VPN ACCESS

- What is a VPN?
- Supported Authentication Protocols
- Choosing a VPN Protocol
- Installing the Remote Access Service
- Configuring the Remote Access Service

What is a VPN?

- VPN stands for Virtual Private Network.
- VPNs allow users to securely connect to the local network from a remote computer.
- The remote computer virtually becomes part of the local network.

Supported Authentication Protocols

- **Unauthenticated – BAD IDEA**
- **PAP – Password Authentication Protocol (Low Security)**
- **CHAP – Challenge Handshake Authentication Protocol (Medium Security)** Non-Microsoft Systems)
- **MS-CHAPv2 – Microsoft Challenge Handshake Authentication Protocol (High Security)**
- **EAP-TLS – Extensible Authentication Protocol Transport Level Security (Highest Security)**

Multi-factor Username,smartcard, biometrics

Choosing a VPN Protocol

- **PPTP – Point to Point Tunneling Protocol**
  - **Uses MPPE encryption**
  - **Primarily used with pre-Windows 2000 clients**
- **L2TP – Layer Two Tunneling Protocol**
  - **Uses IPsec encryption**
  - **First supported in Windows 2000**
- **SSTP – Secure Socket Tunneling Protocol**
  - **Uses the SSL channel of HTTPS for encryption**
  - **New to Windows Server 2008**
  - **Primarily used when PPTP/L2TP are blocked at the firewall**

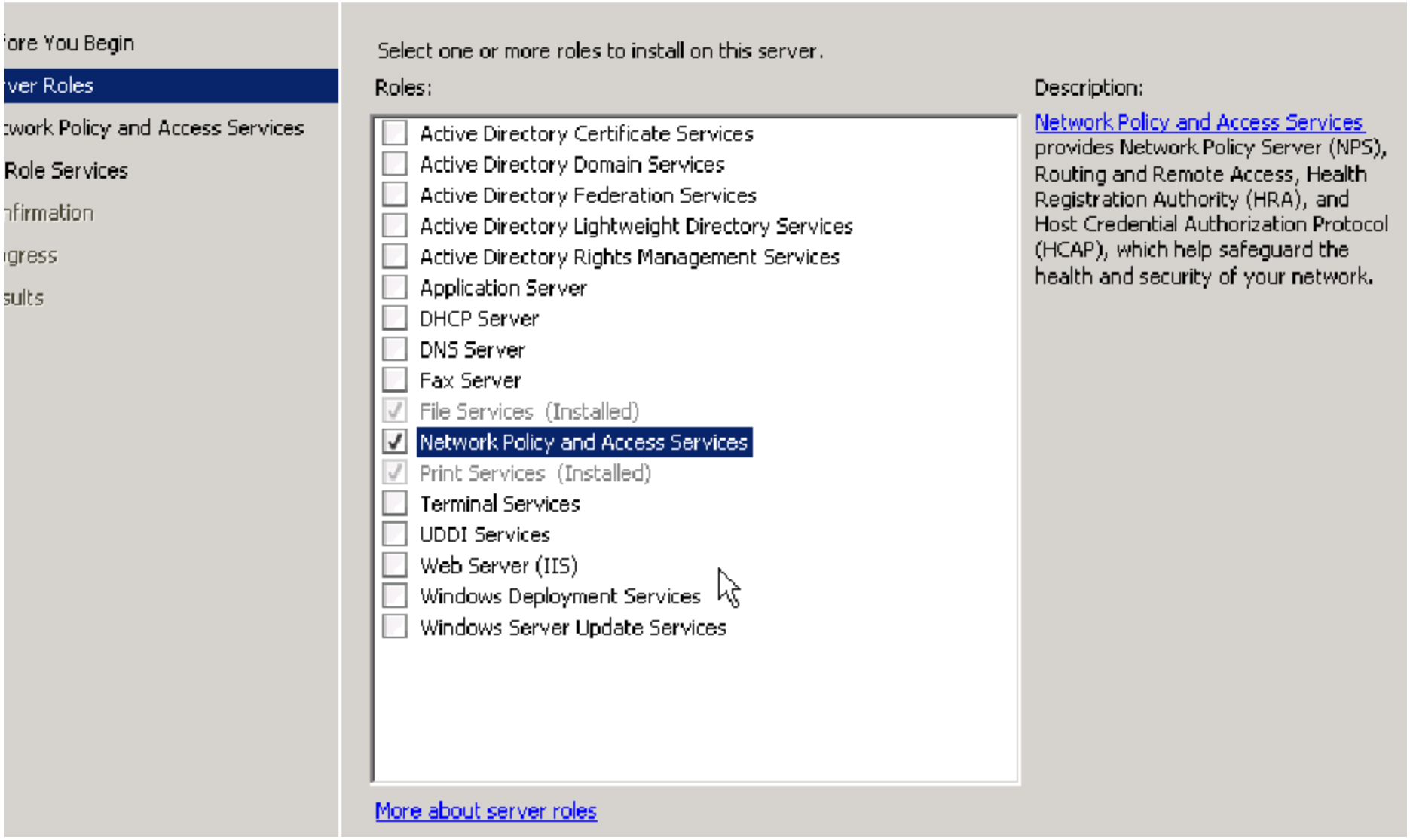
Point-point protocol –original protocol

Must have a certificate assigned to Server if
You will be using sstp for your vpn protocol

- Install the Remote Access Service.
- Configure the Remote Access Service to support VPN connectivity.
- Create a VPN connection from a client.

One card connected to the internal
Network to allow the user to connect
To that network

One card connected to the internet
Where the remote users are going
To connect in


ore You Begin
ver Roles
work Policy and Access Services
Role Services
nfirmation
gress
sults
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services (Installed)
Network Policy and Access Services
Print Services (Installed)
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
More about server roles

Select Role Services

Needed for VPN access

- Before You Begin
- Server Roles
- Network Policy and Access Services
- **Role Services**
- Confirmation
- Progress
- Results

Select the role services to install for Network Policy and Access Services:

Role services:

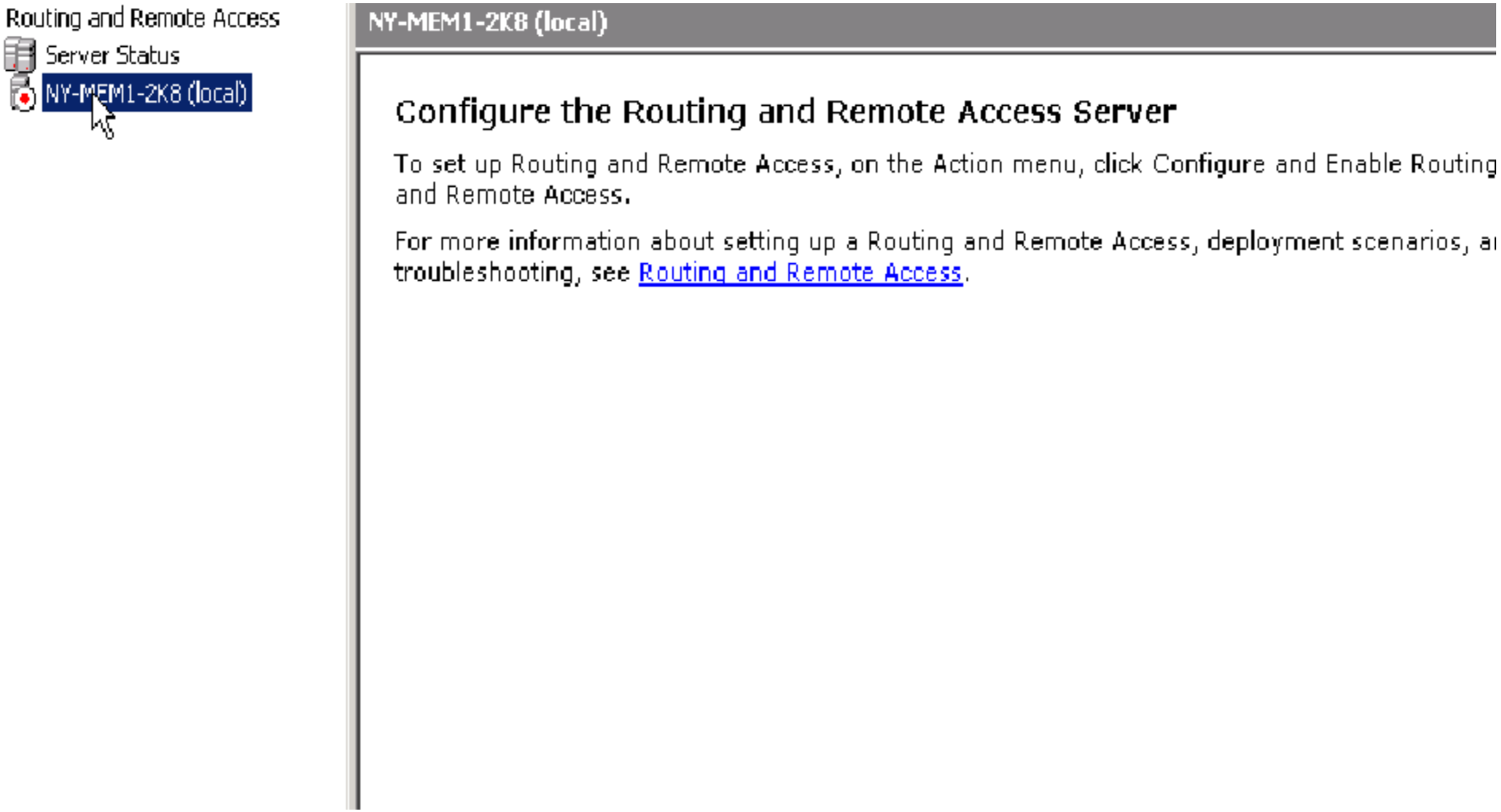
- [ ] Network Policy Server
- [-] [ ] Routing and Remote Access Services
  - [x] Remote Access Service
  - Routing
- [ ] Health Registration Authority
- [ ] Host Credential Authorization Protocol

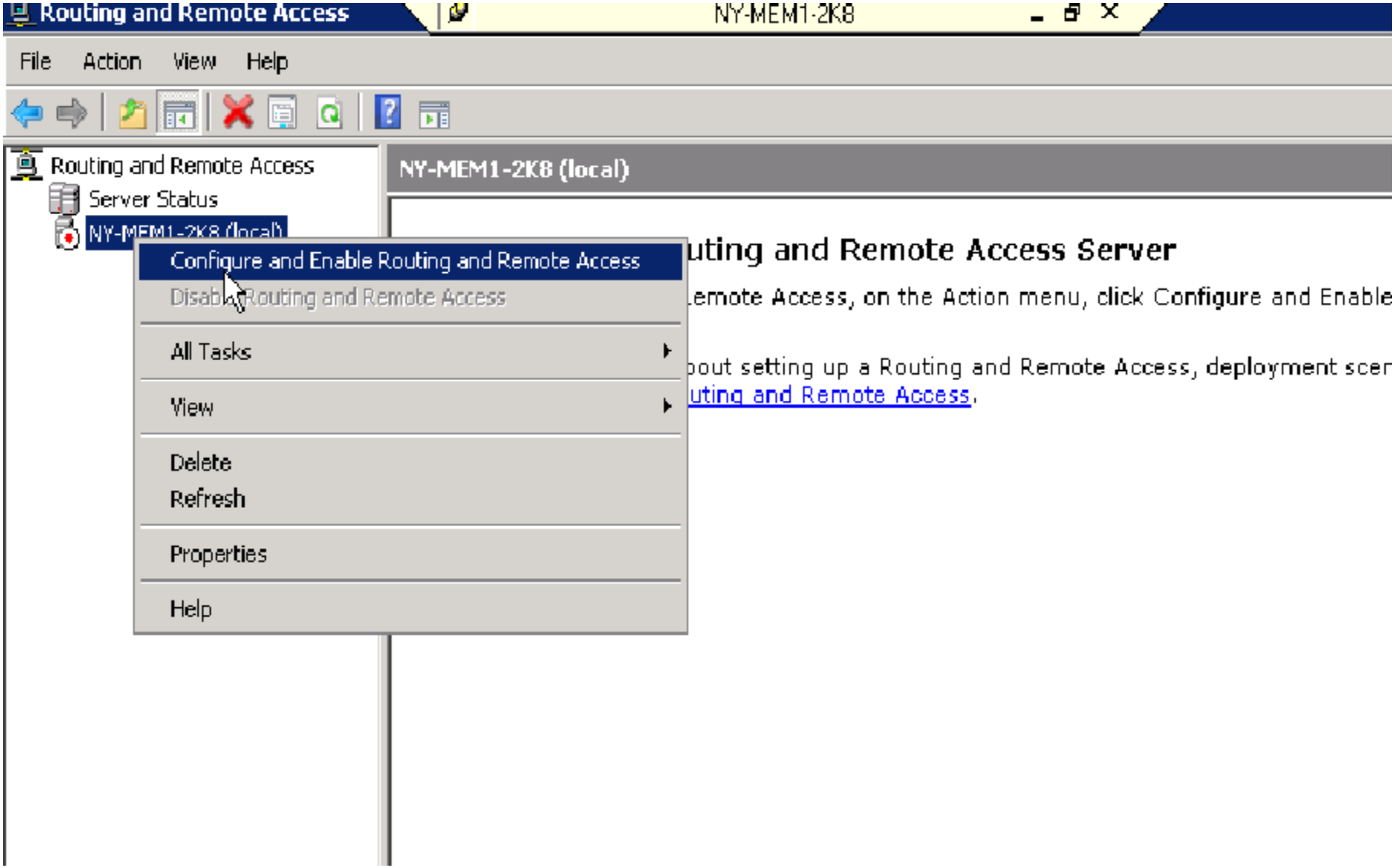
Description:

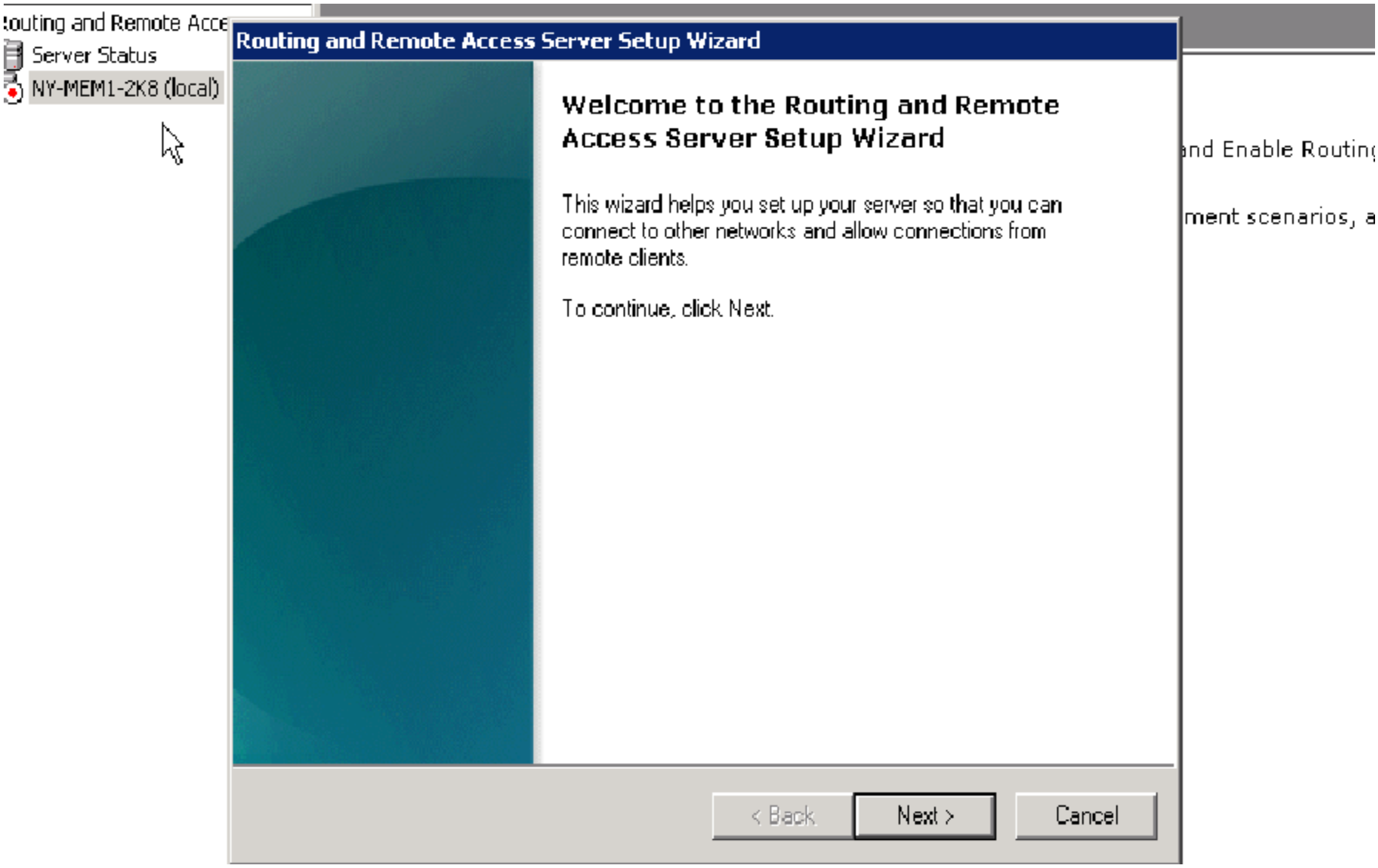
Remote Access Service enables remote offices or mobile workers access private office networks th VPN or dial-up connections.

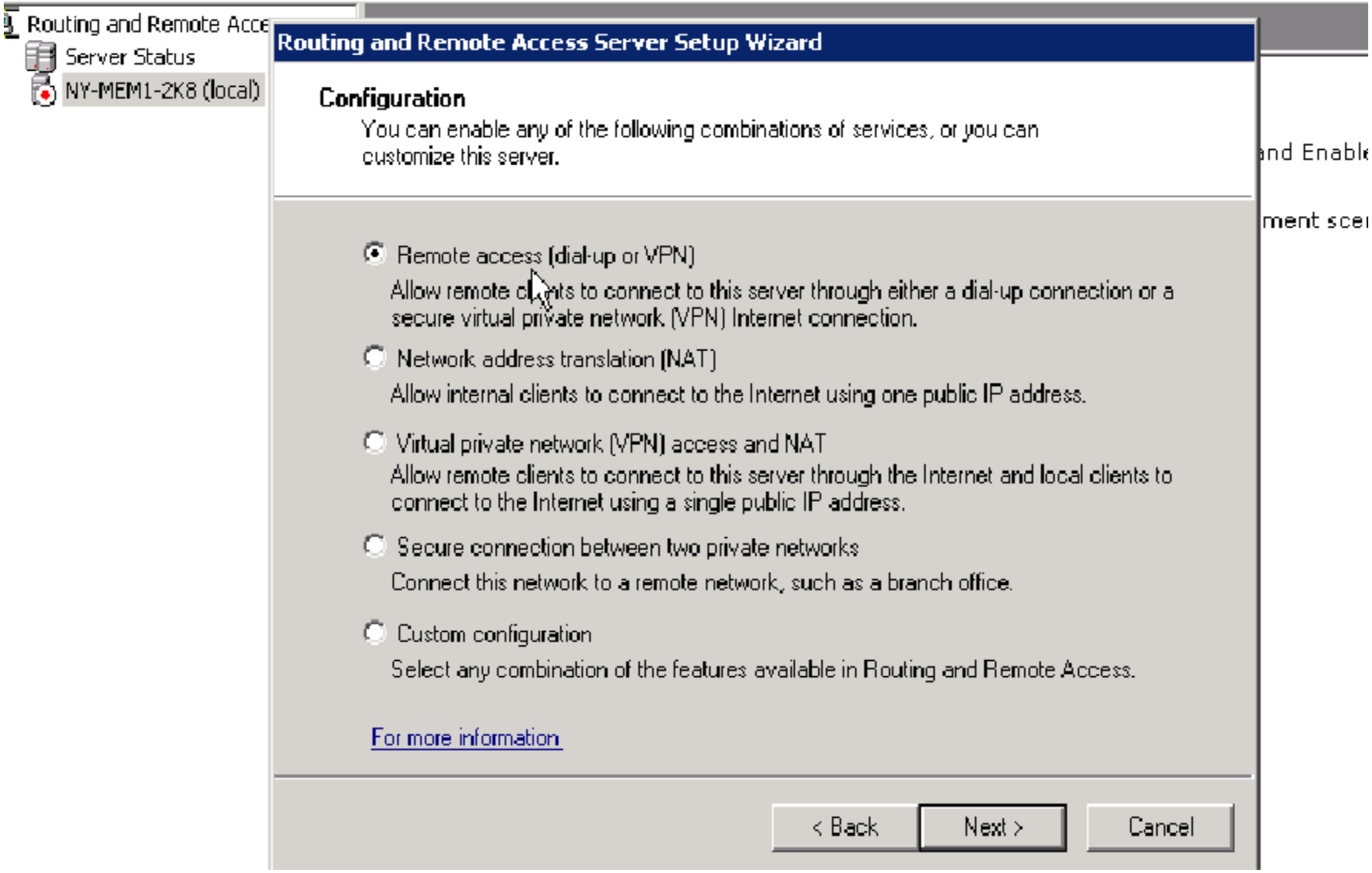
INSTALL

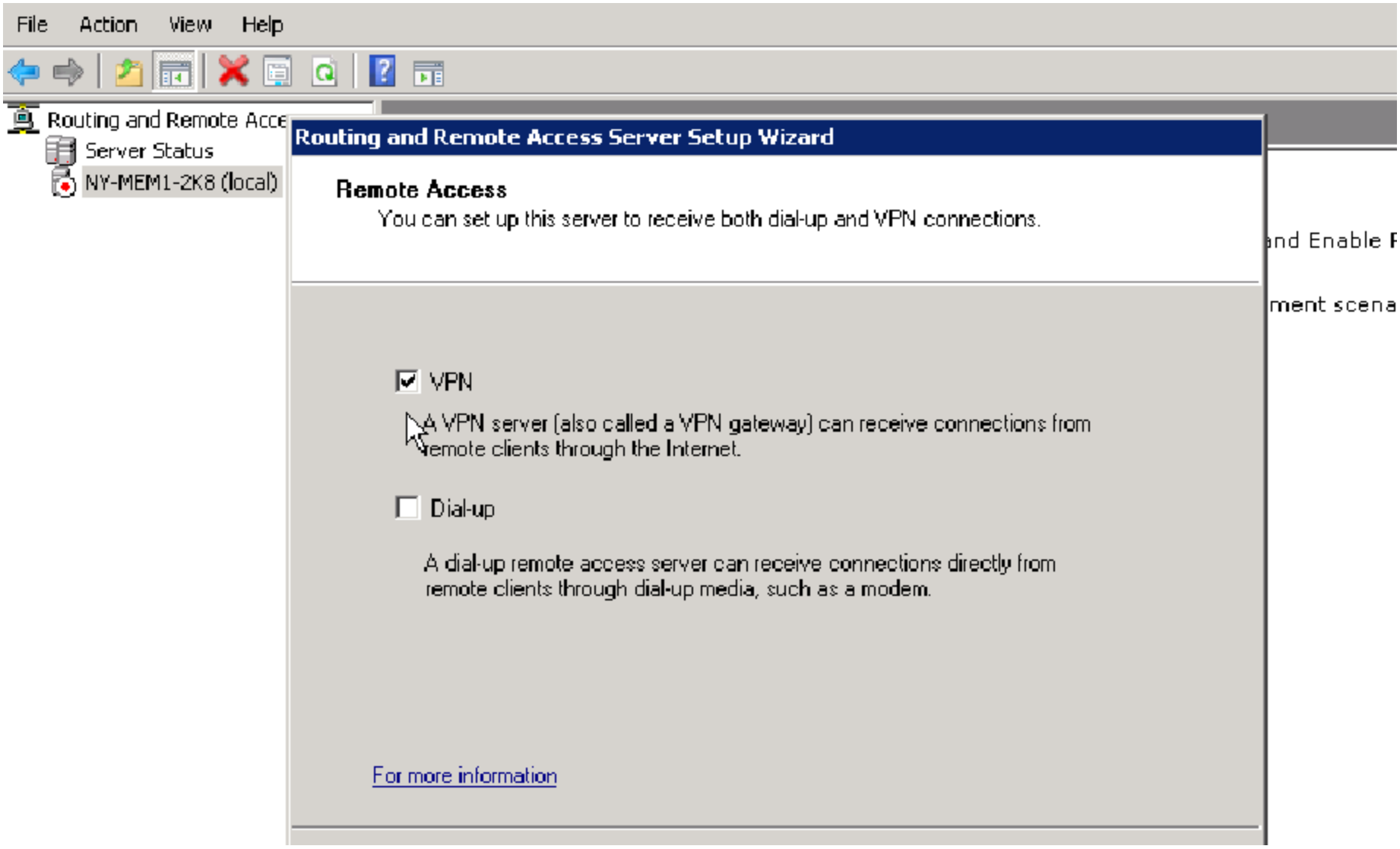
From Ad Tools select Routing and Remote Access

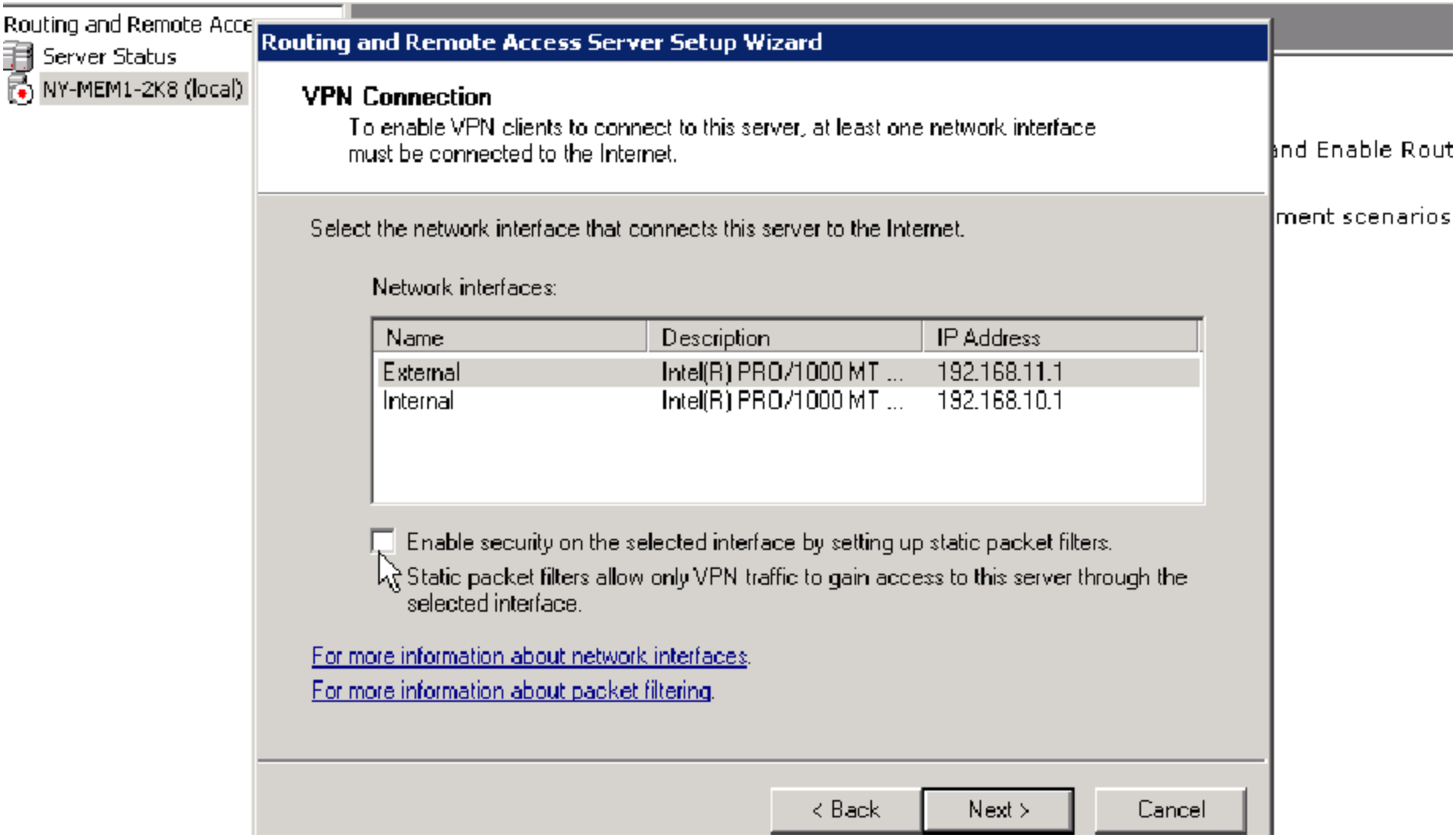


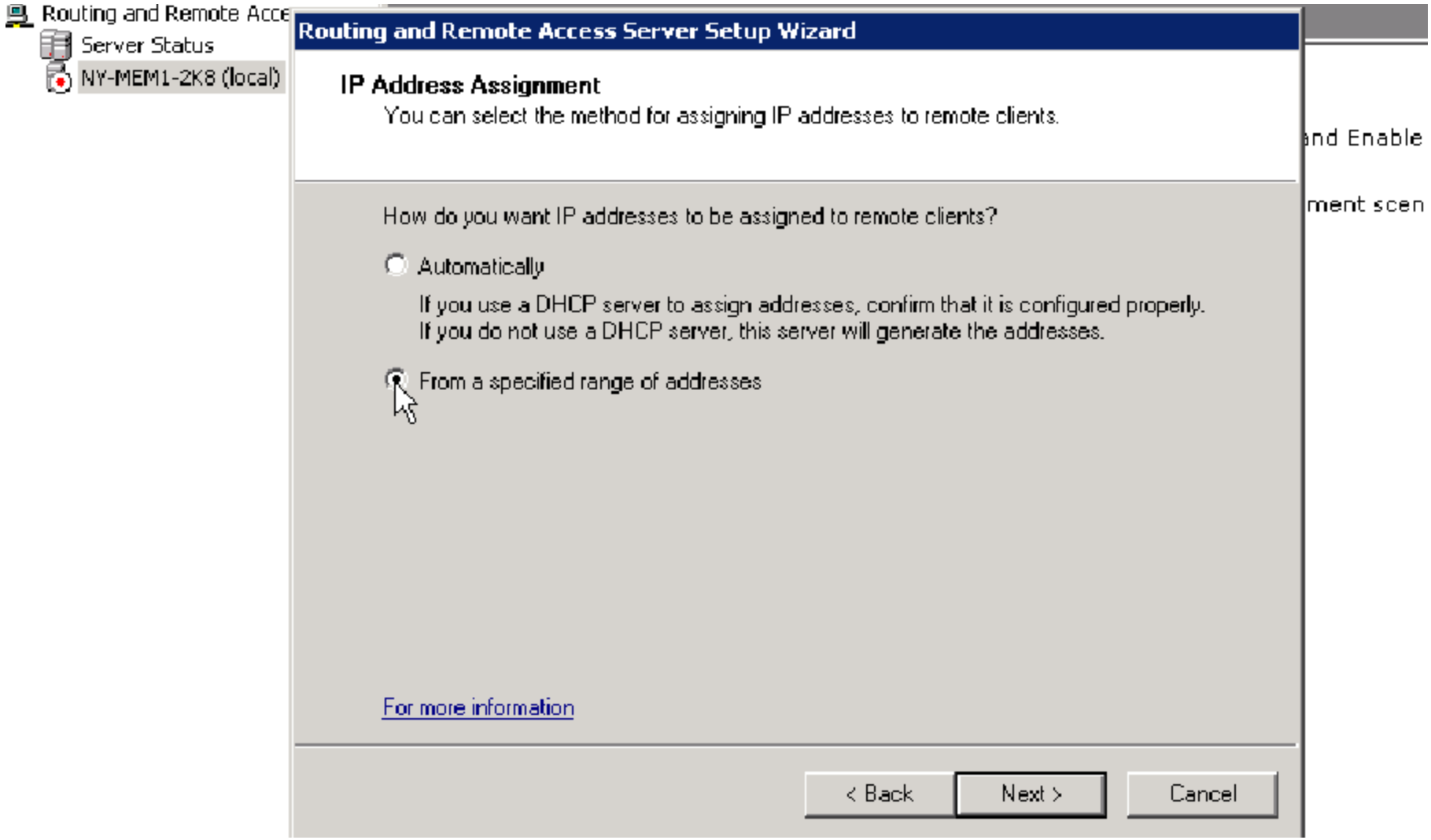

Routing and Remote Access
NY-MEM1-2K8
File
Action
View
Help
Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
NY-MEM1-2K8 (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
uting and Remote Access Server
emote Access, on the Action menu, click Configure and Enable
out setting up a Routing and Remote Access, deployment scer
uting and Remote Access.

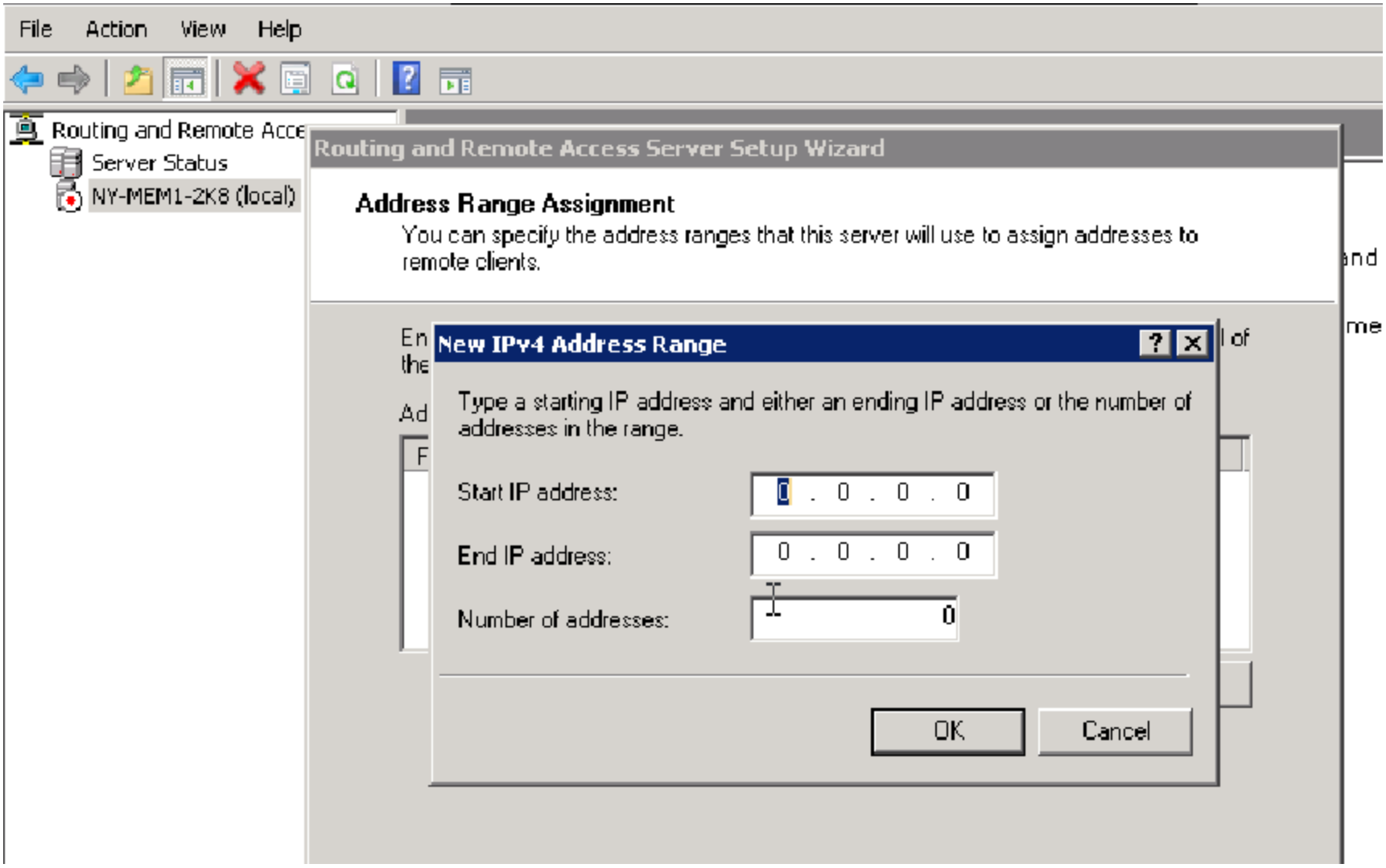

outing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel
nd Enable Routing
ment scenarios, a

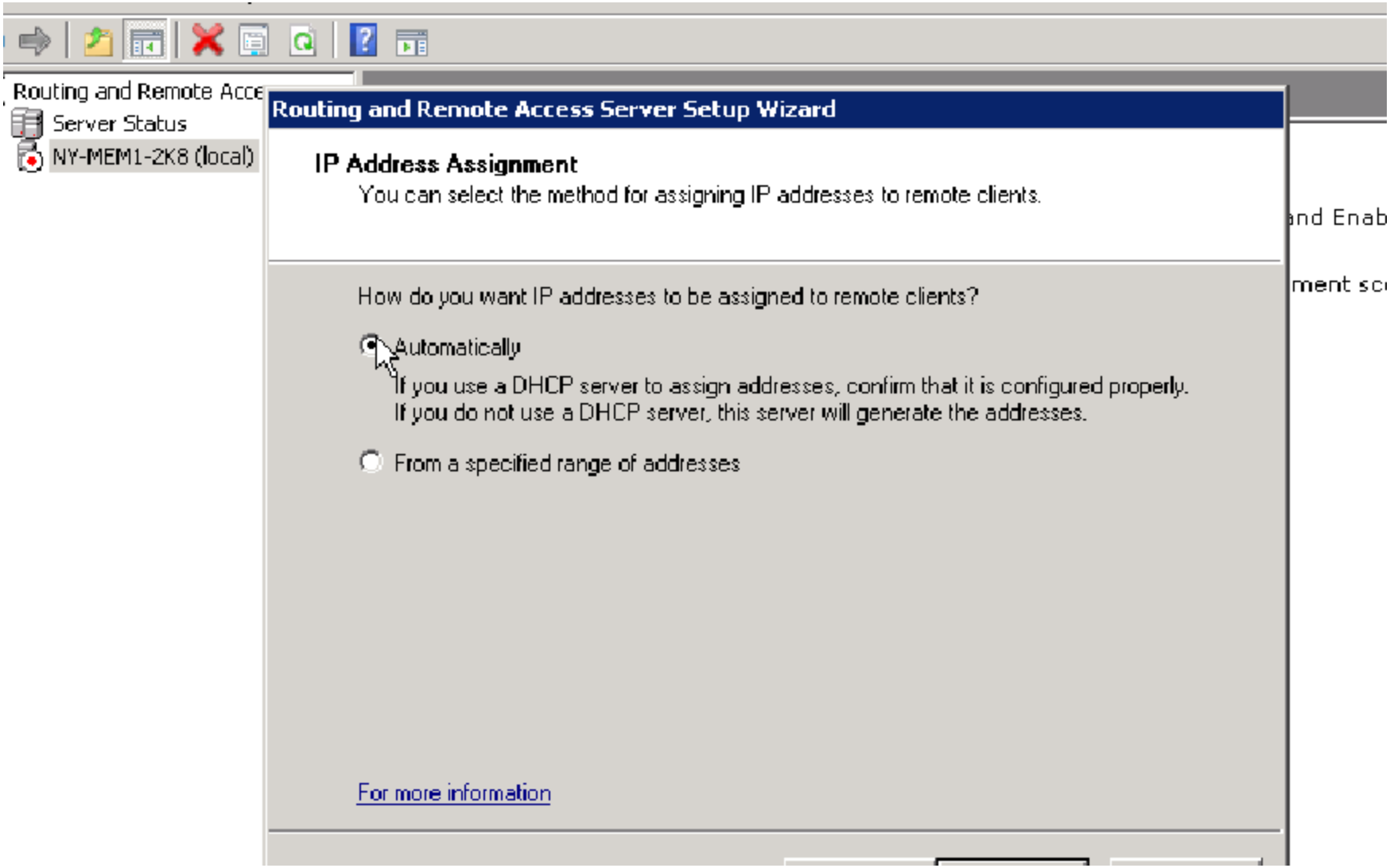

Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
For more information
< Back
Next >
Cancel


File Action View Help
Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
Remote Access
You can set up this server to receive both dial-up and VPN connections.
VPN
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.
Dial-up
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.
For more information

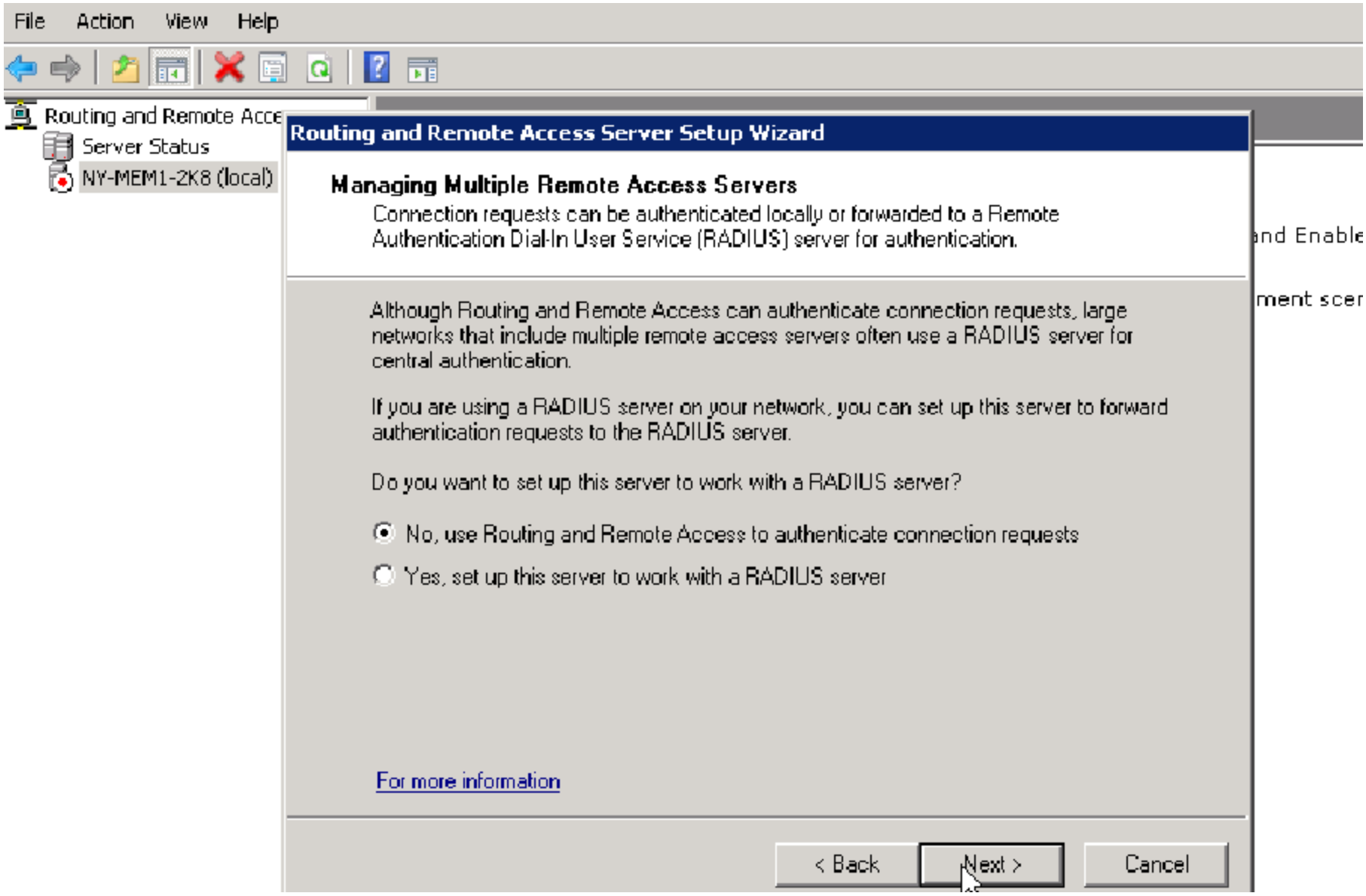

Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
VPN Connection
To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.
Select the network interface that connects this server to the Internet.
Network interfaces:
Name
Description
IP Address
External
Intel(R) PRO/1000 MT ...
192.168.11.1
Internal
Intel(R) PRO/1000 MT ...
192.168.10.1
Enable security on the selected interface by setting up static packet filters.
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.
For more information about network interfaces.
For more information about packet filtering.
< Back
Next >
Cancel

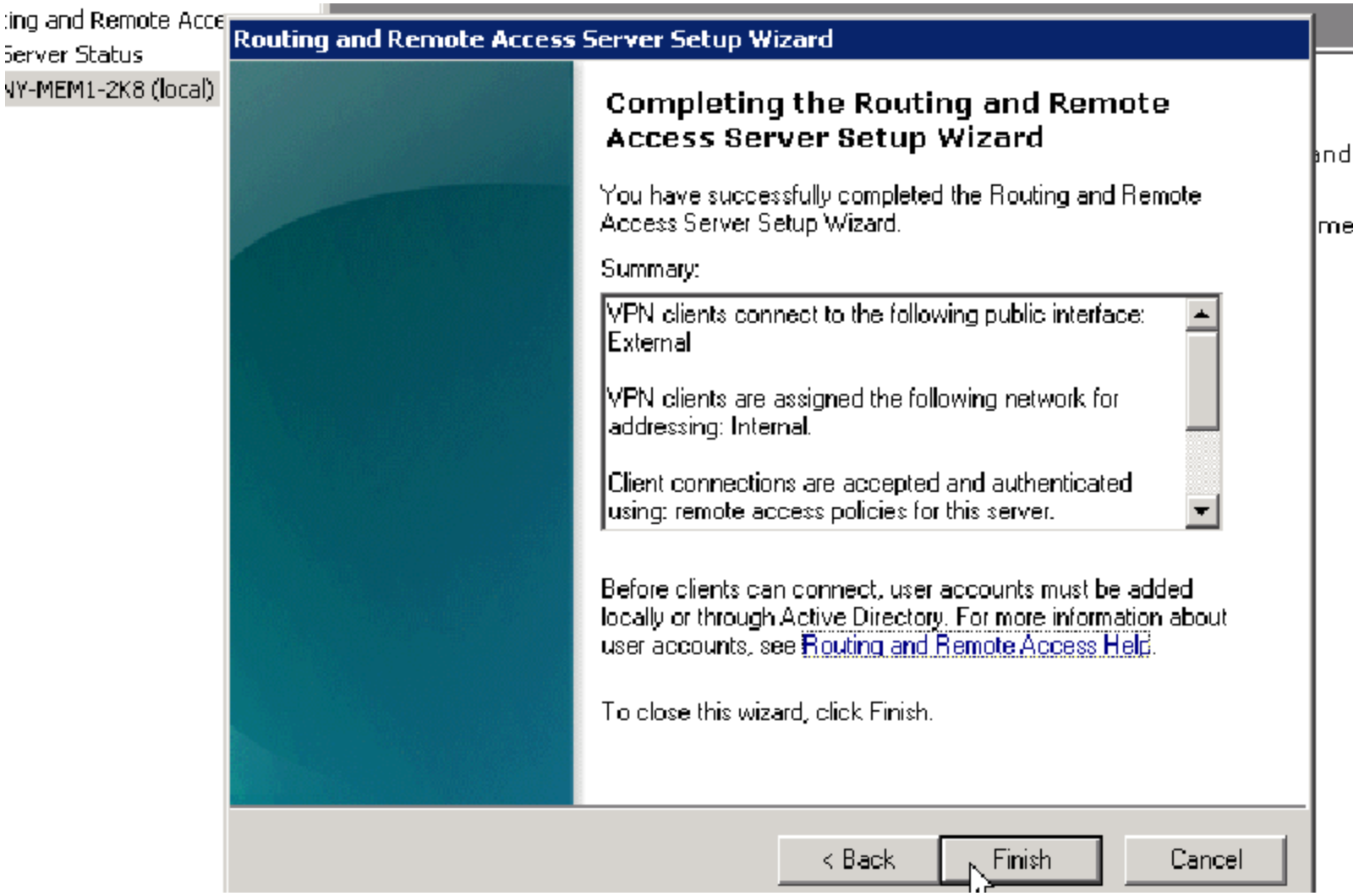

Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
IP Address Assignment
You can select the method for assigning IP addresses to remote clients.
How do you want IP addresses to be assigned to remote clients?
Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.
From a specified range of addresses
For more information
< Back
Next >
Cancel

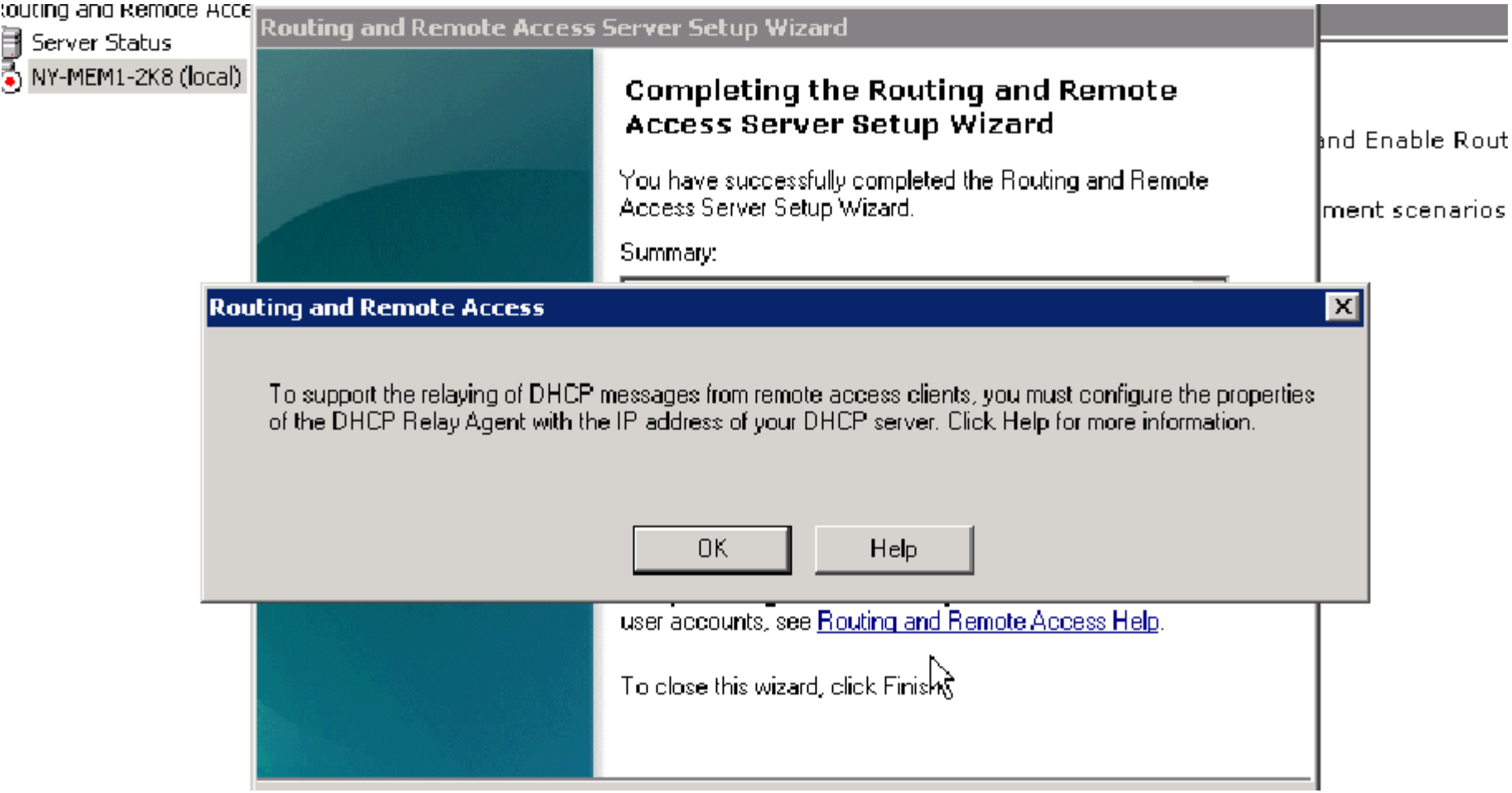

File
Action
View
Help
Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.
New IPv4 Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
0 . 0 . 0 . 0
End IP address:
0 . 0 . 0 . 0
Number of addresses:
0
OK
Cancel


Routing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
IP Address Assignment
You can select the method for assigning IP addresses to remote clients.
How do you want IP addresses to be assigned to remote clients?
Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.
From a specified range of addresses
For more information

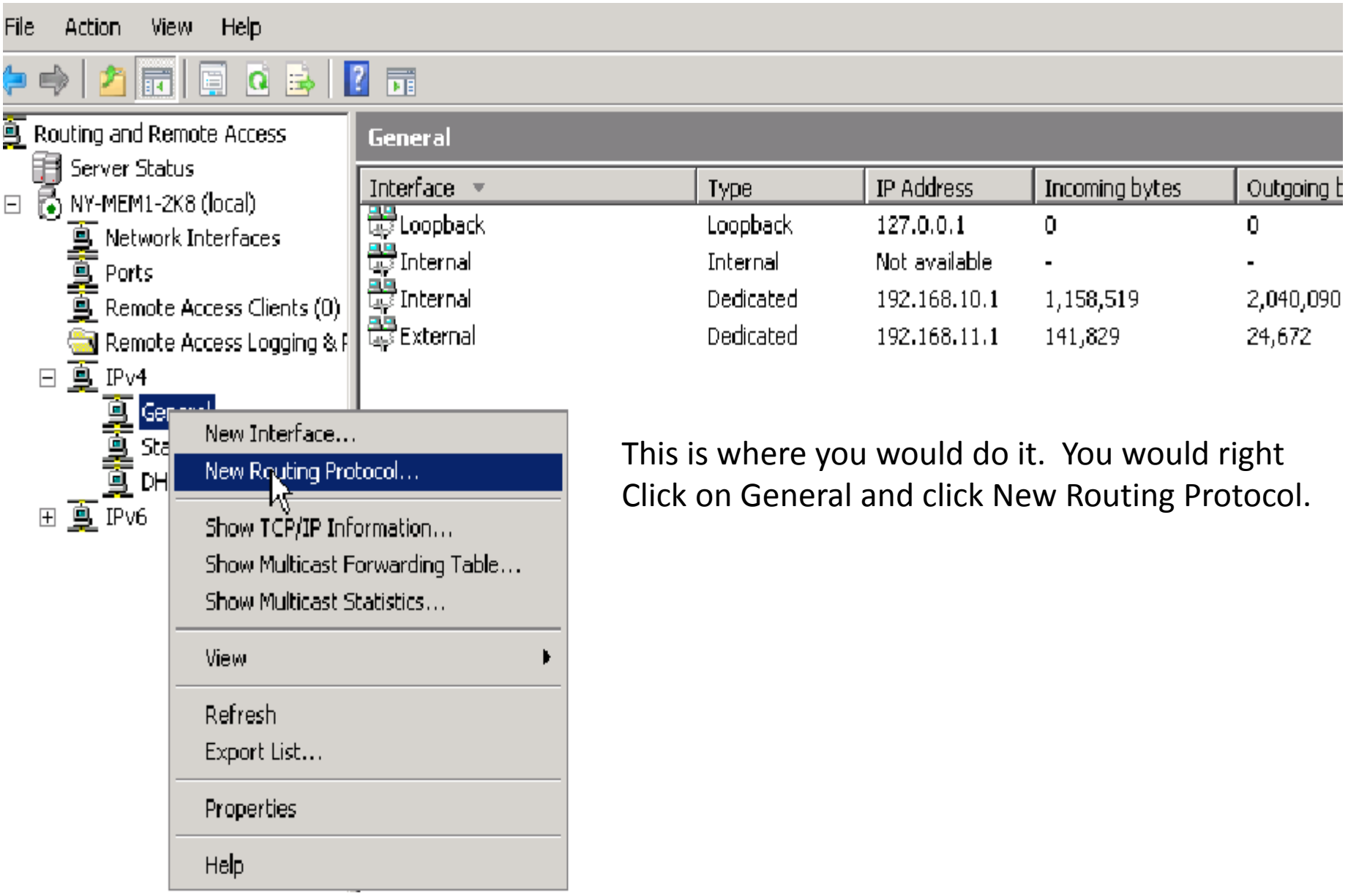
Known as a NPS server



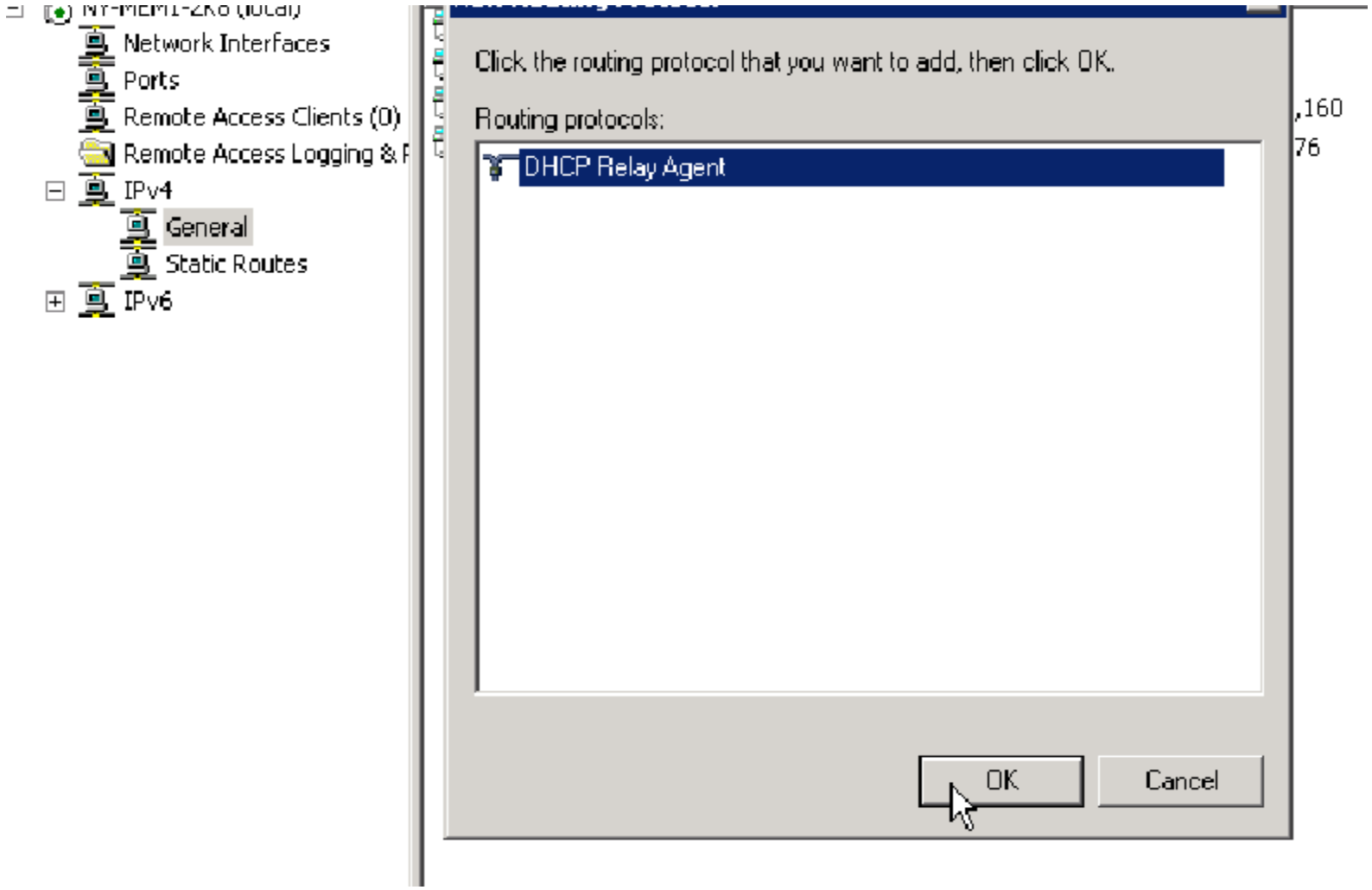

ing and Remote Acce
Server Status
NY-MEM1-2K8 (local)
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup Wizard.
Summary:
VPN clients connect to the following public interface: External
VPN clients are assigned the following network for addressing: Internal.
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

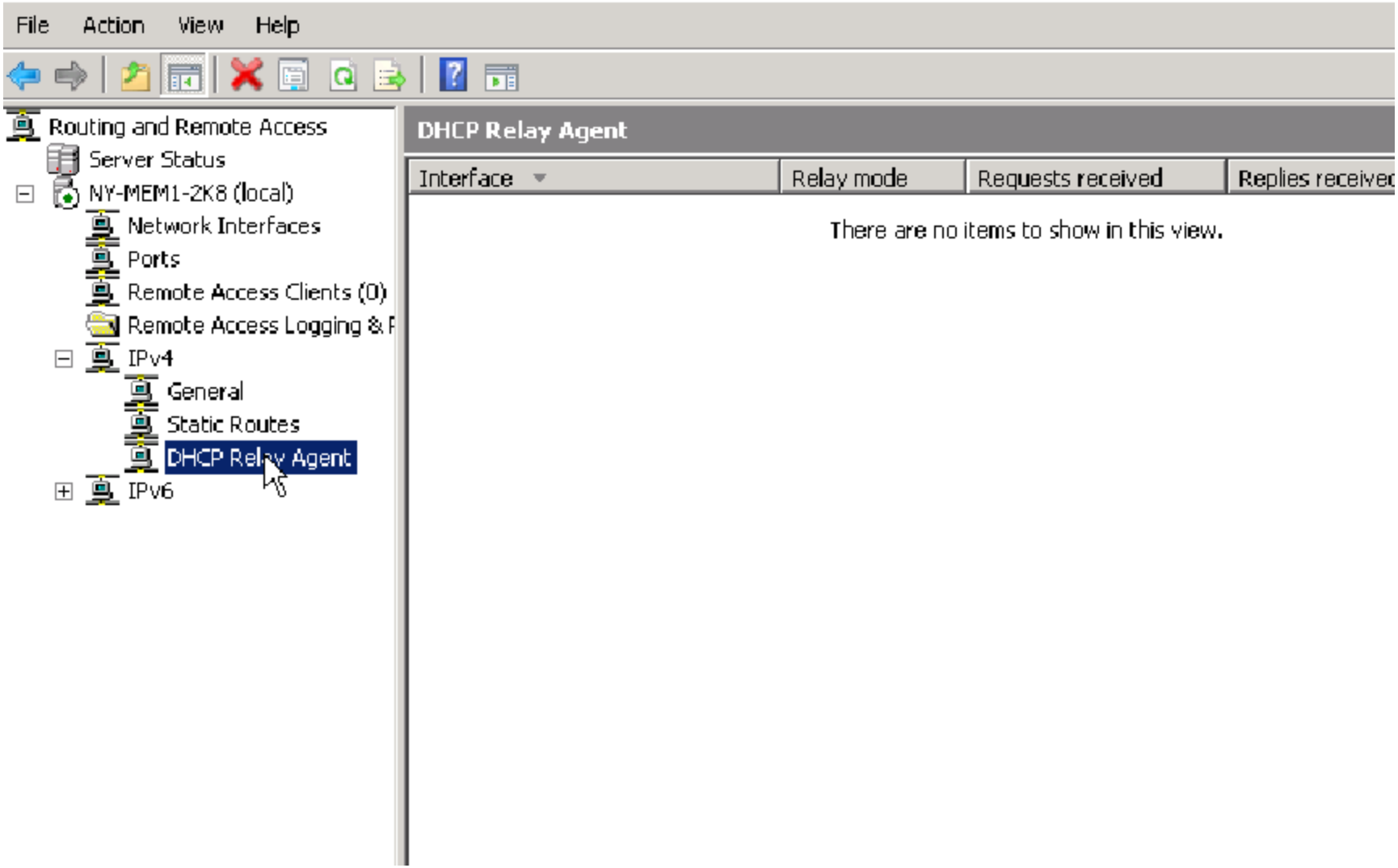


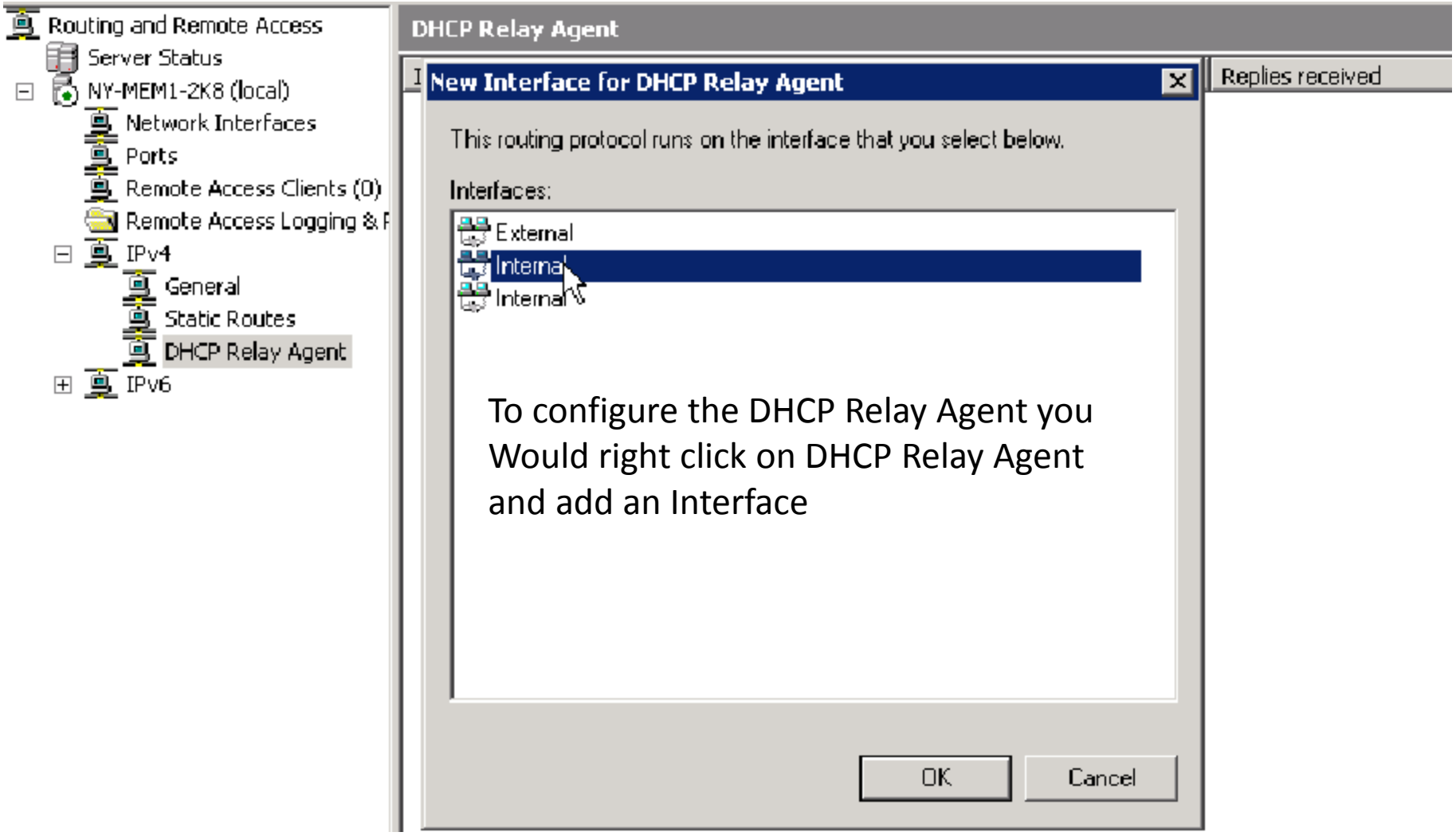
When a client connects to the remote access server it will not get additional options like default gateway, Dns etc. What it does is takes the information that the Remote Access Server has been assigned. So if you want custom DHCP options for your Remote Access Clients, then you are going to have to install the remote access relay agent on this remote Access server

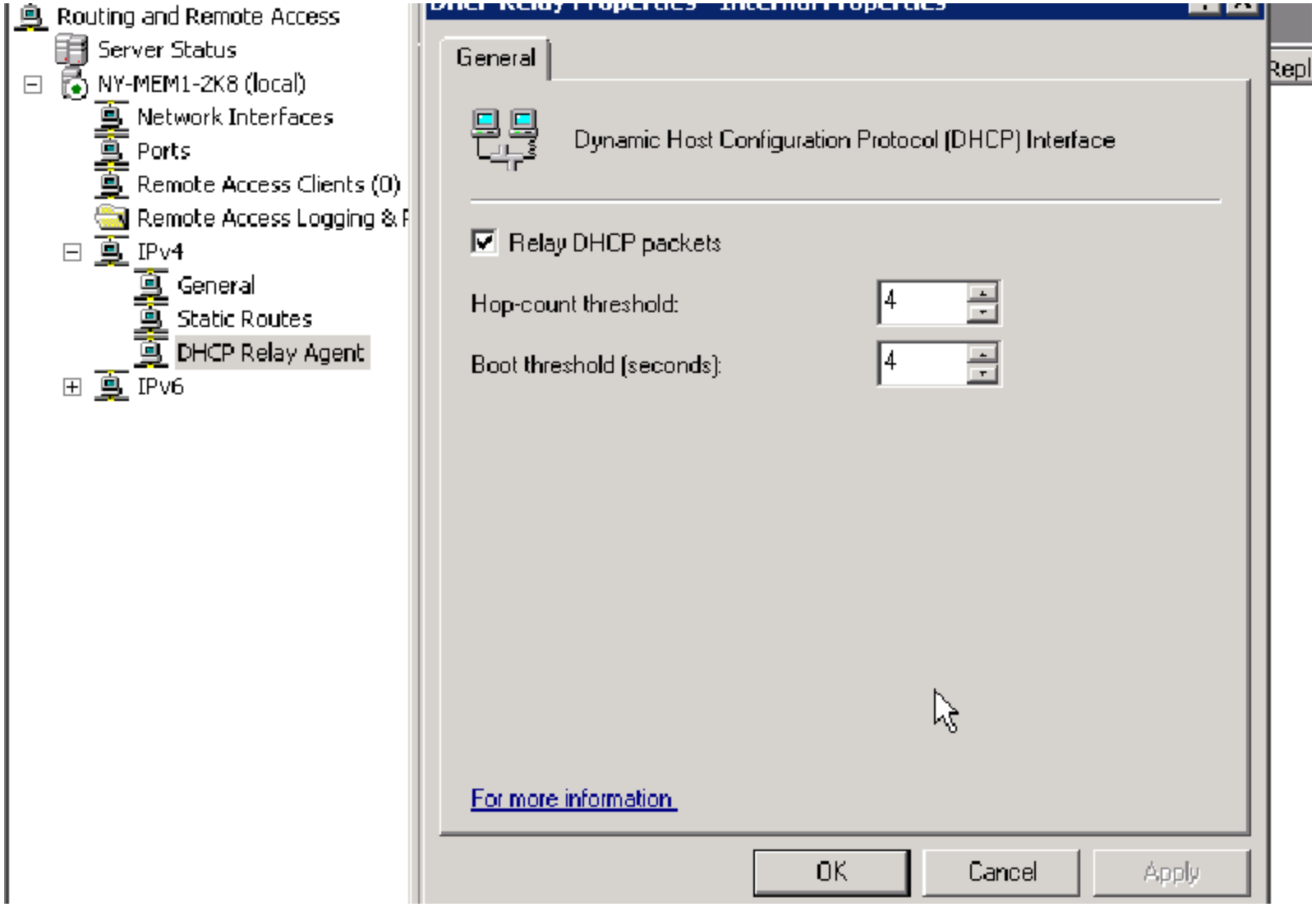


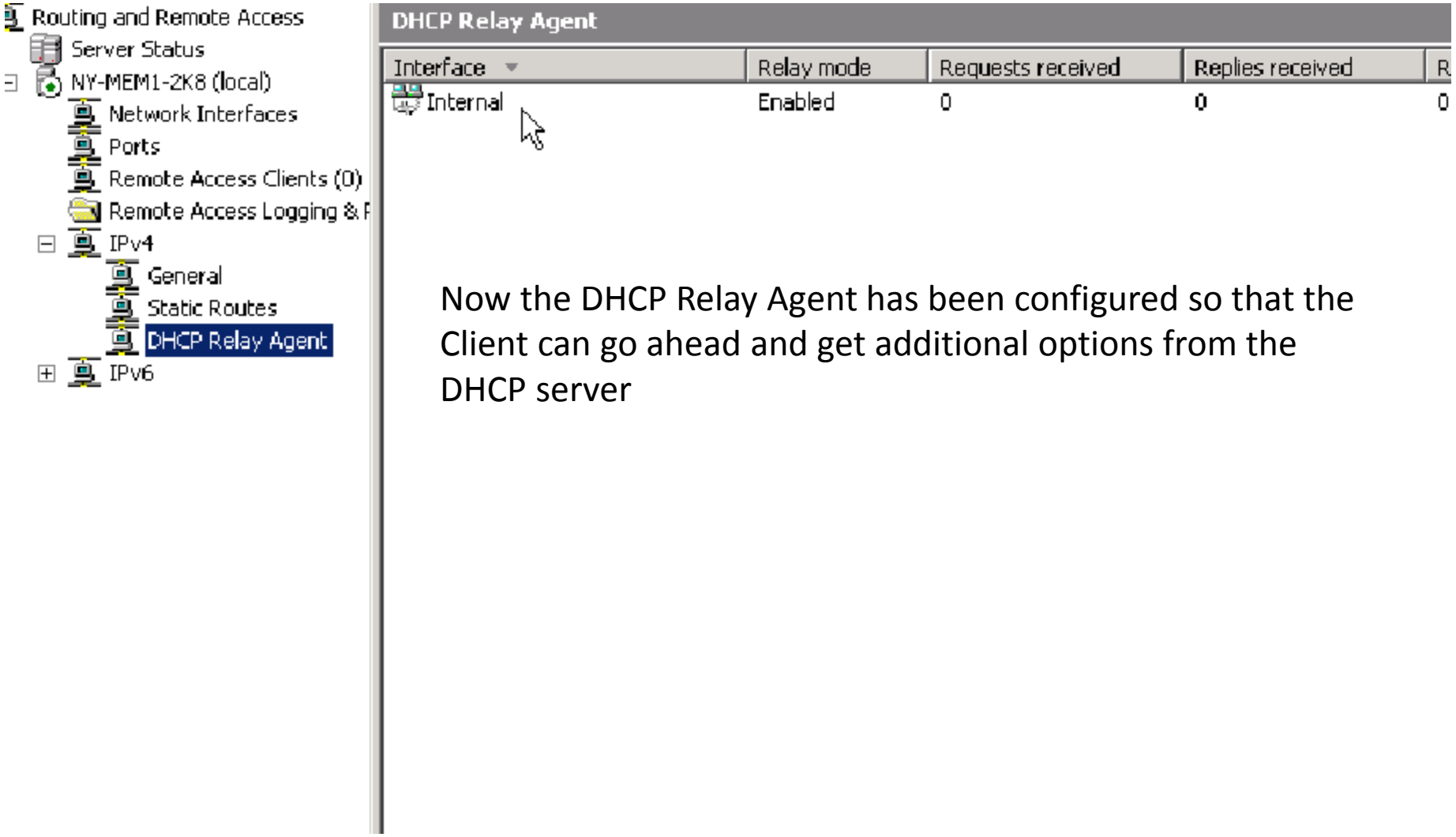
This is where you would do it. You would right Click on General and click New Routing Protocol.


Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
General
Static Routes
IPv6
Click the routing protocol that you want to add, then click OK.
Routing protocols:
DHCP Relay Agent
OK
Cancel
,160
76

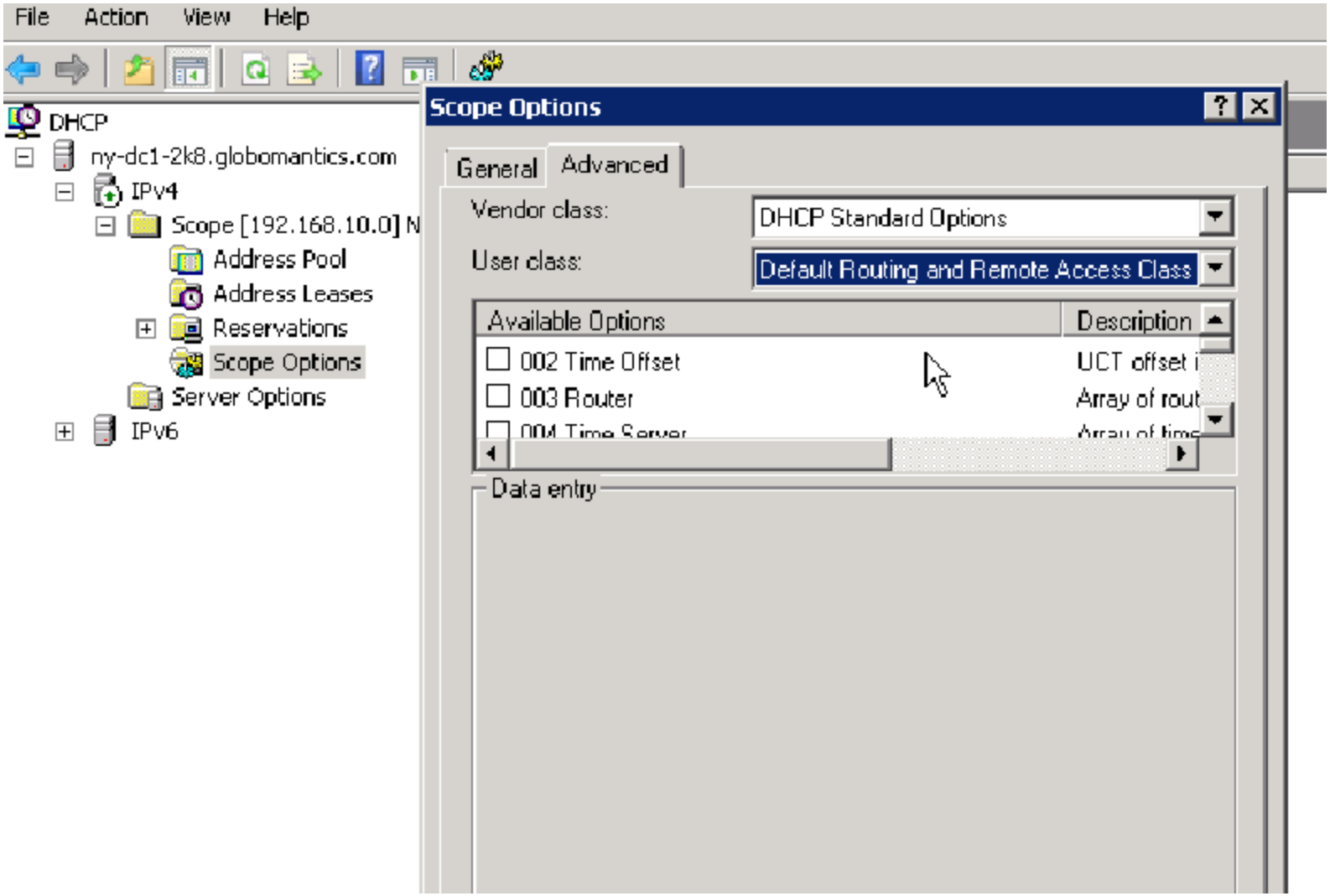

File
Action
View
Help
Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
General
Static Routes
DHCP Relay Agent
IPv6
DHCP Relay Agent
Interface
Relay mode
Requests received
Replies received
There are no items to show in this view.

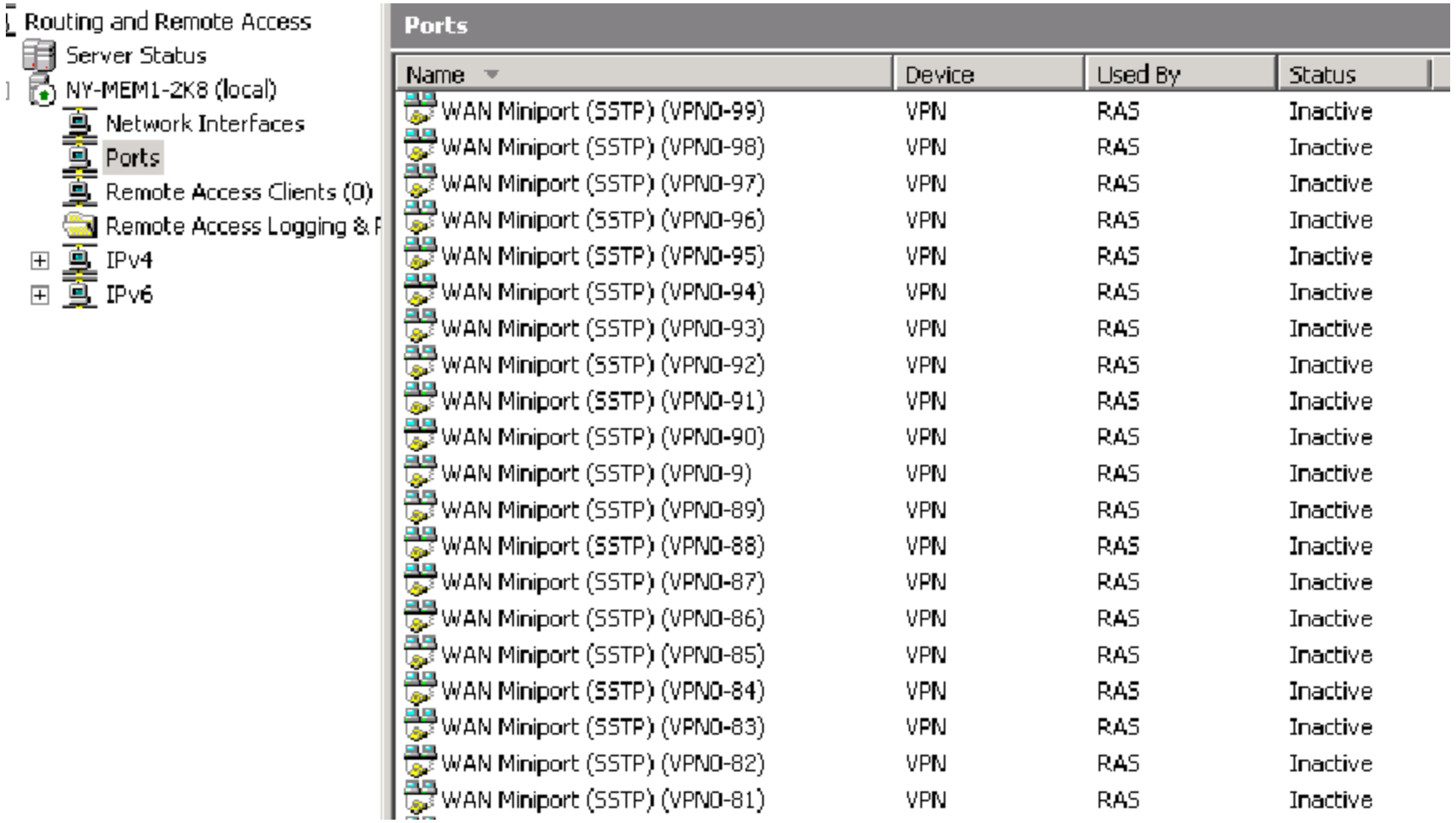

Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
General
Static Routes
DHCP Relay Agent
IPv6
DHCP Relay Agent
New Interface for DHCP Relay Agent
This routing protocol runs on the interface that you select below.
Interfaces:
External
Internal
Internal
To configure the DHCP Relay Agent you Would right click on DHCP Relay Agent and add an Interface
OK
Cancel
Replies received

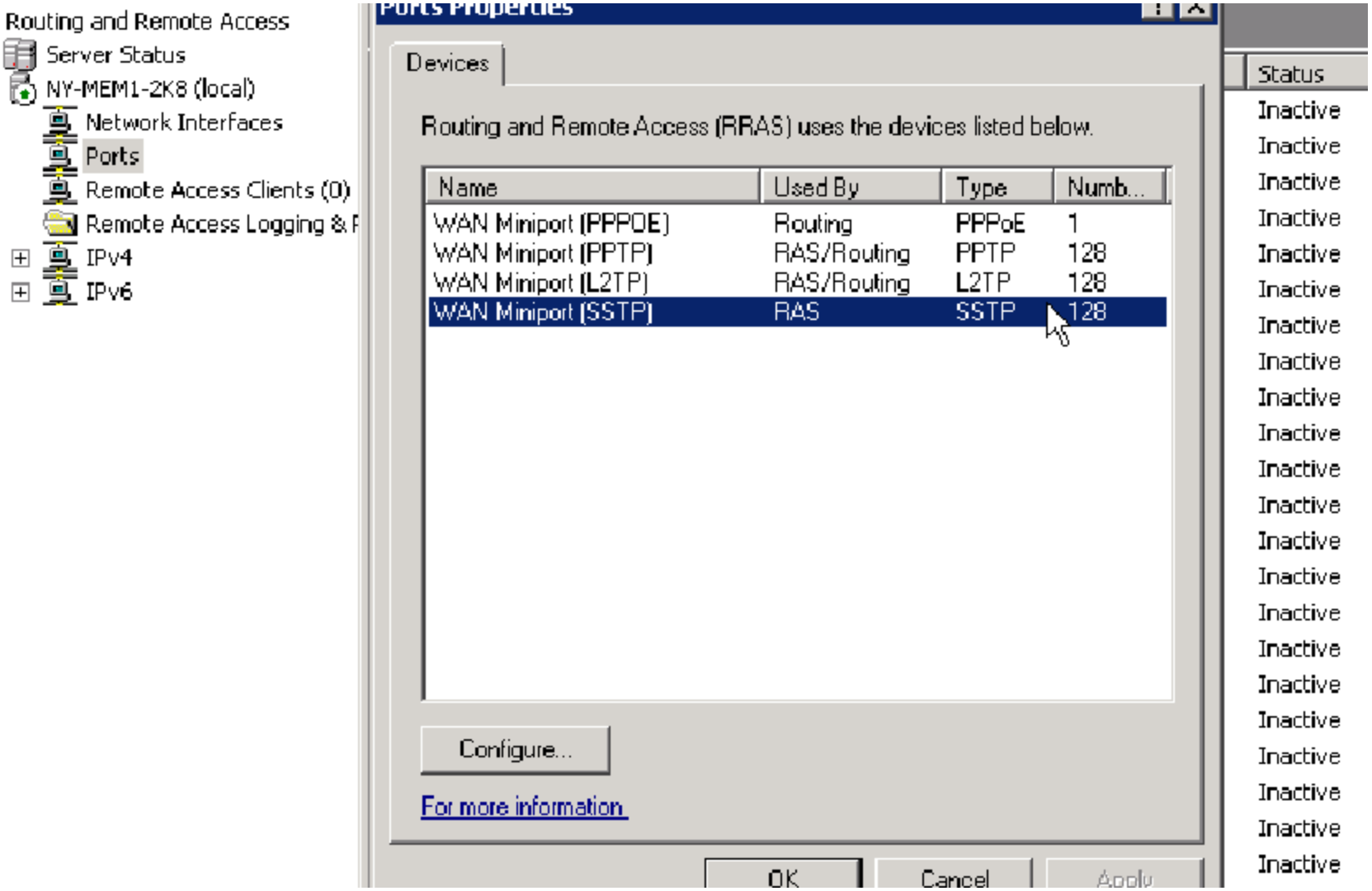

Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
General
Static Routes
DHCP Relay Agent
IPv6
General
Dynamic Host Configuration Protocol (DHCP) Interface
Relay DHCP packets
Hop-count threshold:
4
Boot threshold (seconds):
4
For more information
OK
Cancel
Apply

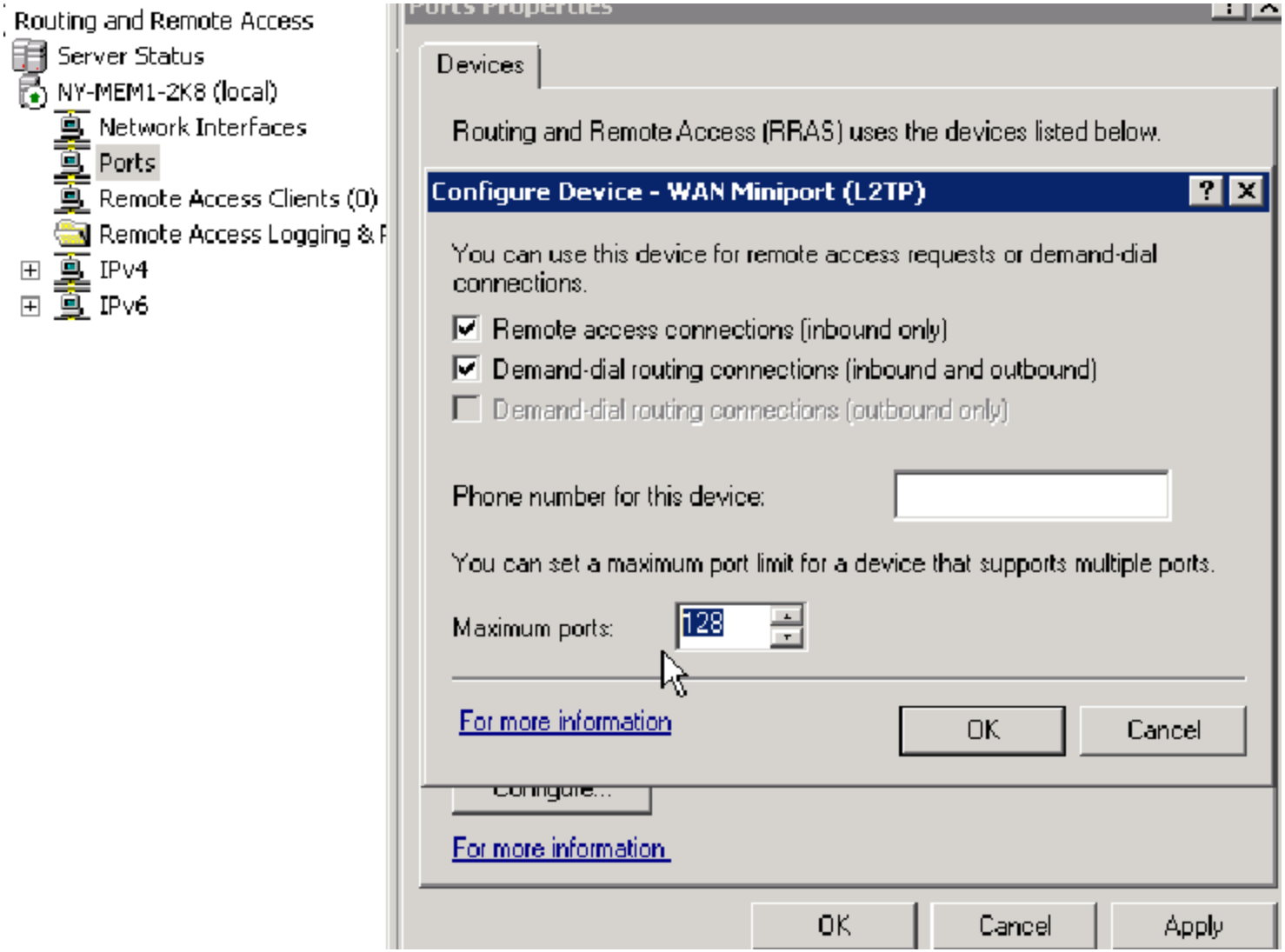


Now the DHCP Relay Agent has been configured so that the Client can go ahead and get additional options from the DHCP server

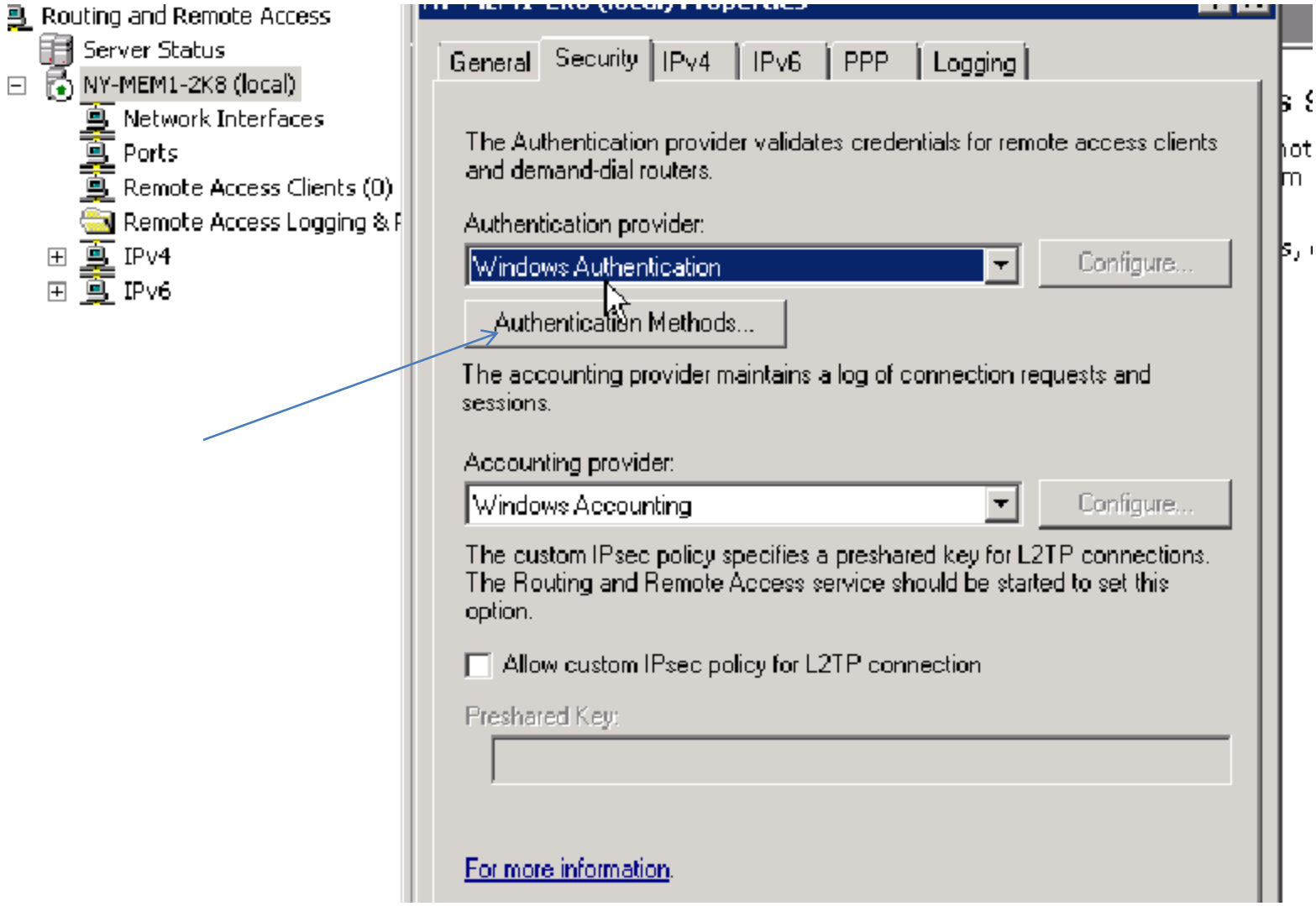

File
Action
View
Help
DHCP
ny-dc1-2k8.globomantics.com
IPv4
Scope [192.168.10.0] N
Address Pool
Address Leases
Reservations
Scope Options
Server Options
IPv6
Scope Options
General
Advanced
Vendor class:
DHCP Standard Options
User class:
Default Routing and Remote Access Class
Available Options
Description
002 Time Offset
UCT offset i
003 Router
Array of rout
Data entry

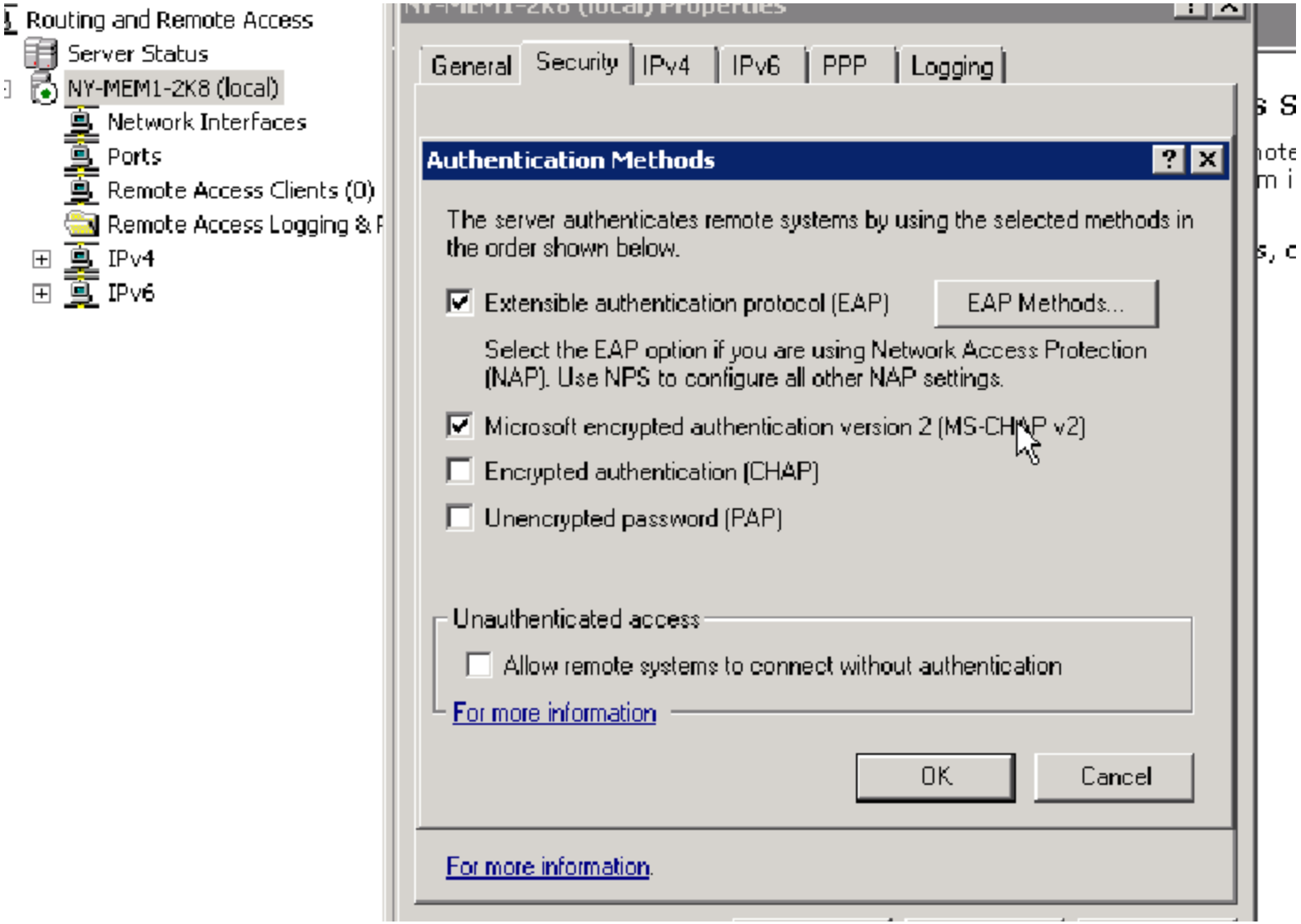

Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & F
IPv4
IPv6
Ports
Name
Device
Used By
Status
WAN Miniport (SSTP) (VPN0-99) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-98) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-97) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-96) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-95) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-94) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-93) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-92) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-91) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-90) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-9) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-89) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-88) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-87) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-86) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-85) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-84) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-83) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-82) VPN RAS Inactive
WAN Miniport (SSTP) (VPN0-81) VPN RAS Inactive


Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & F
IPv4
IPv6
Ports Properties
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Name
Used By
Type
Numb...
WAN Miniport (PPPOE)
Routing
PPPoE
1
WAN Miniport (PPTP)
RAS/Routing
PPTP
128
WAN Miniport (L2TP)
RAS/Routing
L2TP
128
WAN Miniport (SSTP)
RAS
SSTP
128
Configure...
For more information
OK
Cancel
Apply
Status
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive
Inactive

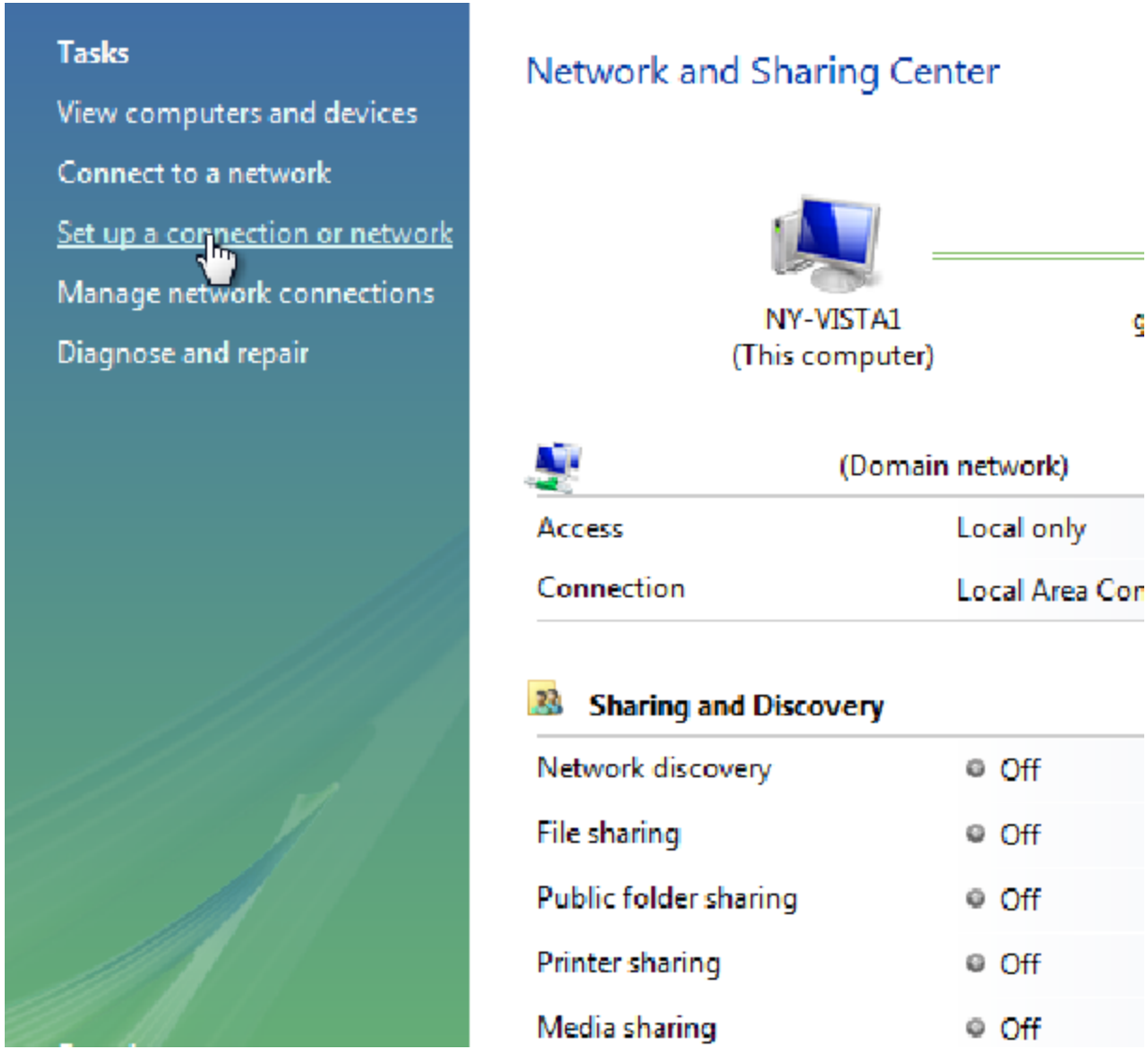

Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
IPv6
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Configure Device - WAN Miniport (L2TP)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Demand-dial routing connections (outbound only)
Phone number for this device:
You can set a maximum port limit for a device that supports multiple ports.
Maximum ports:
128
For more information
OK
Cancel
Configure...
For more information
OK
Cancel
Apply

Authentication protocols

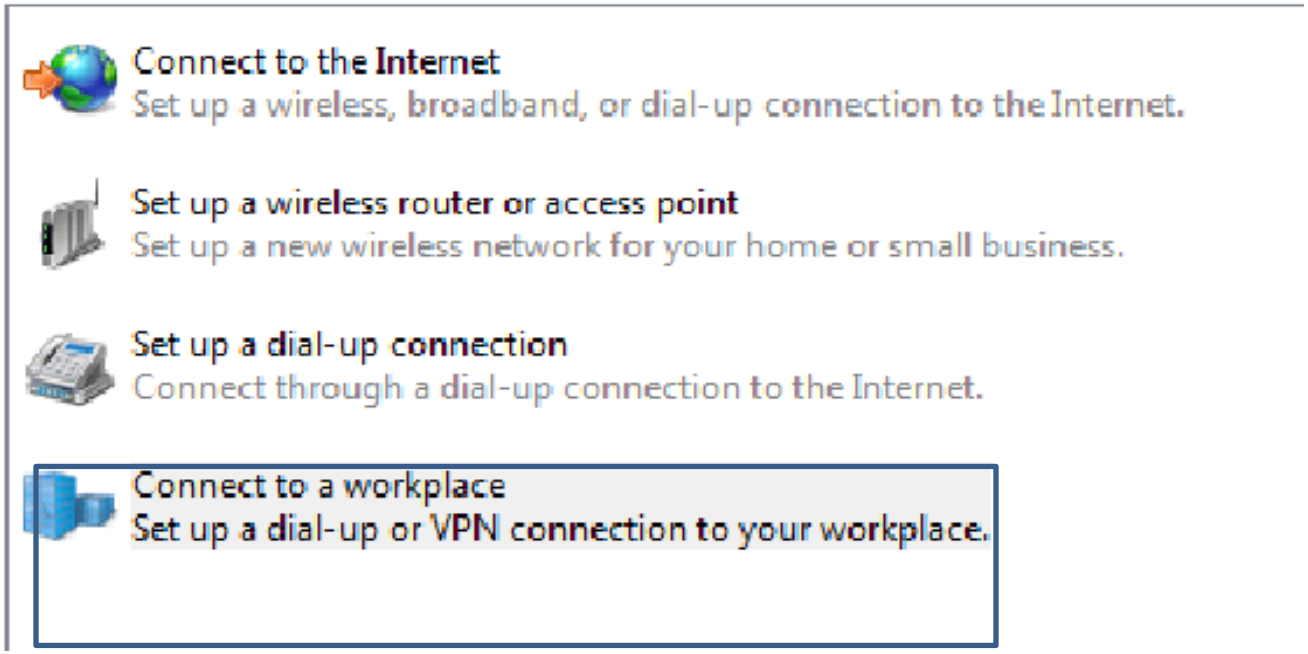



Routing and Remote Access
Server Status
NY-MEM1-2K8 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
IPv6
General
Security
IPv4
IPv6
PPP
Logging
Authentication Methods
The server authenticates remote systems by using the selected methods in the order shown below.
Extensible authentication protocol (EAP)
EAP Methods...
Select the EAP option if you are using Network Access Protection (NAP). Use NPS to configure all other NAP settings.
Microsoft encrypted authentication version 2 (MS-CHAP v2)
Encrypted authentication (CHAP)
Unencrypted password (PAP)
Unauthenticated access
Allow remote systems to connect without authentication
For more information
OK
Cancel
For more information.

SET UP A CLIENT CONNECTION TO A VPN SERVER



Choose a connection option



How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

IP address of the VPN server I am going To connect to