Module 6

Configuring and Troubleshooting Routing and Remote Access

Contents:

Lesson 1: Configuring Network Access  6-3
Lesson 2: Configuring VPN Access  6-12
Lesson 3: Overview of Network Policies  6-22
Lesson 4: Overview of the Connection Manager Administration Kit  6-27
Lesson 5: Troubleshooting Routing and Remote Access  6-33
Lab: Configuring and Managing Network Access  6-41
Module Overview

- Configuring Network Access
- Configuring VPN Access
- Overview of Network Policies
- Overview of the Connection Manager Administration Kit
- Troubleshooting Routing and Remote Access

This module explains how to configure and troubleshoot Routing and Remote Access in Windows Server® 2008.
Lesson 1
Configuring Network Access

Windows Server 2008 includes Network Policy and Access Services, which offers scenario solutions for connectivity, such as:

- Network Access Protection (NAP). With NAP, system administrators can establish and automatically enforce health policies, which include software requirements, security update requirements, required computer configurations, and other settings.

- Secure wireless and wired solutions based on the 802.1X enforcement method.

- Remote access solutions, including virtual private network (VPN), traditional dial-up, and full-featured software routers.

- Central network policy management with Remote Authentication Dial-In User Service (RADIUS) server and proxy.
Components of a Network Access Services Infrastructure

Key Points
The underlying infrastructure in a complete Network Access Service in Windows Server 2008 typically includes the following components:

- VPN Server
- Active Directory® directory services
- Dynamic Host Configuration Protocol (DHCP) Server
- NAP Health Policy Server
- Health Registration Authority
- Remediation Servers

Additional Reading
- Help topic: Remote Access
What is the Network Policy and Access Services Role?

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Server</td>
<td>The Microsoft implementation of Radius Server and proxy</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>Provides VPN and dial-up solutions for users, deploys full-featured software routers, and shares Internet connections across the intranet</td>
</tr>
<tr>
<td>Health Registration Authority</td>
<td>Issues health certificates to clients when using IPSec NAP enforcement</td>
</tr>
<tr>
<td>Host Credential Authorization Protocol</td>
<td>Integrates with Cisco network access control server</td>
</tr>
</tbody>
</table>

Key Points
The Network Policy and Access Services role in Windows Server 2008 provides the following network connectivity solutions:

- Network Access Protection (NAP)
- Secure wireless and wired access
- Remote access solutions
- Central network policy management with RADIUS server and proxy

Additional Reading
- Windows Server 2008 Technical Library
What is Routing and Remote Access?

- Used to provide remote users access to resources on a private network over Dial-up or VPN services
- Can be used to provide NAT services
- Can provide LAN and WAN routing services to connect network segments

Key Points
With Routing and Remote Access, you can deploy VPN and dial-up remote access services and multiprotocol LAN-to-LAN, LAN-to-wide area network (WAN), VPN, and network address translation (NAT) routing services.

You can deploy the following technologies during the installation of the Routing and Remote Access Service role:
- Remote Access Service
- Routing

Additional Reading
- Windows Server 2008 Technical Library
- Routing and Remote Access Service Help
Demonstration: How to Install Routing and Remote Access Services

In this demonstration, you will see how to install the Routing and Remote Access server role in Windows Server 2008
Network Authentication and Authorization

**Key Points**

The distinction between authentication and authorization is important in understanding why connection attempts are accepted or denied:

- **Authentication** is the verification of the connection attempt’s credentials. This process consists of sending the credentials from the remote access client to the remote access server in either plaintext or encrypted form by using an authentication protocol.

- **Authorization** is the verification that the connection attempt is allowed. Authorization occurs after successful authentication.

**Additional Reading**

- Authentication vs. authorization
- Introduction to remote access policies
Types of Authentication Methods

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.</td>
<td>The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.</td>
</tr>
<tr>
<td>CHAP</td>
<td>A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme to encrypt the response.</td>
<td>An improvement over PAP in that the password is not sent over the PPP link. Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.</td>
</tr>
<tr>
<td>MS-CHAPv2</td>
<td>An upgrade of MS-CHAP. Two-way authentication, also known as mutual authentication, is provided. The remote access client receives verification that the remote access server that it is dialing into has access to the user's password.</td>
<td>Provides stronger security than CHAP.</td>
</tr>
<tr>
<td>EAP</td>
<td>Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.</td>
<td>Offers the strongest security by providing the most flexibility in authentication variations.</td>
</tr>
</tbody>
</table>

Key Points

The authentication of access clients is an important security concern. Authentication methods typically use an authentication protocol that is negotiated during the connection establishment process. These protocols include:

- PAP
- CHAP
- MSCHAPv2
- EAP
- PEAP
Additional Reading

- Routing and Remote Access Service Help: Authentication
- Routing and Remote Access Service Help: Troubleshoot Remote Access
- Authentication Methods for use with IAS
Integrating DHCP Servers with the Routing and Remote Access Service

You can provide remote clients with IP configurations by using either:

- A static pool created on the Routing and Remote Access server for use with remote clients
- The corporate DHCP server located on the corporate LAN

DHCP servers running Windows Server 2008:

- Provide a predefined user class called the Default Routing and Remote Access Class
- Are useful for assigning options that are provided to Routing and Remote Access clients only

Key Points
You can deploy the DHCP Server service with the Routing and Remote Access service to provide remote access clients with a dynamically assigned IP address during connection. When you use these services together on the same server, the information provided during dynamic configuration is provided in a way that is different from typical DHCP configuration for LAN-based clients.

Additional Reading
Lesson 2
Configuring VPN Access

- What is a VPN Connection?
- Components of a VPN Connection
- Tunneling Protocols for a VPN Connection
- Configuration Requirements
- Demonstration: Configuring VPN Access
- Completing Additional Tasks
- Components of a Dial-up Connection

VPNs are point-to-point connections across a private or public network, such as the Internet. A VPN client uses special TCP/IP-based protocols, called tunneling protocols, to make a virtual call to a VPN server's virtual port.

In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet. The remote access server answers the call, authenticates the caller, and transfers data between the VPN client and the organization’s private network.
What is a VPN Connection?

Key Points

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header. The header provides routing information that enables the data to traverse the shared or public network to reach its endpoint. To emulate a private link, the data is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without encryption keys. The link in which the private data is encapsulated and encrypted is known as a VPN connection.

There are two types of VPN connections:

- Remote access VPN
- Site-to-site VPN
Components of a VPN Connection

Key Points
A VPN includes the following components:

- VPN client
- VPN server
- VPN tunnel
- Tunneled data
- Transit internetwork

Additional Reading
- Virtual Private Networks
Tunneling enables the encapsulation of a packet from one type of protocol within a different protocol's datagram. For example, VPN uses PPTP to encapsulate IP packets over a public network, such as the Internet. You also can configure a VPN solution based on PPTP, L2TP, or SSTP.

Key Points

Additional Reading

- Routing and Remote Access Service Help: VPN Tunneling Protocols
Configuration Requirements

VPN server configuration requirements include:

- Two network interfaces (public and private)
- IP Address allocation (static pool or DHCP)
- Authentication provider (NPS/Radius or the VPN server)
- DHCP relay agent considerations
- Membership in the Local Administrators group or equivalent

Key Points

Before you configure a remote access VPN server, you must:

- Determine which network interface connects to the Internet and which network interface connects to your private network.
- Determine whether remote clients will receive IP addresses from a Dynamic Host Configuration Protocol (DHCP) server on your private network or from the remote access VPN server that you are configuring.
- Determine whether you want connection requests from VPN clients to be authenticated by a Remote Authentication Dial-In User Service (RADIUS) server or by the remote access VPN server that you are configuring.
- Determine whether VPN clients can send DHCP messages to the DHCP server on your private network.
- Verify that all users have user accounts that are configured for dial-up access.
Additional Reading

- Routing and Remote Access Service Help: Configure a Remote Access VPN Server
Demonstration: Configuring VPN Access

In this demonstration, you will see how to:

- Configure user dial-in settings
- Configure Routing and Remote Access as a VPN server
- Configure a VPN client
Completing Additional Tasks

Key Points
After you complete the steps in the Add Roles Wizard and complete the configuration in Routing and Remote Access, your server is ready for use as a remote access VPN server.

Additional tasks that you can perform on your remote access/VPN server include:

- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure the number of VPN ports
- Create a Connection Manager profile for users
- Add Active Directory Certificate Services (AD CS)
- Increase remote access security
- Increase VPN security
Additional Reading

- Network Policy and Access Services
- Routing and Remote Access Service Help: Configure a Remote Access VPN Server
Components of a Dial-Up Connection

Key Points

Dial-up remote access is a remote access technology that is available as part of the Routing and Remote Access service that Windows Server 2008 includes.

With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit or a virtual circuit to a port on a remote access server. After the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

The physical or logical connection between the remote access server and the remote access client is facilitated by dial-up equipment installed at the remote access client, the remote access server, and the WAN infrastructure.

Additional Reading

- Routing and Remote Access Service Help: What is Dial-Up Networking?
Lesson 3
Overview of Network Policies

- What is a Network Policy?
- Process for Creating and Configuring a Network Policy
- How are Network Policies Processed?

When processing connection requests as a RADIUS server, Network Policy Server (NPS) performs both authentication and authorization for the connection request. NPS verifies the user’s or computer’s identity that is connecting to the network during the authentication process. NPS determines whether the user or computer is allowed to access the network during the authorization process.

To make this determination, NPS uses network policies that you configure in the NPS Microsoft Management Console (MMC) snap-in. To perform authorization, NPS also examines the dial-in properties of the user account in Active Directory.

**Note:** In Internet Authentication Service (IAS) in the Windows Server 2003 family of operating systems, network policies were called remote access policies.
What is a Network Policy?

A network policy consists of the following elements:

- Conditions
- Constraints
- Settings

Key Points
Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can, or cannot, connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that NPS performs client health checks during the authorization process.

Each network policy has four categories of properties:

- Overview
- Conditions
- Constraints
- Settings

Additional Reading
- Network Policy Server Help: Network Policy Properties
Process for Creating and Configuring a Network Policy

Key Points
NPS uses network policies, formerly named remote access policies, and the dial-in properties of user accounts, to determine whether to authorize a connection request to the network. You can configure a new network policy in either the NPS MMC snap-in or the Routing and Remote Access Service MMC snap-in.

To add a network policy using the Windows interface:

1. Open the NPS console and double-click Policies.
2. In the console tree, right-click Network Policies and then click New. The New Network Policy wizard opens.
3. Use the New Network Policy wizard to create a policy.
4. Configure the Network Policy properties.
Additional Reading

- Network Policy Sever Help: Network Policies
- Network Policy Sever Help: Add a Network Policy
How are Network Policies Processed?

Key Points
When NPS performs authorization of a connection request, it compares the request with each network policy in the ordered list of policies, starting with the first policy and moving down the list.

Additional Reading
- Network Policy Server Help: Add a Network Policy
Lesson 4
Overview of the Connection Manager Administration Kit

- What is the Connection Manager Administration Kit?
- Demonstration: Installing CMAK
- Process for Configuring a Connection Profile
- Demonstration: Creating a Connection Profile
- Distributing the Connection Profile to Users

The Connection Manager Administration Kit (CMAK) allows administrators to customize users’ remote-connection options by creating pre-defined connections to remote servers and networks. The CMAK wizard creates an executable file, which you can distribute in many ways or include during deployment activities as part of the operating-system image.
What is the Connection Manager Administration Kit?

**The Connection Manager Administration Kit:**

- Allows you to customize users’ remote connection experience by creating pre-defined connections on remote servers and networks
- Creates an executable file that can be run on a client computer to establish a network connection that you have designed
- Reduces Help Desk requests related to the configuration of RAS connections
- Assists in problem resolution because the configuration is known
- Reduces the likelihood of user errors when configuring their own connection objects

**Key Points**

The CMAK is a tool that you can use to customize the remote connection experience for users on your network by creating pre-defined connections to remote servers and networks. Use the CMAK wizard to create and customize a connection for your users.

**Additional Reading**

- CMAK Help: Welcome to the Connection Manager Administration Kit
Demonstration: Installing CMAK

In this demonstration, you will see how to use the Server Manager tool to install the Connection Manager Administration Kit
Process for Configuring a Connection Profile

The CMAK Connection Profile Wizard assists in the process of creating custom connection profiles for users

Use the CMAK Connection Profile Wizard to configure:

- The target operating system
- Support for VPN
- Support for Dial-up, including the custom phone book
- Proxy
- Custom Help file
- Custom support information

Key Points
You can configure a new or existing connection profile using the CMAK wizard. Each page of the wizard allows you to complete another step of the process.

Note: For complete information about creating a connection profile, see the CMAK Operations Guide.

Additional Reading
- CMAK Operations Guide
- Connection Manager Administration Kit Help: Run the CMAK Wizard to Create a Connection Profile
Demonstration: Creating a Connection Profile

In this demonstration, you will see how to use the Connection Manager Administration Kit to create a connection profile.
Distributing the Connection Profile to Users

The connection profile can be distributed to users in the following ways:

- As part of an image for new computers
- On removable media for the user to install manually
- With software distribution tools, such as Systems Management Server or System Center Configuration Manager 2007

Key Points

The CMAK wizard compiles the connection profile into a single executable file with an .exe file name extension. You can deliver this file to users through any method that is available to you. Some methods to consider are:

- Include the connection profile as part of the image included with new computers.
- Deliver the connection profile on removable media for the user to install manually.
- Deliver the connection profile with automated software distribution tools.

Additional Reading

- Connection Manager Administration Kit Help: Distribute Your Connection Profile to Your Users
Troubleshooting the Routing and Remote Access Service can be a very time-consuming task. The issues may be varied and not easily identified. Given that you may be using dial-up, dedicated, leased or public-based networks to satisfy your remote-connectivity solution, you must perform troubleshooting in a methodical, step-by-step process.
TCP/IP Troubleshooting Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipconfig</td>
<td>Displays current TCP/IP network configuration values, updates, or releases; DHCP allocated leases; and used to display, register, or flush DNS names</td>
</tr>
<tr>
<td>Ping</td>
<td>Sends ICMP Echo Request messages to verify that TCP/IP is configured correctly and that a TCP/IP host is available</td>
</tr>
<tr>
<td>Pathping</td>
<td>Displays a path of a TCP/IP host and packet losses at each router along the way</td>
</tr>
<tr>
<td>Tracert</td>
<td>Displays the path of a TCP/IP host</td>
</tr>
</tbody>
</table>

**Key Points**

Windows Server 2008 includes basic and advanced TCP/IP diagnostic tools that you can use to troubleshoot TCP/IP.

Basic TCP/IP diagnostic tools include:

- Network Diagnostics in Help and Support
- Network Connections folder
- Ipconfig command
- Ping command
Advanced TCP/IP diagnostic tools include:

- Hostname command
- Nbtstat command
- Pathping command
- Route command
- Tracert command

Additional Reading

- How to troubleshoot TCP/IP connectivity with Windows XP
Authentication and Accounting Logging

There are three types of logging for Network Policy Server:

- Event logging for auditing and troubleshooting connection attempts
- Logging authentication and accounting requests to a local file
- Logging authentication and accounting requests to a SQL server database

Key Points
You can configure NPS to perform RADIUS accounting for user authentication requests, **Access-Accept** messages, **Access-Reject** messages, accounting requests and responses, and periodic status updates. You can use this procedure to configure the log files in which you want to store the accounting data.

Additional Reading
- Help topic: Configure Log File Properties
Configuring Remote Access Logging

You can configure remote access logging to:

- Log errors only
- Log errors and warnings
- Log all events
- Not log any events
- Log additional routing and remote access information

Key Points
To configure remote-access logging, open the Routing and Remote Access Service console, right-click `servername`, and then click Properties. Click the Logging tab to view the available options for, and the location of, the tracing log.

The four levels of event logging that Windows Server 2008 Routing and Remote Access Service makes available are:

- Log Errors Only
- Log Errors and Warnings
- Log all events
- Do not log any events

Additional Reading
- Routing and Remote Access Service Help: Server Properties – Logging Tab
Configuring Remote Access Tracing

You can configure remote access tracing by using:

- **The Netsh command:**
  - `Netsh ras diagnostics set rastracing * enabled` (enables tracing on all components in RAS)
- **The Registry:**
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing`

**Tracing consumes resources, so you should use it for troubleshooting only and then disable it**

**Key Points**

The Routing and Remote Access service in Windows Server 2008 has an extensive tracing capability that you can use to troubleshoot complex network problems. You can enable the components in Windows Server 2008 to log tracing information to files using the **Netsh** command or through the Registry.

**Additional Reading**

- Help topic: VPN troubleshooting Tools
Common Troubleshooting Solutions

Common problems regarding remote access include:

- Error 800: VPN unreachable
- Error 721: Remote computer not responding
- Error 741/742: Encryption mismatch
- Unable to establish VPN connection
- L2TP/IPSec issues
- EAP-TLS issues

Key Points

Common issues that you may encounter when using Windows Server 2008 Remote Access include:

- Error 800: VPN server is unreachable
- Error 721: Remote computer is not responding
- Error 741/742: Encryption mismatch error
- Unable to establish a remote access VPN connection
- L2TP/IPsec authentication issues
- EAP-TLS authentication issues
- Connection attempt is accepted when it should be rejected
- VPN clients are unable to access resources beyond the VPN server
- Unable to establish tunnel
Additional Reading

- Help topic: Troubleshoot Remote Access
Lab: Configuring and Managing Network Access

- Exercise 1: Configuring Routing and Remote Access as a VPN Remote Access Solution
- Exercise 2: Configuring a Custom Network Policy
- Exercise 3: Configuring Logging
- Exercise 4: Configuring a Connection Profile

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1, 6421A-NYC-SVR1 and 6421A-NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives
After completing this lab, you will be able to:

- Configure the Routing and Remote Access service as a VPN remote access solution.
- Configure a custom Network Policy.
- Configure logging.
- Configure a connection profile.
Scenario
Woodgrove Bank would like to implement a remote access solution for its employees so they can connect to the corporate network while away from the office. Woodgrove Bank requires a network policy that mandates that VPN connections are encrypted for security reasons.

The IT department of Woodgrove Bank does not want the Remote Access solution to cause a dramatic increase in support calls to the Help Desk for configuration issues regarding VPN connection objects that need to be created on the client computer.

Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the NYC-DC1, NYC-SVR1, and NYC-CL1 virtual machines.
2. Log on to the NYC-SVR1 with the user name Woodgrovebank\administrator and the password Pa$$w0rd.
3. Close the Initial Configuration Tasks window that appears after log on.
4. Close the Server Manager window that appears.
Exercise 1: Configuring Routing and Remote Access Service as a VPN Remote Access Solution

Exercise Overview
In this exercise, you will configure the Routing and Remote Access Service role as a VPN Remote Access solution. The VPN server should use IP address allocation for clients from a static pool of IP addresses that is configured on the Remote Access server. The Remote Access server should only accept PPTP and L2TP connections, with 25 connections allowed for each.

The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Install the Network Policy and Access Services role.
3. Configure 6421A-NYC-SVR1 as a VPN server with a static address pool for Remote Access clients.

▶ Task 1: Ensure that you have completed the steps in the Lab Setup
- Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

▶ Task 2: Install the Network Policy and Access Services role on 6421A-NYC-SVR1
1. Open Server Manager on 6421A-NYC-SVR1 and click Add Roles.
2. In Server Manager, on the Server Roles page, scroll down, select Network Policy and Access Services, and then click Next.
3. On the Select Role Services page, select Network Policy Server and Routing and Remote Access Services, and then click Next.
4. On the Confirm Installation Selections page, click Install.

5. On the Installation Results page, verify Installation succeeded appears in the details pane, and then click Close.

   The Network Policy and Routing and Remote Access Services roles are installed on 6421A-NYC-SVR1.

   Note: Do not log off or shut down the virtual machines at this point.

**Task 3: Configure 6421A-NYC-SVR1 as a VPN server with a static address pool for Remote Access clients**

1. From Administrative Tools, open Routing and Remote Access.

2. In the list pane, select and right-click 6421A-NYC-SVR1, and then click Configure and Enable Routing and Remote Access.

3. Ensure that the default setting, Remote Access (dial-up or VPN), is selected, and then on the Remote Access page, select the VPN option.

4. On the VPN Connection page, select the Local Area Connection 2 interface.

5. On the IP Address Assignment page, select From a specified range of addresses.

6. Use the range of 192.168.1.100 with 75 available addresses for the static pool.

7. Accept the default settings for the remainder of the configuration process.

**Task 4: Configure available VPN ports on the Routing and Remote Access Service server to allow 25 PPTP and 25 L2TP connections**

1. In the Routing and Remote Access administrative tool interface, right-click Ports and then click Properties.

2. In the Ports Properties dialog box, configure L2TP and PPTP to have 25 available connectors. Specify 0 for SSTP.

3. In the Ports Properties dialog box, click OK.

Exercise 2: Configuring a Custom Network Policy

Exercise Overview
In this exercise, you will create a network policy to allow secure connections to the Routing and Remote Access Service server.

The main tasks are as follows:
2. Create a new network policy for Routing and Remote Access Service clients.

► Task 1: Open the Network Policy Server management tool on 6421A-NYC-SVR1
- From the Administrative Tools menu, click Network Policy Server.
  The Network Policy Server administrative tool appears.

► Task 2: Create a new network policy for Routing and Remote Access Service clients
1. In the list pane of the Network Policy Server administrative tool, expand Policies, right-click Network Policies, and then click New.
2. In the New Network Policy wizard, specify the following settings and accept the default values for all other settings:
   - Network Policy Name: Secure VPN
   - Type of network access server: Remote Access Server (VPN-Dial up)
   - Specify Conditions: Tunnel Type: PPTP and L2TP
   - Configure Authentication Methods: Deselect MS-CHAP
   - Configure Constraints: Day and Time: deny access Mon thru Fri 11PM to 6AM
   - Configure Settings: Under Encryption, clear all settings except Strongest encryption
Exercise 3: Configuring Logging

Exercise Overview
In this exercise, you will enable logging in Routing and Remote Access.
The main tasks are as follows:

1. Configure Routing and Remote Access Service logging on 6421A-NYC-SVR1 to log all events to the system log.
2. Test logging levels.

- **Task 1: Configure Routing and Remote Access Service Logging on 6421A-NYC-SVR1 to log all events to the System log**
  1. Click Start, point to Administrative Tools, and then click Routing and Remote Access.
  2. Right-click 6421A-NYC-SVR1 and then click Properties.
  3. In the 6421A-NYC-SVR1 (local) Properties dialog box, click the Logging tab, click Log all events, and then click OK.

- **Task 2: Test logging levels**
  1. Log on to NYC-CL1 with a user name of administrator and a password of Pa$$w0rd.
  2. Click Start, click Network, and then in the Network window, click Network and Sharing Center.
  3. Under Tasks, click Set up a connection or network to create a new VPN connection object.
  4. In the Type the Internet address to connect to dialog box, specify an Internet address of 10.10.0.24 and a Destination Name of Woodgrovebank VPN.
  5. Accept the defaults for the remainder of the wizard settings.
  6. After the VPN connection object is created, connect to WoodgroveBank VPN from the Network Connections page.
7. Use the following information in the Connect Woodgrovebank VPN text boxes:
   - User name: Administrator
   - Password: Pa$$w0rd
   - Domain: Woodgrovebank

   The VPN connects successfully.

8. Right-click Woodgrovebank VPN and then click Disconnect. The VPN disconnects.

9. On 6421A-NYC-SVR1, click Start, point to Administrative Tools, and then click Event Viewer.

10. Use Event Viewer on 6421A-NYC-SVR1 and review the entries from the RemoteAccess source in the System log to see the logged data.

Exercise 4: Configuring a Connection Profile

Exercise Overview
In this exercise, you will configure a Connection Profile by using the Connection Manager Administration Kit (CMAK) tool to create connection objects for mobile computer users.

The main tasks are as follows:
1. Install the Connection Manager Administration Kit.
2. Use the CMAK to create a distributable executable that automates creation of connection objects for users.
3. Install and test the CMAK profile.
4. Close all virtual machines and delete the changes.

▶ Task 1: Install the Connection Manager Administration Kit
1. On 6421A-NYC-SVR1, click Start, and then click Server Manager.
2. Select the Connection Manager Administration Kit feature and then click Install.

▶ Task 2: Use the CMAK to create a distributable executable that automates creation of connection objects for users
1. Click Start, point to Administrative Tools, and then click Connection Manager Administration Kit.
2. On the Welcome page of the Connection Manager Administration Kit wizard, click Next. Specify the following settings in the wizard interface and accept the default values for the other settings:
   - On the Specify the Service Name and the File Name page, use WOODGROVEBANK VPN for the Service name and CORP_VPN for the File name.
- In Add Support for VPN Connections, select Phone book from this profile and specify to always use the same VPN server with an IP address of 10.10.0.24.
- In Add a custom Phone Book, deselect Automatically download phone book updates.

3. On the Your Connection Manager Profile is Complete and Ready to Distribute page, click Finish.

4. From NYC-SVR1, copy the CORP_VPN folder from the C:\Program Files\CMAK\Profiles\Vista\ location to the \NYC-DC1\Module6 location.

**Task 3: Install and test the CMAK profile**

1. On 6421A-NYC-CL1, in the \NYC-DC1\module6\ share, run CORP_VPN.exe to create the VPN connection object.

   The WOODGROVEBANK VPN connection object opens.

2. In the WOODGROVEBANK VPN connection object, type the following credentials and then click Connect:
   - User name: Administrator
   - Password: Pa$$w0rd
   - Logon Domain: Woodgrovebank

3. Set the Network Location to Work.

4. Verify the VPN connects successfully in Network Connections. Right-click the connection icon and then click Disconnect.

**Task 4: Close all virtual machines and discard undo disks**

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Best Practices
- Tools

Review Questions

1. You are adding Remote Access services to an existing infrastructure that uses non-RFC 1542 compliant routers. The DHCP server is not on the same subnet as the Remote Access server. What is one issue that might arise due to this configuration? How would you mitigate the issue?

2. You want to implement a VPN solution for users in your company, but the group that is responsible for security does not want to open the firewall to PPTP and L2TP traffic. Is it possible to create such a solution in Windows Server 2008? If so, what would you use?

3. Based on the scenario in the previous question, what encryption is used to secure traffic?
4. Is it possible to ignore the dial-in properties assigned to accounts in Active Directory with network policies? In what property category would this be set?

5. You have enabled full RADIUS logging on the Remote Access servers in your organization and verified that the logs are gathering the requested information. After a few weeks of logging, users begin to call the Help Desk because their connection attempts are failing. What is the most likely problem?

**Best Practices**

Decisions about the best method for providing remote access will vary depending on the tools you have chosen:

- Install and test servers running the Routing and Remote Access Service before configuring them as RADIUS clients.
- The RADIUS and Remote Access servers should be dedicated servers. This will minimize the likelihood of unauthorized users gaining network access and weakening the security configuration.
- Physically secure the RADIUS and Remote Access servers.
- Disable authentication protocols that you do not use. Do not use Password Authentication Protocol (PAP) unless you must support legacy systems.
- Determine the desired logging levels for auditing purposes and back up RADIUS logs.
- Secure remote administration sessions with IPSec or with VPNs if the sessions are initiated externally.
## Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing and Remote Access management tool</td>
<td>Managing and configuring the Routing and Remote Access service on the local server</td>
<td><strong>Routing and Remote Access</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Network Policy Server</td>
<td>Managing and creating network policy</td>
<td><strong>Network Policy Server</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Connection Manager Administration Kit</td>
<td>Creating customized, distributable connection objects for installation on client’s computers</td>
<td><strong>Connection Manager Administrative Kit</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Viewing logged information from application events, system events and security events</td>
<td><strong>Event Viewer</strong> on the Administrative Tools menu</td>
</tr>
</tbody>
</table>