Lesson 10: Configuring VPN and Routing

MOAC 70-411: Administering Windows Server 2012

Microsoft
Official Academic Course

WILEY

Overview

- Exam Objective 3.3: Configure VPN and Routing
- Implementing the Remote Access Role

Implementing the Remote Access Role

Lesson 10: Configuring VPN and Routing

Routing and Remote Access (RRAS) Terms

- **Remote access server (RAS)**: A server that enables users to connect remotely to a network, even across the Internet, using various protocols and connection types.
- **Routing and Remote Access (RRAS)**: A Microsoft application programming interface that provides remote access.

RRAS Functionality

- A virtual private network (VPN) gateway where clients can connect to an organization's private network using the Internet.
- Connect two private networks using a VPN connection using the Internet.
- A dial-up remote access server, which enables users to connect to a private network using a modem.

RRAS Functionality

- Network address translation (NAT), which enables multiple users to share a single public network address.
- Provide routing functionality, which can connect subnets and control where packets are forwarded based on the destination address.
- Provide basic firewall functionality and allow or disallow packets based on addresses of source and/or destination and protocols.

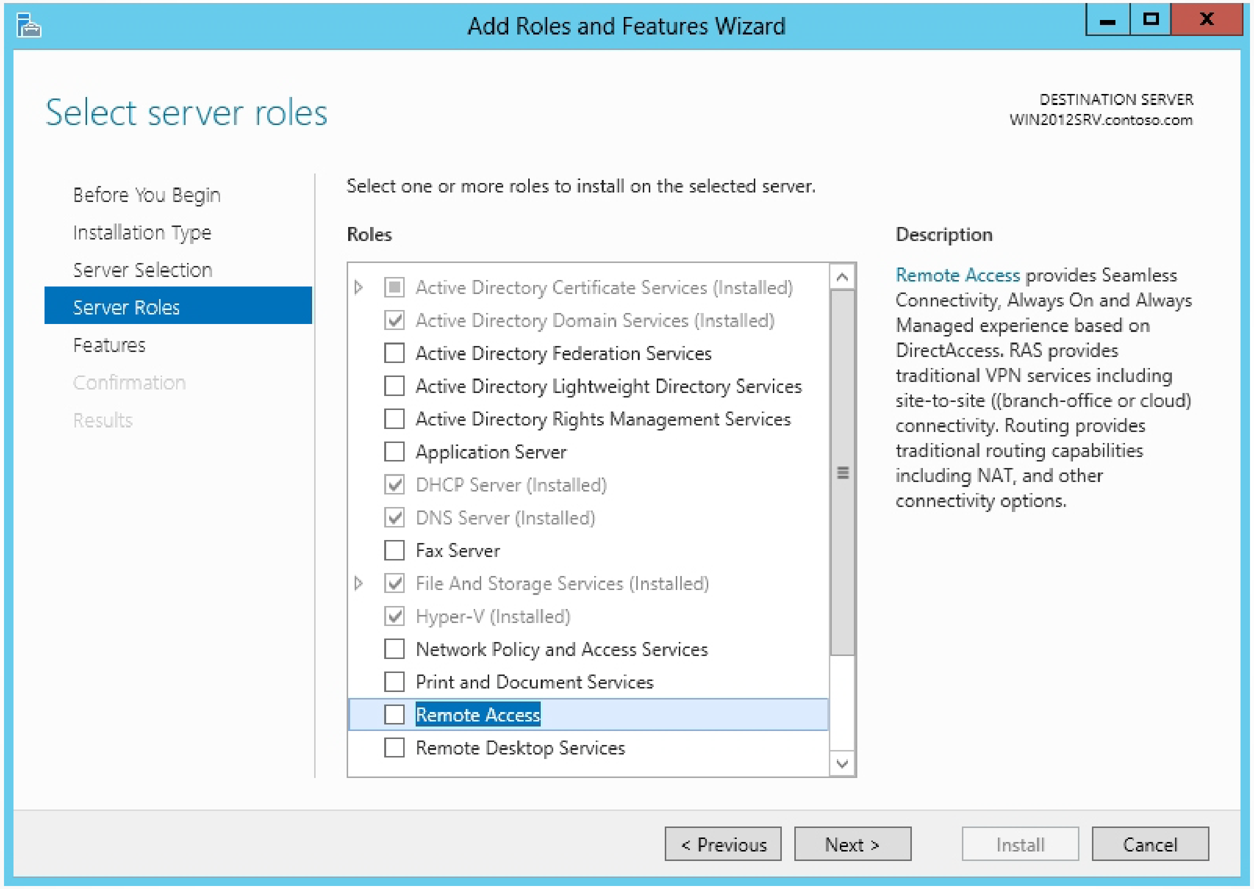
Installing/Configuring Remote Access Role

Before implementing RRAS:

1. Add the Remote Access Role.
2. Initially configure RRAS to specify which options are available with it.

To install Remote Access Role, use the Server Manager to install the proper role.

Install Remote Access Role



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN2012SRV.contoso.com

Select one or more roles to install on the selected server.

Roles

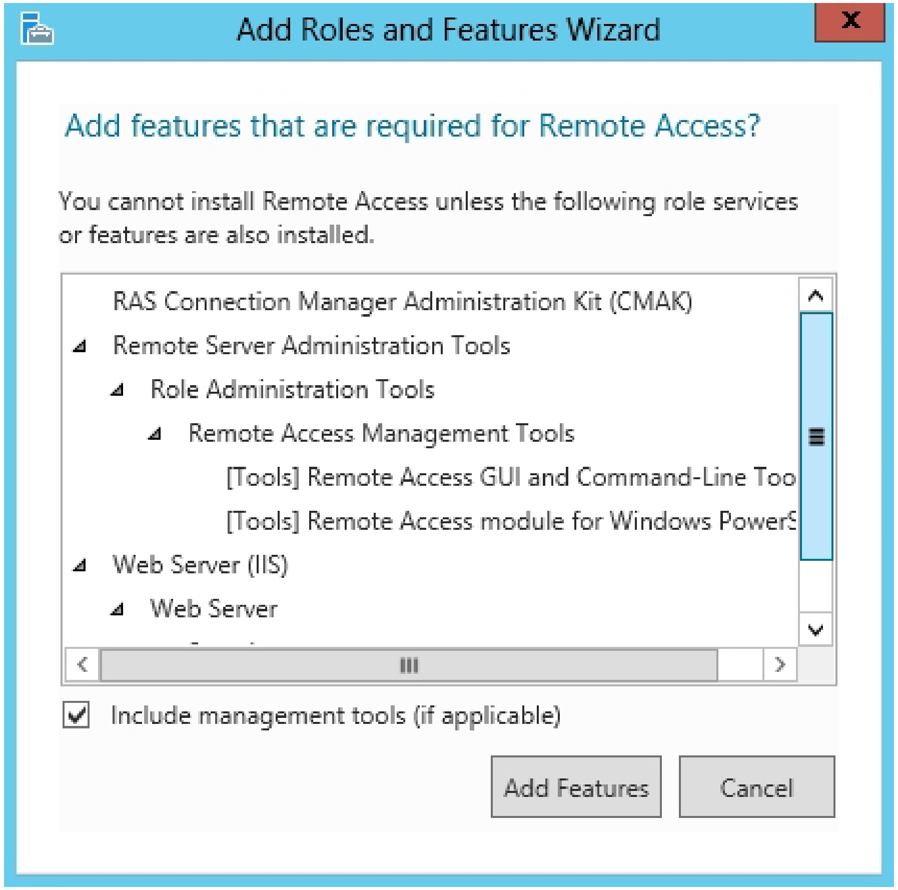
- ☐ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ File And Storage Services (Installed)
- ☑ Hyper-V (Installed)
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Remote Access provides Seamless Connectivity, Always On and Always Managed experience based on DirectAccess. RAS provides traditional VPN services including site-to-site ((branch-office or cloud) connectivity. Routing provides traditional routing capabilities including NAT, and other connectivity options.

Selecting the Remote Access role

Install Remote Access Role



Add features that are required for Remote Access?

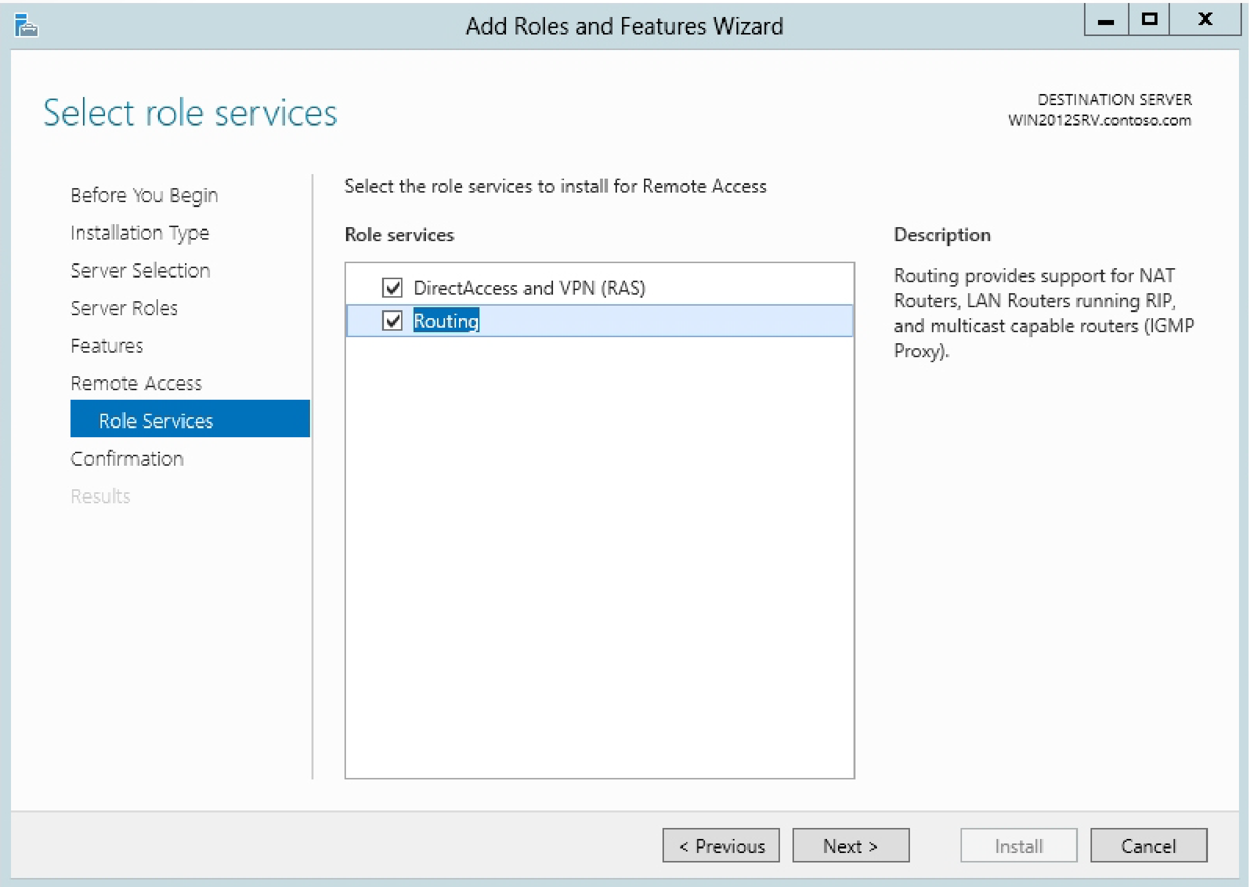
You cannot install Remote Access unless the following role services or features are also installed.

RAS Connection Manager Administration Kit (CMAK)
- Remote Server Administration Tools
  - Role Administration Tools
    - Remote Access Management Tools
      - [Tools] Remote Access GUI and Command-Line Too
      - [Tools] Remote Access module for Windows PowerS
- Web Server (IIS)
  - Web Server

☑ Include management tools (if applicable)

Adding additional features for the Remote Access role

Install Remote Access Role



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN2012SRV.contoso.com

Select the role services to install for Remote Access

Role services

- ☑ DirectAccess and VPN (RAS)
- ☑ Routing

Description

Routing provides support for NAT Routers, LAN Routers running RIP, and multicast capable routers (IGMP Proxy).

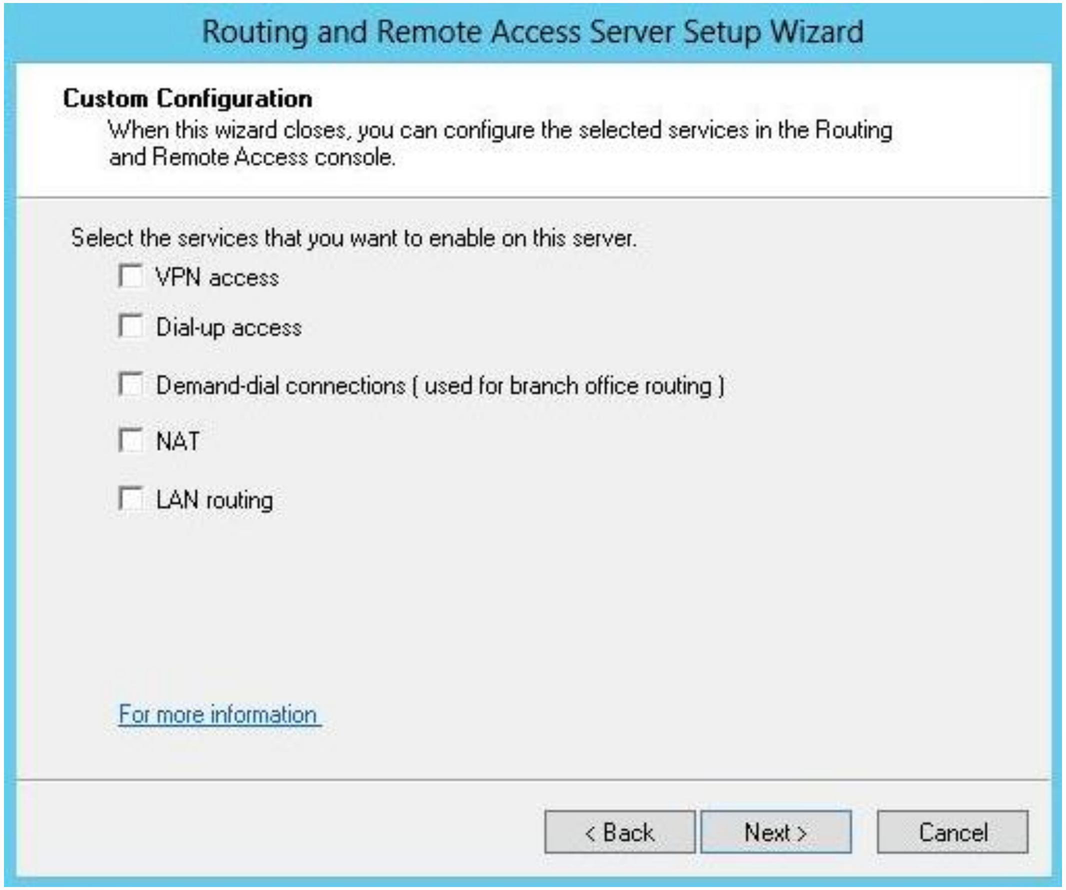
Selecting role services

Configuring Routing and Remote Access

Options for configuring RRAS:

- Remote access (dial-up or VPN)
- Network address translation (NAT)
- Virtual private network (VPN) access and NAT
- Secure connection between two private networks
- Custom configuration

Configuring Routing and Remote Access



Routing and Remote Access Server Setup Wizard

Custom Configuration

When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

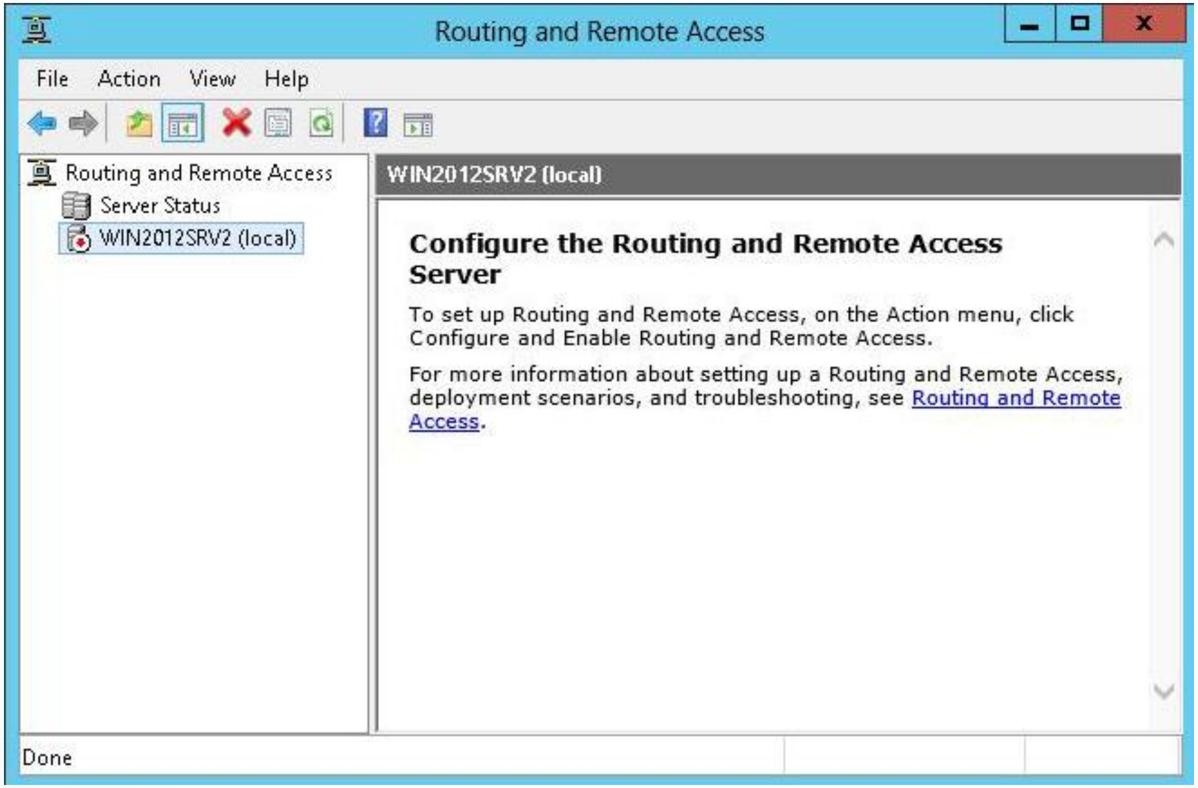
- □ VPN access
- □ Dial-up access
- □ Demand-dial connections (used for branch office routing)
- □ NAT
- □ LAN routing

Selecting services on the Custom Configuration page

Configuring RRAS for Dial-Up Remote Access

- Dial-up remote access enables remote computers to connect to a network via a modem.
- Remote computers act as though connected locally.
- Dial-up connections have much slower transfer speeds compared to DSL, cable technology, and other forms of networking.
- To support multiple dial-users that connect simultaneously, you must have a modem bank that supports multiple modem connections over the phone lines.

Configure Dial-Up Remote Access



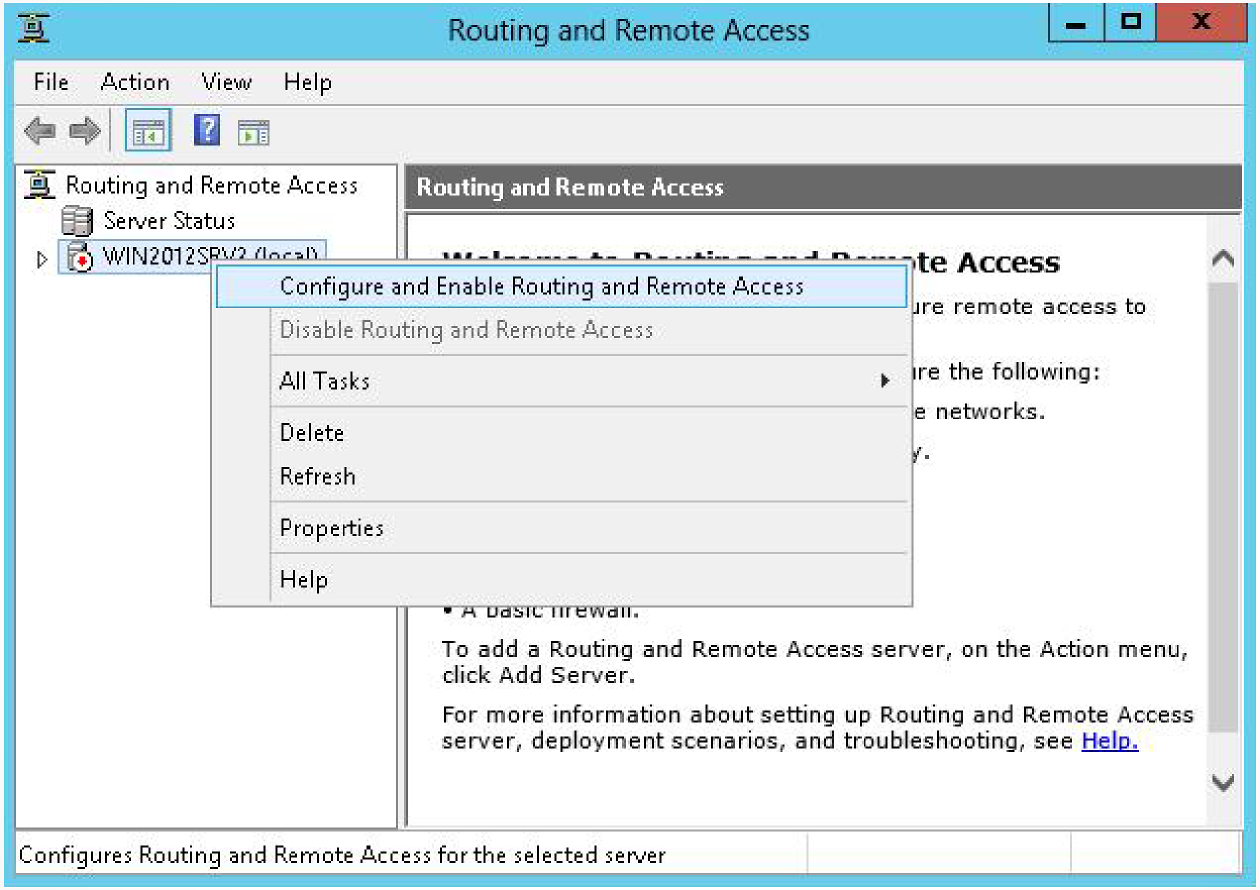
Configure the Routing and Remote Access Server

To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.

For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access.

Opening the Routing and Remote Access console

Configure Dial-Up Remote Access



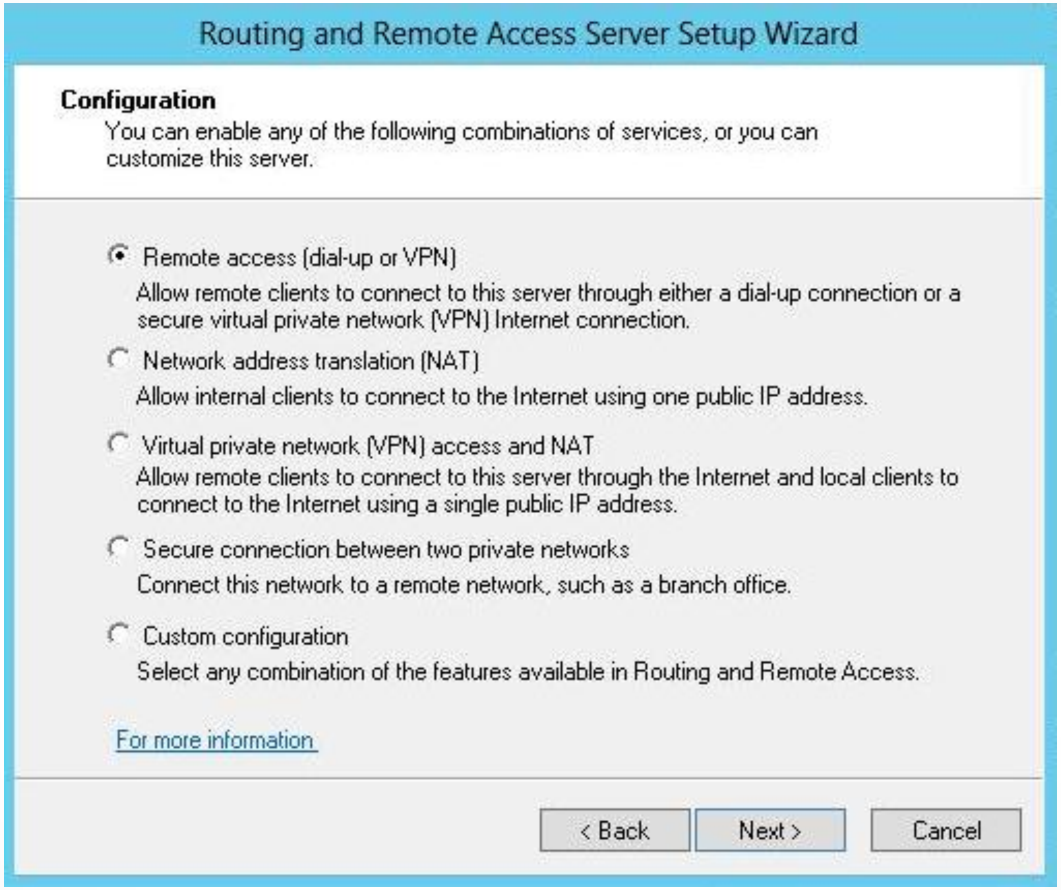
To add a Routing and Remote Access server, on the Action menu, click Add Server.

For more information about setting up Routing and Remote Access server, deployment scenarios, and troubleshooting, see Help.

Configures Routing and Remote Access for the selected server

Configuring and enabling RRAS

Configure Dial-Up Remote Access



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

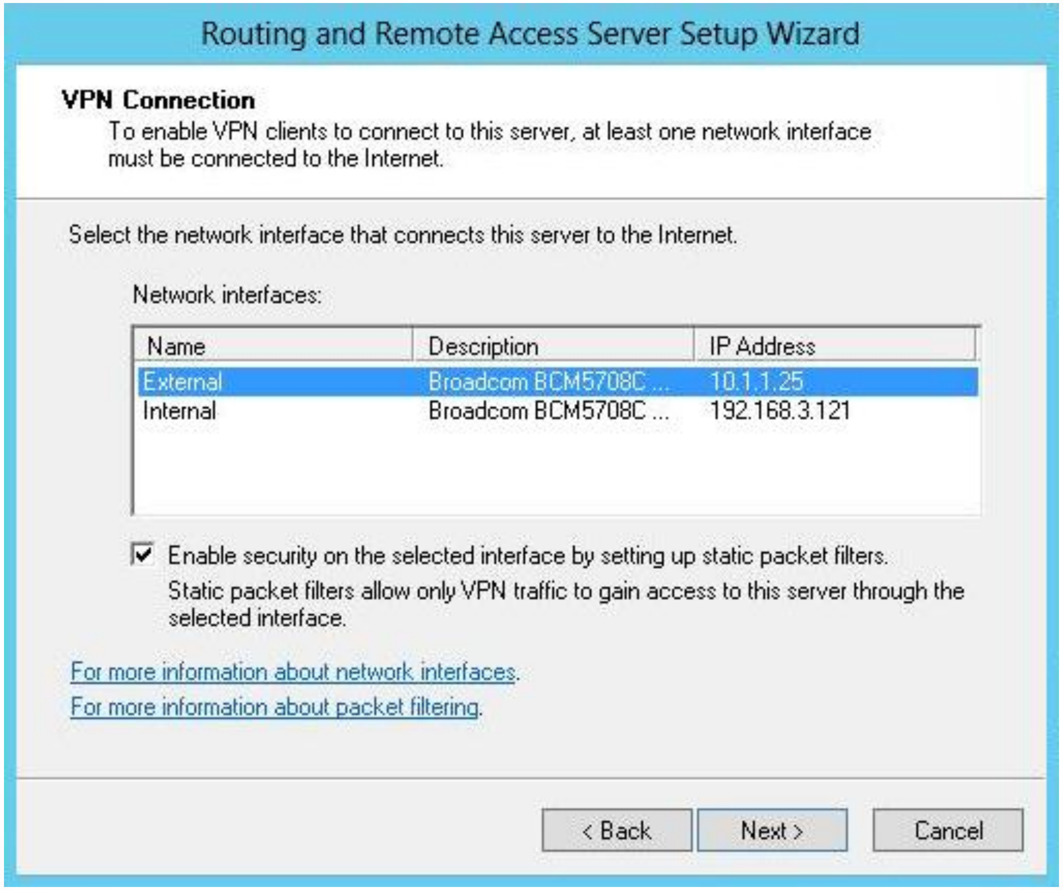
Connect this network to a remote network, such as a branch office.

○ Custom configuration

Select any combination of the features available in Routing and Remote Access.

Specifying the RRAS services on the Configuration page

Configure Dial-Up Remote Access



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	Broadcom BCM5708C ...	10.1.1.25
Internal	Broadcom BCM5708C ...	192.168.3.121

☑ Enable security on the selected interface by setting up static packet filters.

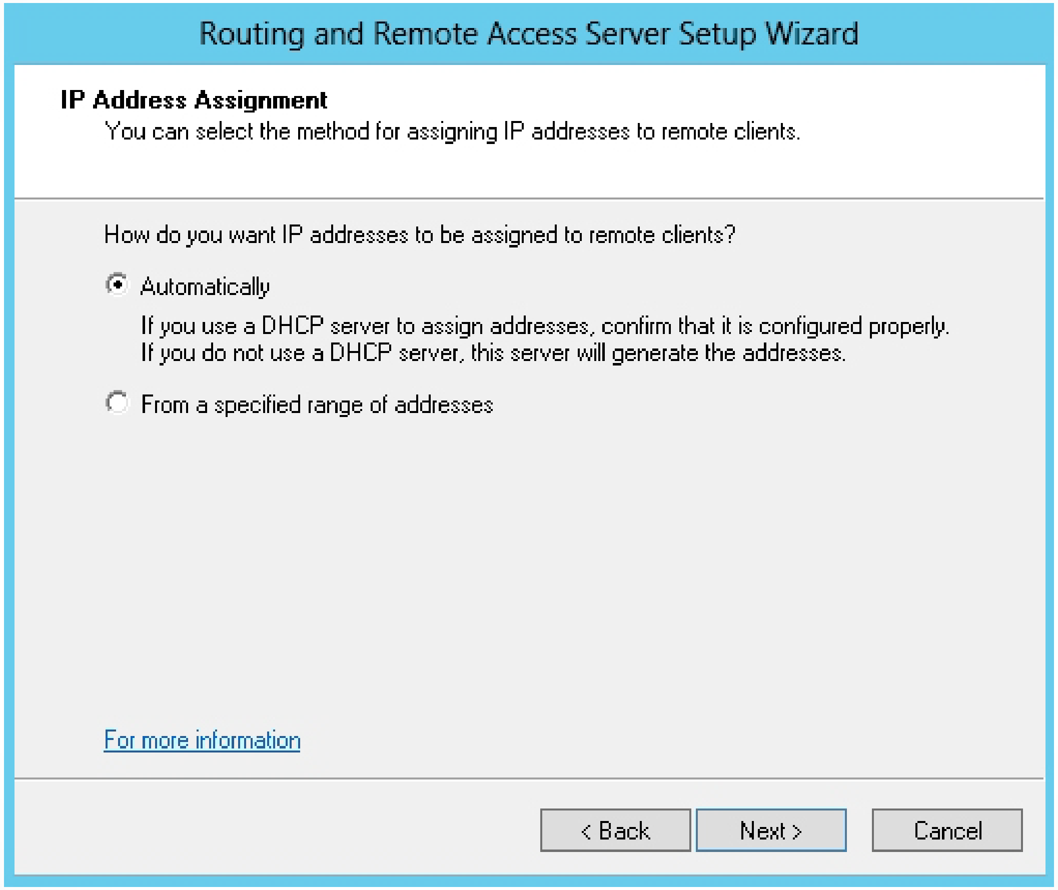
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

For more information about network interfaces.

For more information about packet filtering.

Selecting the VPN interface

Configure Dial-Up Remote Access



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?

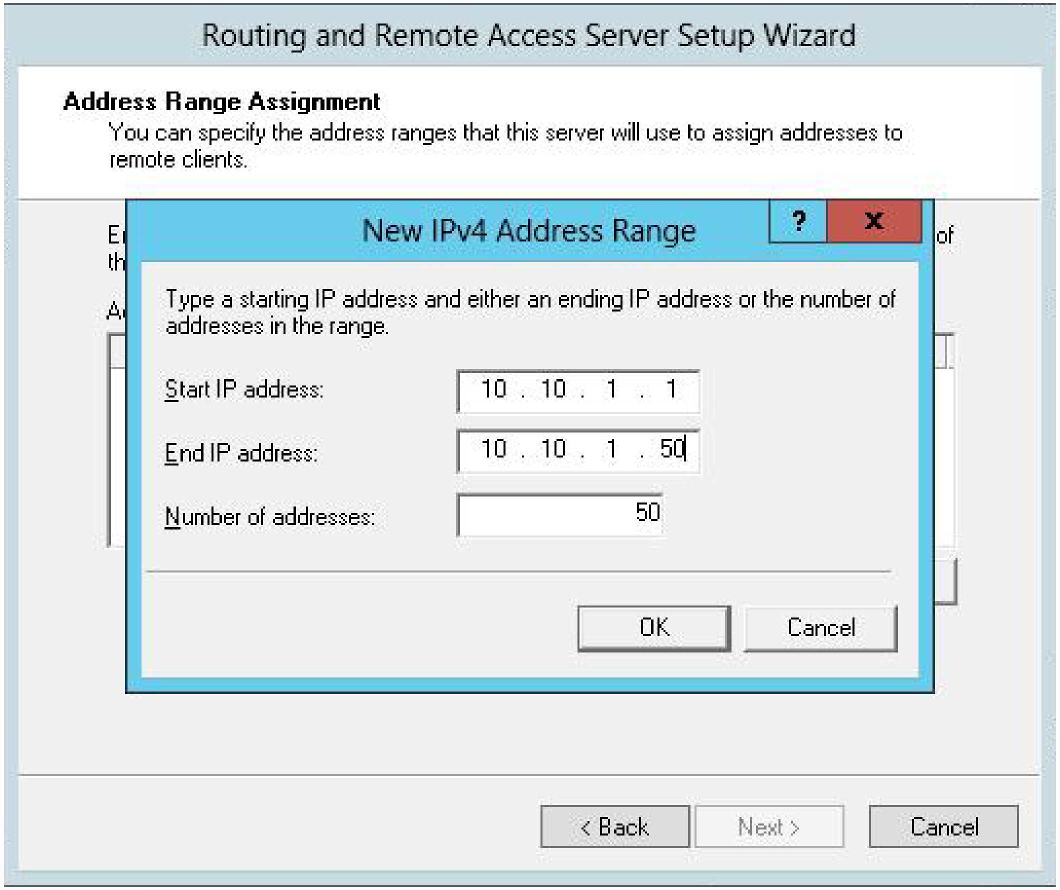
● Automatically

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

Specifying the method of IP address assignment

Configure Dial-Up Remote Access



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.

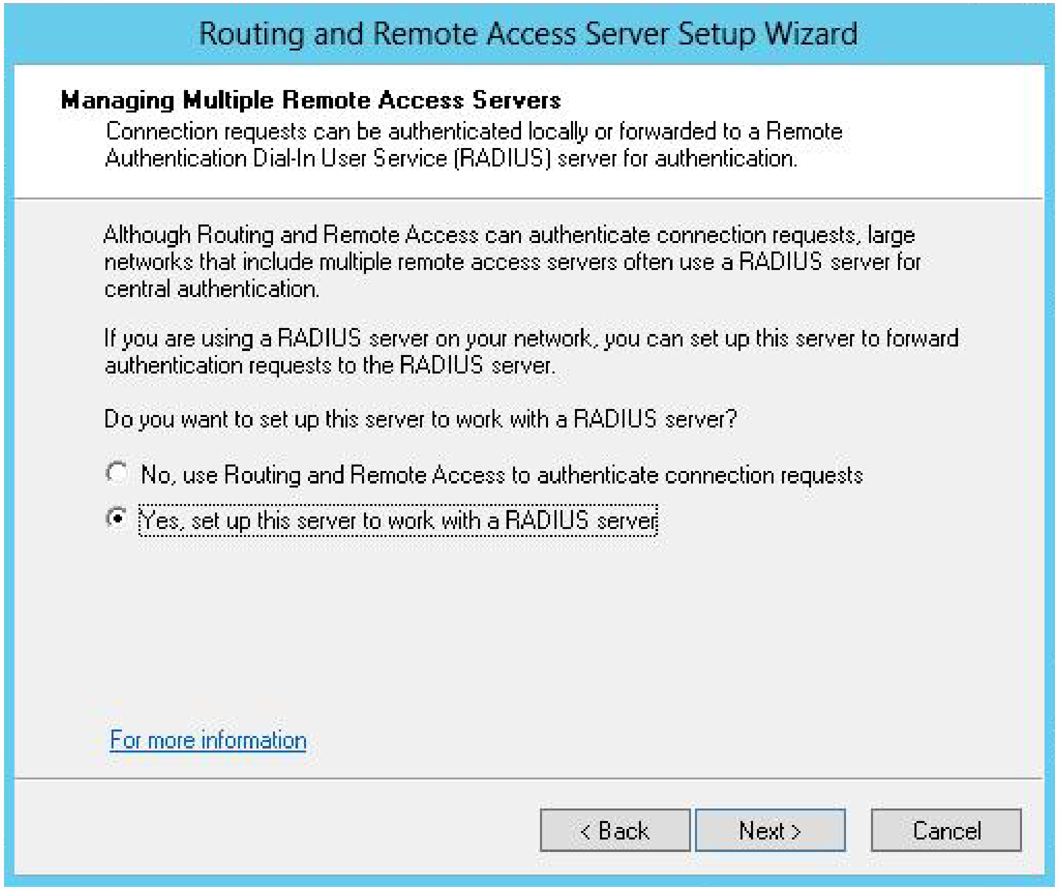
Start IP address: 10 . 10 . 1 . 1

End IP address: 10 . 10 . 1 . 50

Number of addresses: 50

Using the New IPv4 Address Range dialog box

Configure Dial-Up Remote Access



Routing and Remote Access Server Setup Wizard

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.

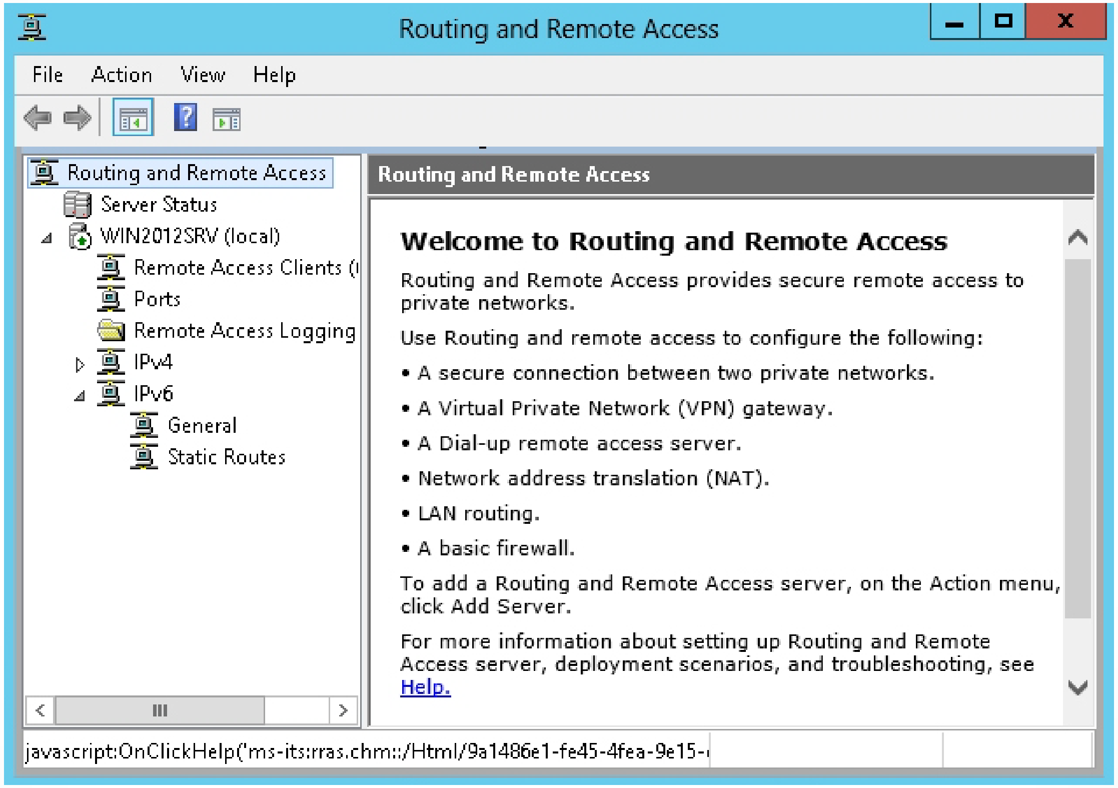
Do you want to set up this server to work with a RADIUS server?

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

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

Managing Multiple Remote Access Servers page

Configure Dial-Up Remote Access



Welcome to Routing and Remote Access

Routing and Remote Access provides secure remote access to private networks.

Use Routing and remote access to configure the following:

- A secure connection between two private networks.
- A Virtual Private Network (VPN) gateway.
- A Dial-up remote access server.
- Network address translation (NAT).
- LAN routing.
- A basic firewall.

To add a Routing and Remote Access server, on the Action menu, click Add Server.

For more information about setting up Routing and Remote Access server, deployment scenarios, and troubleshooting, see Help.

javascript:OnClickHelp('ms-its:rras.chm::/Html/9a1486e1-fe45-4fea-9e15-

Viewing the configured Routing and Remote Access console

Virtual Private Networks

- **Virtual private networks (VPNs)** link two computers or network devices through a wide-area network (WAN) such as the Internet.
- The data sent between the two computers or devices across a VPN is encapsulated and encrypted.

VPN Connections

- Encapsulation
- Authentication
- Data encryption
- Data integrity

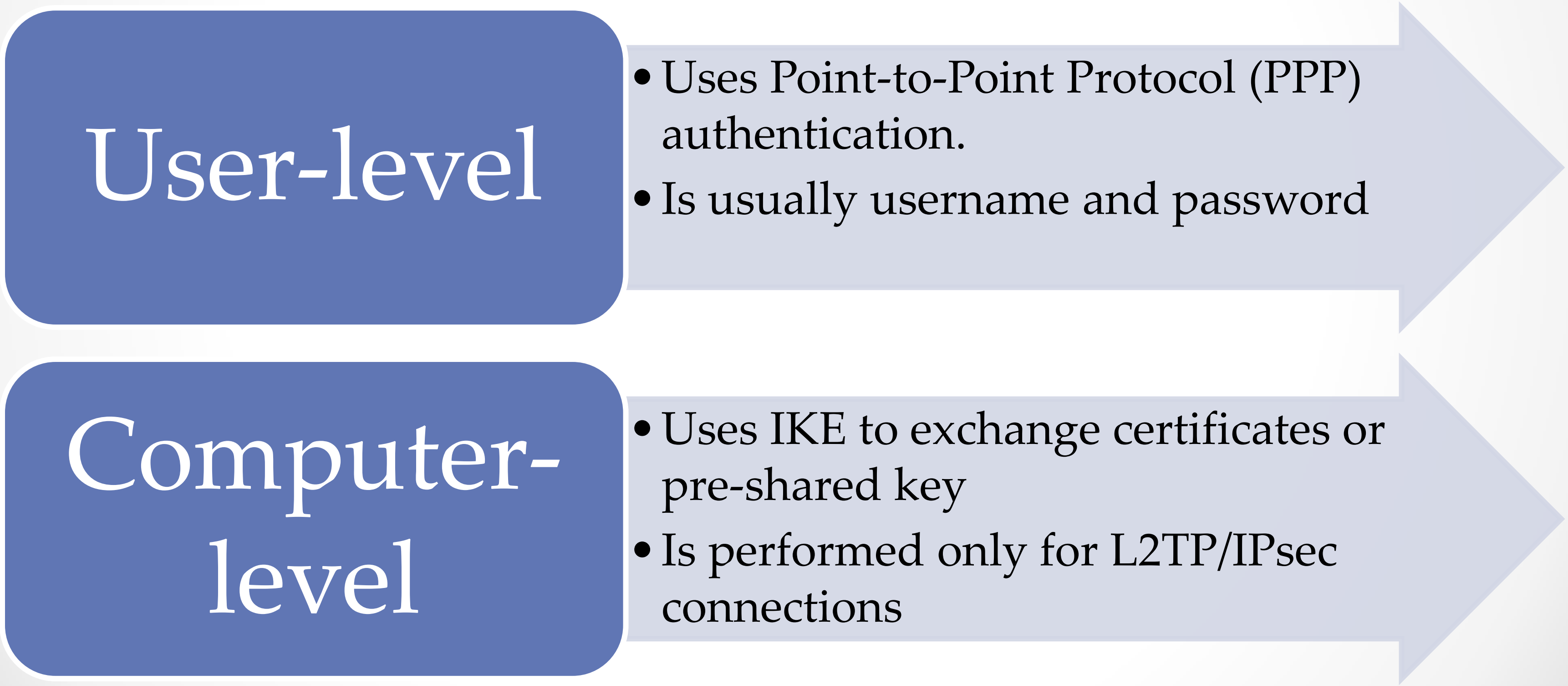
VPN Usage Scenarios

- A client connects to the RAS server to access internal resources from off-site.
- Two remote sites link together by creating a VPN tunnel between a RAS server located at each site.
- Two different organizations create a VPN tunnel so users from one organization can access the resources in the other organization.

Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- IKEv2
- Secure Socket Tunneling Protocol (SSTP)

VPN Authentication



User-level

- Uses Point-to-Point Protocol (PPP) authentication.
- Is usually username and password

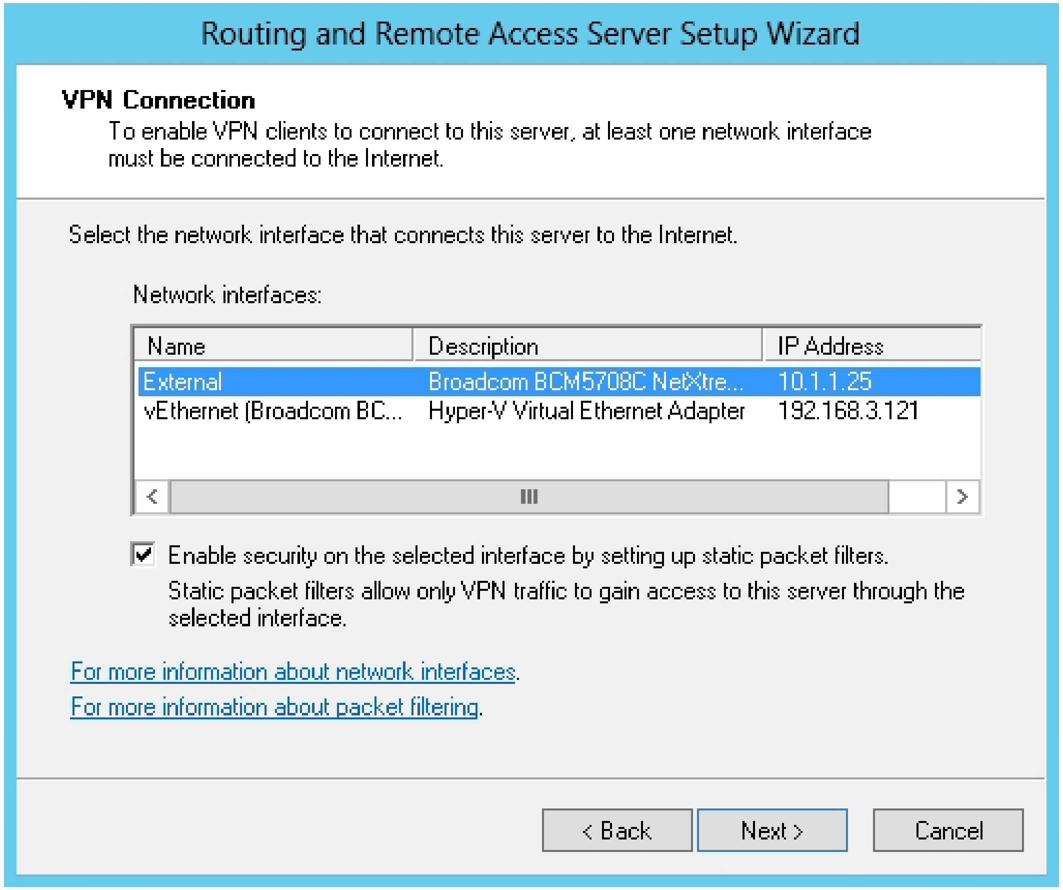
Computer-level

- Uses IKE to exchange certificates or pre-shared key
- Is performed only for L2TP/IPsec connections

Windows 8/Server 2012 VPN Authentication

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP version 2 (MS-CHAP v2)
- Extensible Authentication Protocol (EAP-MS-CHAPv2)

Configure and Enable VPN Remote Access



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	Broadcom BCM5708C NetXtre...	10.1.1.25
vEthernet (Broadcom BC...	Hyper-V Virtual Ethernet Adapter	192.168.3.121

☑ Enable security on the selected interface by setting up static packet filters.

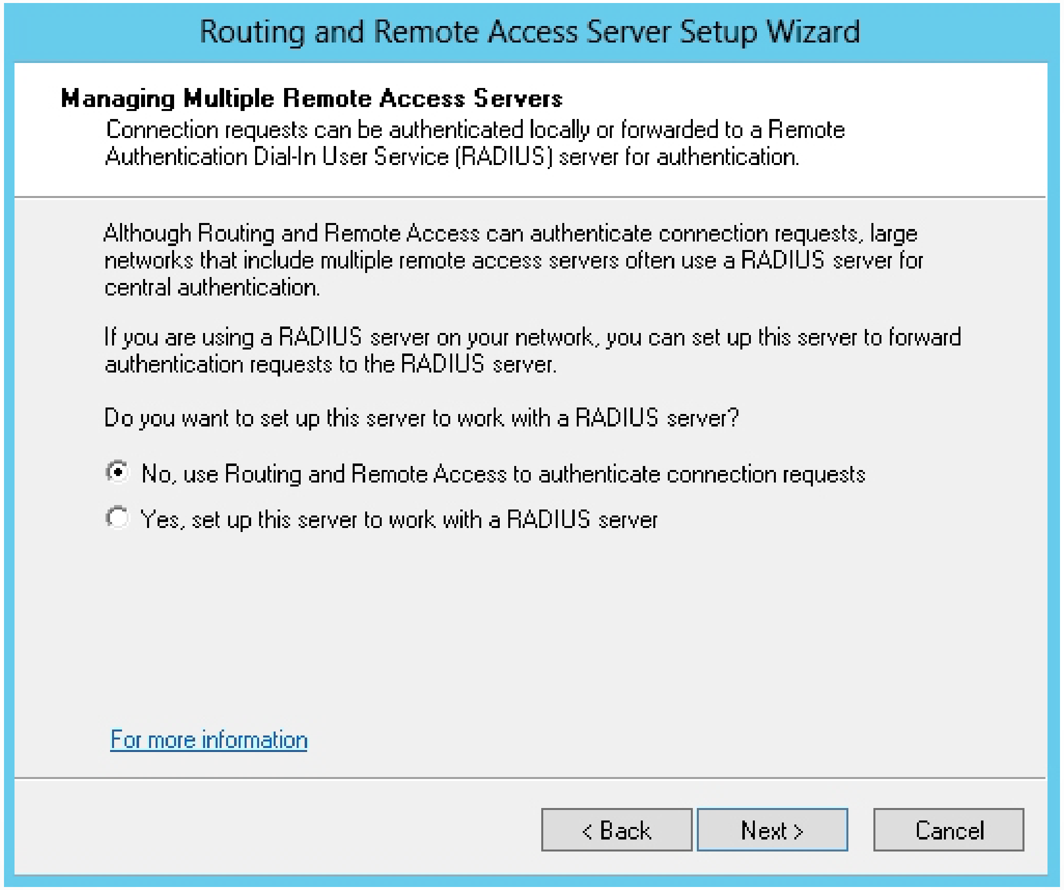
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

For more information about network interfaces.

For more information about packet filtering.

Configuring and enabling routing and remote access

Configure and Enable VPN Remote Access



Routing and Remote Access Server Setup Wizard

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.

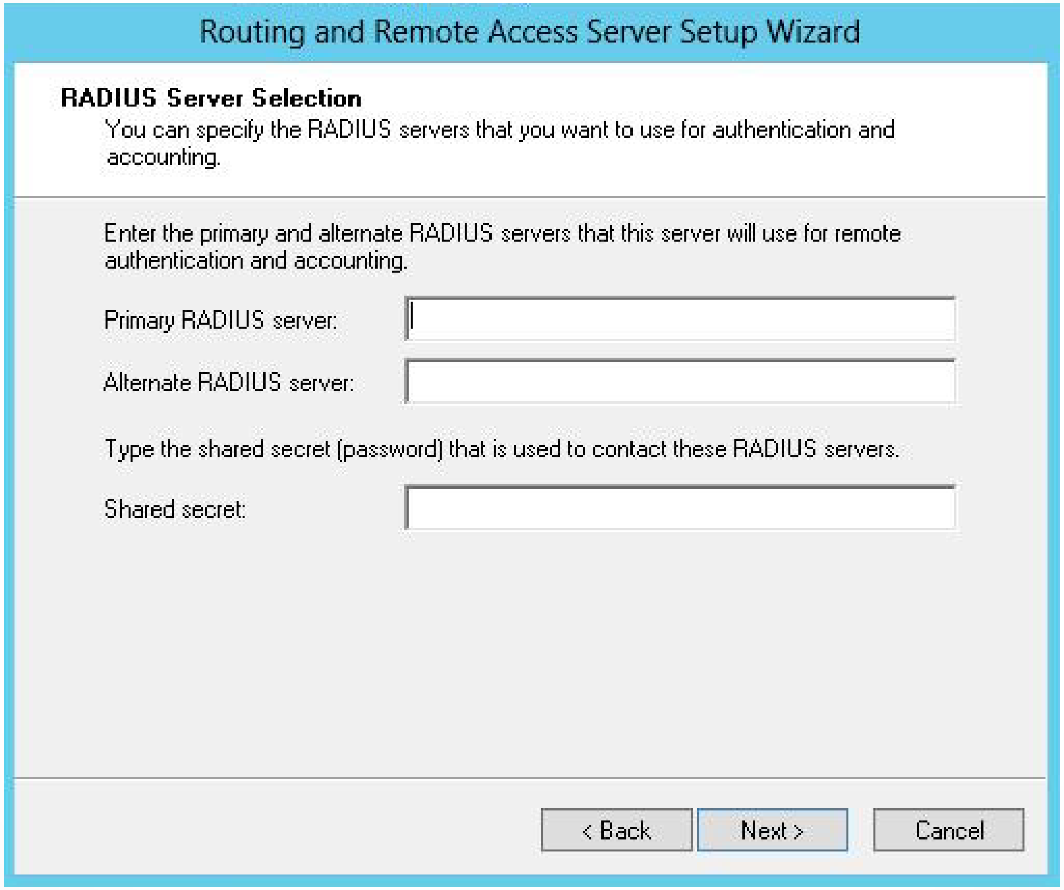
Do you want to set up this server to work with a RADIUS server?

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

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

Managing Multiple Remote Access Servers page

Configure and Enable VPN Remote Access



Routing and Remote Access Server Setup Wizard

RADIUS Server Selection

You can specify the RADIUS servers that you want to use for authentication and accounting.

Enter the primary and alternate RADIUS servers that this server will use for remote authentication and accounting.

Primary RADIUS server:

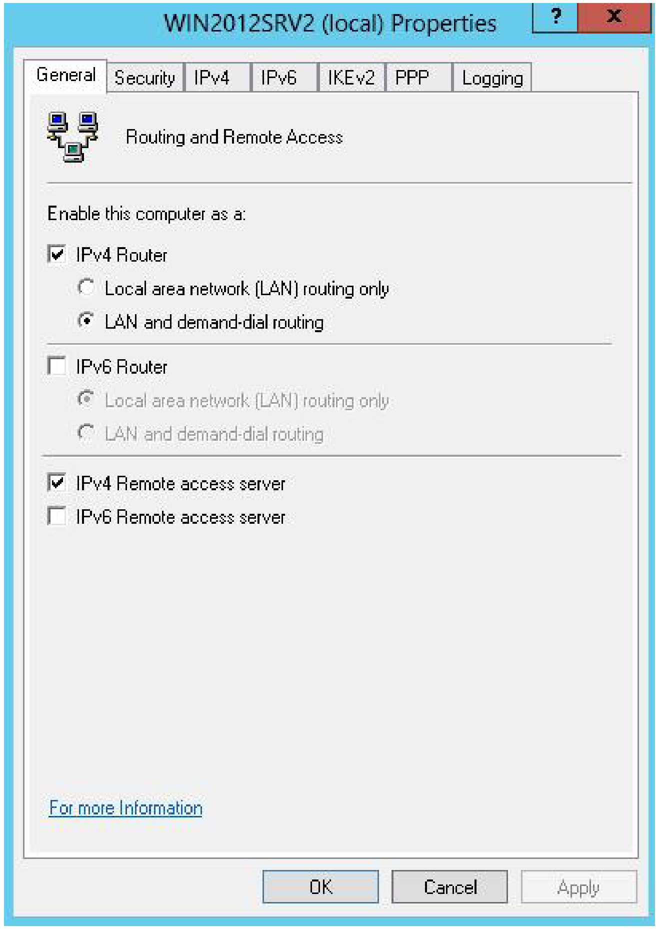
Alternate RADIUS server:

Type the shared secret (password) that is used to contact these RADIUS servers.

Shared secret:

Specifying the RADIUS Servers on the RADIUS Server Selection page

Configure and Enable VPN Remote Access



Routing and Remote Access

Enable this computer as a:

☑ IPv4 Router

○ Local area network (LAN) routing only

● LAN and demand-dial routing

□ IPv6 Router

● Local area network (LAN) routing only

○ LAN and demand-dial routing

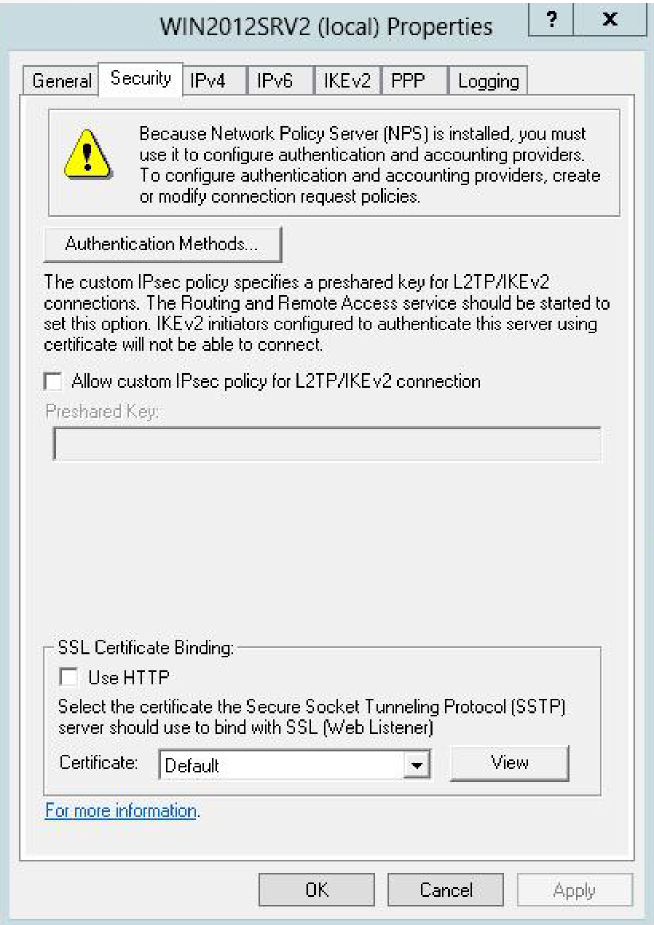
☑ IPv4 Remote access server

□ IPv6 Remote access server

For more Information

Enabling routing and remote access with the General tab

Configure and Enable VPN Remote Access



Because Network Policy Server (NPS) is installed, you must use it to configure authentication and accounting providers. To configure authentication and accounting providers, create or modify connection request policies.

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

□ Allow custom IPsec policy for L2TP/IKEv2 connection

Preshared Key:

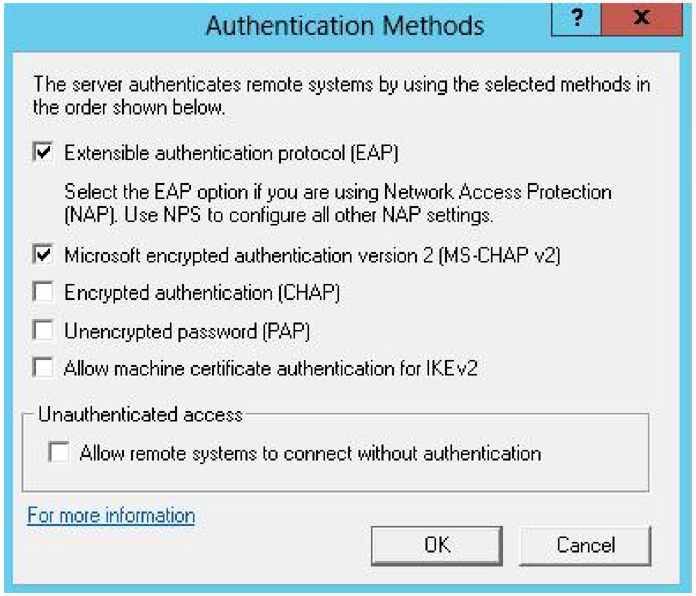
SSL Certificate Binding:

□ Use HTTP

Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: Default

For more information.



The server authenticates remote systems by using the selected methods in the order shown below.

☑ Extensible authentication protocol (EAP)

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)

□ Allow machine certificate authentication for IKEv2

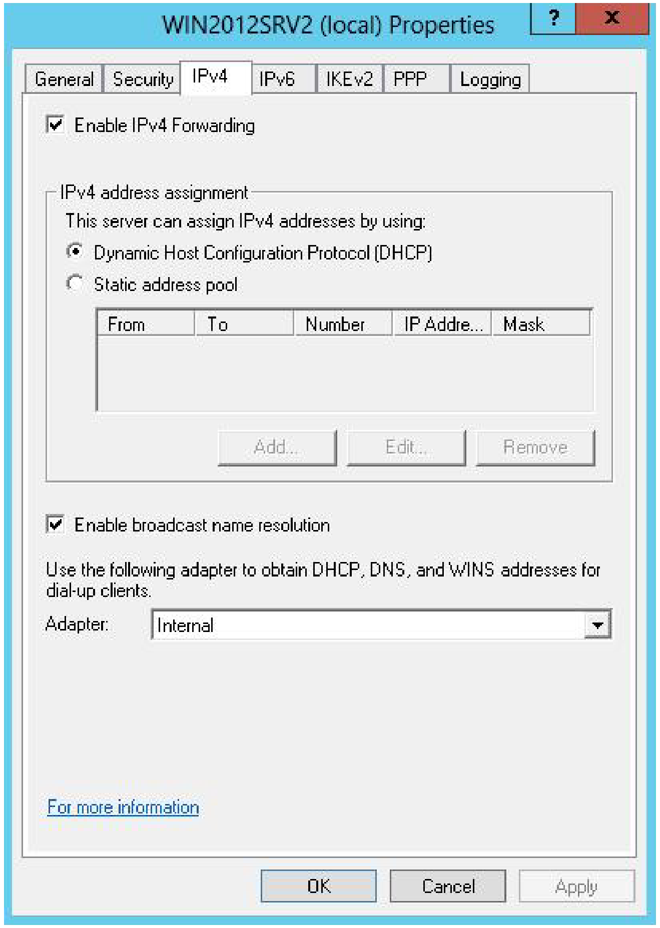
Unauthenticated access

□ Allow remote systems to connect without authentication

For more information

Using the Security tab

Configure and Enable VPN Remote Access



WIN2012SRV2 (local) Properties

General | Security | IPv4 | IPv6 | IKEv2 | PPP | Logging

☑ Enable IPv4 Forwarding

IPv4 address assignment

This server can assign IPv4 addresses by using:

● Dynamic Host Configuration Protocol (DHCP)

○ Static address pool

From	To	Number	IP Addre...	Mask

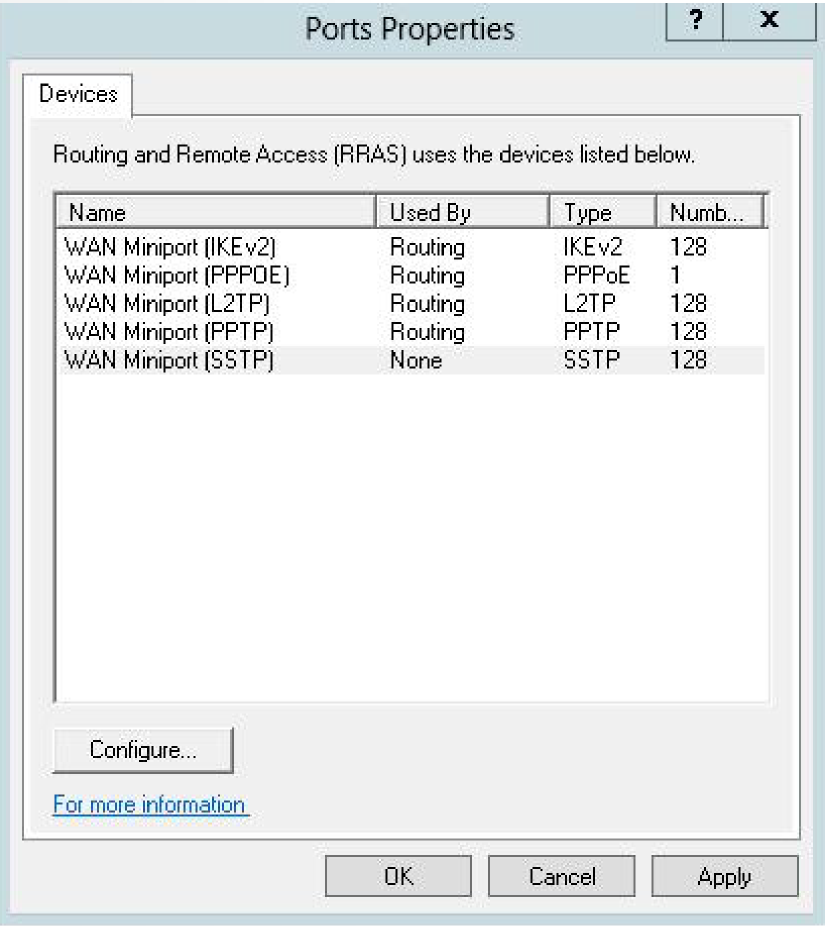
☑ Enable broadcast name resolution

Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.

Adapter: Internal

Using the IPv4 tab

Configure and Enable VPN Remote Access

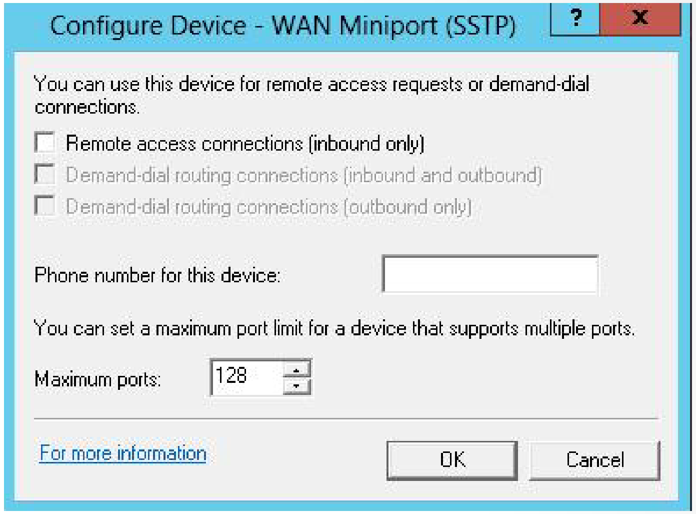


Ports Properties

Devices

Routing and Remote Access (RRAS) uses the devices listed below.

Name	Used By	Type	Numb...
WAN Miniport (IKEv2)	Routing	IKEv2	128
WAN Miniport (PPPOE)	Routing	PPPoE	1
WAN Miniport (L2TP)	Routing	L2TP	128
WAN Miniport (PPTP)	Routing	PPTP	128
WAN Miniport (SSTP)	None	SSTP	128



Configure Device - WAN Miniport (SSTP)

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)

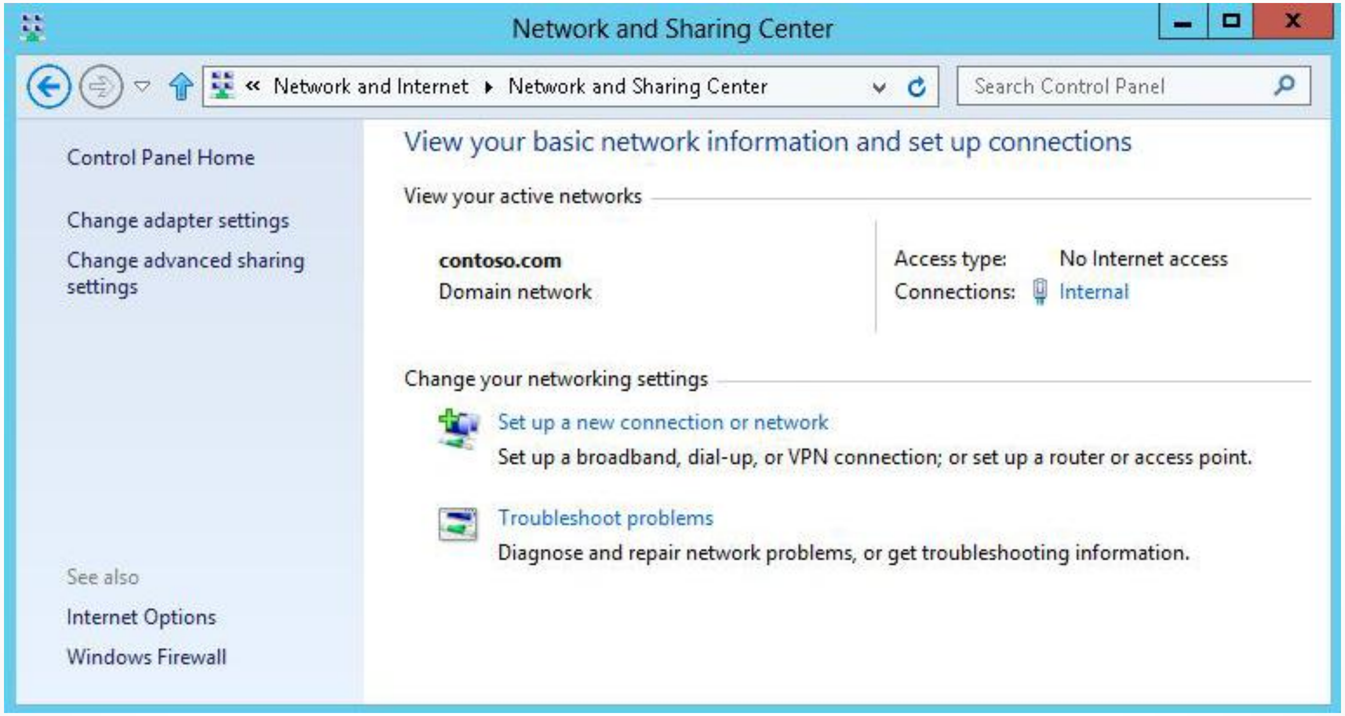
Phone number for this device:

You can set a maximum port limit for a device that supports multiple ports.

Maximum ports: 128

Specifying the number of ports

Create a VPN Tunnel



Network and Sharing Center

« Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

Internet Options

Windows Firewall

View your basic network information and set up connections

View your active networks

contoso.com
Domain network

Access type: No Internet access

Connections: Internal

Change your networking settings

Set up a new connection or network

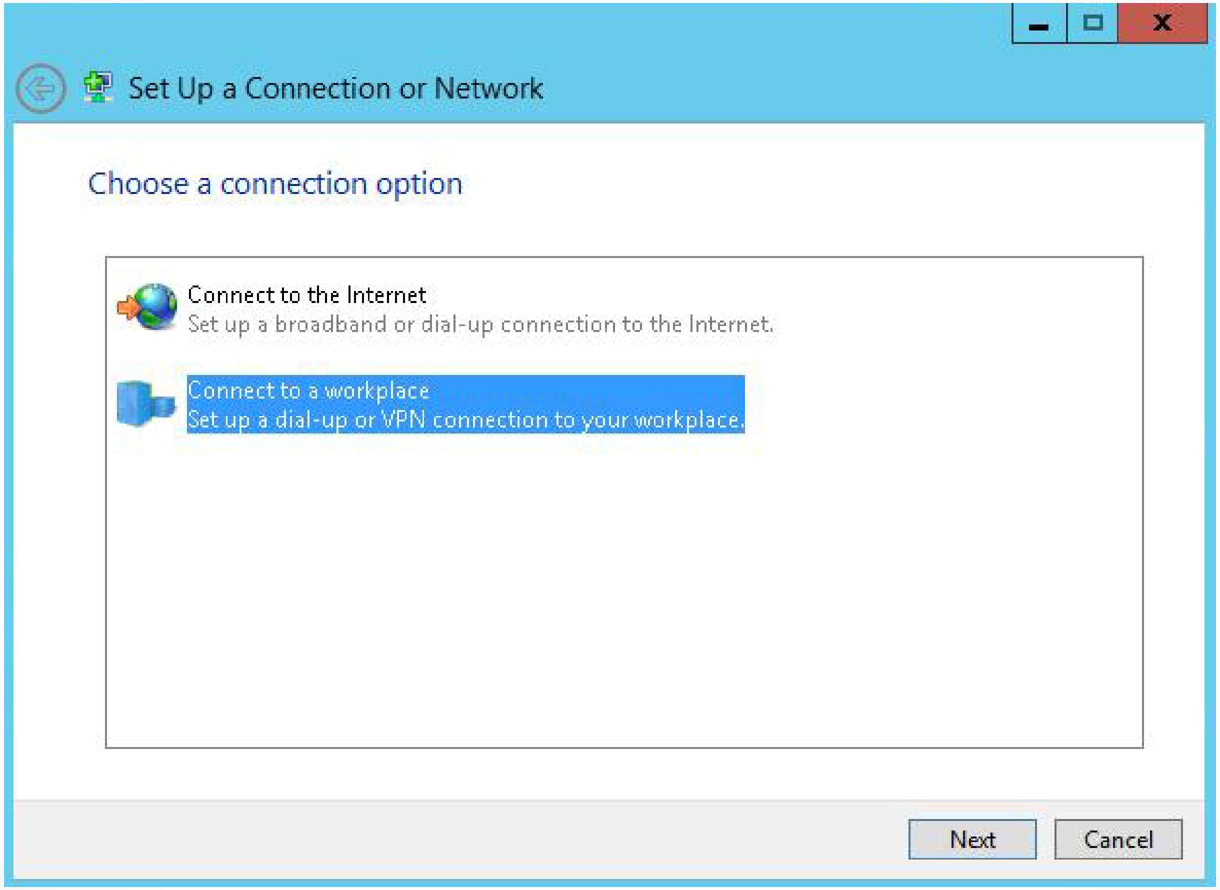
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

Opening the Network and Sharing Center

Create a VPN Tunnel



Set Up a Connection or Network

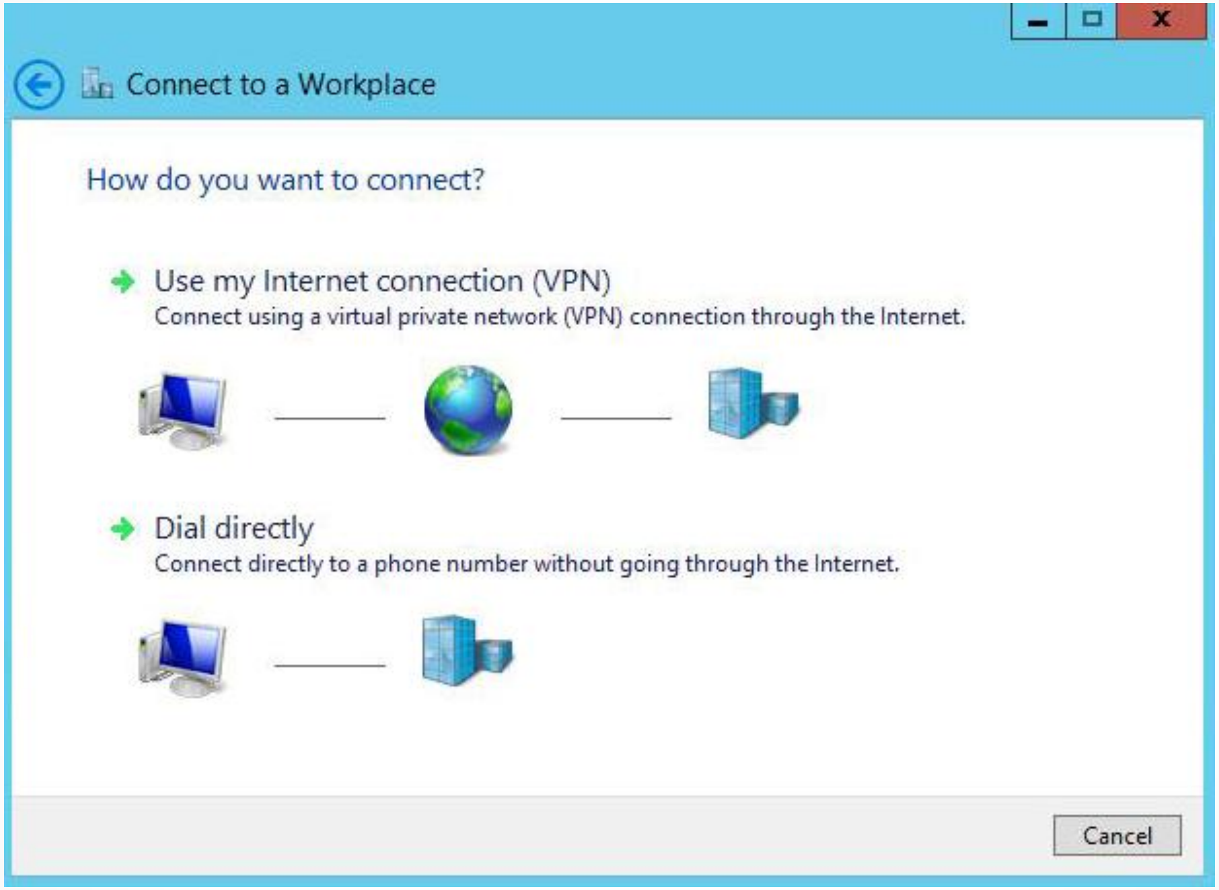
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Connecting to a workplace with the Set Up a Connection or Network page

Create a VPN Tunnel



Connect to a Workplace

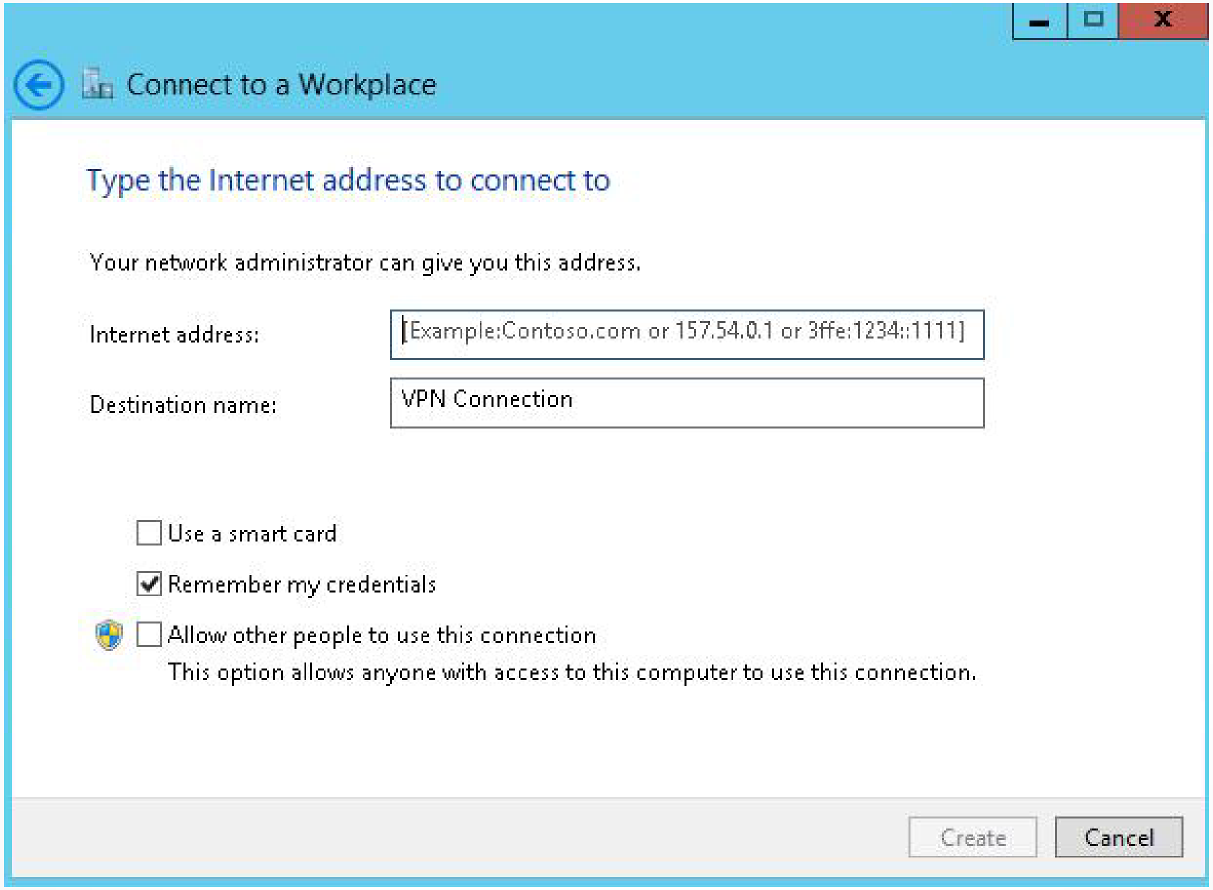
How do you want to connect?

- 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.

Connecting to a workplace

Create a VPN Tunnel



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

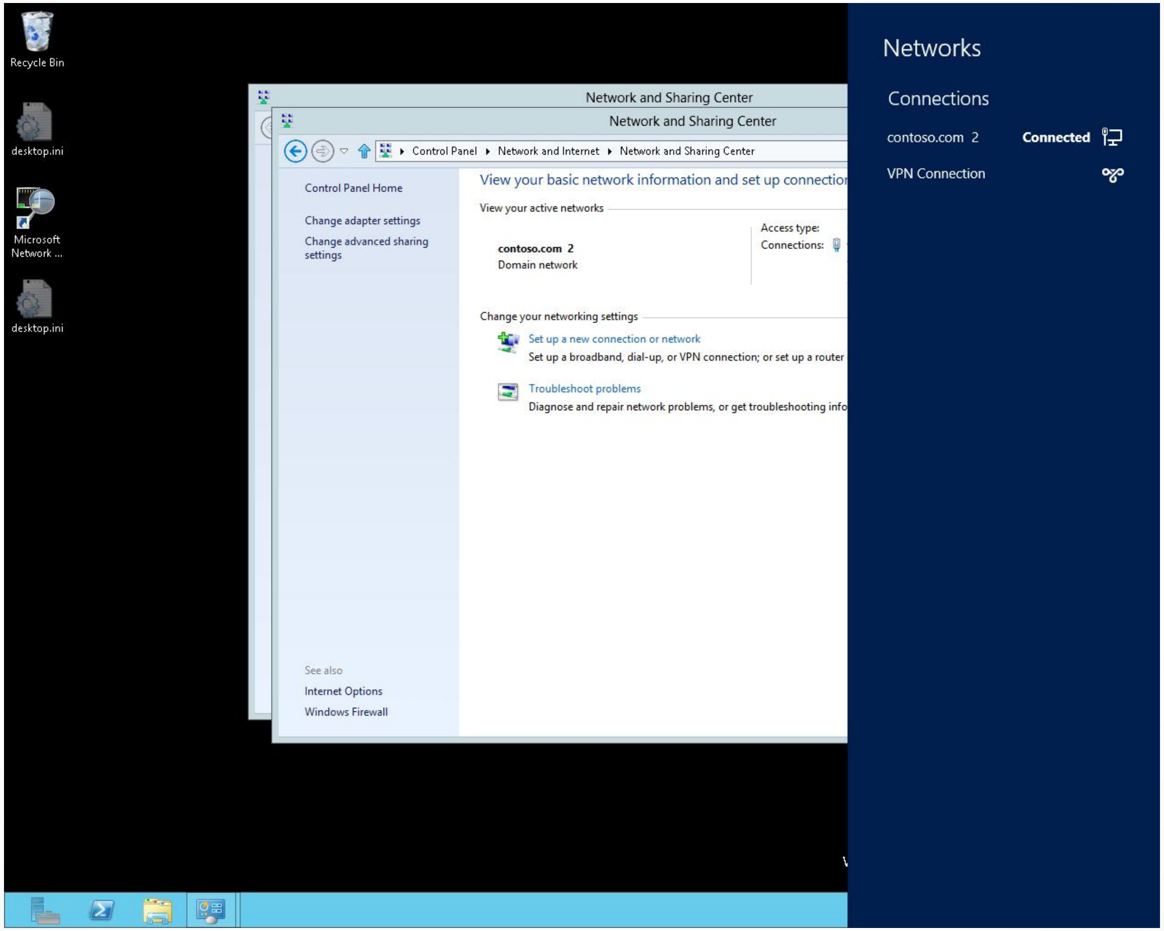
□ Use a smart card

☑ Remember my credentials

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Entering the Internet address and destination name

Create a VPN Tunnel



Network and Sharing Center

Network and Sharing Center

Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connectio

View your active networks

contoso.com 2
Domain network

Access type:
Connections:

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting info

See also

Internet Options

Windows Firewall

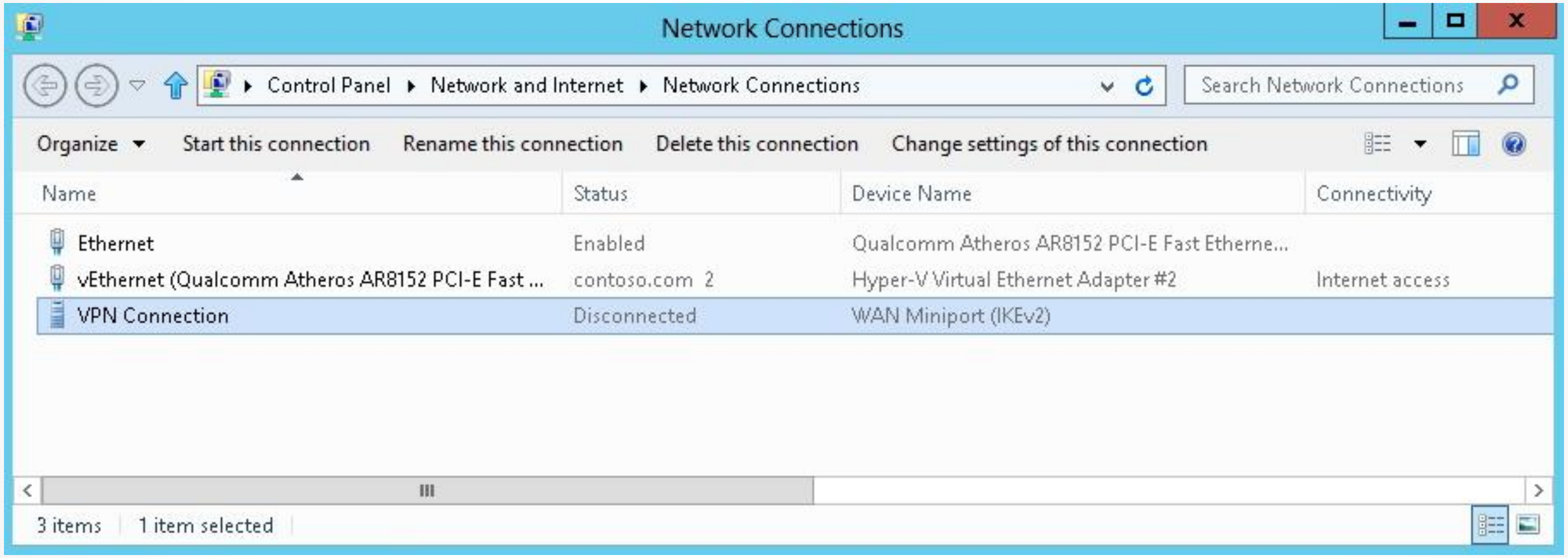
Networks

Connections

contoso.com 2	**Connected**
VPN Connection	

Connecting to a network connection after the connections are created

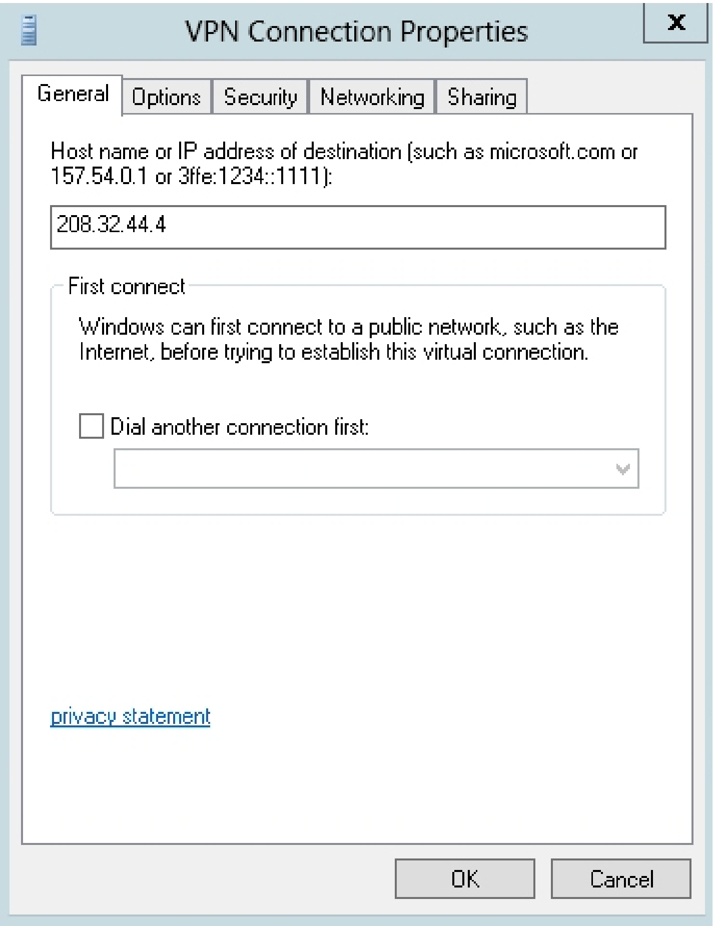
Create a VPN Tunnel


Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize ▾
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
3 items
1 item selected

Name	Status	Device Name	Connectivity
Ethernet	Enabled	Qualcomm Atheros AR8152 PCI-E Fast Etherne...	
vEthernet (Qualcomm Atheros AR8152 PCI-E Fast ...	contoso.com 2	Hyper-V Virtual Ethernet Adapter #2	Internet access
VPN Connection	Disconnected	WAN Miniport (IKEv2)	

Viewing network connections in the Network and Sharing Center

Create a VPN Tunnel



Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

208.32.44.4

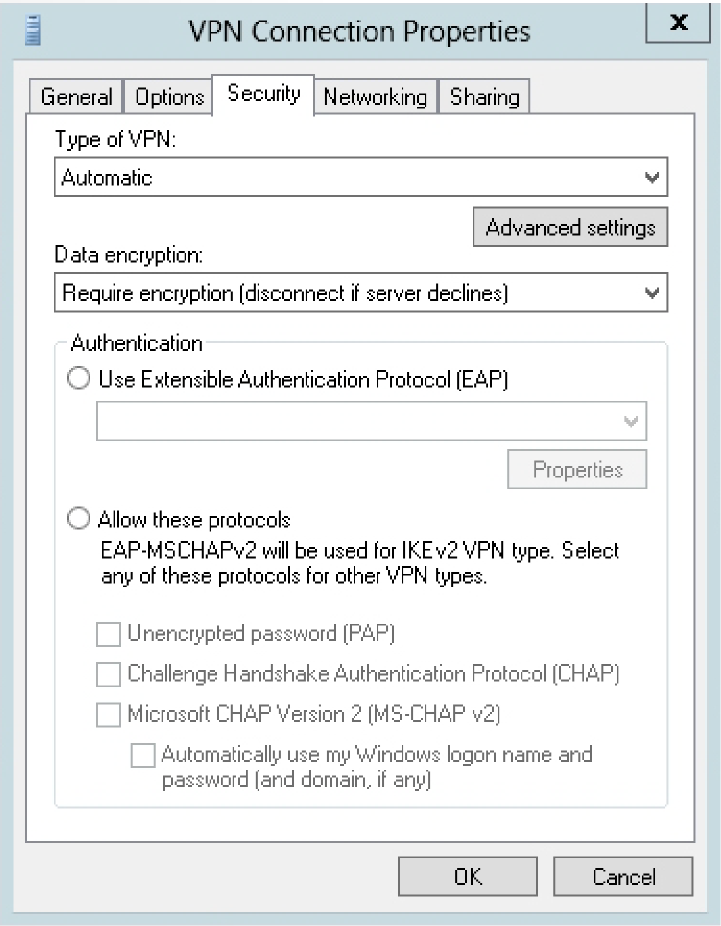
First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:

Specifying the hostname or IP address of the VPN server on the General tab

Create a VPN Tunnel



Type of VPN: Automatic

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

○ Allow these protocols

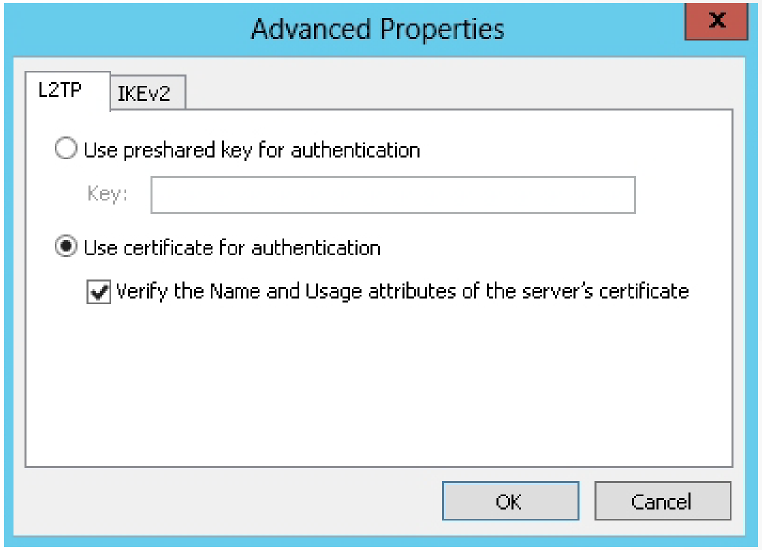
EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



○ Use preshared key for authentication

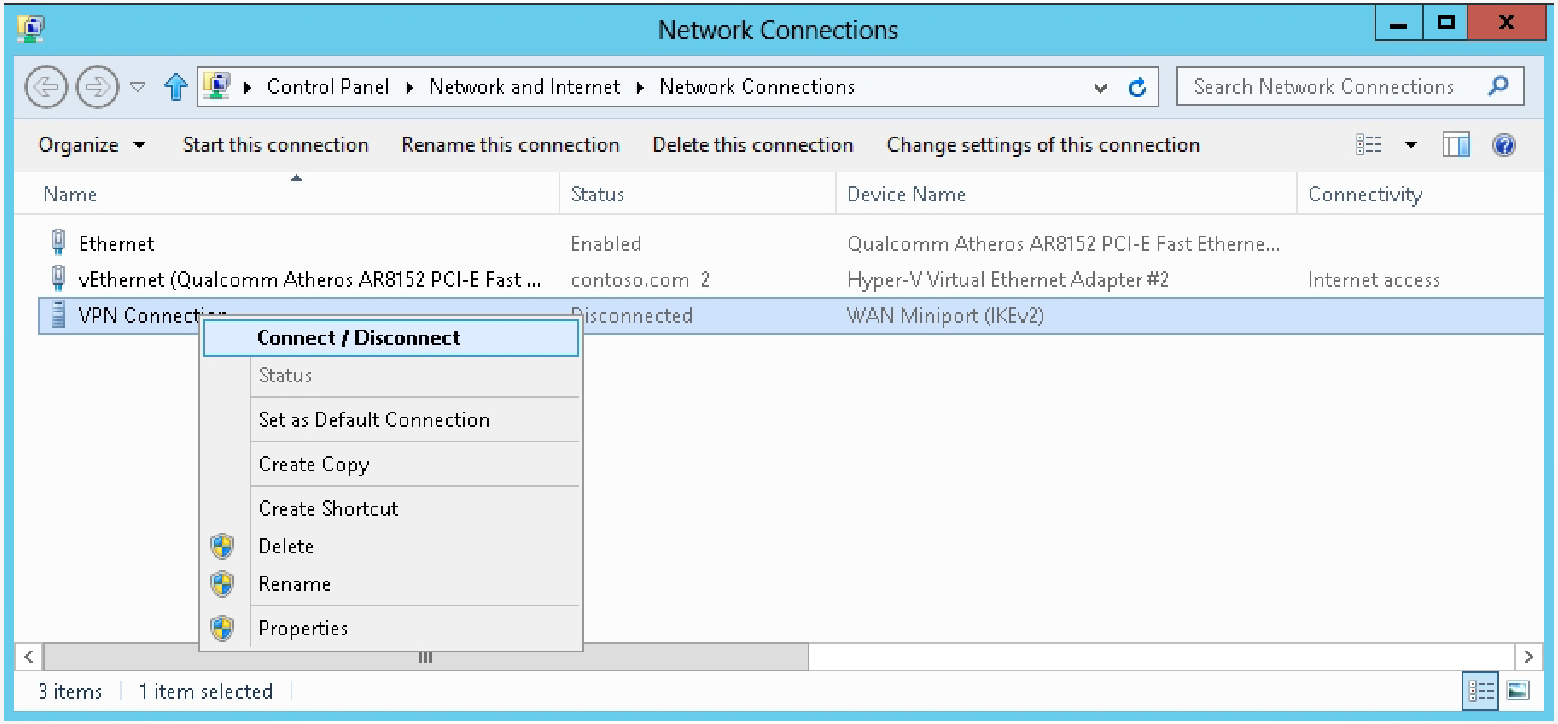
Key:

● Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

Security tab

Create a VPN Tunnel



Name	Status	Device Name	Connectivity
Ethernet	Enabled	Qualcomm Atheros AR8152 PCI-E Fast Etherne...	
vEthernet (Qualcomm Atheros AR8152 PCI-E Fast ...	contoso.com 2	Hyper-V Virtual Ethernet Adapter #2	Internet access
VPN Connecti	Disconnected	WAN Miniport (IKEv2)	

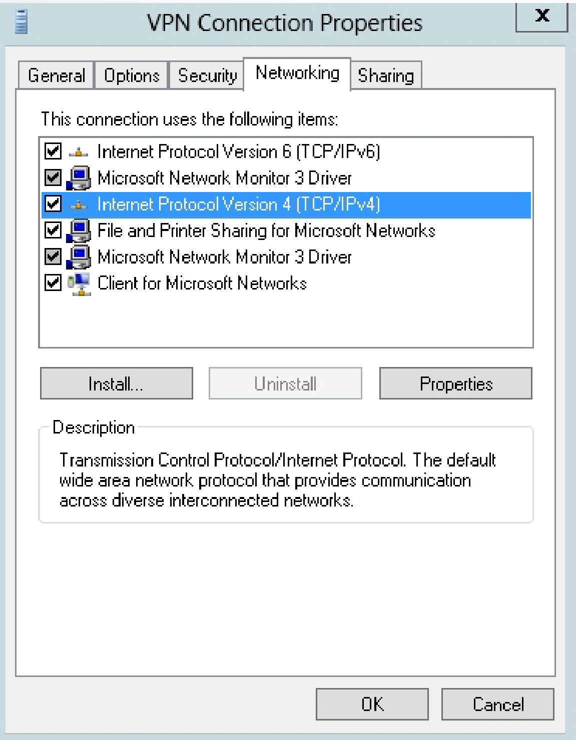
3 items | 1 item selected

Connecting to a VPN server

Configuring Split Tunneling

- Can route a client's Internet browsing through a home Internet connection rather than going through the corporate network.
- Disable the *Use Default Gateway on Remote Network* option.
- Disabling this option is called using a ***split tunnel***.

Enable a Split Tunnel



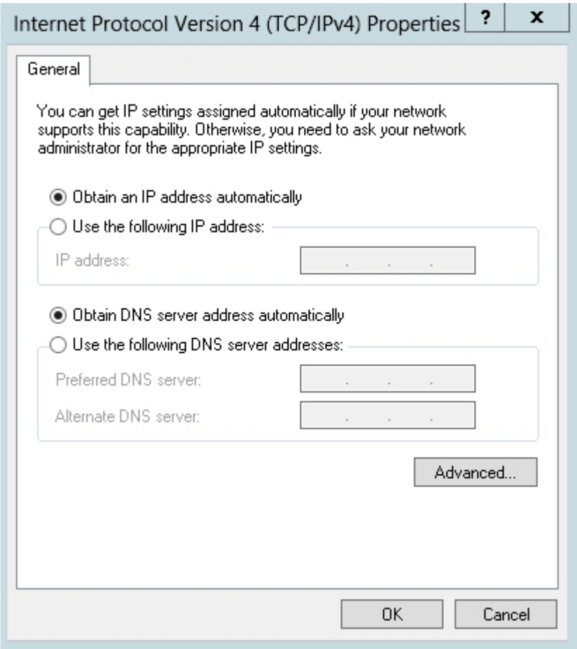
VPN Connection Properties

This connection uses the following items:

☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Microsoft Network Monitor 3 Driver
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ File and Printer Sharing for Microsoft Networks
☑ Microsoft Network Monitor 3 Driver
☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

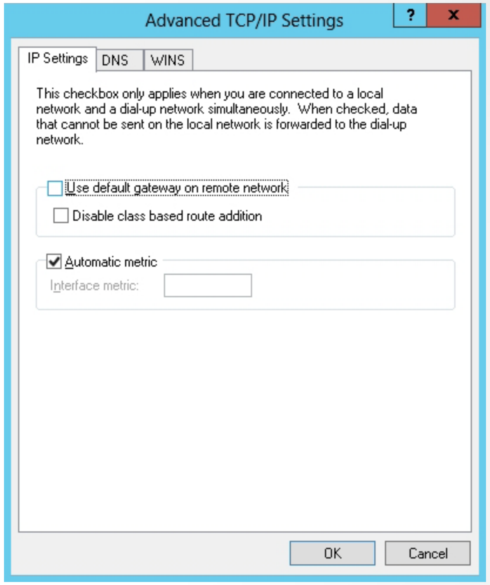


Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .



Advanced TCP/IP Settings

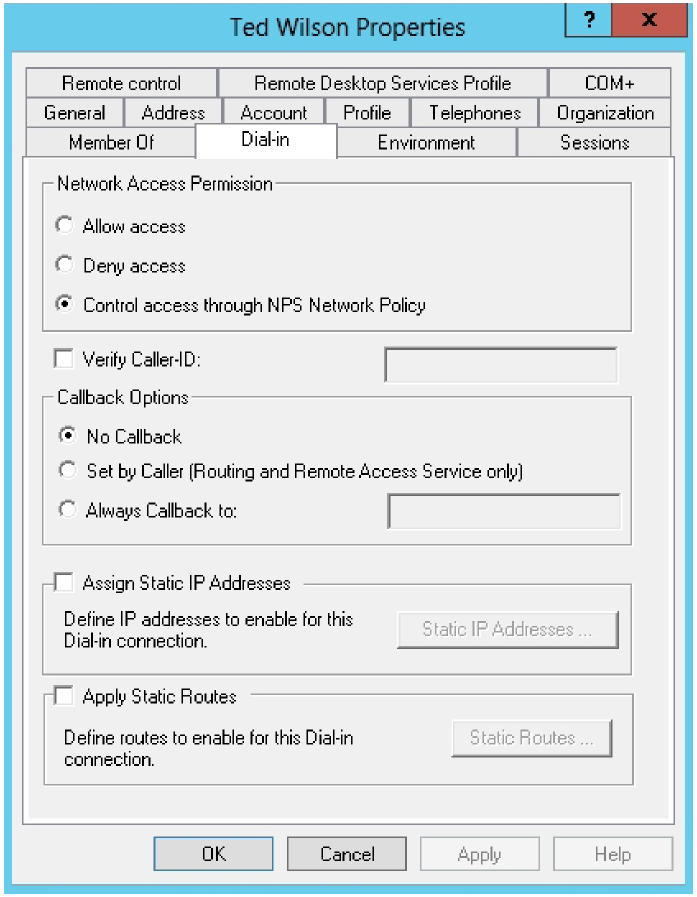
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

□ Use default gateway on remote network
□ Disable class based route addition

☑ Automatic metric
Interface metric:

Enabling split tunneling by enabling the Use Default Gateway on Remote Network option

Configuring Remote Dial-In Settings for Users



Ted Wilson Properties

Network Access Permission

○ Allow access

○ Deny access

● Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

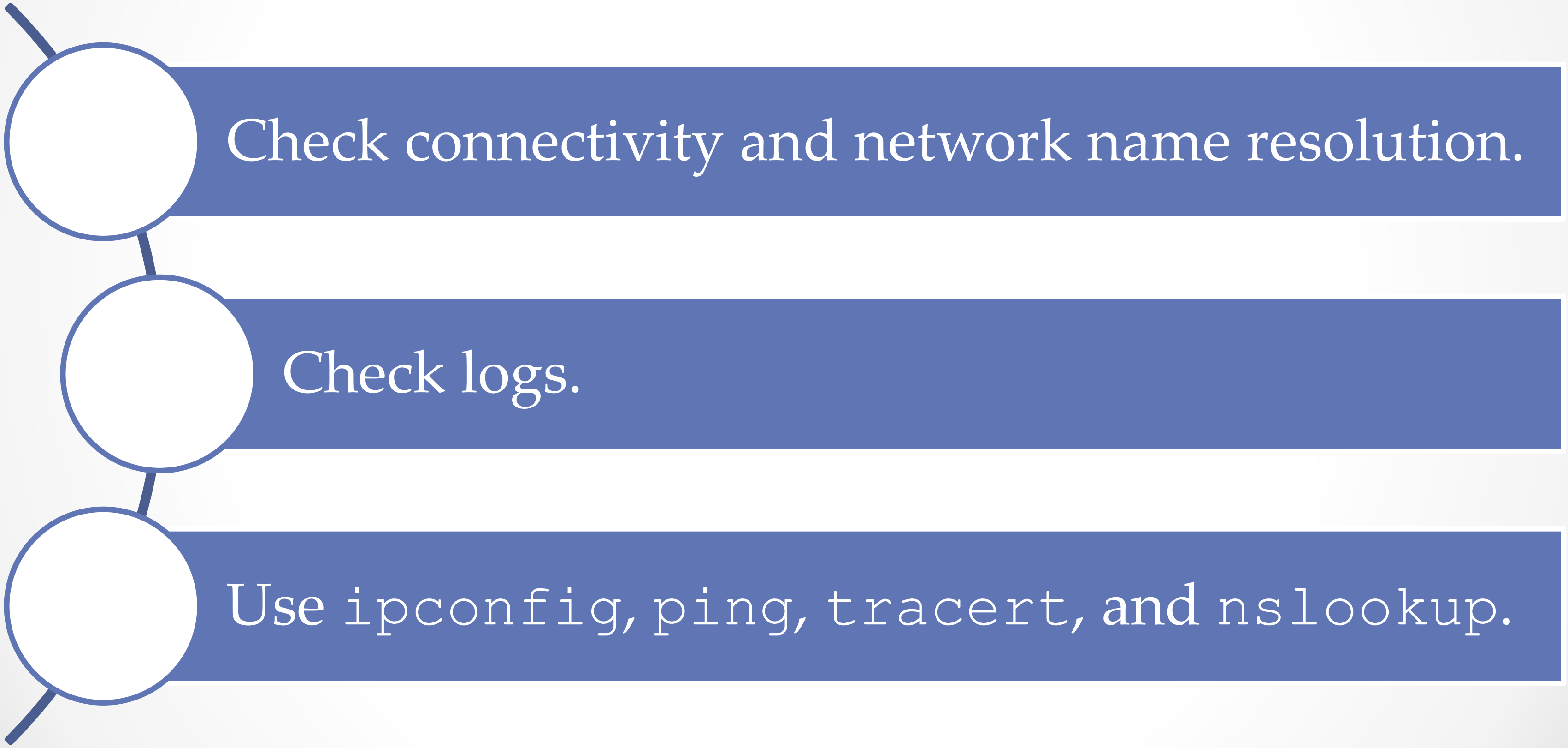
Static IP Addresses ...

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Static Routes ...

Troubleshooting Remote Access Problems



Check connectivity and network name resolution.

Check logs.

Use `ipconfig`, `ping`, `tracert`, and `nslookup`.

Network Address Translation (NAT)

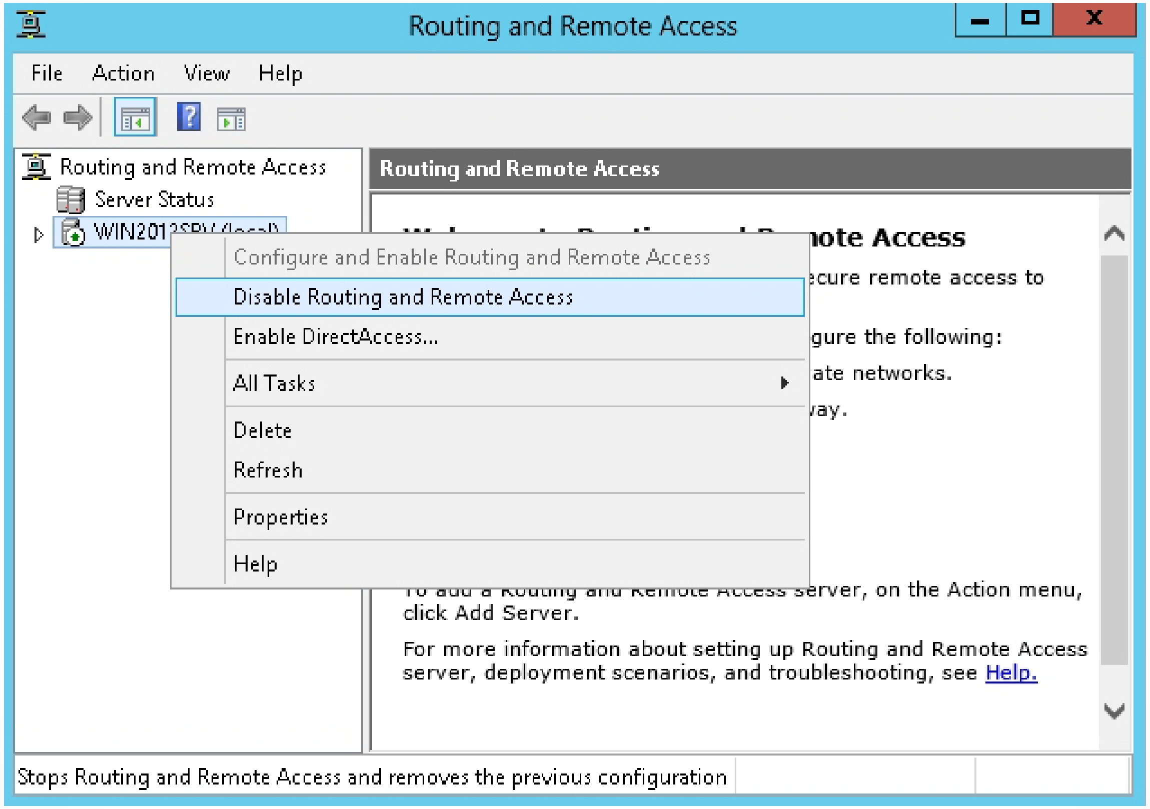
- Enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
- As a result, you can:
  - Provide a type of firewall by hiding internal IP addresses.
  - Enable multiple internal computers to share a single external public IP address.

Network Address Translation (NAT)

The private network addresses as expressed in RFC 1918:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

Disable Routing and Remote Access



To add a Routing and Remote Access server, on the Action menu, click Add Server.

For more information about setting up Routing and Remote Access server, deployment scenarios, and troubleshooting, see Help.

Stops Routing and Remote Access and removes the previous configuration

Disabling Routing and Remote Access

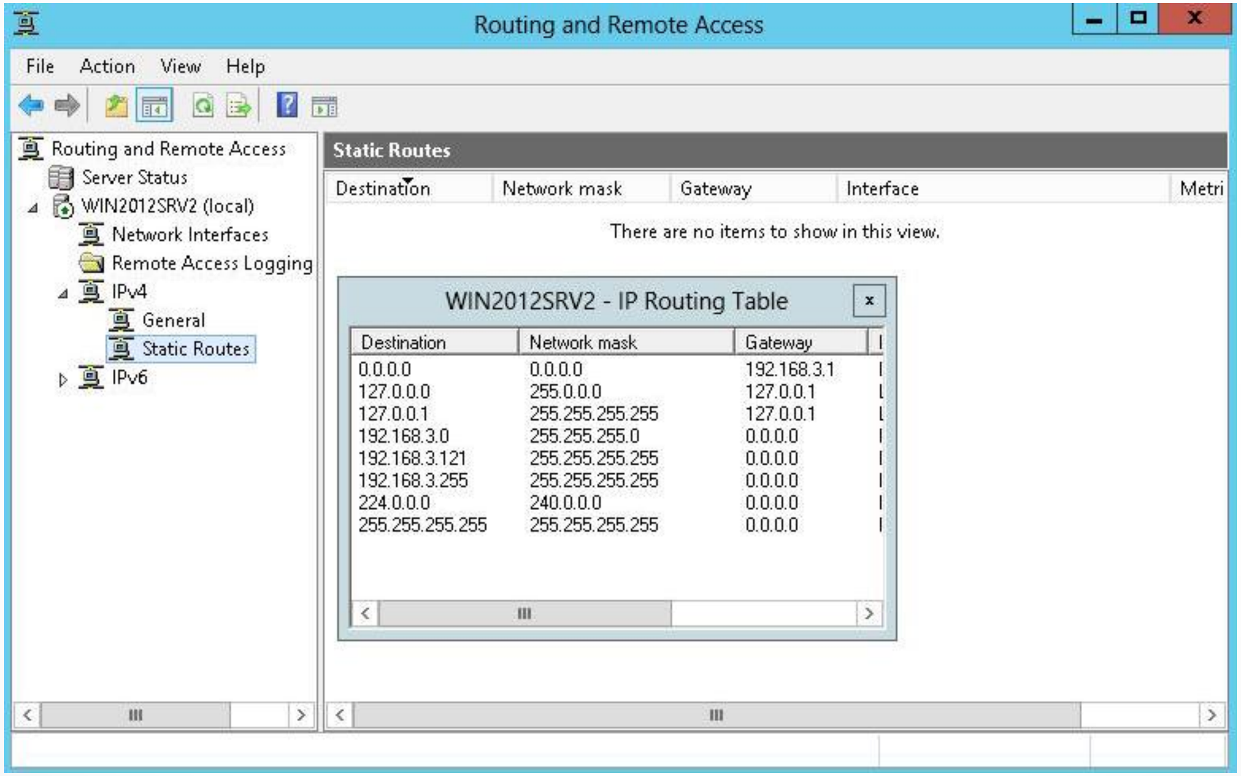
Routing Terms

- **Routing**: The process of selecting paths in a network where data will be sent.
- **Routers**: Operate at the OSI Reference Model Layer 3, Network layer.
- **Layer 2 switches**: Operate at the layer 2 OSI model and are used to connect a host to a network by performing packet switching that allows traffic to be sent only to where it needs to be sent based on mapping MAC addresses of local devices.
- **Layer 3 switches**: Can perform layer 2 switching, but also perform routing based on IP addresses within an organization. Cannot be used for directly connecting WAN connections.

Routing Terms

- **Routing table**: A data table stored in a router or networked computer that lists the routes of particular network distances and the associated metrics or distances associated with those routes.
- **Static route**: A route created manually in a routing table.
- **Dynamic route**: A route created dynamically based on the current routing topology. Created with a routing protocol such as Routing Information Protocol (RIP).

Managing Static Routes



Destination	Network mask	Gateway	Interface	Metri

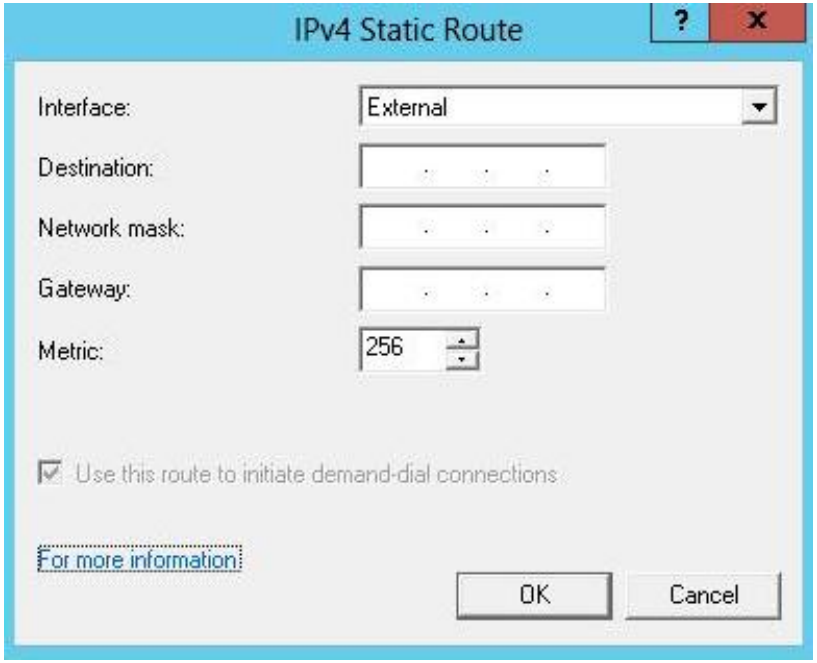
There are no items to show in this view.

WIN2012SRV2 - IP Routing Table

Destination	Network mask	Gateway
0.0.0.0	0.0.0.0	192.168.3.1
127.0.0.0	255.0.0.0	127.0.0.1
127.0.0.1	255.255.255.255	127.0.0.1
192.168.3.0	255.255.255.0	0.0.0.0
192.168.3.121	255.255.255.255	0.0.0.0
192.168.3.255	255.255.255.255	0.0.0.0
224.0.0.0	240.0.0.0	0.0.0.0
255.255.255.255	255.255.255.255	0.0.0.0

Displaying static routes using RRAS

Create a New Static Route using RRAS



IPv4 Static Route

Interface: External

Destination: . . .

Network mask: . . .

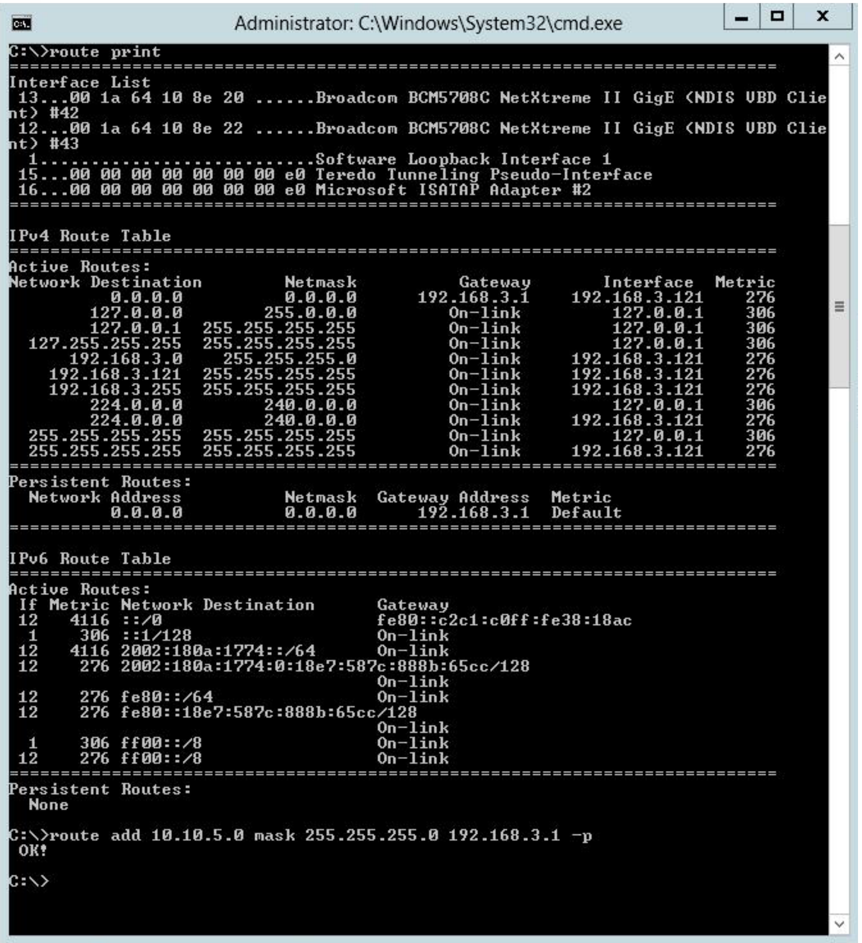
Gateway: . . .

Metric: 256

☑ Use this route to initiate demand-dial connections

Defining an IPv4 static route

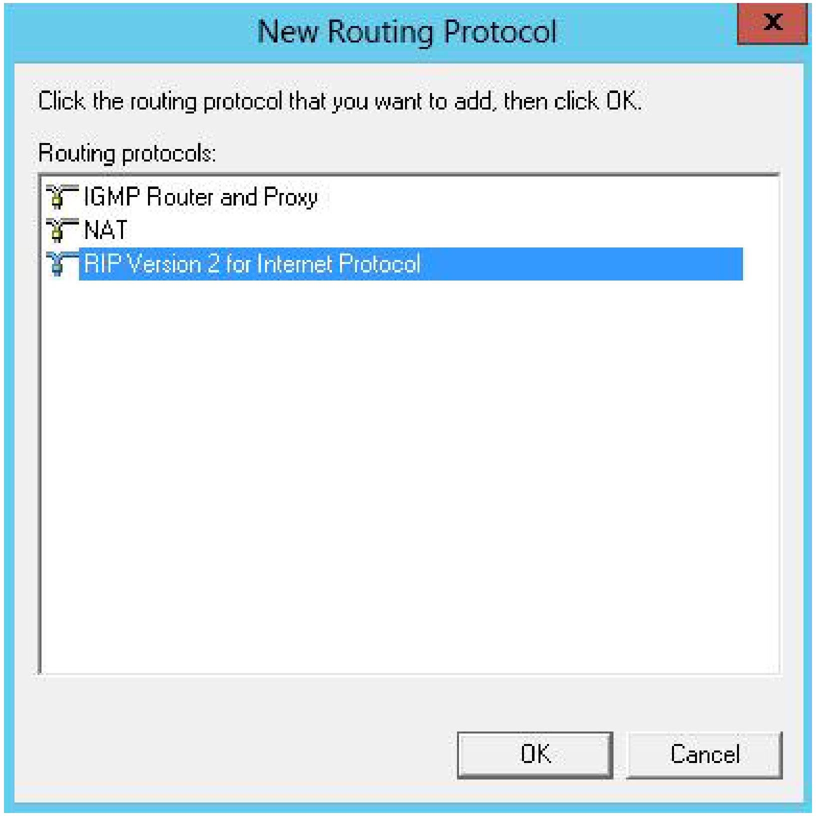
Create a New Static Route using RRAS



```
C:\>route print
===========================================================================
Interface List
 13...00 1a 64 10 8e 20 ......Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Clie
nt) #42
 12...00 1a 64 10 8e 22 ......Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Clie
nt) #43
  1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.3.1    192.168.3.121    276
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.3.0    255.255.255.0         On-link     192.168.3.121    276
    192.168.3.121  255.255.255.255         On-link     192.168.3.121    276
    192.168.3.255  255.255.255.255         On-link     192.168.3.121    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.3.121    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.3.121    276
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.3.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 12   4116 ::/0                     fe80::c2c1:c0ff:fe38:18ac
  1    306 ::1/128                  On-link
 12   4116 2002:180a:1774::/64      On-link
 12    276 2002:180a:1774:0:18e7:587c:888b:65cc/128
                                    On-link
 12    276 fe80::/64                On-link
 12    276 fe80::18e7:587c:888b:65cc/128
                                    On-link
  1    306 ff00::/8                 On-link
 12    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\>route add 10.10.5.0 mask 255.255.255.0 192.168.3.1 -p
 OK!

C:\>
```

Route command

Configure RIP



New Routing Protocol

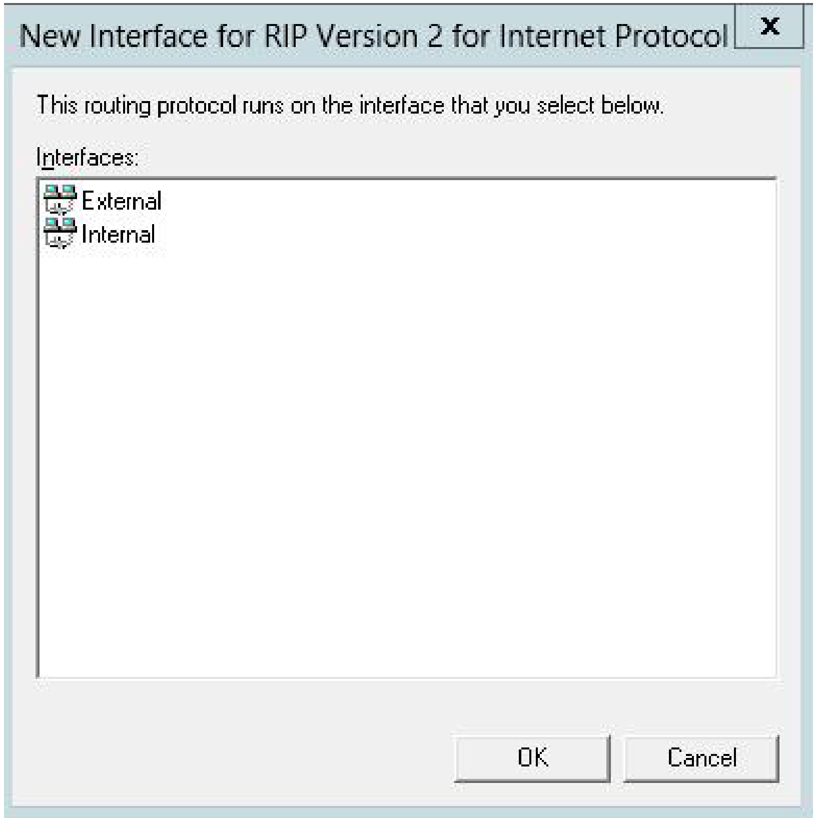
Click the routing protocol that you want to add, then click OK.

Routing protocols:

- IGMP Router and Proxy
- NAT
- RIP Version 2 for Internet Protocol

Specifying a new routing protocol

Configure RIP



New Interface for RIP Version 2 for Internet Protocol

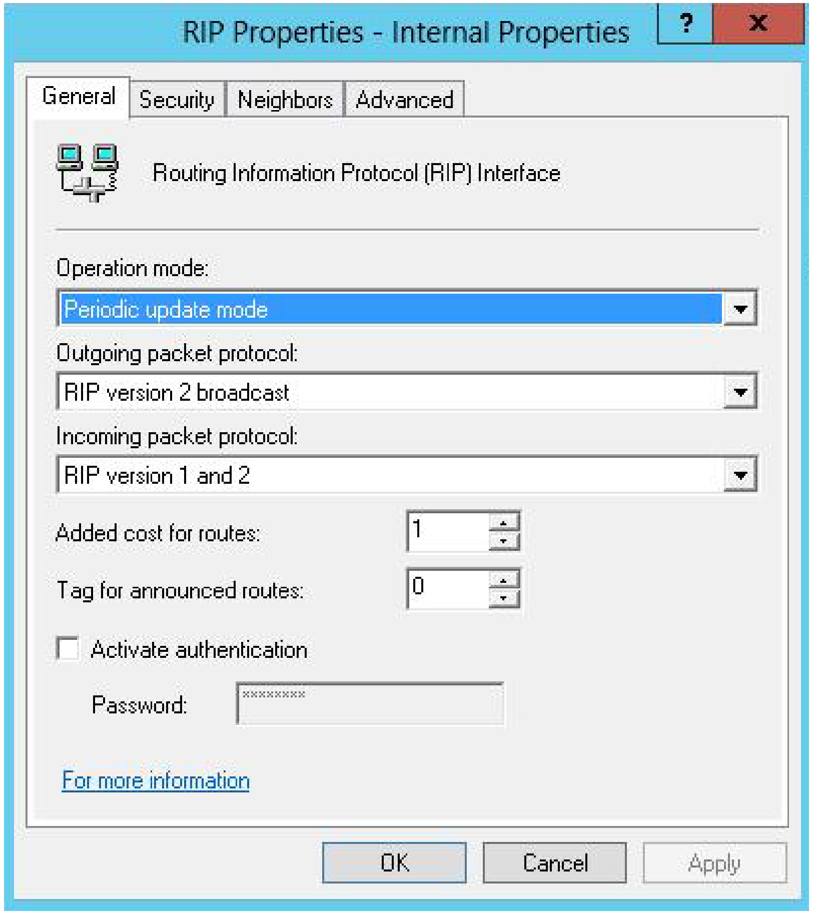
This routing protocol runs on the interface that you select below.

Interfaces:

- External
- Internal

Specifying the new interface for RIP Version 2 for Internet Protocol

Configure RIP


RIP Properties - Internal Properties
?
x
General
Security
Neighbors
Advanced
Routing Information Protocol (RIP) Interface
OK
Cancel
Apply

Operation mode: Periodic update mode

Outgoing packet protocol: RIP version 2 broadcast

Incoming packet protocol: RIP version 1 and 2

Added cost for routes: 1

Tag for announced routes: 0

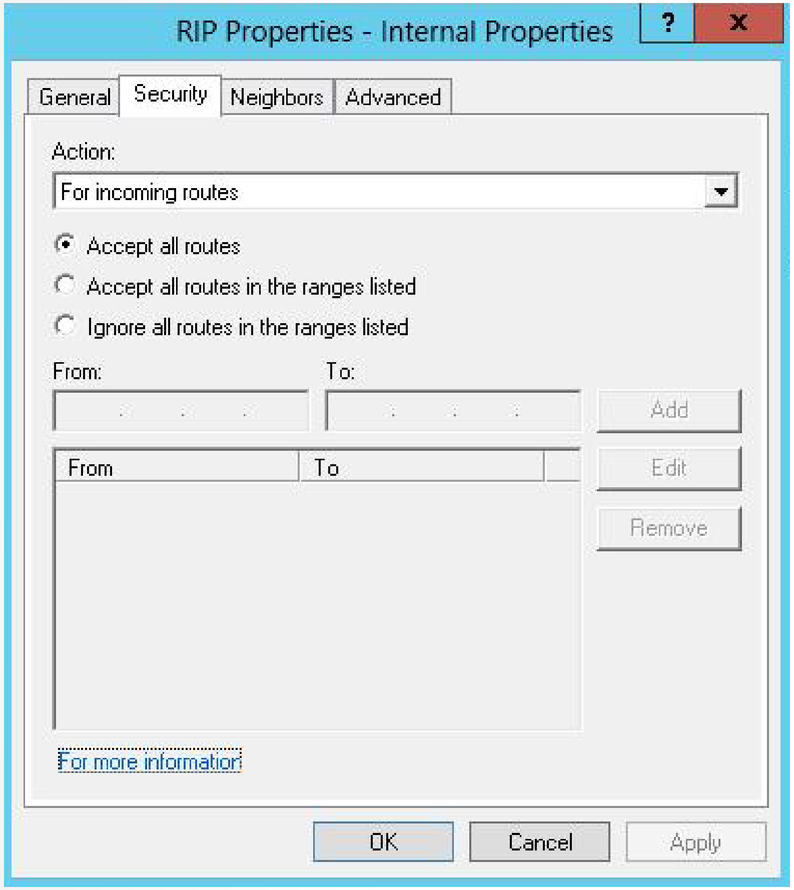
□ Activate authentication

Password: *********

For more information

Configuring the RIP Properties

Configure RIP



RIP Properties - Internal Properties

Action:

For incoming routes

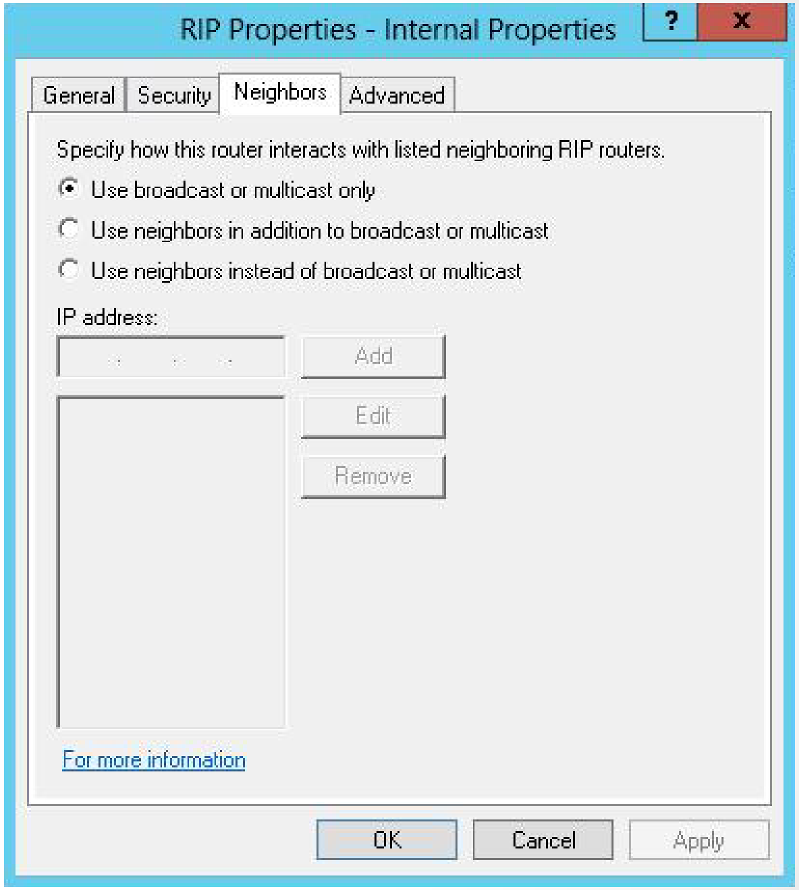
● Accept all routes

○ Accept all routes in the ranges listed

○ Ignore all routes in the ranges listed

From: To:

From	To



RIP Properties - Internal Properties

Specify how this router interacts with listed neighboring RIP routers.

● Use broadcast or multicast only

○ Use neighbors in addition to broadcast or multicast

○ Use neighbors instead of broadcast or multicast

IP address:

Configuring the RIP Security and Neighbors tabs

Demand-Dial Routing

- ***Demand-dial routing*** is a connection to a remote site that is activated when data is sent to the remote site and disconnected when there is no more data to be sent.
- Can reduce connection costs.

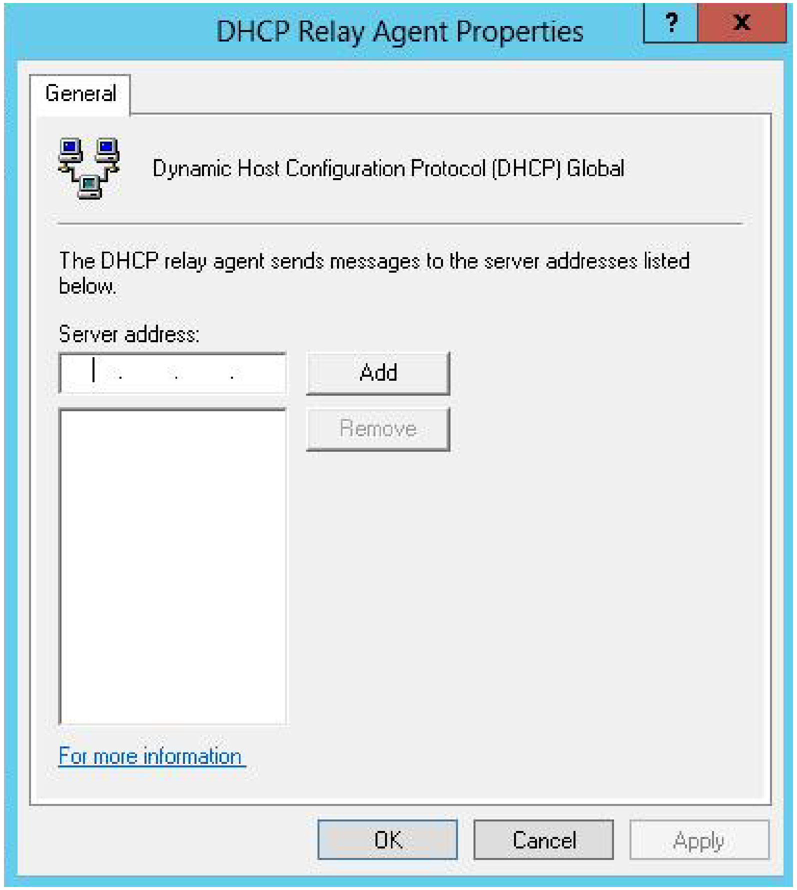
Configuring Demand-Dial Routing

1. Right-click the server, select *Properties* and select the *General* tab.
2. Select *LAN and demand-dial routing*.
3. Right-click *Network Interfaces*.
4. Select *New Demand-dial Interface* to go through a wizard to define the dial-up connection or VPN connection.

DHCP Relay Agent

- DHCP requires a range of IP addresses that can be distributed.
- A ***scope*** defines a single physical subnet on a network to which DHCP services are offered.
- DHCP server has to be physically connected to the subnet, or you have to install a DHCP Relay Agent or DHCP Helper on the subnet that relays the DHCP requests to the DHCP server.

Configure the DHCP Relay Agent



Dynamic Host Configuration Protocol (DHCP) Global

The DHCP relay agent sends messages to the server addresses listed below.

Server address: . . .

Specifying the DHCP Server that the DHCP Relay Agent Relays To

Lesson Summary

- Remote access server (RAS) enables users to connect remotely to a network using various protocols and connection types.
- To provide remote access server, Microsoft includes Routing and Remote Access (RRAS), which provides a Virtual Private Network (VPN), a dial-up remote access server, and Network Address Translation (NAT).
- VPNs link two computers or network devices through a wide-area network (WAN) such as the Internet.
- To provide constant connectivity, use Internet Key Exchange version 2 (IKEv2).
- Routing your Internet browsing through your home Internet connection rather than the corporate network when using a VPN connection is called split tunneling.

Lesson Summary

- A remote access connection must be authorized by the server running Network Policy Server (NPS), RRAS role service, or other third-party RADIUS server.
- Network address translation (NAT) is used with masquerading to hide an entire address space behind a single IP address.
- Routing is the process of selecting paths in a network where data will be sent.
- Microsoft Windows supports the Routing Information Protocol (RIP) through RRAS.
- Routing tables are manually created with static routes or are dynamically created with routing protocols such as RIP.
- RRAS also supports demand-dial routing.