Server** và chọn **Properties**. Hộp thoại **Server Properties** xuất hiện. Trong **Tab General**, bạn chọn các mục **Router, LAN and demand-dial routing** và mục **Remote access server**.



### Chọn LAN and demand-dial routing

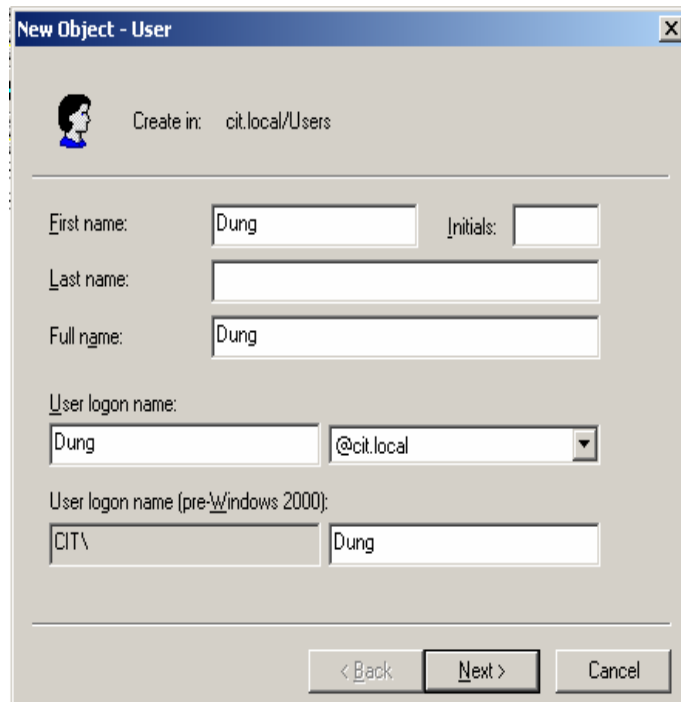
- Sau đó chọn DHCP.
- Sau khi cấu hình xong nhấn OK để đóng hộp thoại



### Bổ sung danh sách địa chỉ

- Sau đó tạo tài khoản và cấp phát quyền cho người dùng truy cập vào





New Object - User

Create in: cit.local/Users

First name: Dung Initials:

Last name:

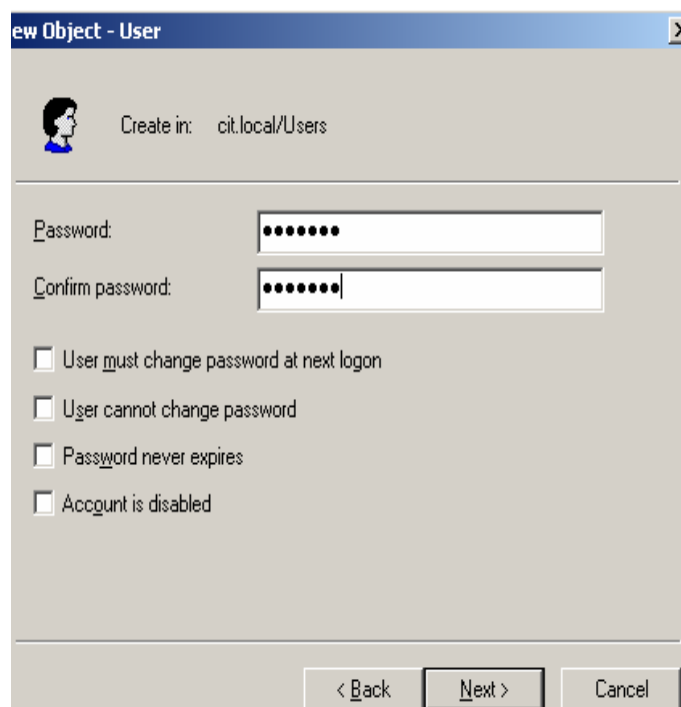
Full name: Dung

User logon name: Dung @cit.local

User logon name (pre-Windows 2000): CIT\ Dung

< Back Next > Cancel

**Hình 3- Tạo tài khoản người dùng**



New Object - User

Create in: cit.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

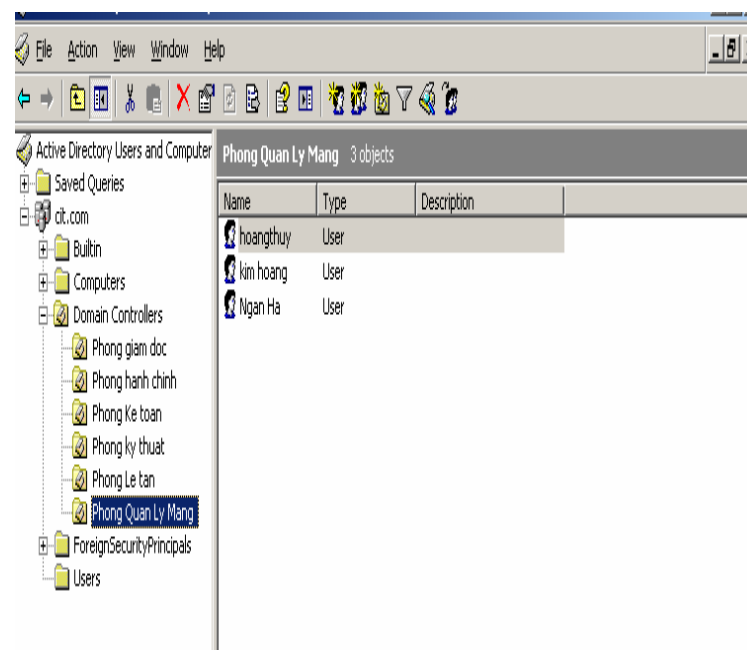
☐ Account is disabled

< Back Next > Cancel

**Tạo Password người dùng**



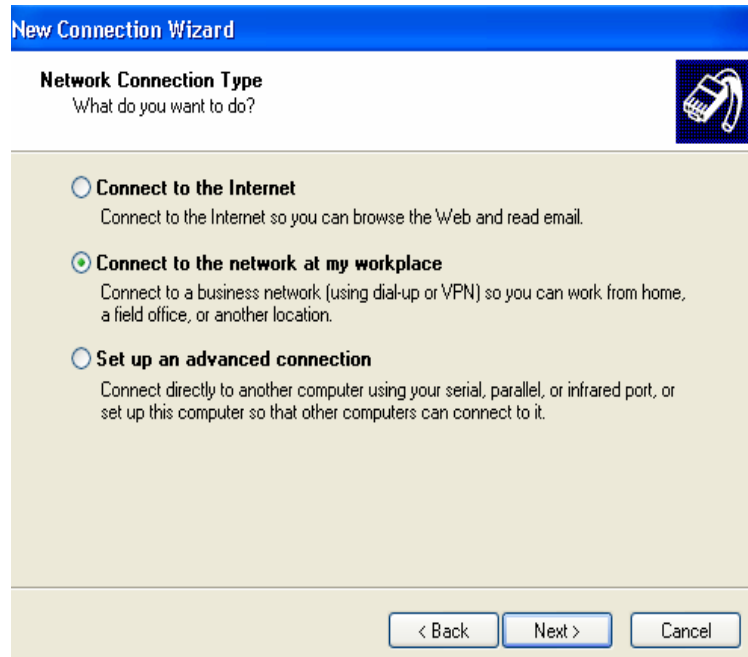
### Cho phép truy cập vào



### Tài khoản người dùng

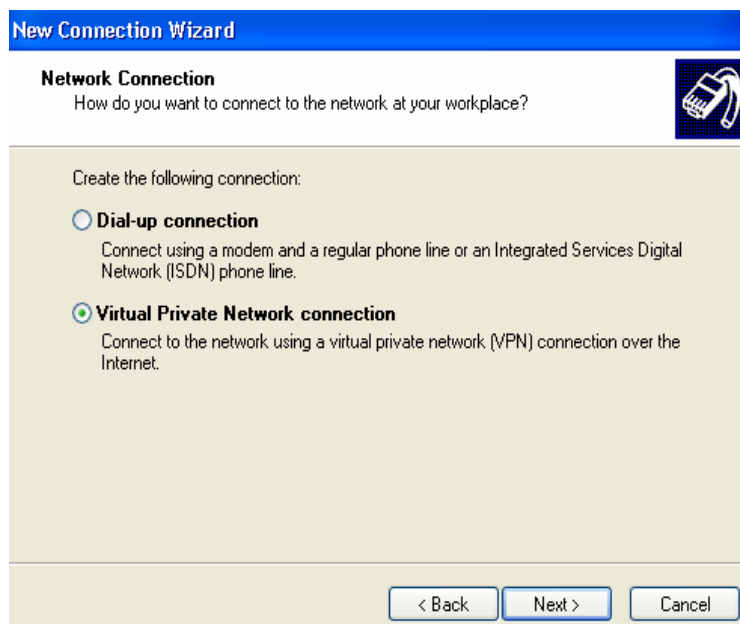
## 2. Cài đặt và cấu hình trên Client

Trên client muốn truy cập tới VPN Server thì cần tạo một kết nối client đến server. Chuột phải vào My Network Places chọn properties, chọn mục Create a new connection, tiếp theo chọn connection to the network at my work place.



### Chọn loại hình mạng kết nối

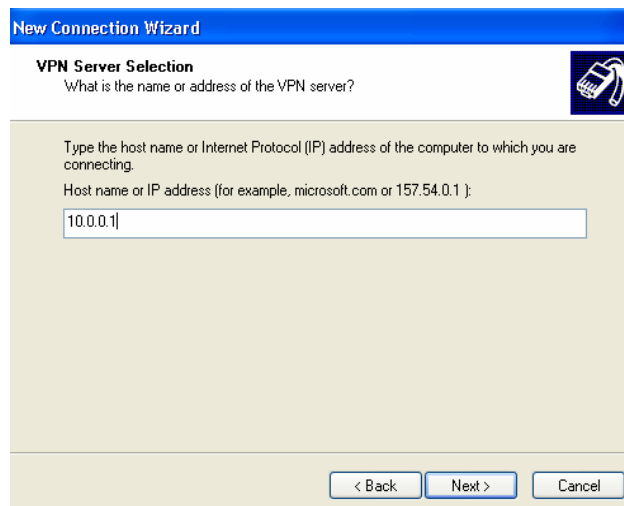
- Next tiếp theo chọn Virtual Private Network connection, Next



### Chọn kiểu kết nối VPN

## Bài thực hành số 13

- Tiếp theo đánh tên công ty (tên miền muốn truy cập nếu công ty đó có tên miền) vào ô Company name
- Sau đó là đánh địa chỉ IP của nơi muốn truy cập tới. Nếu là truy cập trong mạng nội bộ thì chúng ta đánh địa chỉ của server ở đây. Nếu truy cập qua hạ tầng mạng Internet thì chúng ta phải đánh địa chỉ ISP của modem nơi truy cập đến. Nếu chúng ta đăng kí với ISP mà có được địa chỉ IP tĩnh thì chúng ta đánh vào đây, còn nếu sử dụng địa chỉ IP động thì cần dùng đến một số chương trình update IP như dyndns hoặc noIP để biết địa chỉ IP modem hiện tại đang là gì.



### Đánh địa chỉ IP của máy muốn kết nối

- Next đến mục hỏi kết nối cho mọi người hay chỉ một mình user, nếu chúng ta kết nối một mình thì chọn My user only và ấn Next.



### Cửa sổ kết nối

## Bài thực hành số 13

- Tiếp theo một cửa sổ kết nối mở ra cho chúng ta đánh username và password để kết nối đến server. User này nằm trong domain thì phải được cho phép kết nối (Allow Access) trong tab Dial-in trong mục thuộc tính của user này. Khi ấn vào connect nếu kết nối thành công .Sau đó click Accept để đồng ý kết nối đến server VPN.



### Kết nối thành công đến máy chủ

Lúc này chúng ta đã kết nối thành công tới server VPN và mọi thao tác có thể như ngồi trên LAN.