
Module 10: Configuring a Windows 2000–Based Server as a Router

Contents

Overview	1
Overview of Routers and Routing Tables	2
Configuring Network Connections	7
Enabling Routing by Using Routing and Remote Access	11
Configuring Static Routes	13
Lab A: Configuring Windows 2000 As a Static Router	17
Configuring a Routing Interface	23
Implementing Demand-Dial Routing	30
Configuring the Routing Information Protocol	40
Lab B: Configuring a Windows 2000–Based Router	51
Review	62



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
90 Minutes

This module provides students with the knowledge and skills necessary to configure a computer running Microsoft® Windows® 2000 as a network router.

Labs:
60 Minutes

At the end of this module, students will be able to:

- Explain the function and purpose of routing.
- Configure network connections.
- Enable routing by using Routing and Remote Access.
- Configure static routes.
- Configure a routing interface.
- Implement demand-dial connections.
- Configure the Routing Information Protocol (RIP).

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the Microsoft PowerPoint® file 2153a_10.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Read the white paper *Microsoft Windows 2000 TCP/IP Implementation Details*, under **Additional Reading** on the Web page on the Student Materials compact disc.
- Read the following RFCs under **Additional Reading** on the Web page on the Student Materials compact disc:
 - RFC 1058 *Routing Information Protocol*
 - RFC 2328 *OSPF Version 2*
 - RFC 2453 *RIP Version 2*
- Review RFC 1700 under **Additional Reading** on the Web page on the Student Materials compact disc.

- Read the entire “Routing” section in the Microsoft Internet Information Services 5.0 Resource Kit.
- Read the entire “Routing” section in Windows 2000 Server Help.
- Read appendix B, “IP Addressing Basics,” under **Appendices** on the Web page on the Student Materials compact disc.
- Review appendix C, “Port Assignments for Commonly Used Services,” under **Appendices** on the Web page on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Overview of Routers and Routing Tables

Begin the module by describing the terminology used in an internetwork. Point out that Windows 2000 Routing and Remote Access is a service that performs routing as one of its multiple processes. Demonstrate the procedure for displaying the Internet Protocol (IP) routing table by using the **route print** command, and then describe the routing table entries.

- Configuring Network Connections

Explain the purpose of renaming connections for network adapters, and then describe the settings that you configure in the Windows 2000–based router interface. Demonstrate how to verify the address relationship between the network adapter and the IP settings by using the **ipconfig/all** command.

- Enabling Routing by Using Routing and Remote Access

Demonstrate the procedure for configuring routing, pointing out the settings for demand-dial connections. Briefly describe the procedure for configuring a remote access server for routing.

- Configuring Static Routes

Demonstrate the procedure for viewing static routing tables, and then describe routing table entries. Be careful not to spend too much time discussing network masks; instead, refer students to the appendix for additional information. Make sure that the students understand the difference between the routing table in Routing and Remote Access and the routing table displayed in the command prompt. Demonstrate the procedure for adding a static route, describing the settings specified in the **Static Route** dialog box.

- Configuring a Routing Interface

Describe the three types of routing interfaces, explaining the difference between on-demand and persistent connections. Use the build slide to explain the process of packet filtering. Demonstrate the procedure for configuring filters, and then describe the settings that you can define when adding a filter. Point out that students can get a list of ports in the Appendices folder on the Student Materials compact disc.

- Implementing Demand-Dial Routing

Explain the purpose and use of demand-dial routing. Using the example in the slide, demonstrate the procedure for creating a demand-dial interface. Explain the use of static IP address pools, and then demonstrate the procedure for configuring IP assignment for inbound demand-dial connections. Explain the use of demand-dial filtering and dial-out hours. Be sure to point out the relationship between demand-dial filtering and IP packet filters, as described in the Important box at the end of the procedure. Finally, explain the purpose of adding static routes to a demand-dial interface, and explain the procedure for testing the routes.

- Configuring the Routing Information Protocol

Explain the use of routing protocols, describing the difference between RIP and Open Shortest Path First (OSPF). Explain the RIP operation by using the build slide. Demonstrate the procedure for adding the RIP protocol, explaining that an interface must be added to support RIP. Describe the settings that you can configure for a RIP interface. Make sure that you explain that the authentication option is primarily used for identification rather than for security. Demonstrate the procedure for configuring route filtering. Finally, explain the purpose of a neighbors list, and demonstrate the steps for configuring a neighbors list.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Lab Setup

The lab in this module requires that you perform the procedure specified in the Classroom Setup Guide before performing the lab.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about configuring a Windows 2000–based computer as a network router.

- Overview of Routers and Routing Tables
- Configuring Network Connections
- Enabling Routing by Using Routing and Remote Access
- Configuring Static Routes
- Configuring a Routing Interface
- Implementing Demand-Dial Routing
- Configuring the Routing Information Protocol

*****ILLEGAL FOR NON-TRAINER USE*****

This module provides the knowledge and skills necessary to configure a computer running Microsoft® Windows® 2000 as a network router. When enabled as a network router, Windows 2000 supports both local routing and remote routing. In addition to physical dial-up, frame relay, Integrated Services Digital Network (ISDN), or X.25 connections, the connection can be a direct connection to the corporate network or a point-to-point, virtual private network (VPN) connection through the Internet.

At the end of this module, you will be able to:

- Explain the function and purpose of routing.
- Configure network connections.
- Enable routing by using Routing and Remote Access.
- Configure static routes.
- Configure a routing interface.
- Implement demand-dial connections.
- Configure the Routing Information Protocol (RIP).

◆ Overview of Routers and Routing Tables

Topic Objective

To identify the topics relevant to routers and routing tables.

Lead-in

A thorough understanding of routers and routing tables will help you effectively configure routers for your network environment

- Router Functions
- Routing Tables

*****ILLEGAL FOR NON-TRAINER USE*****

A network consists of a number of different devices such as hubs, bridges, switches, and routers. Routers allow you to scale your network and maintain bandwidth by segmenting network traffic. Routers determine where to forward packets based on routing tables. Routing tables enable routers to make decisions about forwarding traffic to the proper destination for efficient packet delivery. A thorough understanding of routers and routing tables will help you effectively configure routers for your network environment.

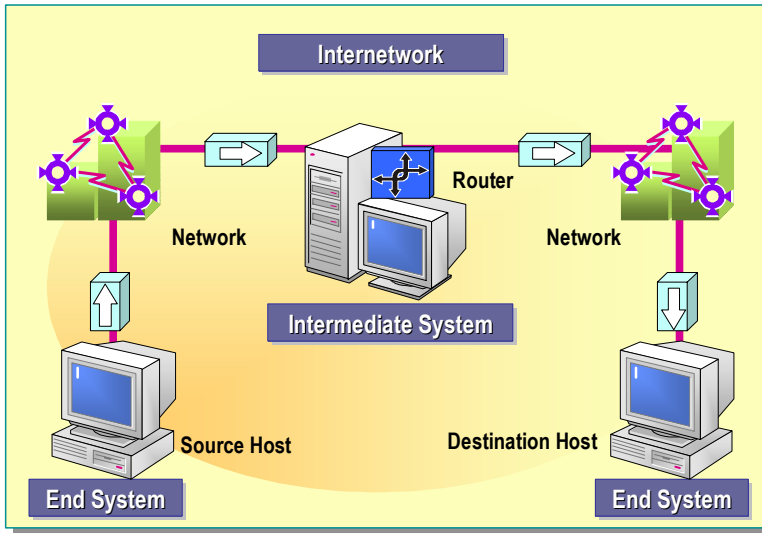
Router Functions

Topic Objective

To illustrate the function of a router in an internetwork.

Lead-in

Routing is the process of transferring data across an internetwork from a source host to a destination host.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain that *hosts* are nonrouter computers that run TCP/IP.

Routing is the process of forwarding packets between connected networks. Routing is part of the Internet Protocol (IP) and is used in combination with other network protocol services to provide forwarding capabilities between hosts that are located on separate network segments within a larger Transmission Control Protocol/Internet Protocol (TCP/IP)–based network. Each incoming or outgoing packet is called an IP *datagram* or a *packet*. An IP datagram contains two IP addresses: the source address of the sending host and the destination address of the receiving host.

Routing Terminology

The following terms are essential to an understanding of routing:

Key Point

Windows 2000 Routing and Remote Access is a service that performs routing as one of its multiple processes.

- *End systems.* Network devices without the ability to forward packets between portions of a network. End systems are also known as *hosts*.
- *Intermediate systems.* Network devices with the ability to forward packets between portions of a network. Bridges, switches, and routers are examples of intermediate systems.
- *Network.* A portion of the networking infrastructure that is bound by a network layer intermediate system and that is associated with the same network layer address.
- *Router.* A network layer intermediate system used to connect networks together based on a common network layer protocol.
- *Hardware router.* A router that performs routing as a dedicated function and has specific hardware that is designed and optimized for routing.
- *Software router.* A router that is not dedicated to performing routing but performs routing as one of multiple processes running on the router computer. Windows 2000 Routing and Remote Access is a service that performs routing as one of its multiple processes.
- *Internetwork.* At least two networks that are connected by using routers.

Purpose of Routing

IP routers provide the primary means of joining together two or more physically separated IP network segments. All IP routers share two essential characteristics:

- IP routers are multihomed hosts.

A *multihomed* host is a network host that uses two or more network connection interfaces to connect to separate network segments. In addition, a multihomed host can have a single network adapter and multiple logical adapters; an example of a multihomed host would be a demand-dial VPN that connects offices over the Internet.

- IP routers provide packet forwarding for other TCP/IP hosts.

An IP router must be able to forward IP-based communication between networks for other IP network hosts.

Routing Tables

Topic Objective

To illustrate an example of routing table data for a computer running Windows 2000.

Lead-in

Routers use data from routing tables to determine how to forward IP packets.

To Display the IP Routing Table on a Computer Running Windows 2000, Use the Route Print Command

```
C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x1000003 ...00 90 27 16 84 10 ..... Intel(R) PRO PCI Adapter
=====
Active Routes:
Network Destination    Netmask          Gateway         Interface    Metric
0.0.0.0                0.0.0.0          192.168.1.200   192.168.1.201 1
127.0.0.0              255.0.0.0        127.0.0.1      127.0.0.1    1
192.168.0.0            255.255.248.0    192.168.1.201   192.168.1.201 1
192.168.1.201          255.255.255.255  127.0.0.1      127.0.0.1    1
192.168.1.255          255.255.255.255  192.168.1.201   192.168.1.201 1
224.0.0.0              224.0.0.0        192.168.1.201   192.168.1.201 1
255.255.255.255        255.255.255.255  192.168.1.201   192.168.1.201 1
Default Gateway:       192.168.1.200
=====
Persistent Routes:
None
C:\>
```

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the steps for displaying the output of the **route print** command, and then explain each entry in the routing table.

Routers forward packets between network segments based on rules that allow for efficient packet delivery. Routers use data stored in a routing table to determine the correct destination. The routing table data includes IP information about all of the segments to which the router is connected. The data also includes instructions on how to forward packets destined for other networks that are not directly connected to the router. Typically, a router contains a routing table entry for each network to which it connects. The entry identifies where the router should forward packets that are destined for a given network.

Displaying the IP Routing Table

Every computer that runs TCP/IP makes routing decisions that are controlled by the routing table. The routing table is built automatically, based on the current TCP/IP configuration of a computer.

To display the IP routing table on a computer that is running Windows 2000, type **route print** at a command prompt.

Examining Routing Table Entries

The following describes each of the columns displayed in the IP routing table:

- *Network destination.* Used along with the netmask to match the destination IP address. The network destination can range from 0.0.0.0 for the default route through 255.255.255.255 for a limited broadcast. A computer uses the default route if no other host or network route matches the destination address that is included in an IP datagram.
- *Netmask.* Applied to the destination IP address when matching to the value in the network destination. Netmask is also called a *subnet mask*. A subnet mask distinguishes network identifiers (IDs) and host IDs within an IP address.

Explain that a datagram is one packet, or unit, of information that is sent through a packet-switching network, along with relevant delivery information such as the destination address.

- *Gateway*. Indicates the IP address that the local host uses to forward IP datagrams to other IP networks. A gateway is either the IP address of a local network adapter or the IP address of an IP router on the local network segment.
- *Interface*. Indicates the IP address of the network adapter that the local computer uses when it forwards an IP datagram on the network.
- *Metric*. Indicates the cost of a route. If multiple routes to the IP destination exist, the metric is used to decide which route is to be taken. The route with the lowest metric is the preferred route, and other routes are only used if the preferred route becomes unavailable. Metrics can indicate different ways of expressing a route preference. The measurement that is used for the metric depends on the routing protocol: When the routing protocol does not specify how a metric is defined, the administrator who configures the router chooses how the metric is defined.

A metric is commonly defined by using one of the following criteria:

- *Hop count*. Indicates the number of routers in the path to the destination. Anything on the local subnet is one hop, and each router crossed after that is an additional hop.
- *Delay*. Indicates a measure of time that is required for the packet to reach the network ID. Delay is used to indicate the speed of a path or a congested condition of a path; for example, local area network (LAN) links have a low delay, and wide area network (WAN) links have a high delay.
- *Throughput*. Indicates the effective amount of data that can be sent along the path per second.
- *Reliability*. A measure of the path constancy. Some types of links are more prone to link failures than others. For example, with WAN links, leased lines are more reliable than dial-up lines.

Explain that throughput is not necessarily a reflection of the bit rate of the link; for example, a very busy Ethernet link may have a lower throughput than an unused WAN link operating at 64 kilobits per second (Kbps).

Default Routing Table Entries

The following are default routing table entries for a Windows 2000–based computer running TCP/IP. These IP addresses are reserved for use by TCP/IP. A Windows 2000–based router also contains, by default, entries for the network address for all local interfaces.

Network address	Description
0.0.0.0	All IP addresses for which no other routes have been defined, the <i>default route</i>
127.0.0.0	The local loopback address
224.0.0.0	IP multicast addresses
255.255.255.255	IP broadcast address

◆ Configuring Network Connections

Topic Objective

To identify the topics relevant to configuring network connections.

Lead-in

After you install networking hardware and configure the relevant drivers, you must configure the IP properties of the network adapter so that the router can communicate with the network.

- **Configuring Network Connection Names**
- **Configuring IP Settings for a Network Adapter**

*****ILLEGAL FOR NON-TRAINER USE*****

Configuring a Windows 2000–based server as a router requires a number of steps. After you install networking hardware and configure the relevant drivers, you must configure the IP properties of the network adapter so that the router can communicate with the network. To manage a router with multiple network adapters more easily, you can rename each network adapter connection with a descriptive name.

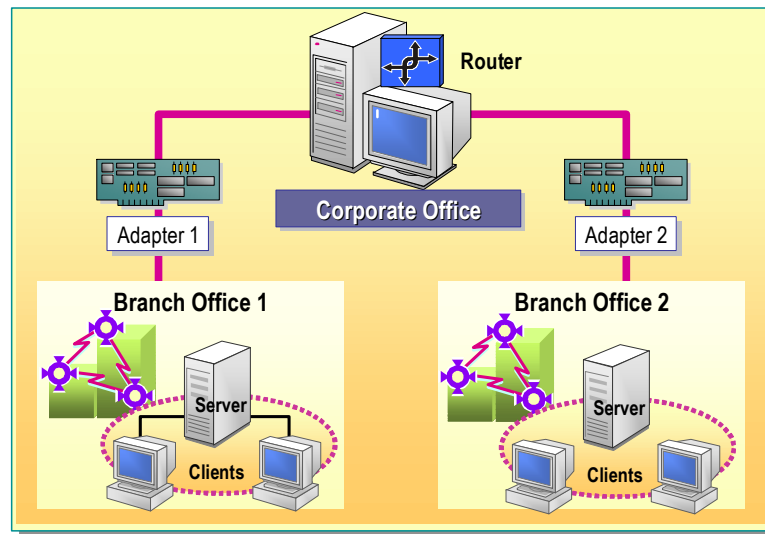
Configuring Network Connection Names

Topic Objective

To illustrate how to configure multiple network adapters.

Lead-in

You can rename network connections to eliminate confusion.



*****ILLEGAL FOR NON-TRAINER USE*****

Remind students that they renamed connections as an instructor-led exercise in module 0 of course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Typically, two or more network adapters are installed in a computer that performs routing. For each adapter, Windows 2000 displays a **local area connection** icon in the Network and Dial-up Connections folder. To eliminate confusion, you can rename each local area connection to reflect the network to which the adapter connects.

To rename a connection, open Network and Dial-up Connections in the Control Panel, right-click the connection that you want to rename, and then click **Rename**.

Configuring IP Settings for a Network Adapter

Topic Objective

To list the topics relevant to configuring IP settings for a network adapter.

Lead-in

In general, when adding a network adapter to a server, you assign a single IP address for each network connection.

- **Configuring Settings for a Network Connected to the Internet**
- **Configuring Settings for a Private Network**
- **Verifying the Address Relationship**

*****ILLEGAL FOR NON-TRAINER USE*****

In general, when adding a network adapter to a server, you assign a single IP address for each network connection. Each network adapter is uniquely identified by its physical, or media access control (MAC), address. Each network adapter displays in Network and Dial-up Connections as a **local area connection** icon. To match a network adapter to a network interface, you must match the physical address of the adapter to the connection. You can verify the physical address and interface name relationship by using the **ipconfig /all** command.

Configuring Settings for a Network Connected to the Internet

You must manually configure the Windows 2000–based router interfaces with an IP address. You configure the IP address through the properties of the TCP/IP protocol for the connection in Network and Dial-up Connections.

You configure the connection for a Windows 2000–based router with the following:

- *IP address*. Obtained from the address range that you received from the Internet service provider (ISP).
- *Subnet mask*. Obtained from the address range that you received from the ISP.
- *Domain Name System (DNS) server*. Obtained from the IP address that you received from the ISP. This server is required if your router forwards DNS queries to an ISP.

Configuring Settings for a Private Network

For private TCP/IP networks that are not directly or indirectly connected to the Internet, you can use any range of valid IP addresses.

For private TCP/IP networks that are indirectly connected to the Internet by using a network address translator (NAT) or an application layer gateway such as a proxy server, the Internet Assigned Numbers Authority (IANA) recommends that you use the private IP addresses shown in the following table.

Private Network ID	Subnet mask	Range of IP addresses
10.0.0.0	255.0.0.0	10.0.0.1–10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1–172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1–192.168.255.254

Important Even though you can use any addressing scheme when configuring a network that is not connected to the Internet, it is highly recommended that you use private network addresses. Doing so will prevent address conflicts if you ever decide to connect your network to the Internet by indirect means, such as a proxy server.

Verifying the Address Relationship

You can verify the address relationship between the network adapter and the IP settings by using the Ipconfig utility. The Ipconfig utility displays all of the current TCP/IP configuration values, including the physical address and IP address, for the connection. To obtain detailed results, type **ipconfig /all** at a command prompt.

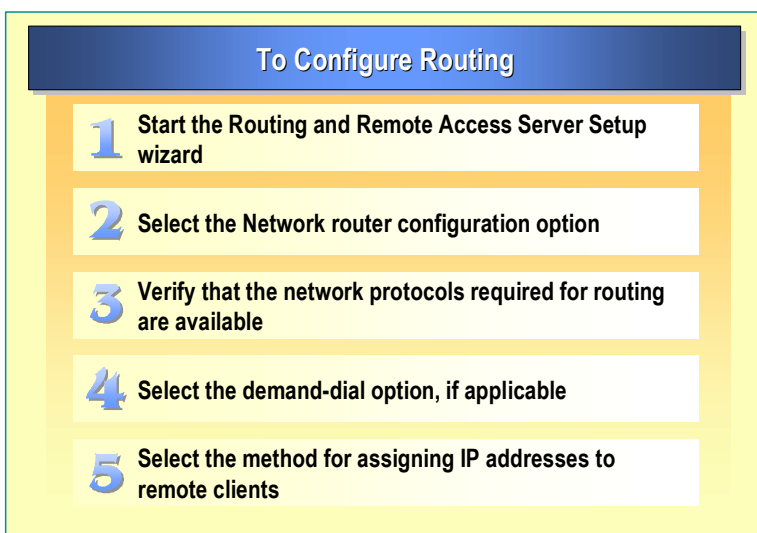
Enabling Routing by Using Routing and Remote Access

Topic Objective

To list the steps for configuring routing by using the Routing and Remote Access Server Setup wizard.

Lead-in

You configure a Windows 2000–based router by using the Routing and Remote Access Server Setup wizard.



*****ILLEGAL FOR NON-TRAINER USE*****

For your Windows 2000–based server to function as a network router, you must enable Routing and Remote Access. Understanding how to configure a network router by using Routing and Remote Access lets you to create versatile connections between branch offices and a corporate network.

Note If the server is a member of an Active Directory™ directory service domain in Windows 2000 and you enable demand-dial routing, you must add the computer account of the server to the RAS and IAS Servers security group before you can use demand-dial routing. When a member of the Domain Admins group enables the Routing and Remote Access service, Windows 2000 adds the server to this group automatically.

Delivery Tip

Demonstrate the steps for configuring routing.

Configuring a Windows 2000 Server for Routing

You configure a Windows 2000–based server as a network router by using the Routing and Remote Access Server Setup wizard.

To configure a Windows 2000–based server for routing, open Routing and Remote Access from the Administrative Tools menu, then:

1. In the console tree, right-click *server* (where *server* is the name of your computer), click **Configure and Enable Routing and Remote Access**, and then click **Next** to start the Routing and Remote Access Server Setup wizard.
2. On the **Common Configurations** page, click **Network router**, and then click **Next**.
3. On the **Routed Protocols** page, verify that the network protocols required for routing are available, and then click **Next**.

The Windows 2000–based router can route IP, Internetwork Packet Exchange (IPX), and AppleTalk traffic.

Key Points

Demand-dial routing activates a connection only when data is being sent to the remote site.

Tell students that demand-dial routing will be covered later in the module.

4. On the **Demand-Dial Connections** page, click **Yes** if you want to use demand-dial connections, and then click **Next**.

By using a demand-dial interface, a connection becomes active only when data is sent to the remote site. When no data has been sent over the link for a specified amount of time, the link is disconnected. Demand-dial connections use existing dial-up telephone lines instead of leased lines for low-traffic situations.

Important If you do not select the demand-dial option in the wizard, you will not be able to create demand-dial connections, although the option will appear on the **Action** menu.

5. If you have enabled demand-dial connections, click the method for assigning IP addresses to remote clients, and then click **Finish**.

The Windows 2000–based router can assign IP addresses automatically by using the Dynamic Host Configuration Protocol (DHCP), or from a specified range of addresses.

Configuring a Remote Access Server for Routing

If you have already used Routing and Remote Access to configure remote access functionality, you still need to enable routing for your server.

To enable routing on a remote access server:

1. Open Routing and Remote Access.
2. In the console tree, right-click click *server* (where *server* is the name of your computer), and then click **Properties**.
3. On the **General** tab, select the **Router** check box, click **Local area network (LAN) routing only** or **LAN and demand-dial routing**, and then click **OK**.

◆ Configuring Static Routes

Topic Objective

To identify the topics related to static routes.

Lead-in

After you configure your Windows 2000–based computer as a router, the router includes a number of routing table entries by default.

- Examining a Static Routing Table
- Adding a Static Route

*****ILLEGAL FOR NON-TRAINER USE*****

After you configure a Windows 2000–based server as a router, the router includes a number of routing table entries by default. These entries are built from LAN interfaces that are already available on that protocol. For your router to successfully forward packets to networks to which it is not directly connected, you need to create routing table entries for these networks. In a small network, you can add these entries manually by configuring static routes in the routing table of your router.

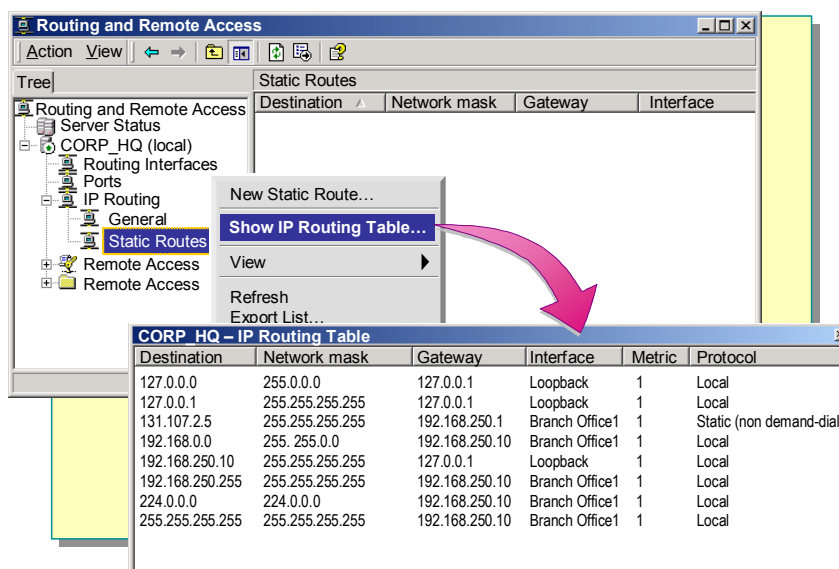
Examining a Static Routing Table

Topic Objective

To illustrate an example of a static routing table.

Lead-in

Static routing tables are built and updated manually.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Static routes do not scale well due to their manual administration.

Static routing tables are built and updated manually. If a route changes, the network administrator must manually update the routing tables. Static routes can work well for small internetworks. However, static routes do not scale well because they must be administered manually.

Viewing Static Routing Tables

To view static routing tables:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), and then expand **IP Routing**.
3. Right-click **Static Routes**, and then click **Show IP routing**.

The IP routing table contains information in the following columns:

- *Destination*. Indicates the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- *Network mask*. Used in conjunction with the destination to determine when a route is used. A mask of 255.255.255.255 means that only an exact match of the destination uses this route. A mask of 0.0.0.0 means that any destination can use this route.

The example presented in this module is intended as an overview. For more information about IP addresses, refer students to appendix B, "IP Addressing Basics," under **Appendices** on the Student Materials compact disc.

For example, a destination of 172.16.8.0 has a network mask of 255.255.248.0. This network mask means that the first two octets must match exactly, the first five bits of the third octet must match (248=11111000), and the last octet does not matter. The third octet of 172.16.8.0 (that is, 8) equals **00001000** in binary. Without changing the first five bits (the masked-off portion shown in **bold**), you can go up to 15, or **00001111** in binary. So a route with a destination of 172.16.8.0 and a mask of 255.255.248.0 applies to all packets destined for 172.16.**8**.0 through 172.16.**15**.255.

-
- *Gateway*. Indicates the IP address of the next router where a packet needs to be sent. On a LAN link, the gateway must be directly reachable by the router by using the interface indicated in the **Interface** column. For a demand-dial interface, the gateway address is not configurable.
 - *Interface*. Indicates the LAN or demand-dial interface that is to be used to send the packet.
 - *Metric*. Indicates the relative cost of using the route to reach the destination. For example, the metric hops indicate the number of routers to cross to reach the destination.
 - *Protocol*. Indicates how the route was learned. If the **Protocol** column lists anything other than **Local**, an administrator manually configured the routes or the router is receiving routes from other routers.

Note For more information about IP Addressing, see appendix B, “IP Addressing Basics,” under **Appendices** on the Web page on the Student Materials compact disc.

Adding a Static Route

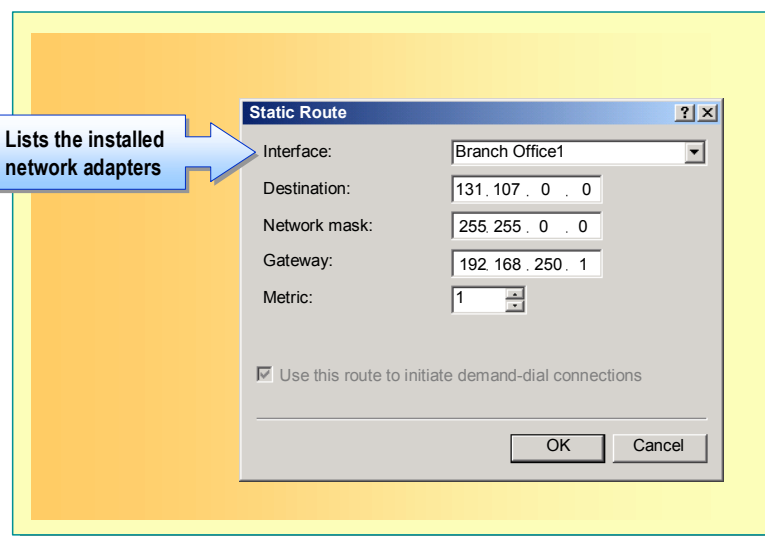
Topic Objective

To identify the settings for adding static routes.

Lead-in

For efficient routing, routers must contain route information for other networks.

Lists the installed network adapters



*****ILLEGAL FOR NON-TRAINER USE*****

For efficient routing, routers must contain route information for other networks. On an internetwork, it is important to maintain routing tables so that traffic follows the best path and adjusts for out-of-service routers and routes.

Use the **Static Route** dialog box to add static IP routes to the routing table. When your configuration is complete, use the **ping** and **tracert** commands to test connectivity between host computers so that all routing paths are checked.

Explain to students that it is a common practice to assign the first IP addresses of a given IP network to router interfaces. For example, for an IP network ID of 192.168.100.0 with a subnet mask of 255.255.255.0, the router interface is assigned the IP address of 192.168.100.1.

To add static IP routes to the routing table:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), expand **IP Routing**, right-click **Static Routes**, and then click **Add Static Route**.
3. Specify the following parameters in the **Static Route** dialog box, and then click **OK** to add the route to the routing table.

Parameter	Description
Interface	The interface that is used to send the packet when using this route.
Destination	The destination network ID, which can be a class-based network ID, a subnetted network ID, a supernetted network ID, or a host ID.
Network mask	The corresponding subnet mask, which must encompass all of the bits in the destination network ID. The network ID cannot be more specific than the subnet mask. For host-specific routes, the network mask is 255.255.255.255.
Gateway	The IP address of the router to which packets for this destination are to be forwarded.
Metric	The “cost” of using this route. The cost can reflect a hop count or a preference for using this route. This value is an integer.

Lab A: Configuring Windows 2000 As a Static Router

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure Windows 2000 as a router and add static routes.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure Windows 2000 as a router.
- Add static routes to a Windows 2000–based computer that is configured as a router.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller in native mode
- A lab partner with a similarly configured computer
- IP addresses for the two network adapters in your computer
- IP addresses for the two network adapters in your partner's computer

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

If you are unsure about any of these values, please ask your instructor.

Adapter	Record IP address here
----------------	-------------------------------

Your Classroom adapter	
------------------------	--

Your PartnerNet adapter	
-------------------------	--

Your partner's Classroom adapter	
----------------------------------	--

Your partner's PartnerNet adapter	
-----------------------------------	--

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

Your company is expanding the number of branch offices that are connected to the head-office network, and you are responsible for configuring Windows 2000 as a static router to enable this connectivity.

Estimated time to complete this lab: 30 minutes

Exercise 1

Configuring a Computer Running Windows 2000 As a Static Router

Scenario

Your organization is using a computer running Windows 2000 as a branch-office router for your network, and you need to configure it with a static route to enable routing to take place.

Goal

In this exercise, you will work with your partner to configure a router for your network.

Tasks	Detailed Steps
 Important: Perform the following steps only on the computer with the lower student number.	
1. Disable the Classroom network adapter. Set the default gateway for the network adapter PartnerNet to be the IP address of your partner's PartnerNet adapter.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. Right-click My Network Places, and then click Properties. - In Network and Dial-up Connections, right-click Classroom, and then click Disable. - Right-click PartnerNet, and then click Properties. - In the PartnerNet Properties dialog box, click Internet Protocol (TCP/IP), and then click Properties. - In the Default gateway box, type the IP address of your partner's PartnerNet adapter, and then click OK. - Click OK to close the PartnerNet Properties dialog box. - Close Network and Dial-up Connections.
 Important: Perform the following steps only on the computer with the higher student number.	
2. Configure Routing and Remote Access to function as a router.	- Log on as administrator@domain.nwtraders.msft with a password of password. - Open Routing and Remote Access from the Administrative Tools menu. - In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Configure and Enable Routing and Remote Access. - In the Routing and Remote Access Server Setup wizard, click Next. - On the Common Configurations page, click Network router, and then click Next. - On the Routed Protocols page, under Protocols, verify that TCP/IP displays, and then click Next.

(continued)

Tasks	Detailed Steps
2. (continued)	g. On the Demand-Dial Connections page, verify that No is selected, and then click Next. h. Click Finish to close the Routing and Remote Access Server Setup wizard.  The Routing and Remote Access service will now start. i. Close Routing and Remote Access.
 Perform the following procedures on both student computers.	
3. Ping the instructor computer.	a. At a command prompt, type ping 192.168.z.200 (where <i>z</i> is the number assigned to your classroom).  The ping should be successful from the student computer with the higher student number (the router), but unsuccessful from the student computer with the lower student number (the computer on the remote network).
 Why didn't the ping work from the student computer on the remote network? The instructor computer does not have a routing table entry for your network. When the instructor computer received the ping, it didn't know where to send the packet in response to the ping. _____ _____ _____	
 Would adding a default gateway to the instructor computer help solve this problem? Why or why not? No. Adding a default gateway to the instructor computer would help it find one network, but there are many networks that need to be found from the instructor computer. You can only have one default gateway. _____ _____ _____	
3. (continued)	b. Minimize the command prompt window.
 Important: Perform the following procedures only on the computer with the higher student number.	

(continued)

Tasks	Detailed Steps
4. Add a static route on the instructor computer for the network between your computer and your partner's computer. Use the following information to create the routing entry. Interface: Classroom Destination: The first three octets of your PartnerNet connection, and then use 0 for the last octet. Subnet Mask: 255.255.255.0 Gateway: IP address of the PartnerNet adapter on the computer with the higher student number.	- Click Start, point to Programs, point to Administrative Tools, right-click Routing and Remote Access, and then click Run as. - In the Run As Other User dialog box, in the User name box, type administrator@nwtraders.msft - In the Password box, type password - Delete the contents of the Domain box, and then click OK. - In the console tree, right-click Routing and Remote Access, and then click Add Server. - In the Add Server box, click The following computer, type London and then click OK. - In the console tree, expand London, expand IP Routing, and then click Static Routes. - Right-click Static Routes, and then click New Static Route. - In the Static Route dialog box, in the Interface box, verify that Classroom is selected. - In the Destination box, type the first three octets of your PartnerNet connection, and then use 0 for the last octet. - In the Network mask box, type 255.255.255.0 - In the Gateway box, type 192.168.z.x (where <i>z</i> is the number assigned to your classroom and <i>x</i> is your student number). - Click OK to close the Static Route dialog box. - In the console tree, right-click London, and then click Delete. - Close Routing and Remote Access.
 Perform the following procedures on both student computers.	
5. Ping the instructor computer.	- At a command prompt, type ping 192.168.z.200  <i>The ping should be successful from both student computers.</i> - Close the command prompt window.
6. Open Routing and Remote Access and connect to the computer with the higher student number. Examine the routing table.	- Open Routing and Remote Access from the Administrative Tools menu. - In the console tree, right-click Routing and Remote Access, and then click Add Server. - In the Add Server box, click The following computer, type <i>partner_server</i> (where <i>partner_server</i> is the name of your partner's computer), and then click OK. - In the console tree, expand <i>partner_server</i>, expand IP Routing, and then click Static Routes. - Right-click Static Routes, and then click Show IP Routing Table. - Examine all of the entries in the routing table.

(continued)

Tasks	Detailed Steps
 Your network has other internal partnernet networks connected to it. If you want to enable IP communication with the other networks, what static entries do you need to add to which routers? You need to add a static entry to your router for the destination network, and you will also need to add a static entry for your partnernet network to your destination network’s router. _____ _____	
6. <i>(continued)</i>	g. Close the <i>server - IP Routing Table</i> window, and then close Routing and Remote Access.
 Perform the following procedure on both student computers.	
7. Close any open windows, and then log off.	a. Close any open windows, and then log off.

◆ Configuring a Routing Interface

Topic Objective

To identify the topics relevant to configuring a routing interface.

Lead-in

When you enable network routing for your server, by default Routing and Remote Access adds all of the enabled network adapters that are installed as routing interfaces.

- Routing Interfaces in Routing and Remote Access
- Packet Filtering
- Configuring Filters on an IP Routing Interface
- Configuring Filter Settings on an IP Routing Interface

*****ILLEGAL FOR NON-TRAINER USE*****

When you enable network routing for your server, by default Routing and Remote Access adds all of the enabled network adapters that are installed as routing interfaces. The Windows 2000–based router uses the routing interfaces to forward packets to the network.

You can configure filters to allow or disallow the forwarding of specific types of IP traffic. Filters enable a network administrator to define what IP traffic is allowed to cross the router.

Routing Interfaces in Routing and Remote Access

Topic Objective

To identify the three types of routing interfaces in Windows 2000.

Lead-in

A routing interface is a physical or logical interface over which IP packets are forwarded.

- LAN Interfaces
- Demand-Dial Interfaces
- IP-in-IP Tunnel Interfaces

*****ILLEGAL FOR NON-TRAINER USE*****

A routing interface is a physical or logical interface over which IP packets are forwarded. The Windows 2000–based router uses a routing interface to forward IP, IPX, or AppleTalk packets. To view installed and configured routing interfaces, in Routing and Remote Access, in the console tree, click **Routing Interfaces**.

There are three types of routing interfaces:

- *LAN interfaces*. Represent a local area connection that uses LAN technology such as Ethernet or Token Ring. A LAN interface is represented as an installed network adapter. LAN interfaces are always active and typically do not require an authentication process to become active.
- *Demand-dial interfaces*. Represent a point-to-point connection. The point-to-point connection is based on either a physical connection, such as two routers that use modems to connect over an analog telephone line, or a logical connection, such as two routers that use the Internet to connect over a VPN. Demand-dial connections are either *on-demand* (established only when needed) or *persistent* (established and then remain in a connected state). Demand-dial interfaces typically require an authentication process to become connected.
- *IP-in-IP tunnel interfaces*. Represent a tunneled point-to-point connection. IP-in-IP tunnel interfaces do not require an authentication process to become connected. A typical use for IP-in-IP interfaces is the forwarding of IP multicast traffic from one area of the intranet to another area of the intranet, across a portion of the intranet that does not support multicast forwarding or routing.

Explain the difference between on-demand and persistent connections.

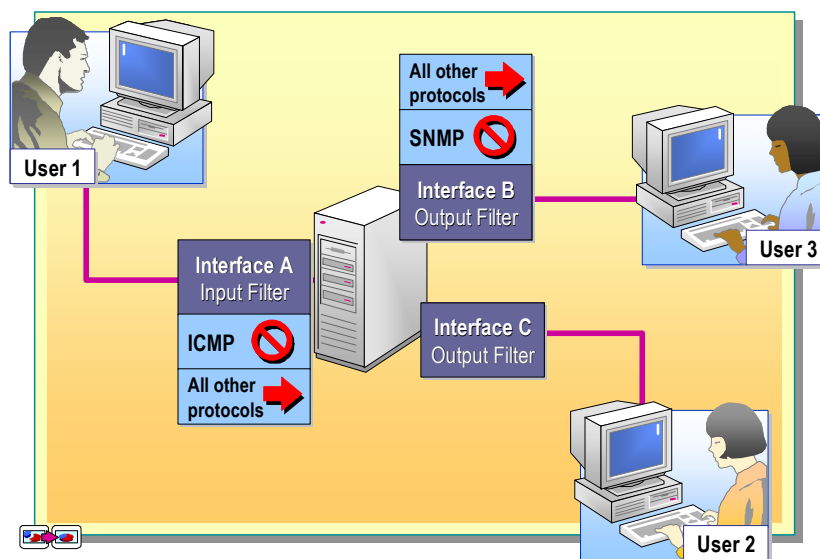
Packet Filtering

Topic Objective

To illustrate the packet filtering process.

Lead-in

IP packet filtering provides the ability to allow or disallow the forwarding of specific types of IP traffic.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tips

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

Use the slide graphic to explain the example in the module.

Explain that SNMP is used to provide status information about a host on a TCP/IP network or to configure the host.

An IP router can provide the ability to allow or disallow the forwarding of specific types of IP traffic. This capability, called *IP packet filtering*, provides a way for the network administrator to precisely define what IP traffic is allowed to cross the router. IP packet filtering becomes important when you connect corporate intranets to public networks such as the Internet.

For example, user 1 attempts to ping user 2's computer. Because there is an input filter on interface A that is configured to block incoming Internet Control Message Protocol (ICMP) traffic, the ICMP packet is discarded at the router. When user 1 tries to communicate with user 2 by using other protocols, those packets are forwarded unmodified. By blocking ICMP traffic with an input filter, a network administrator can prevent users from causing unnecessary traffic to pass across the router.

When user 1 attempts to use Simple Network Management Protocol (SNMP) to manage user 3's computer, the attempt is unsuccessful because the router has an output filter on interface B that is configured to transmit all protocols except SNMP.

An output filter can also be configured to prevent SNMP traffic from entering certain networks. For example, if an organization has computers that are in an insecure location, such as a lab network, an administrator can configure a routing filter to block SNMP from that network. Blocking SNMP traffic prevents a user in that network from performing management functions on computers that are connected to the rest of the network.

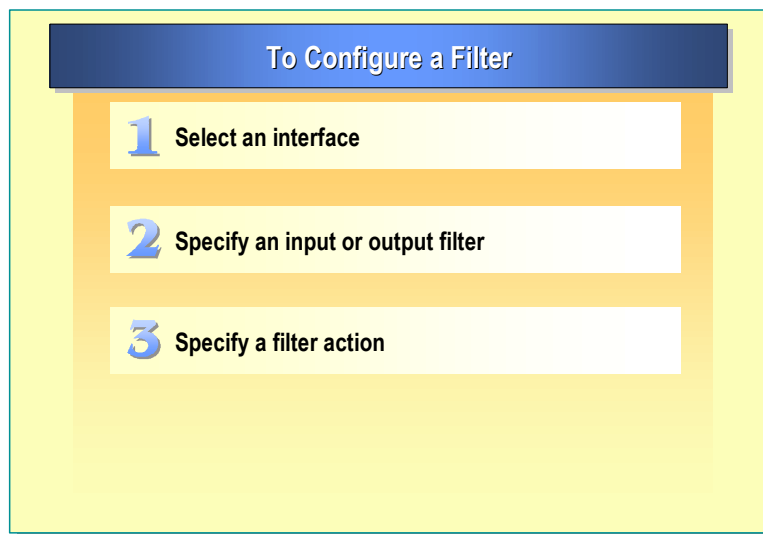
Configuring Filters on an IP Routing Interface

Topic Objective

To list the steps for configuring filters on an interface.

Lead-in

IP packet filtering provides a way for the network administrator to define what IP traffic is allowed to cross the router.



*****ILLEGAL FOR NON-TRAINER USE*****

A network administrator can configure input and output filters on key fields in the IP, TCP, User Datagram Protocol (UDP), and ICMP headers in each interface.

Delivery Tip

Demonstrate the steps for configuring filters.

To configure IP packet filtering in Routing and Remote Access, you create filters to allow or disallow certain types of traffic on a routing interface. An IP filter triggers a decision about what to do with the packet that is based on a match with the source, destination, and type of IP traffic. Configuring a filter involves selecting an interface, specifying an input or output filter, and specifying a filter action.

Selecting an Interface

Filters are defined on interfaces that you manage in Routing and Remote Access.

To select an interface:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), and then click **General**.
3. In the details pane, right-click the interface on which you want to add a filter, and then click **Properties**.

Specifying an Input or Output Filter

You can apply filters to either incoming or outgoing packets on an interface.

To specify an input or output filter, on the **General** tab, click either **Input Filters** or **Output Filters**.

Specifying a Filter Action

Filters are configured on an exception basis. You can configure the filter action to either receive all traffic except that which is specified, or drop all traffic except that which is specified. For example, you can configure a filter to allow all traffic except Telnet traffic (TCP port 23). Or, you can set up filters on a dedicated Web server to process only Web-based TCP traffic (TCP port 80) and HTTPS traffic (TCP port 443).

To specify a filter action, select one of the following options in the **IP Configuration** dialog box. You can select a filter action only after you have defined at least one filter.

- **Receive all packets except those that meet the criteria below.** Forwards all packets unless you specify to block them, which protects a network against specific threats. Use this setting when a high level of security is not required.
- **Drop all packets except those that meet the criteria below.** Forwards only packets that match specific criteria. Use this setting when a high level of security is required.

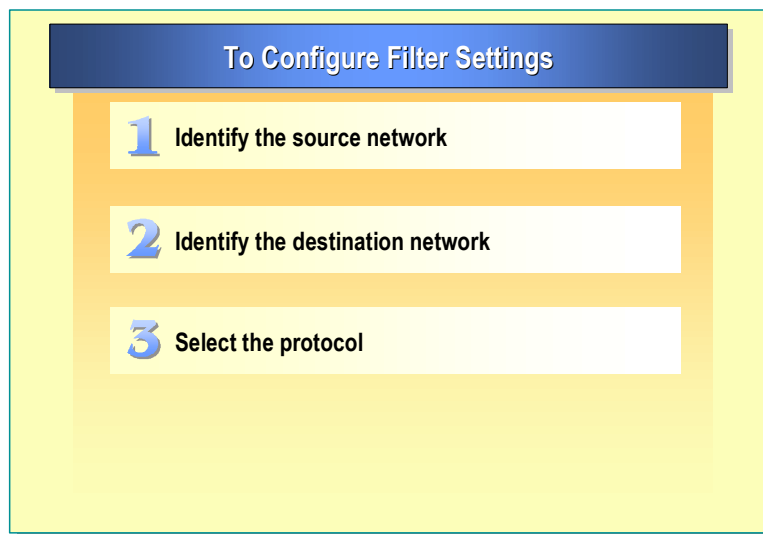
Configuring Filter Settings on an IP Routing Interface

Topic Objective

To list the steps for configuring filter settings on an interface.

Lead-in

Configuring filter settings generally requires a thorough understanding of the protocols involved.



*****ILLEGAL FOR NON-TRAINER USE*****

Configuring filter settings generally requires a thorough understanding of the protocols involved. After adding a filter, test your settings to make sure that the filters perform the action that you want and do not have any unintended side effects.

Delivery Tip

Demonstrate the steps for configuring filter settings.

To add a filter, configure the following settings in the **Add IP Filter** or **Edit IP Filter** dialog boxes. Depending on the intended action, you only need to define some of these settings when you create a filter.

1. Identify the source network:
 - **IP Address.** Type the source IP network ID or a source IP address.
 - **Subnet Mask.** Type the subnet mask corresponding to the source network ID, or type 255.255.255.255 for a source IP address. The subnet mask bits must encompass all of the bits being used in the IP Address field. The IP address cannot be more specific than the subnet mask.
2. Identify the destination network:
 - **IP Address.** Type the destination IP network ID or a destination IP address.
 - **Subnet Mask.** Type the subnet mask corresponding to the destination network ID, or type 255.255.255.255 for a destination IP address. The subnet mask bits must encompass all of the bits being used in the IP Address field. The IP address cannot be more specific than the subnet mask.

3. Select the protocol:

- **TCP**. Select this option to specify a source TCP port and a destination TCP port. You can specify one or both. If you do not specify a port, the setting defaults to 0, meaning any port.
- **TCP (Established)**. Select this option to only include TCP packets that are part of a TCP connection that has been previously established.
- **UDP**. Select this option to specify a source UDP port and a destination UDP port. You can specify one or both. If you do not specify a port, the setting defaults to 0, meaning any port.
- **ICMP**. Select this option to specify ICMP code and an ICMP type. You can specify one or both. If you do not specify a port, the setting defaults to 255, meaning any code or any type.
- **Any**. Select this option to make *any* IP protocol value applicable.
- **Other**. Select this option to specify any IP protocol. You must specify the protocol by number.

The file *systemroot\system32\drivers\etc\protocol* contains a list of protocols compatible with Windows 2000 and the number for each protocol. You can enable Windows 2000 to recognize additional protocols by editing this file.

Note To identify the ports that an application uses, see the documentation for that application. For a list of protocol numbers and well-known ports, see RFC 1700 under **Additional Reading** on the Student Materials compact disc. For a list of ports that Windows 2000 uses, see appendix C, “Port Assignments for Commonly Used Services,” under **Appendices** on the Web page on the Student Materials compact disc.

◆ Implementing Demand-Dial Routing

Topic Objective

To identify the topics relevant to configuring demand-dial connections.

Lead-in

You can configure a demand-dial connection for locations that need occasional network connectivity to the main corporate network.

- Overview of Demand-Dial Routing
- Configuring Demand-Dial Connections
- Configuring IP Addressing for Inbound Demand-Dial Connections
- Restricting Demand-Dial Connections
- Configuring Static Routes for a Demand-Dial Interface

*****ILLEGAL FOR NON-TRAINER USE*****

Some locations, such as branch offices, may only need occasional network connectivity to the main corporate network. To accommodate this need, you can configure a demand-dial connection that, when necessary, can use any remote access connection to connect to the main corporate network.

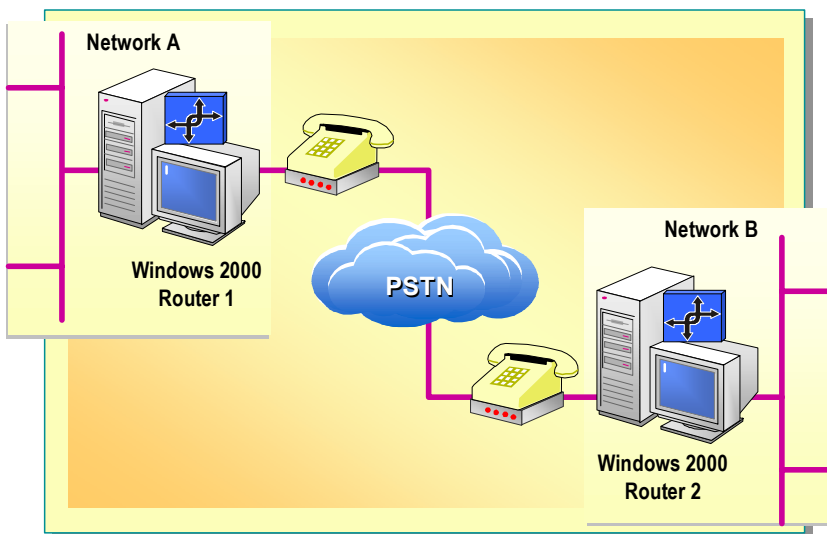
Overview of Demand-Dial Routing

Topic Objective

To illustrate the demand-dial routing process.

Lead-in

By using a demand-dial interface, a Windows 2000–based router can initiate a connection to a remote site when the router receives the packet to be routed.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Demand-dial routing can significantly reduce your connection costs by using existing dial-up telephone lines instead of leased lines.

Routing and Remote Access can route packets across other communications networks, such as the public switched telephone network (PSTN). By using a demand-dial interface, a Windows 2000–based router can initiate a connection to a remote site when the router receives the packet to be routed. The connection is initiated only when data is sent to or from a remote site. When no data has been sent over the link for a specified amount of time, the link is disconnected. By making a demand-dial connection, you can use existing dial-up telephone lines, instead of leased lines, for low-traffic situations. Demand-dial routing can significantly reduce your connection costs.

The Windows 2000–based router includes support for:

- *Demand-dial filters*, which are used to specify the type of traffic that enables the router to establish the connection.

Note Demand-dial filters are separate from IP packet filters, which you configure to specify what traffic is allowed into and out of an interface after the connection is made.

- *Dial-out hours*, which are used to specify the hours that a router is allowed to dial out to make demand-dial connections.

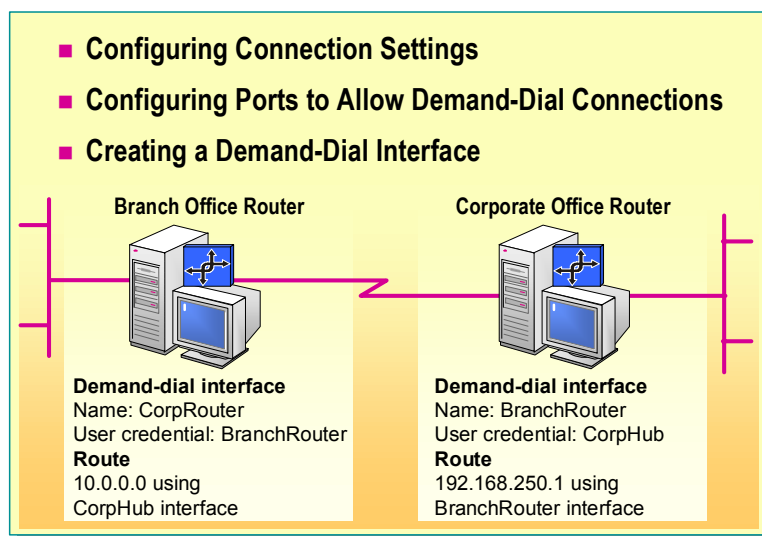
Configuring Demand-Dial Connections

Topic Objective

To illustrate a demand-dial routing connection.

Lead-in

You need to configure the routers at both locations to implement a demand-dial connection between a branch office and a corporate office.



*****ILLEGAL FOR NON-TRAINER USE*****

This deployment assumes a demand-dial connection between a branch-office router and a corporate-office router. You can also apply this deployment to the demand-dial connections between two corporate offices.

To implement a two-way, initiated demand-dial routing connection from a branch-office router to a corporate-office router, you must configure both the branch-office router and the corporate-office router to initiate and receive demand-dial connections.

To configure a corporate-office or branch-office router to support two-way initiated demand-dial connections:

- Configure connection settings to the corporate-office intranet.
- Configure ports to allow demand-dial connections.
- Configure demand-dial interfaces.

Configuring Connection Settings

After you install networking hardware and configure the relevant drivers, configure each of the dial-up adapters with:

- An IP address and a subnet mask that are valid for the network segment that connects the routers.
- The DNS and Windows Internet Name Service (WINS) servers that provide naming services for the corporate intranet.

Configuring Ports to Allow Demand-Dial Connections

For each dial-up port, you need to enable demand-dial connections in Routing and Remote Access.

To configure ports for demand-dial connections:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), right-click **Ports**, and then click **Properties**.
3. In the **Ports Properties** dialog box, click a device, and then click **Configure**.

Tip If **Ports** does not appear in the console tree, you must first enable demand-dial routing in the **Properties** dialog box for your computer.

4. In the **Configure Device** dialog box for the device, select the **Demand-dial routing connections (inbound and outbound)** check box if necessary, and then click **OK** twice.

Creating a Demand-Dial Interface

You create a demand-dial interface by using the Demand-Dial Interface wizard in Routing and Remote Access.

To create a demand-dial interface:

1. Open Routing and Remote Access.
2. In the console tree, right-click **Routing Interface**, and then click **New Demand-dial Interface**.
3. In the Demand Dial Interface wizard, provide the following:
 - **Interface name.** Specify a name for the interface that represents the connection; for example, **CorpHub**.
 - **Connection type.** Click **Connect using a modem, ISDN adapter, or other physical device**.
 - **Select a device.** Click the device being used to create the connection. This page only appears when you have more than one device installed that is capable of making dial-up connections.
 - **Phone number or address.** Type the telephone number of the remote router. To specify alternate telephone numbers that Routing and Remote Access will dial when an initial connection attempt is unsuccessful, click **Alternates**, and then type additional telephone numbers.

Explain that the Demand-Dial Interface wizard automatically creates the account and sets its remote access permission to **Allow access**.

- **Protocols and security.** Select the protocols to route and select the **Add a user account so a remote router can dial in** check box.
- **Dial-in credentials.** Type the user credentials for authenticating the local router to the remote router. The name of the account is the same as the demand-dial **Interface name**; for example, **CorpHub**.
- **Dial-out credentials.** Type the user credentials for authenticating the remote router to the local router. For example, for the branch-office router, the name of the account is **BranchRouter**.

Important For two-way initiated demand-dial routing to work properly, the **Dial-out credentials** of the calling router must match the **Interface name** of the demand-dial interface on both sides of the connection.

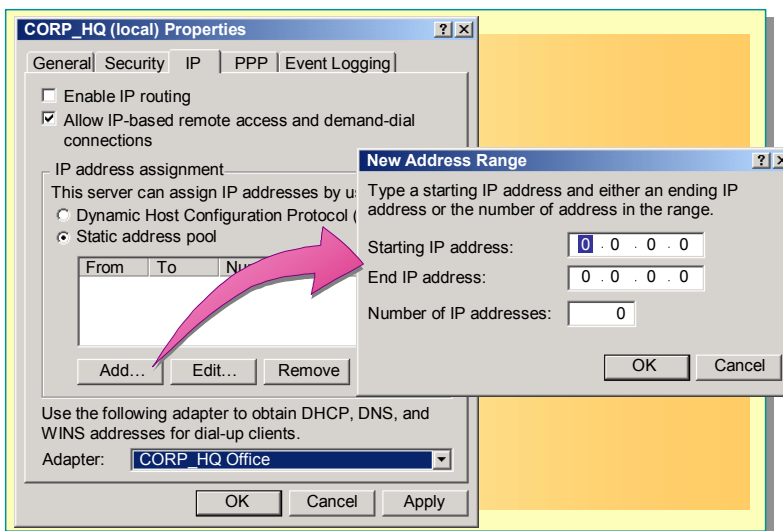
Configuring IP Addressing for Inbound Demand-Dial Connections

Topic Objective

To illustrate the interface for configuring static address pools for inbound demand-dial connections.

Lead-in

Each remote computer that connects to a remote access server running Windows 2000 on a TCP/IP network is automatically provided an IP address.



*****ILLEGAL FOR NON-TRAINER USE*****

Each remote computer that connects to a remote access server running Windows 2000 on a TCP/IP network is automatically provided an IP address. The remote access server obtains the IP address that is allocated to the remote access client either from a DHCP server or from a static range of IP addresses that the Administrator assigns to the remote access server.

Using Static IP Address Pools

When the remote access server is configured to use a static pool of addresses, each range of IP addresses can be entered as either:

- A starting IP address and an ending IP address for the range
- or-
- A starting IP address and the total number of IP addresses in the range

To configure IP address assignment for inbound demand-dial connections:

1. Open Routing and Remote Access.
2. In the console tree, right-click *server* (where *server* is the name of your computer), and then click **Properties**.
3. Click the **IP** tab, and then click **Static address pool**.
4. Click **Add**, and then configure the ranges of IP addresses that are dynamically allocated to demand-dial routers.

If the static IP address pool consists of ranges of IP addresses that are a subset of the range of IP addresses for the network to which the remote access server is attached, ensure that the ranges of IP addresses in the remote access IP address pool are not assigned to other hosts either statically or through DHCP.

Restricting Demand-Dial Connections

Topic Objective

To identify the topics relevant to restricting demand-dial connections.

Lead-in

To prevent the calling router from making unnecessary on-demand dial-up connections, you can restrict connection activity by configuring demand-dial filtering and dial-out hours.

- **Configuring Demand-Dial Filtering**
- **Configuring Dial-Out Hours**

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Use demand-dial filtering and dial-out hours to prevent a calling router from making unnecessary on-demand dial-up connections.

To prevent the calling router from making unnecessary on-demand dial-up connections, you can restrict connection activity by configuring demand-dial filtering and dial-out hours.

Configuring Demand-Dial Filtering

You can set demand-dial filters to permit or deny the type of IP traffic that can create a connection. For example, although ICMP traffic does not use much network bandwidth, a single ping can cause an expensive demand-dial connection to be connected. You can prevent ICMP traffic from initiating a demand-dial connection by creating a demand-dial filter to pass all traffic except ICMP.

To configure demand-dial filtering:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), and then click **Routing Interfaces**.
3. In the details pane, right-click the demand-dial interface that you want to configure, and then click **Set IP Demand dial Filters**.
4. In the **Set Demand-Dial Filters** dialog box, click one of the following options below **Initiate connection**. You can click an option only after you have defined at least one filter:
 - **Only for the following traffic**. This setting is used for connecting to a few networks or selected protocols. Use this setting when the dial-up connection is expensive and the connection is only used occasionally.
 - **For all traffic except**. This setting is used for allowing most traffic to initiate a dial-up connection, except for specific traffic. Use this setting to allow all packets to initiate the connection, with only a few specific exceptions.

5. Click **Add**.
6. In the **Add IP Filter** dialog box, specify the IP address, subnet mask, and protocol for the source and destination network.
7. Click **OK** to accept the changes, and then close all open dialog boxes.

Although demand-dial rules perform a different role from routing filters, they both use the same format.

Important To prevent the demand-dial connection from being established for traffic that the IP packet filters discard, configure the same set of filters for demand dialing that you configured for IP packet filtering.

Configuring Dial-Out Hours

You can set dial-out hours to permit or deny a day or time for creating a connection. For example, you can configure a demand-dial connection that is only to be used during off-peak hours.

To configure dial-out hours:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), and then click **Routing Interfaces**.
3. In the details pane, right-click the demand-dial interface that you want to configure, and then click **Dial-out Hours**.
4. In the **Dial-out Hours** dialog box, click either **Permitted** or **Denied**, click the appropriate day and time boxes, and then click **OK**.

Configuring Static Routes for a Demand-Dial Interface

Topic Objective

To identify the tasks for configuring static routes for a demand-dial interface.

Lead-in

For two-way communication to occur across a demand-dial link, you must establish static routes on both sides of the link.

- **Adding Static Routes**
- **Testing Static Routes**
 - Verifying the connection status
 - Using command-line utilities

*****ILLEGAL FOR NON-TRAINER USE*****

For two-way communication to occur across a demand-dial link, you must establish static routes on both sides of the link. On each side of the link, you must create static routes for all networks to which you connect by using the demand-dial link. After configuring demand-dial connections, add static routes for demand-dial connections so that the routers can initiate the connection. After configuring the static routes, use the **ping** or **tracert** command to test the demand-dial connection.

Adding Static Routes

To add a static route:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), and then click **Static Routes**.
3. Right-click **Static Routes**, and then click **New Static route**.
4. In the **Static Route** dialog box, select the interface for the demand-dial connection, and then enter the destination, network mask, gateway, and metric.

Note The gateway setting is unavailable for a demand-dial interface.

Testing Static Routes

After you configure static routes, you can send packets across the demand-dial interface to test the demand-dial connection.

Verifying the Connection Status

Before testing the connection, ensure that the demand-dial connection state is disconnected. To verify the status of a connection, in the console tree, click **Routing Interface**, and then in the details pane, view the **Connection Status** column for the demand-dial interface.

Using Command-Line Utilities

Use either the **ping** or **tracert** command to send ICMP packets across the demand-dial interface. With the **ping** command, use the **-t** option to ping the specified host continuously. If you do not use **-t**, the **ping** command only sends four packets and then stops. This is typically not long enough for the router to establish a connection and receive results.

To use **ping** to test a static route, type **ping -t IP_address** (where *IP_address* is the IP address of a host on the network to which you have configured a route).

To use **tracert** to test a static route, type **tracert IP_address** (where *IP_address* is the IP address of a host on the network to which you have configured a route).

Note When using a utility to test a connection for the first time, the results are unsuccessful because the demand-dial interface is not active. However, after sending the first packet, the interface is activated. After the connection has been established, subsequent use of the testing utility should be successful.

◆ Configuring the Routing Information Protocol

Topic Objective

To identify the topics relevant to configuring RIP.

Lead-in

You can use RIP to dynamically build routing tables for all routers in your network.

- Routing Protocols
- RIP Operation
- Adding the RIP Protocol
- Adding an Interface to Support RIP
- Configuring a RIP Interface

*****ILLEGAL FOR NON-TRAINER USE*****

After you configure your router to route packets between networks, you need a way to dynamically update the routing table if a change occurs on the network. On larger networks, it is not possible to configure all routing tables manually by changing static routes each time that a change occurs.

You can use routing protocols, such as the Routing Information Protocol (RIP), to automatically manage the routing table changes that become necessary because of network changes. RIP dynamically builds routing tables by announcing the contents of its routing table to its configured interfaces. Routers connected to those interfaces receive these announcements and use them to build the appropriate routing tables. Those routers then make announcements to build the routing tables for all routers in your network. Collectively, the RIP process prevents the management of the routing tables from becoming an administrative burden.

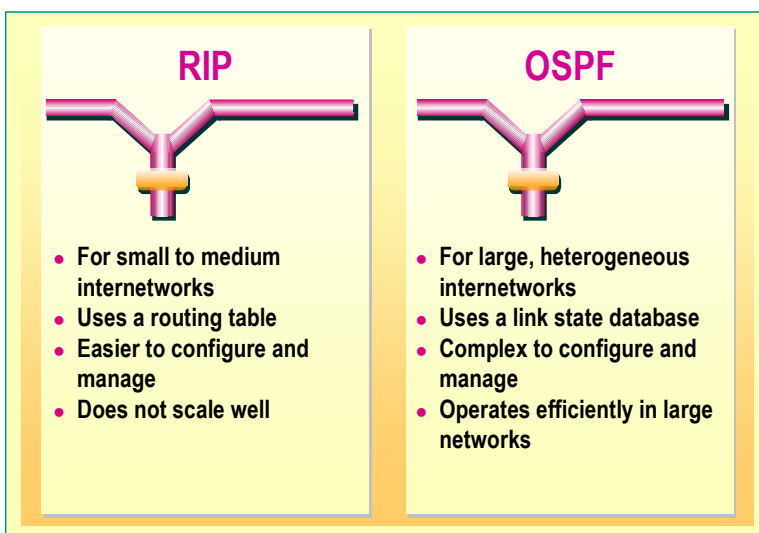
Routing Protocols

Topic Objective

To compare the RIP and OSPF routing protocols.

Lead-in

Routers use routing protocols to exchange information between routers to propagate network address and connection information.



*****ILLEGAL FOR NON-TRAINER USE*****

Routers use routing protocols to exchange information between routers to propagate network address and connection information. The two most common IP routing protocols that are used on intranets are RIP and Open Shortest Path First (OSPF).

RIP

RIP is designed for exchanging routing information within a small- to medium-sized internetwork. A RIP router maintains a routing table and periodically sends announcements to inform other RIP routers on the network about which networks it can reach and which it can no longer reach. RIP version 1 uses IP broadcast packets for its announcements, whereas RIP version 2 uses IP multicast packets for its announcements.

Compared with other protocols, RIP is simple to configure and deploy. However, as networks grow larger in size, the periodic announcements by each RIP router can cause excessive traffic on the network. RIP is typically used in networks with up to 50 servers.

Note RIP is also the name of a similar but separate routing protocol for IPX networks.

OSPF

OSPF is a link-state protocol based on the Shortest Path First (SPF) algorithm that computes the shortest path between one source node and the other nodes in the network.

OSPF allows a router to calculate the shortest path for sending packets to each node. The router sends information about the nodes to which it is linked to other routers on the network in order to accumulate link-state information and make its calculations. The information that the router sends is called link-state advertisements.

OSPF routers maintain a “map” of the network that is updated after any change in the network topology. This map is called the link-state database. OSPF routers maintain both a link-state database and a routing table.

OSPF was designed in response to the inability of RIP to serve large, heterogeneous internetworks. The advantage of OSPF, compared with other routing protocols, is that it operates efficiently in large networks because it computes the best route to use, and requires fewer status messages. Unlike RIP, OSPF does not advertise all known routes to other routers, but only changes to its routes. The disadvantage of OSPF is its complexity: It is harder to configure and requires more management time than RIP.

Note For more information about RIP, RIP version 2, and OSPF version 2, see RFC 1058, RFC 2328, and RFC 2453 under **Additional Reading** on the Student Materials compact disc.

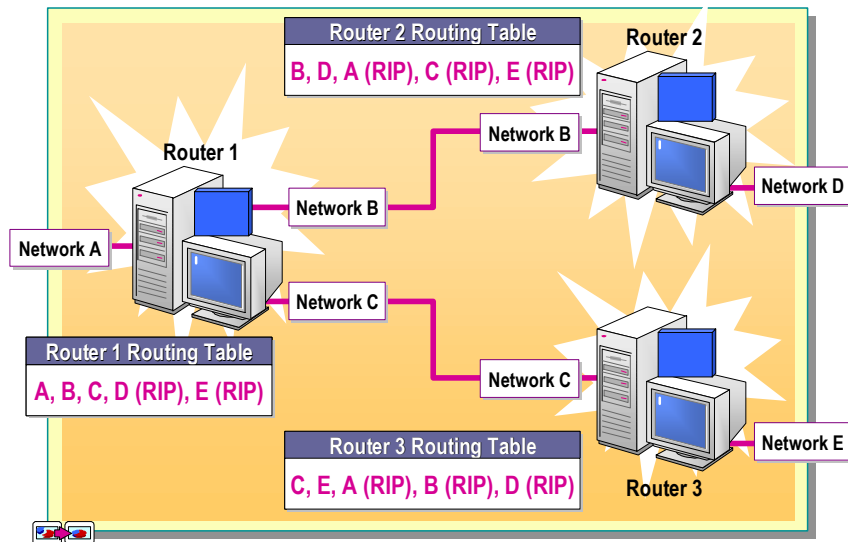
RIP Operation

Topic Objective

To illustrate the RIP operation process.

Lead-in

A router uses RIP to constantly build its routing table, until all networks are represented in a router's routing table.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

Use the slide graphic to explain the example in the module.

A router that uses RIP shares routing table information with the other routers in a network by announcing the contents of its routing table to all of its interfaces, and by receiving the same type of announcements from other routers. By using RIP, a router is constantly updating its routing table, until all networks are represented in a router's routing table.

For example, all routers begin with a default routing table that contains a routing entry for all of the networks to which the router is directly connected, as shown in the following list.

Router	Routing table entries
Router 1	A, B, C
Router 2	B, D
Router 3	C, E

Then, Router 2 sends a RIP announcement on all network interfaces, advertising that it has entries for networks B and D. The routing tables of the routers are updated, as shown in the following list.

Router	Routing table entries
Router 1	A, B, C, D (RIP)
Router 2	B, D
Router 3	C, E

Next, Router 3 sends a RIP announcement on all network interfaces, advertising that it has entries for C and E. The routing tables of the routers are updated again, as shown in the following list.

Router	Routing table entries
Router 1	A, B, C, D (RIP), E (RIP)
Router 2	B, D
Router 3	C, E

Finally, Router 1 sends a RIP announcement on all network interfaces, advertising entries for A, B, C, D, and E. The routing tables of the routers are updated yet again, as shown in the following list.

Router	Routing table entries
Router 1	A, B, C, D (RIP), E (RIP)
Router 2	B, D, A (RIP), C (RIP), E (RIP)
Router 3	C, E, A (RIP), B (RIP), D (RIP)

Now, all routers are aware of all of the networks to which they are connected. In RIP version 1, this announcement is always a broadcast. In RIP version 2, routers can instead use multicasts for these announcements, which reduces broadcast load on the network.

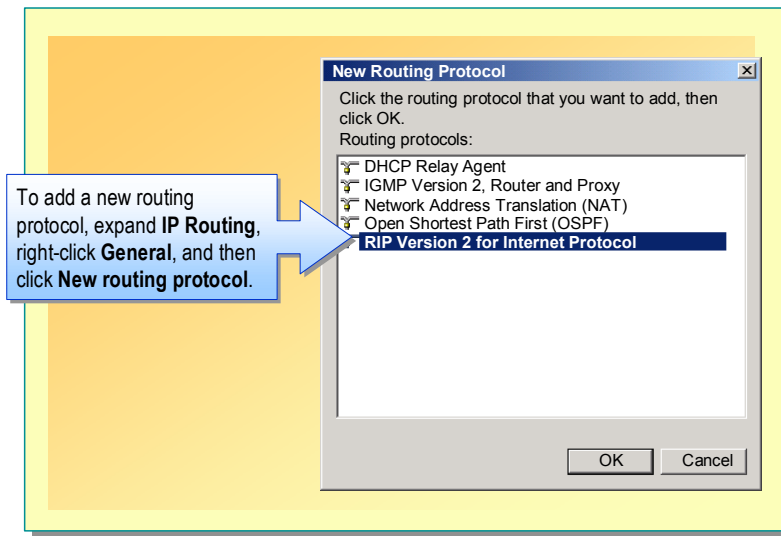
Adding the RIP Protocol

Topic Objective

To illustrate the interface for adding the RIP protocol.

Lead-in

You use Routing and Remote Access to add the RIP protocol.



*****ILLEGAL FOR NON-TRAINER USE*****

You use Routing and Remote Access to add the RIP protocol.

To add RIP for IP:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), expand **IP Routing**, right-click **General**, and then click **New routing protocol**.
3. From the list of routing protocols, click **RIP version 2 for Internet Protocol**, and then click **OK**.

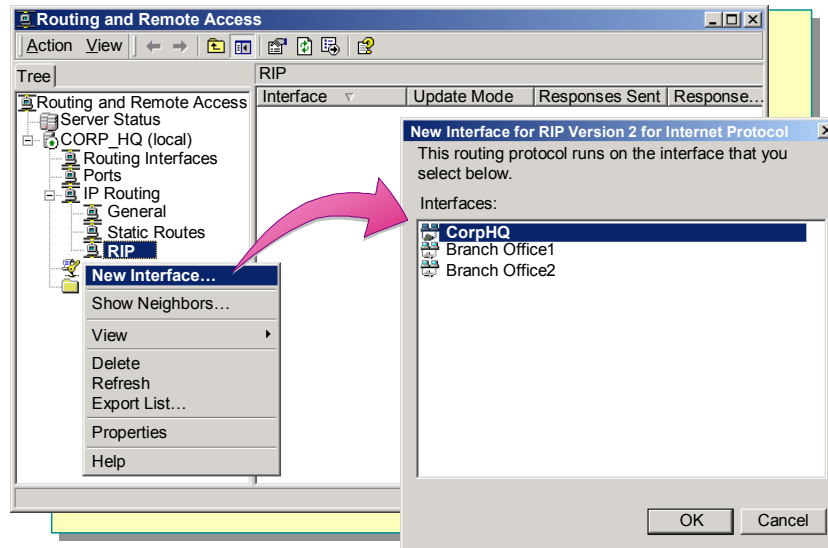
Adding an Interface to Support RIP

Topic Objective

To illustrate the interface for adding a routing interface that supports RIP.

Lead-in

After adding the RIP protocol, you can add an interface that supports RIP.



*****ILLEGAL FOR NON-TRAINER USE*****

After adding the RIP protocol, you must add an interface that supports RIP from the list of interfaces that RIP uses on your computer. By default, interfaces do not support RIP until you add them.

To add an interface that supports RIP:

1. Open Routing and Remote Access.
2. Expand *server* (where *server* is the name of your computer), expand **IP Routing**, and then click **RIP**.
3. Right-click **RIP**, and then click **New Interface**.
4. In the **New Interface for RIP Version 2 for Internet Protocol** dialog box, click the interface that you want to add, and then click **OK**.

Routing and Remote Access prompts you to configure RIP for the interface.

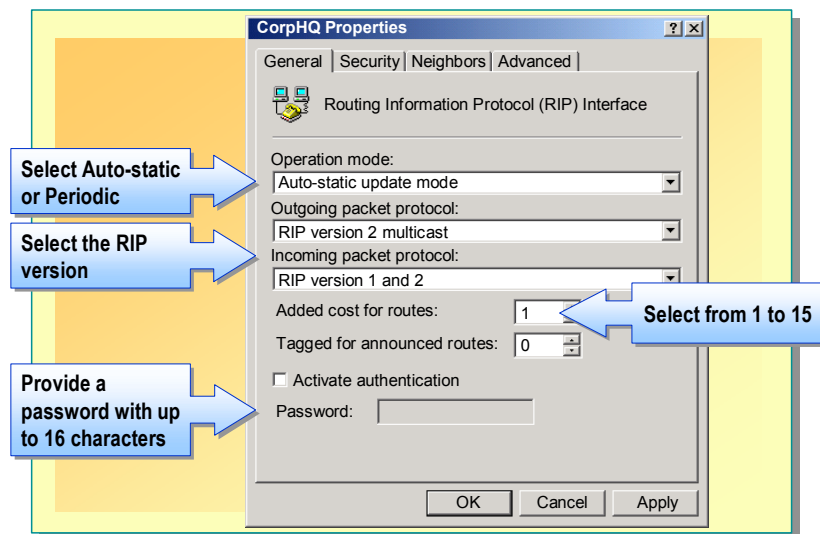
Configuring a RIP Interface

Topic Objective

To identify the configuration settings for a RIP interface.

Lead-in

After adding an interface that supports RIP, you can configure settings for the update modes, versions, costs, and authentication.



*****ILLEGAL FOR NON-TRAINER USE*****

After adding an interface that supports RIP, you must configure settings for the update modes, versions, costs, and authentication.

Routing and Remote Access prompts you to configure RIP when you add an interface to RIP. You can also configure an interface that has been previously added.

To configure an interface for RIP:

1. Open Routing and Remote Access.
2. In the console tree, expand *server* (where *server* is the name of your computer), expand **IP Routing**, and then click **RIP**.
3. In the details pane, right-click the interface that you want to configure for RIP, and then click **Properties**.

Configuring Operation Mode

A RIP router periodically sends announcements that contain all of its routing table entries to inform other local RIP routers of the networks that it can contact. RIP routers can also communicate routing information through triggered updates. With triggered updates, the routing information is sent immediately instead of waiting for the next periodic announcement.

You can select the following operation mode settings in the **Operation mode** box on the **General** tab:

- **Auto-static update mode.** Sends RIP announcements only when other routers request an update. Routes learned over RIP are marked as static routes and remain in the routing table until manually deleted. Auto-static update is the default setting for a demand-dial interface.
- **Periodic update mode.** Sends RIP announcements periodically, as specified by the **Periodic announcement interval** setting on the **Advanced** tab. Periodic update is the default setting for a LAN interface.

Configuring Protocols for RIP Announcements

You can select the following protocols for outgoing RIP announcements in the **Outgoing packet protocol** box on the **General** tab:

- **RIP version 1 broadcast.** Sends RIP version 1 announcements as broadcasts. Use this setting if you are in an environment that contains only RIP version 1 routers.
- **RIP version 2 broadcast.** Sends RIP version 2 announcements as broadcasts. This is the default protocol for a LAN interface. Use this setting if you are in a mixed environment containing both RIP version 1 and RIP version 2.
- **RIP version 2 multicast.** Sends RIP version 2 announcements as multicasts. This is the default protocol for a demand dial-up interface. Use this setting only if the adjacent RIP network routers connected to this interface are also RIP version 2 routers.
- **Silent RIP.** Disables outgoing RIP announcements. The router listens to other announcements and updates its own routing table, but does not send announcements of its own routes.

You can select the following protocols for incoming RIP announcements in the **Incoming packet protocol** box on the **General** tab:

- **RIP version 1 and 2.** Accepts both RIP version 1 and RIP versions 2 announcements. This is the default selection.
- **RIP version 1.** Accepts only RIP version 1 announcements.
- **RIP version 2.** Accepts only RIP version 2 announcements.

Configuring the Cost of a RIP Interface

The cost setting specifies a numeric value that is associated with sending packets with the interface. Because RIP uses hops for interface cost, this number is added to the hop count as advertised in the RIP message. When a RIP router has multiple routes to a remote network in its routing table, the router always tries to use the route with the lowest cost. Setting a high cost for a routing interface ensures that the interface is only used when other lower-cost interfaces are not available.

You can select a value from 1 to 15. A high value indicates a slower route.

Activating Authentication

To require router authentication, on the **General** tab, select the **Activate authentication** check box, and then type a password in the **Password** box. RIP authentication requires that RIP advertisements include a password. For authentication, all incoming RIP version 2 packets must contain the same password, so you need to configure all routers that are connected to the interface with the same password. Because RIP uses clear-text passwords, this option is primarily used for identification and provides only minimal security.

Key Point

This option is primarily used for identification rather than for security.

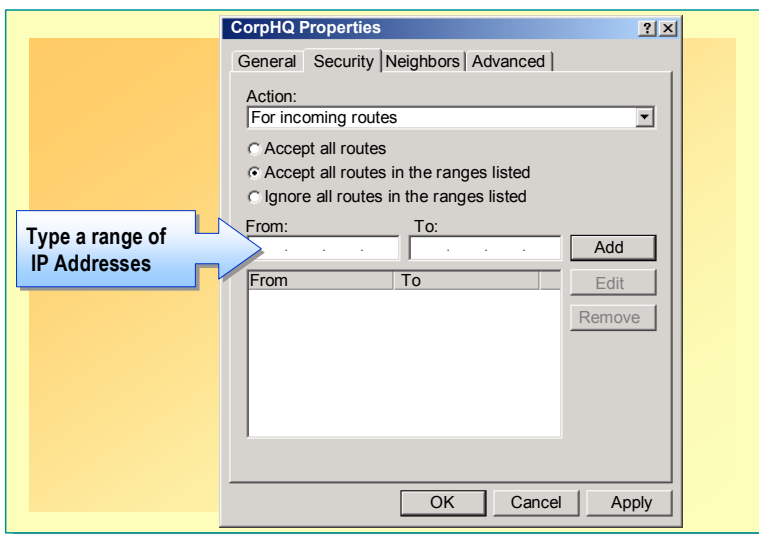
Configuring Route Filtering

Topic Objective

To identify the settings for configuring route filtering.

Lead-in

You set security to specify how a router accepts routes and how a router announces routes.



*****ILLEGAL FOR NON-TRAINER USE*****

You set security to specify how a router accepts routes and how a router announces routes. You can use the security settings to prevent unauthorized routers from sending unauthorized route information. For example, you can prevent routers on the Internet from advertising routes to your router that are internal to your network. You can also prevent routes from being advertised on an external interface to ensure confidentiality of your network topology.

To configure routes for a RIP interface:

1. Open Routing and Remote Access.
2. Expand *server* (where *server* is the name of your computer), expand **IP Routing**, and then click **RIP**.
3. In the details pane, right-click the interface that you want to configure, and then click **Properties**.
4. On the **Security** tab, on the **Action** list, click **For incoming routes** or **For outgoing routes**.

Click one of the following options:

- **Accept all routes**
- **Accept all routes in the ranges listed**
- **Do not announce all routes in the ranges listed**

5. Specify a range of IP address for the option, if necessary, and then click **OK**.

Configuring RIP for a Non-Broadcast Network

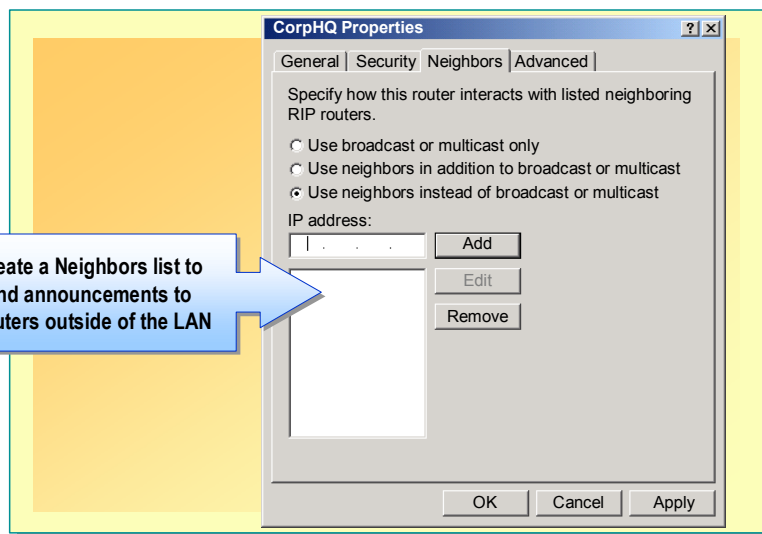
Topic Objective

To identify the settings for creating a list of routers in a non-broadcast network.

Lead-in

You use a neighbors list to send RIP messages between specific routers in non-broadcast networks.

Create a Neighbors list to send announcements to routers outside of the LAN



*****ILLEGAL FOR NON-TRAINER USE*****

You use a neighbors list to send RIP messages between specific routers in non-broadcast networks. A neighbors list identifies a group of routers that are not on the same network segment as the router that you are configuring, but which may receive announcements. You create a neighbors list on the **Neighbors** tab in the **RIP Properties** dialog box.

To configure a neighbors list for a RIP interface:

1. Open Routing and Remote Access.
2. Expand *server* (where *server* is the name of your computer), expand **IP Routing**, and then click **RIP**.
3. In the details pane, right-click the interface that you want to configure, and then click **Properties**.

Briefly explain the difference between unicast and multicast announcements.

On the **Neighbors** tab, click one of the following options:

- **Use broadcast or multicast only.** Sends RIP announcements by using the outgoing packet protocol specified on the **General** tab. This is the default setting.
 - **Use neighbors in addition to broadcast or multicast.** Sends RIP announcements by unicast in addition to using the outgoing packet protocol specified on the **General** tab.
 - **Use neighbors instead of broadcast or multicast.** Sends RIP announcements by unicast only to the specified neighboring routers. Use this selection if you have non-broadcast networks, such as Frame Relay.
4. Specify one or more IP addresses, and then click **OK**.

Lab B: Configuring a Windows 2000–Based Router

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure routing interfaces, filtering, demand-dial interfaces, and RIP.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure router interfaces.
- Configure filtering on router interfaces.
- Configure a demand-dial interface.
- Configure a router to use RIP.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller in native mode
- A lab partner with a similarly configured computer
- IP addresses for the two network adapters in your computer
- IP addresses for the two network adapters in your partner's computer

If you are unsure about any of these values, please ask your instructor.

Adapter

Record IP address here

Your Classroom adapter

Your PartnerNet adapter

Your partner's Classroom adapter

Your partner's PartnerNet adapter

Scenario

Your company is expanding to more locations, and you need to connect these locations to the head-office network. Some branch-office locations do not yet have permanent connections available, so you will configure demand-dial connections for these offices. Also, now that your network is becoming large, you can no longer manually maintain the routing tables. To make routing more efficient, you will install RIP to build and maintain routing tables automatically.

Estimated time to complete this lab: 30 minutes

Exercise 1

Configuring a Router to Filter Protocols

Scenario

You have configured a router for your branch-office network so that you have connectivity to your head-office network, but for security and management reasons, you want to stop certain protocols from passing across the router to other networks.

Goal

In this exercise, you will work with your partner to configure the router interface for your branch-office router so that it will not route ICMP request traffic, as used by the **ping** command.

Tasks	Detailed Steps
 Important: Perform the following procedures only on the computer with the higher student number.	
1. Configure the Classroom router interface so that it will transmit all packets except ICMP packets with an ICMP type of 8 and an ICMP code of 0 .	- Log on as <code>administrator@domain.nwtraders.msft</code> (where <i>domain</i> is the name of your domain) with a password of password. - Open Routing and Remote Access from the Administrative Tools menu. - In the console tree, expand <i>server</i> (where <i>server</i> is the name of your computer), expand IP Routing, and then click General. - In the details pane, right-click Classroom, and then click Properties. - In the Classroom Properties dialog box, click Output Filters. - In the Output Filters dialog box, click Add. - In the Add IP Filter dialog box, in the Protocol box, click ICMP. - In the ICMP type box, type 8. - In the ICMP code box, type 0 and then click OK. - Click OK to close the Output Filters dialog box, and then click OK to close the Classroom Properties dialog box. - Minimize Routing and Remote Access.
 Important: Perform the following procedure on both student computers. The student with the higher student number must have completed the previous procedure before continuing to this task.	

(continued)

Tasks	Detailed Steps
2. Ping the instructor computer (London), and then view the shared resources on London by typing net view \\192.168.z.200	a. At a command prompt, type ping 192.168.z.200 (where <i>z</i> is the number assigned to your classroom), and then press ENTER.  <i>You will receive a different error message on each computer. Ping will resolve London to the IP address for London on both, but you will receive a “Destination host unreachable” message on the computer with the higher student number and a “Request timed out” message from the computer with the lower student number. This indicates that the output filter is working and blocking ICMP packets from being transmitted from the Classroom interface.</i> b. Type net view \\192.168.z.200 and then press ENTER.  <i>On both computers, you will see the shared resources at \\london. This means that the filter is only filtering out ICMP packets.</i> c. Close the command prompt window.
 Note: You have configured the Classroom adapter to filter ICMP traffic from being transmitted, but it will not block incoming ICMP traffic. If you ping your computer from the instructor computer, London, the ping will be successful.	
 Perform the following procedure only on the computer with the lower student number.	
3. In Routing and Remote Access, add your partner’s computer as a server, and then configure an input filter for your partner’s Classroom adapter that filters ICMP packets of type 8 and code 0.	a. Open Routing and Remote Access from the Administrative Tools menu. b. In the console tree, expand <i>partner_server</i> (where <i>partner_server</i> is the name of your partner’s computer), expand IP Routing, and then click General. c. In the details pane, right-click Classroom, and then click Properties. d. In the Classroom Properties dialog box, click Input Filters. e. In the Input Filters dialog box, click Add. f. In the Add IP Filter dialog box, in the Protocol box, click ICMP. g. In the ICMP type box, type 8 h. In the ICMP code box, type 0 and then click OK. i. Click OK to close the Input Filters dialog box, and then click OK to close the Classroom Properties dialog box. j. Minimize Routing and Remote Access.
 Note: You have successfully filtered ICMP echo requests from being passed by your router. If you ping your computer from the instructor computer, London, Ping will reply “Request timed out.”	
 Perform the following procedure only on the computer with the higher student number.	

(continued)

Tasks	Detailed Steps
4. In Routing and Remote Access, remove the input and output filter.	a. Restore Routing and Remote Access. b. In the console tree, expand <i>server</i> (where <i>server</i> is the name of your computer), expand IP Routing, and then click General. c. In the console pane, right-click Classroom, and then click Properties. d. In the Classroom Properties dialog box, click Input Filters. e. In the Input Filters dialog box, verify that the routing filter is selected, click Remove, and then click OK. f. In the Classroom Properties dialog box, click Output Filters. g. In the Output Filters dialog box, verify that the routing filter is selected, click Remove, and then click OK. h. Click OK to close the Classroom Properties dialog box. i. Minimize Routing and Remote Access.

Exercise 2

Configuring Demand-Dial Connections

Scenario

You want your branch office to have connectivity to your head-office network via a secure, remote connection. The remote connection need not be permanent, but it needs to connect automatically whenever data from the branch office is destined for the head-office network.

Goal

In this exercise, you will configure a demand-dial VPN connection from one computer to the classroom network, through the branch office router. You will then test this connection by pinging the instructor computer to activate the connection.

Tasks	Detailed Steps
 Perform the following procedure only on the computer with the higher student number.	
1. Create a user account for the demand-dial interface. Grant the user dial-in permissions. User logon name: routerx, (where <i>x</i> is your student number.) Password: password Grant this user dial-in permissions.	- Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand domain.nwtraders.msft (where <i>domain</i> is the name of your domain), and then click Users. - Right-click Users, point to New, and then click User. - In the New Object – User dialog box, in the First name box, type Routerx (where <i>x</i> is your student number). - In the New Object – User dialog box, under User logon name, type routerx, and then click Next. - In the Password and Confirm password boxes, type password - Click Next, and then click Finish. - In the console tree, right-click routerx, and then click Properties. - On the Dial-in tab, click Allow access, and then click OK. - Close Active Directory Users and Computers.
2. Configure your computer to be a remote access server, and configure the router component to support LAN and demand-dial routing.	- Restore Routing and Remote Access. - In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Properties. - On the General tab, click LAN and demand-dial routing, select the Remote access server check box, and then click OK. - Click Yes to close the Routing and Remote Access message box.  <i>The Routing and Remote Access service is restarted to reflect the latest configuration changes.</i>

(continued)

Tasks	Detailed Steps
3. Configure both the Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) remote access ports to support both remote access connections and demand-dial routing connections.	- In the console tree, right-click Ports, and then click Properties. - In the Ports Properties dialog box, click WAN Miniport (PPTP), and then click Configure. - Verify that both the Remote access connections (inbound only) and Demand-dial routing connections (inbound and outbound) check boxes are selected, and then click OK. - Repeat steps b and c to configure WAN Miniport (L2TP) to allow remote access and demand-dial routing connections. - Minimize Routing and Remote Access.
 Perform the following procedure only on the computer with the lower student number.	
4. Configure your computer to be a remote access server, and configure the router component to support LAN and demand-dial routing.	- Restore Routing and Remote Access from the Administrative Tools menu. - In the console tree, right-click <i>server</i>, and then click Configure and Enable Routing and Remote Access. - In the Routing and Remote Access Server Setup wizard, click Next. - On the Common Configurations page, click Network router, and then click Next. - On the Routed Protocols page, under Protocols, verify that TCP/IP displays, and then click Next. - On the Demand-Dial Connections page, click Yes, and then click Next. - On the IP Address Assignment page, verify that Automatically is selected, and then click Next. - Click Finish to close the Routing and Remote Access Server Setup wizard.  <i>The Routing and Remote Access service will now start.</i>
5. Create a demand-dial interface called Head Office. The demand-dial interface must have the following properties: Connection Type: VPN VPN Type: Automatic Destination Address: IP address of your partner's PartnerNet adapter User name: <i>router.y</i> , where <i>y</i> is your partner's student number Domain: <i>domain</i> Password: <i>password</i>	- In the console tree, expand <i>server</i>, right-click Routing Interfaces, and then click New Demand-dial Interface. - In the Demand Dial Interface wizard, click Next. - On the Interface Name page, in the Interface name box, type head office and then click Next. - On the Connection Type page, click Connect using virtual private networking (VPN), and then click Next. - On the VPN Type page, verify that Automatic selection is selected, and then click Next. - On the Destination Address page, type the IP address of your partner's PartnerNet adapter, and then click Next. - On the Protocols and Security page, verify that Route IP packets on this interface is selected, and then click Next.

Tasks	Detailed Steps
5. (continued)	h. On the Dial Out Credentials page, in the User name box, type router<i>y</i> (where <i>y</i> is your partner's student number). i. In the Domain box, type <i>domain</i> j. In the Password and Confirm password boxes, type password k. Click Next, and then click Finish.
6. Add a static route to initiate the demand-dial interface. Use the following information to create the route: Interface: Head Office Destination: 192.168.1.0 Network mask: 255.255.255.0 Select the Use this route to initiate demand-dial connections check box.	a. In the console tree, expand IP Routing, right-click Static Routes, and then click New Static Route. b. In the Static Route box, in the Interface box, verify that head office is selected. c. In the Destination box, type 192.168.1.0 d. In the Network mask box, type 255.255.255.0 e. Verify that the Use this route to initiate demand-dial connections check box is selected, and then click OK. f. Minimize Routing and Remote Access.
7. Ping the instructor computer by IP address, and then verify that the demand-dial connection has been initiated by checking in Routing and Remote Access.	a. At a command prompt, type ping 192.168.z.200 (where <i>z</i> is the number assigned to your classroom), and then press ENTER.  <i>The Ping will receive successful replies after initiating the demand-dial connection. If the connection has not yet been made, try step a again.</i> b. Close the command prompt window, and then restore Routing and Remote Access. c. In the console tree, right-click Routing Interfaces, and then click Refresh.  <i>The Head Office interface is now connected.</i> d. Close Routing and Remote Access.

Exercise 3

Configuring Windows 2000 to use RIP

Scenario

Your network is expanding, and you want RIP to automatically update routing tables so that you do not need to enter additional static routes.

Goal

In this exercise, you will add RIP to your branch-office router and examine the routing tables that result to verify the correct operation.

You will work with a partner during this exercise to configure RIP on the computer with the higher student number. So that both partners get experience in configuring RIP, the lab instructions request that different parts of the configuration of RIP be performed on different computers.

Tasks	Detailed Steps
 Perform the following procedure only on the computer with the lower student number.	
1. Enable the Classroom network adapter, and clear the default gateway for the PartnerNet network adapter.	- Right-click My Network Places, and then click Properties. - In Network and Dial-up Connections, right-click Classroom, and then click Enable. - In Network and Dial-up Connections, right-click PartnerNet, and then click Properties. - In the PartnerNet Properties dialog box, click Internet Protocol (TCP/IP), and then click Properties. - In the Default gateway box, delete the IP address, and then click OK. - Click OK to close the PartnerNet Properties dialog box. - Close Network and Dial-up Connections.
 Perform the following procedure only on the computer with the higher student number.	
2. Add the RIP protocol and add the Classroom interface to support RIP.	- Restore Routing and Remote Access. - In the console tree, expand <i>server</i> (where <i>server</i> is the name of your computer), expand IP Routing, and then click General. - In the console tree, right-click General, and then click New Routing Protocol. - In the New Routing Protocol box, under Routing Protocols, click RIP Version 2 for Internet Protocol, and then click OK.  <i>RIP is added to the console tree below IP Routing. Any routing protocols that you add will appear in the console tree under each network protocol that they support.</i> - In the console tree, right-click RIP, and then click New Interface. - Under Interfaces, click Classroom, and then click OK. - In the RIP Properties – Classroom Properties dialog box, verify that the Added cost for routes is 1, and then click OK.

(continued)

Tasks	Detailed Steps
 Perform the following procedure only on the computer with the lower student number.	
3. Add the PartnerNet interface to support RIP. Configure the PartnerNet interface with an Added cost for routes of 2.	- Open Routing and Remote Access from the Administrative Tools menu. - In the console tree, expand <i>partner_server</i> (where <i>partner_server</i> is the name of your partners computer), expand IP Routing, and then click RIP. - In the console tree, right-click RIP, and then click New Interface. - In the New Interface for RIP Version 2 for Internet Protocol dialog box, verify that PartnerNet is selected, and then click OK. - In the RIP Properties – PartnerNet Properties dialog box, in the Added cost for routes box, type 2 and then click OK.  <i>You have configured RIP on your branch-office router interfaces. After the other students in your class have added RIP to their computers, the routing tables for your computer will be updated by RIP.</i>
 Perform the following procedure on both student computers.	
4. In Routing and Remote Access, display the IP routing table for the computer with the higher student number.	- In Routing and Remote Access, under <i>server</i>, under IP Routing, right-click Static Routes, and then click Show IP Routing Table. - Drag the border of the window so that you can see all columns in the routing table.  <i>Notice that after waiting a short time, entries for other networks will appear in your routing table. The entries that RIP added have RIP in the Protocol column.</i>
 In the IP Routing table, there will be several entries for the different networks in your classroom. If there are two entries for the same network, how will the router choose which route to use?	
The router will use the route with the lowest cost. The cost of a route is equal to the sum of the costs per interface through which a packet will travel to reach the destination network.	
4. (continued)	c. Close the <i>server</i> – IP Routing Table window.

Exercise 4

Removing Routing and Remote Access

Goal

In this exercise, you will remove Routing and Remote Access.

Task	Detailed Steps
 Perform the following procedure on both student computers.	
1. Disable Routing and Remote Access on your computer, close all windows, and log off.	- In Routing and Remote Access, in the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Disable Routing and Remote Access. - Click Yes to close the Routing And Remote Access dialog box. - Close Routing and Remote Access, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Overview of Routers and Routing Tables
- Configuring Network Connections
- Enabling Routing by Using Routing and Remote Access
- Configuring Static Routes
- Configuring a Routing Interface
- Implementing Demand-Dial Routing
- Configuring the Routing Information Protocol

*****ILLEGAL FOR NON-TRAINER USE*****

1. You manage a large network with many computers that are connected to the same network by using hubs. Because of slowing network performance, you decide to segment the network by using routers. Describe two ways in which a router will help to increase available bandwidth to users.

A router will keep network traffic within certain subnets because each subnet will contain fewer computers. Because network traffic from one computer to another within a subnet will not be forwarded to other subnets, there is a reduced amount of traffic on each subnet. Also, a router does not forward broadcast traffic, which will reduce the number of broadcasts that each computer on the network receives.

2. What information does a router use to make decisions about where to forward IP packets?

Routers use their routing tables and the routing table entries to determine where to forward IP packets.

3. You have installed three network adapters in your server, and you must configure each of them with a specific IP address. The adapters look identical. How can you identify each adapter in the Windows 2000 interface so that you can more easily assign the correct IP address to each adapter?

Use the `ipconfig /all` command to display the name and physical address of each interface. The physical address of each interface is usually marked on each network adapter. Use this information to identify each adapter uniquely. When you have this information about each adapter, you can also rename the adapters.

4. You are configuring the interface of a router that will be connected directly to the Internet. This router will be forwarding DNS queries to an ISP. What three settings must you configure?

IP address, obtained from the address range you have received from the ISP; a subnet mask for the IP address range; and a DNS server IP address.

5. You have a Windows 2000–based server that you are currently using as a remote access server and that you also want to use as a router. When you open Routing and Remote Access, the option to **Configure and Enable Routing and Remote Access** is not available. How do you enable routing?

Open Routing and Remote Access, right-click your server, and then click Properties. On the General tab, select the Router check box, choose whether the router will support demand-dial routing, and then click OK.

6. You are testing network connectivity in your network after installing a Windows 2000–based router and enabling Routing and Remote Access. From the router, you can ping computers on networks that are connected to the router, but not computers on networks that are one or more routers away. What must you do to enable network communication?

Add static route entries for each of the networks that are not directly connected to the router, and then add a static route for your router's networks to the other routers in the network. If the other routers on your network support RIP, you can also install and configure the RIP protocol.

7. You are testing connectivity from one network to another. You notice that you are not able to ping any hosts in a remote network, but you can view shared resources on those hosts. What is a likely cause of this symptom?

Routing filters have been enabled on a router between the host that you are using and the hosts that you are pinging.

8. Your network has expanded, and you have added more routers. To make updating routing tables with static routes easier, you have installed RIP on all of the Windows 2000–based routers. After viewing the routing tables on the routers, you notice that there are no entries in the routing tables from RIP. What must you do so that RIP can update the routing tables?

Add the network interfaces to support RIP, so that the interfaces will both announce routes and listen to route announcements.