Lesson 10: Configuring VPN and Routing

MOAC 70-411: Administering Windows Server 2012
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

### Select server roles

**Before You Begin**
- Installation Type
- Server Selection

### Server Roles

- Features
- Confirmation
- Results

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

<table>
<thead>
<tr>
<th>Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Certificate Services</td>
<td>Provides seamless connectivity, always on and always managed experience based on DirectAccess.</td>
</tr>
<tr>
<td>Active Directory Domain Services</td>
<td>Provides traditional VPN services including site-to-site (branch-office or cloud) connectivity.</td>
</tr>
<tr>
<td>Active Directory Federation Services</td>
<td>Provides traditional routing capabilities including NAT, and other connectivity options.</td>
</tr>
<tr>
<td>Active Directory Lightweight Directory Services</td>
<td></td>
</tr>
<tr>
<td>Active Directory Rights Management Services</td>
<td></td>
</tr>
<tr>
<td>Application Server</td>
<td></td>
</tr>
<tr>
<td>DHCP Server</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td></td>
</tr>
<tr>
<td>Fax Server</td>
<td></td>
</tr>
<tr>
<td>File And Storage Services</td>
<td></td>
</tr>
<tr>
<td>Hyper-V</td>
<td></td>
</tr>
<tr>
<td>Network Policy and Access Services</td>
<td></td>
</tr>
<tr>
<td>Print and Document Services</td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td>Provides seamless connectivity, always on and always managed experience based on DirectAccess.</td>
</tr>
<tr>
<td>Remote Desktop Services</td>
<td></td>
</tr>
</tbody>
</table>

**Selecting the Remote Access role**
Install Remote Access Role

Adding additional features for the Remote Access role
Install Remote Access Role

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

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

© 2013 John Wiley & Sons, Inc.
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

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

Opening the Routing and Remote Access console
Configure Dial-Up Remote Access

Configuring and enabling RRAS
Configure Dial-Up Remote Access

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

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Broadcom BCM5708C...</td>
<td>10.1.1.25</td>
</tr>
<tr>
<td>Internal</td>
<td>Broadcom BCM5708C...</td>
<td>192.168.3.121</td>
</tr>
</tbody>
</table>

Tick 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

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**

For more information

Specifying the method of IP address assignment
Configure Dial-Up Remote Access

Using the New IPv4 Address Range dialog box

© 2013 John Wiley & Sons, Inc.
# Configure Dial-Up Remote Access

## Routing and Remote Access Server Setup Wizard

### Managing Multiple Remote Access Servers

- **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](image)
  - **Yes, set up this server to work with a RADIUS server**

---

*For more information*

---

**Managing Multiple Remote Access Servers page**

© 2013 John Wiley & Sons, Inc.
Configure Dial-Up Remote Access

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

- 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.

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

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.

<table>
<thead>
<tr>
<th>Network interfaces:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>External</td>
</tr>
<tr>
<td>vEthernet (Broadcom BC...</td>
</tr>
</tbody>
</table>

- 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
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

For more information
Configure and Enable VPN Remote Access

Specifying the RADIUS Servers on the RADIUS Server Selection page
Configure and Enable VPN Remote Access

Enabling routing and remote access with the General tab
Configure and Enable VPN Remote Access

Using the Security tab

© 2013 John Wiley & Sons, Inc.
Configure and Enable VPN Remote Access

Using the IPv4 tab
Configure and Enable VPN Remote Access

Specifying the number of ports
Create a VPN Tunnel

Opening the Network and Sharing Center
Create a VPN Tunnel

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

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

Entering the Internet address and destination name

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.
Create a VPN Tunnel

Connecting to a network connection after the connections are created
Create a VPN Tunnel

Viewing network connections in the Network and Sharing Center
Create a VPN Tunnel

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

Security tab
Create a VPN Tunnel

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

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

- Callback Options
  - No Callback
  - Set by Caller (Routing and Remote Access Service only)
  - Always Callback to: [Field]

- Assign Static IP Addresses
  - Define IP addresses to enable this Dial-in connection.

- Apply Static Routes
  - Define routes to enable this Dial-in connection.
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:
  o Provide a type of firewall by hiding internal IP addresses.
  o 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

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

Displaying static routes using RRAS
Create a New Static Route using RRAS

Defining an IPv4 static route
Create a New Static Route using RRAS

Route command
Configure RIP

Specifying a new routing protocol
Specify the new interface for RIP Version 2 for Internet Protocol
Configure RIP

Configuring the RIP Properties
Configure RIP

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

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.
Copyright 2013 John Wiley & Sons, Inc.
All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.