

Module 11: Configuring Internet Access for a Network

Contents

Overview	1
Options for Connecting a Network to the Internet	2
Configuring Internet Access by Using a Router	12
Configuring Internet Access by Using NAT	14
Lab A: Configuring Internet Access by Using NAT	20
Review	28



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:
45 Minutes

This module provides students with the knowledge and skills necessary to configure Internet access in a Microsoft® Windows® 2000 network.

Lab:
30 Minutes

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

- Describe the options that are available for connecting a network to the Internet.
- Configure Internet access by using a router.
- Configure Internet access by using network address translation (NAT).

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_11.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the white paper, *Connecting Your Network to the Internet* under **Additional Reading** on the Web page on the Student Materials compact disc.
- Read RFC 1631 *The IP Network Address Translator (NAT)*, under **Additional Reading** on the Web page on the Student Materials compact disc.
- Read the entire section, “Network Address Translator” in the Windows 2000 Server Resource Kit.

Module Strategy

Use the following strategy to present this module:

- Options for Connecting a Network to the Internet

This section is designed to provide an overview of options for connecting to the Internet by using a router, a firewall, NAT, Internet Connection Sharing, or a proxy server. Describe the options that are available for connecting a network to the Internet, but do not explain how to configure Internet access by using a router or by using NAT, because those topics are covered later in the module.

Explain how to enable Internet Connection Sharing. This information is included in this section because enabling Internet Connection Sharing involves only one configuration step.

Configuring Internet access by using a firewall or a proxy server is not covered in this module, because both of these technologies can only be implemented by installing add-on products that are not part of Windows 2000.

- Configuring Internet Access by Using a Router

This section is designed to provide specific information about the tasks that are necessary for configuring Internet access by using a router. Explain the procedure for configuring a Windows 2000–based router, and then describe the Transmission Control Protocol/Internet Protocol (TCP/IP) settings that must be configured on the client computers. Emphasize that the Internet service provider (ISP) needs to configure its routers with routing information for the IP address ranges on your network.

- Configuring Internet Access by Using Network Address Translation

This section is designed to provide specific information about the tasks that are necessary for configuring Internet access by using NAT. Describe the procedure for installing NAT by explaining how to add the NAT routing protocol to the router. Next, explain how to configure the router to use NAT by describing the configuration options in the **Network Address Translation (NAT) Properties** dialog box. Finally, explain how to install the router interface for NAT by describing the procedures for adding and configuring the router interface.

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 labs in this module are 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

Performing the labs in this module introduces no configuration changes.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about the various methods that you can use to configure Internet access. You will also learn how to configure Internet access by using a router, and by using NAT.

- Options for Connecting a Network to the Internet
- Configuring Internet Access by Using a Router
- Configuring Internet Access by Using NAT

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

Microsoft® Windows® 2000 includes several technologies that you can use to connect your network to the Internet and to configure the connection to optimize network performance and security.

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

- Describe the options that are available for connecting a network to the Internet.
- Configure Internet access by using a router.
- Configure Internet access by using network address translation (NAT).

◆ Options for Connecting a Network to the Internet

Topic Objective

To list the topics that are related to connecting a network to the Internet.

Lead-in

Windows 2000 provides several technologies that you can use to connect your network to the Internet, optimize network performance, and secure Internet connections.

- Connecting to the Internet by Using a Router
- Securing Internet Connections by Using a Firewall
- Connecting to the Internet by Using NAT
- Connecting to the Internet by Using Internet Connection Sharing
- Connecting to the Internet by Using a Proxy Server
- Comparing Internet Connectivity Options

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

Windows 2000 simplifies Internet access by including several technologies that you can use to connect to the Internet. You can configure permanent or part-time connectivity, connect your home or small office network to the Internet, and automate the process of connecting to the Internet. In addition, you can use a proxy server to optimize performance and reliability, or add a firewall to restrict Internet access.

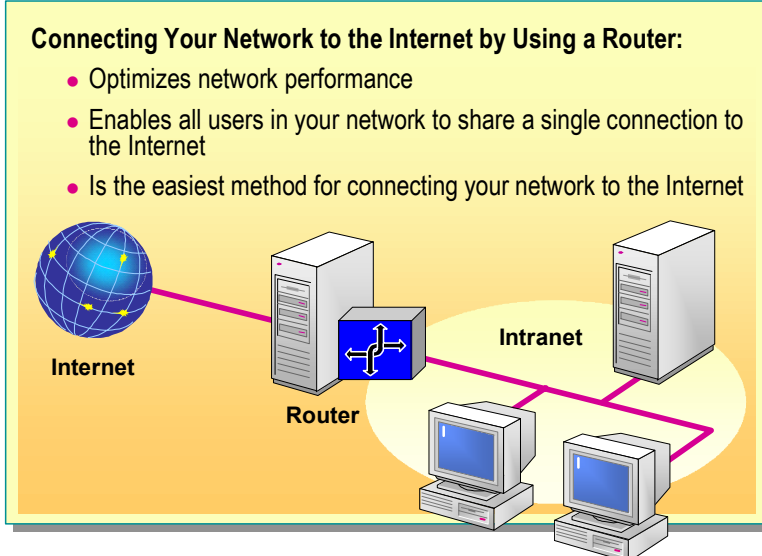
Connecting to the Internet by Using a Router

Topic Objective

To illustrate the concept of connecting to the Internet by using a router.

Lead-in

Connecting your network to the Internet by using a router enables all users in your network to share a single connection to the Internet, while optimizing network performance.



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

A router is a device that forwards packets of data from one local area network (LAN) or wide area network (WAN) to another. You can use routers to subdivide a LAN into subnets to balance traffic within your network. You can also place a router at the edge of your network to enable connections to remote offices and the Internet.

Routing Functionality

The router reads packet headers and selects the best path available for the packet based on the information contained in routing tables. The router then forwards the packet to its destination, or to another router. Routers optimize network performance because they do not perform any additional processing of packets.

Routing Services

Routers can be configured to enable all users in a network to share a single connection to the Internet. Routing and Remote Access in Windows 2000 provides built-in routing services that can be used to connect an organization to the Internet through a routed connection to an Internet service provider (ISP). For example, you can configure demand-dial routing to make a connection to an ISP only when packets are sent to or received from the Internet.

Delivery Tip

Explain to students that using a router is the easiest way to connect a network to the Internet, but it does not provide security against unauthorized access.

Routing Considerations

Using a router is the easiest method for connecting your network to the Internet, but it does not secure your network against unauthorized access through the Internet. In addition, you must ensure that you have public Internet Protocol (IP) addresses for each host that resides in your network.

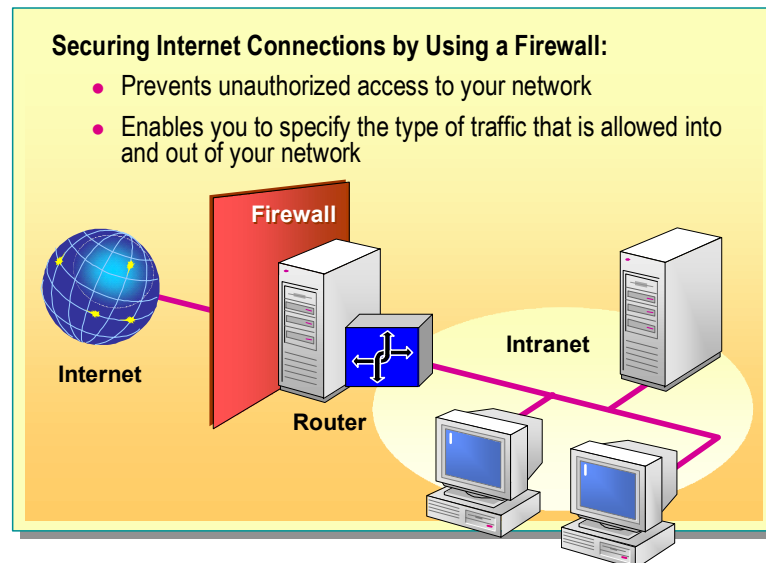
Securing Internet Connections by Using a Firewall

Topic Objective

To illustrate the concept of connecting to the Internet by using a firewall.

Lead-in

You can secure Internet connections by using a firewall to prevent unauthorized access to your network.



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

A firewall is a combination of hardware and software that provides a security system, usually to prevent unauthorized access from outside to an internal network or intranet.

A firewall can be configured to prevent unauthorized access to your internal network by enforcing a set of rules about which packets are allowed to pass from the external network to the internal network. Firewalls can be implemented by using hardware, software, or a combination of both. Many firewalls also include reporting features to alert an administrator when a security breach is attempted.

Configuring a Firewall

You can configure a firewall to specify the type of traffic that comes into and goes out from your network. A firewall routes all packets that comply with these specifications, or security rules, to the appropriate host. The firewall drops packets that do not comply with the security rules.

Establishing Security Rules

You can establish a simple security rule to forward selected incoming packets from the Internet. For example, you can create a rule to forward packets that are addressed to Transmission Control Protocol (TCP) port 80 (the default port that the Hypertext Transfer Protocol [HTTP] uses) to a Web server that resides inside the firewall, and to drop all other packets. This enables users who are outside the firewall to view Web pages on that Web server only, and prevents any other type of access into your internal network.

You can establish another common security rule to forward incoming packets from the Internet only when they are part of a communication that was initiated by a computer that resides on the internal network.

Note For information about installing and configuring a firewall, refer to the product information that is included with the particular firewall you are using.

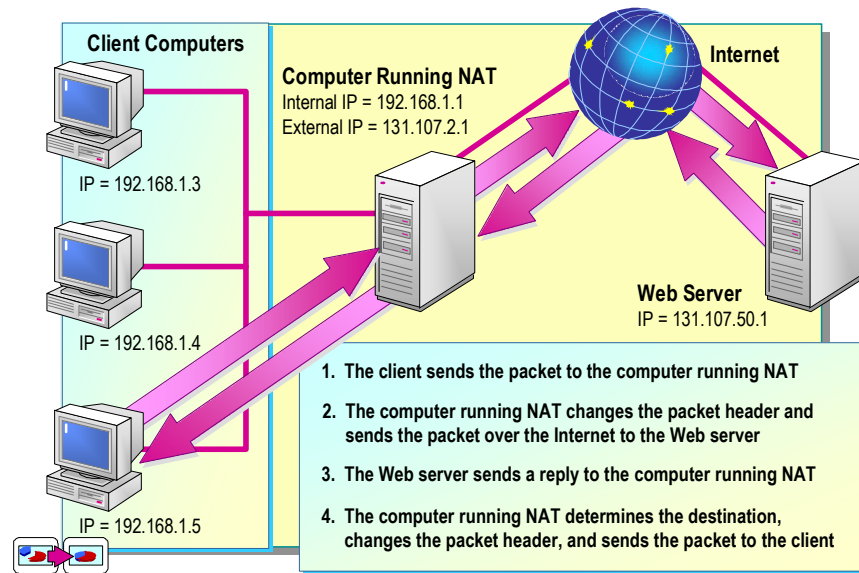
Connecting to the Internet by Using NAT

Topic Objective

To illustrate the NAT process.

Lead-in

You can use NAT to reduce IP address registration costs and to conceal internal IP addresses from external networks, such as the Internet.



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

Delivery Tip

The slide for this topic includes animation to illustrate the NAT process. Click, or press the SPACEBAR to advance the animation.

Network devices that are assigned private IP addresses cannot access Internet sites directly. Therefore, traffic must be routed through a NAT device, called a network address translator that has both an internal private IP address and a public IP address assigned to it.

Warning NAT is not a recommended method to use for network connectivity without the inclusion of a firewall.

A network address translator is an IP router that can translate IP addresses and TCP or User Datagram Protocol (UDP) port numbers of packets as they are being forwarded. NAT translates private IP addresses to external, public IP addresses. This reduces IP address registration costs because you can use unregistered IP addresses internally and translate them to a small number of registered IP addresses that are used to communicate with external networks, such as the Internet. NAT also hides internal IP addresses from external networks, which protects against unauthorized access to your network. The only IP address that is visible to the Internet is the IP address of the computer running NAT.

Note For more information on NAT, see RFC 1631 under **Additional Reading** on the Web page on the Student Materials compact disc.

How NAT Works

When a computer running NAT receives a packet from an internal client, it replaces the packet header and translates the client's port number and internal IP address to its own port number and external IP address. It then sends the packet to the destination host on the Internet, and keeps track of the mapping information in a table, so that it can route the reply to the appropriate client computer. When the computer running NAT receives a reply from the Internet host, it again replaces the packet header and sends the packet to the client. Both the client computer and the Internet host appear to be communicating directly with each other.

Delivery Tip

Use the slide to illustrate the NAT process that is described in the example.

For example, a client computer with the IP address 192.168.1.5 wants to contact a Web server with the IP address 131.107.50.1. The client is configured to use 192.168.1.1 as the default gateway, which is the internal IP address of the computer running NAT. The external IP address of the computer running NAT is 131.107.2.1. In this example, the NAT process occurs as follows:

1. The client computer sends a packet to the computer running NAT. The packet header indicates that the packet originates from port 1074 on the computer with the IP address 192.168.1.5, and has a destination of port 80 on 131.107.50.1.
2. The computer running NAT changes the packet header to indicate that the packet originates from port 1563 on host 131.107.2.1, but does not change the destination. The computer running NAT then sends the packet to the Web server over the Internet.
3. The external Web server receives the packet and sends a reply. The packet header for the reply indicates that the packet originates from port 80 on 131.107.50.1, and has a destination of port 1563 on host 131.107.2.1.
4. The computer running NAT receives the packet and checks its mapping information to determine the destination client computer. The computer running NAT changes the packet header to indicate a destination of port 1074 on 192.168.1.5, and then sends the packet to the client. The source of the packet remains as port 80 on 131.107.50.1, which is the IP address of the Web server.

NAT Features and Benefits

Delivery Tip

Describe the features and benefits of NAT.

The NAT routing protocol in Windows 2000 provides the following features and benefits:

- NAT enables multiple users to use a single connection to access the Internet through dial-up networking and local networking media.
- NAT can provide Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) services if no other servers on your network provide them.
- NAT enables any IP-attached device on your intranet, including Windows-based and non-Windows-based clients, to communicate with computers on the Internet without requiring additional client software.

Connecting to the Internet by Using Internet Connection Sharing

Topic Objective

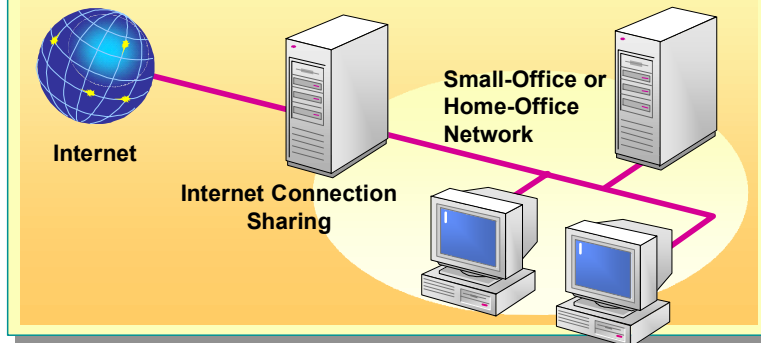
To illustrate the concept of connecting to the Internet by using Internet Connection Sharing.

Lead-in

Internet Connection Sharing enables small-office and home-office networks to share a single connection to the Internet.

Connecting to the Internet by Using Internet Connection Sharing:

- Simplifies the process of configuring NAT
- Enables small-office and home-office networks to share a single connection to the Internet



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

Internet Connection Sharing simplifies the configuration steps that are required to enable multiple computers to share a single connection to the Internet. Internet Connection Sharing performs the same function as NAT, but it allows very little configuration flexibility.

Warning ICS is not a recommended method to use for network connectivity without the inclusion of a firewall.

Delivery Tip

Explain that Internet Connection Sharing is designed for use in a small network. It must not be used in larger networks because it can interfere with the existing network configuration.

Internet Connection Sharing is designed for a small office or home office network, and provides an easy-to-configure, but limited interface that connects clients to the Internet. Internet Connection Sharing configures NAT with preconfigured settings, which include a specific range of IP addresses for client computers, and the automatic assignment of IP addresses to client computers.

Note Do not use Internet Connection Sharing in an existing network with Windows 2000 Server domain controllers, DNS servers, gateways, DHCP servers, or systems that are configured to use static IP addresses, because it may interfere with your existing network configuration. In an existing network, you must use NAT instead of Internet Connection Sharing.

To enable Internet Connection Sharing, select the **Enable Internet Connection Sharing for this connection** check box in the in the Network Connection wizard, or on the **Sharing** tab of the **Properties** dialog box for the connection.

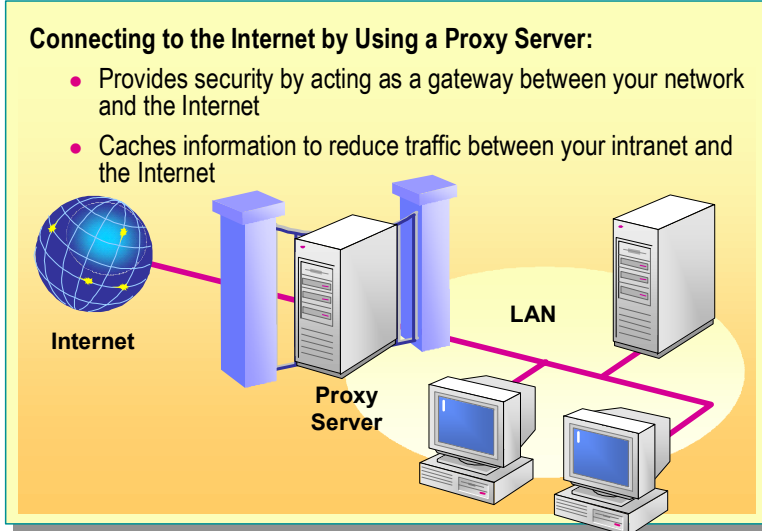
Connecting to the Internet by Using a Proxy Server

Topic Objective

To illustrate the concept of connecting to the Internet by using a proxy server.

Lead-in

A proxy server acts as a gateway between your network and the Internet.



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

A proxy server manages traffic between your network and servers on the Internet, and determines whether network packets are allowed to pass through to the network. When a client computer makes a request, the proxy server translates the request and passes it on to the Internet. When a computer on the Internet responds, the proxy server passes the response back to the client computer.

Restricting Connections

You can configure a proxy server to block inbound connections in order to enable LAN clients to initiate connections to Internet servers, but also prevent Internet clients from initiating connections to LAN servers. You can also configure a proxy server to restrict outbound connections so that LAN clients are authenticated by using their standard security credentials. You can restrict outbound connections in several ways—by user, program, protocol, TCP/UDP port number, time of day, domain name, or IP address.

Caching Information

Proxy servers typically cache information from the Internet. For example, if multiple users view the same Web page on the Internet, a proxy server can retrieve that page only once from the Internet, keep a copy of the page in its cache, and then forward the copy to all users. This reduces traffic between your intranet and the Internet because the proxy does not have to retrieve the Web page from the Internet separately for each user.

Delivery Tip

Refer students to the Microsoft Proxy Server Web site for more information about Microsoft Proxy Server.

Note Microsoft Internet Security and Acceleration Server 2000 (ISA Server) provides many advanced security features, and is a certified firewall. For more information, see the Microsoft ISA Server Web site at <http://www.microsoft.com/ISAServer>.

Comparing Internet Connectivity Options

Topic Objective

To list the advantages of the various Internet connectivity options.

Lead-in

Each of the Internet connectivity options has different capabilities and advantages.

- **NAT vs. Routing**
- **NAT vs. Proxy Server**
- **Internet Connection Sharing vs. NAT**

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

There are several options for connecting your network to the Internet, and each has different capabilities and advantages. Therefore, it is important to understand the differences between the various Internet connectivity options before you configure a connection between your intranet and the Internet.

NAT vs. Routing

NAT provides greater flexibility for designing your internal network, because it enables you to use unregistered IP addresses internally, and a small number of registered IP addresses externally. NAT provides network security that a router cannot provide, but it is more processor-intensive than routing and it does not support all protocols. In addition, NAT in Windows 2000 translates a computer's IP address in the packet header only, which prevents the use of Internet Protocol Security (IPSec).

NAT vs. Proxy Server

Both NAT and a proxy server allow connections to the Internet while restricting access to the internal network, and both provide address translation that enables clients on the intranet to use private IP addresses. Typically, all traffic on the Internet uses the IP address of the public network interface of the NAT or proxy server, whereas computers on the intranet use the IP address that is configured for the private network interface.

A proxy server must be configured to use the TCP or UDP ports that are used by all of the protocols for which it forwards packets to the Internet. This enables the proxy server to perform security checks. In addition, clients must be configured to use a proxy server. The client sends a request to the proxy server and the proxy server performs the necessary tasks to fulfill the request by supplying information from its cache or by sending a new packet to retrieve the information.

In contrast, NAT does not analyze the packets for security or caching purposes. Therefore, NAT only modifies IP addresses and port numbers in the IP and TCP/UDP headers, and is transparent to client and server.

Internet Connection Sharing vs. NAT

Internet Connection Sharing and NAT provide the same capabilities, but they differ in ease of use. You can enable Internet Connection Sharing by selecting a single check box, whereas enabling NAT requires more configuration tasks. In addition, Internet Connection Sharing must only be used in a small network because it:

- Requires a fixed IP address range for internal hosts.
- Is limited to a single public IP address for communicating with external networks.
- Only allows for a single internal network interface.

Note It is strongly recommended that *any* connection to the Internet be secured by using a certified firewall such as ISA Server. For more information, see the Microsoft ISA Server Web site at <http://www.microsoft.com/ISAServer>.

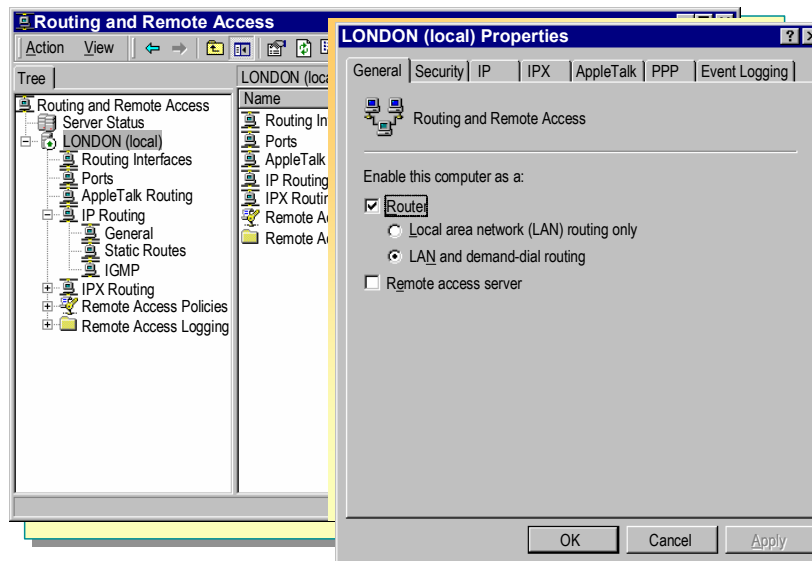
Configuring Internet Access by Using a Router

Topic Objective

To illustrate the user interface for configuring Internet access by using a router.

Lead-in

You can configure a router to connect to the Internet by using either a permanent or temporary connection.



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

You can configure Routing and Remote Access to create a permanent connection from your network to the Internet, by using a dedicated, private, point-to-point connection. You can also configure Routing and Remote Access for demand-dial routing, which enables you to configure a connection that becomes active only when data is sent to the remote site. Demand-dial routing reduces connection costs because you can use existing dial-up telephone lines instead of leased lines.

To configure a routed connection to the Internet for a network, you must configure the Windows 2000–based router and the client computers in your internal network.

Configuring the Windows 2000–Based Router

To configure the Windows 2000–based router:

1. Confirm that the computer is configured with two network connections. One network interface must be connected to your internal network and represents a permanent connection. The other network connection can be a permanent connection or a dial-up connection.
2. Configure the network connection to your internal network with the IP address, subnet mask and gateway that you received from your ISP.
3. Install and enable Routing and Remote Access.

Delivery Tip

Explain the procedure for configuring the Windows 2000–based router.

4. If you are using a demand-dial connection:
 - a. Open Routing and Remote Access from the **Administrative Tools** menu.
 - b. In the console tree, right-click the server that you want to configure, and then click **Properties**.
 - c. In the **Properties** dialog box for the server, verify that **LAN and demand-dial routing** is selected, and then click **OK**.
 - d. In the console tree, right-click **Ports**, and then click **Properties**.
 - e. In the **Ports Properties** dialog box, click the dial-up connection that you want to enable for routing, and then click **Configure**.
 - f. In the **Configure Device** dialog box, verify that **Demand-dial routing connections (inbound and outbound)** is selected, and then click **OK**.
 - g. Click **OK** to close the **Properties** dialog box for the server.
5. Configure the default route to the IP address provided by your ISP:
 - a. In the console tree, expand **IP Routing**, and then click **Static Routes**.
 - b. Right-click **Static Routes**, and then click **New Static Route**.
 - c. In the **Static Route** dialog box, type **0.0.0.0** in both the **Destination** and **Network mask** boxes.
 - d. Type the IP address provided by your ISP in the **Gateway** box, and then select a metric, if required.
 - e. If you use a dial-up connection, select the **Use this route to initiate demand-dial connections** check box, and then click **OK**.
6. If your internal network consists of multiple subnets, add routes for all of those subnets, and ensure that these routes use the internal network interface.

Configuring Client Computers On The Network

Delivery Tip

Describe the TCP/IP settings that must be configured on the client computers.

After you have configured the Windows 2000–based router, you must configure TCP/IP on the client computers in your network with the following settings:

- An IP address from the address range obtained from the ISP
- A subnet mask that corresponds to the address range obtained from the ISP
- A default gateway, which is the internal IP address of the Windows 2000–based router
- A DNS server (use a DNS server address that is assigned by the ISP or your own DNS server)

Note For IP packets to be properly routed from your ISP to your network, your ISP needs to configure its routers with routing information for the IP address ranges on your network so that the ISP routers forward IP packets from the Internet to destinations on your network.

◆ Configuring Internet Access by Using NAT

Topic Objective

To list the topics that are related to configuring Internet access by using NAT.

Lead-in

Install NAT by using the Routing and Remote Access administrative tool.

- Installing NAT
- Configuring NAT
- Installing the Router Interface for NAT

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

To configure the computer running NAT, you must first install and enable Routing and Remote Access on a computer that is connected both to your intranet and the Internet. You must then add and configure the NAT routing protocol on the router, by using Routing and Remote Access in Microsoft Management Console (MMC).

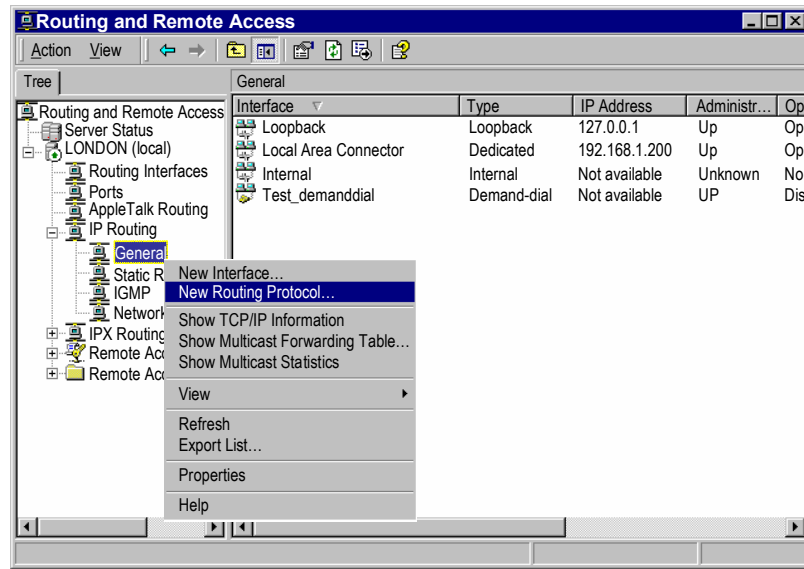
Installing NAT

Topic Objective

To illustrate the user interface for installing NAT.

Lead-in

Install NAT by adding the NAT routing protocol to the router.



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

To install NAT, you must add the NAT routing protocol to the router.

To add the NAT routing protocol:

1. Open Routing and Remote Access.
2. In the console tree, double-click the name of the server that you want to configure, and then expand **IP Routing**.
3. Right-click **General**, and then click **New Routing Protocol**.
4. In the **New Routing Protocol** dialog box, click **Network Address Translation (NAT)**, and then click **OK**.

Delivery Tip

Explain the procedure for adding the NAT routing protocol.

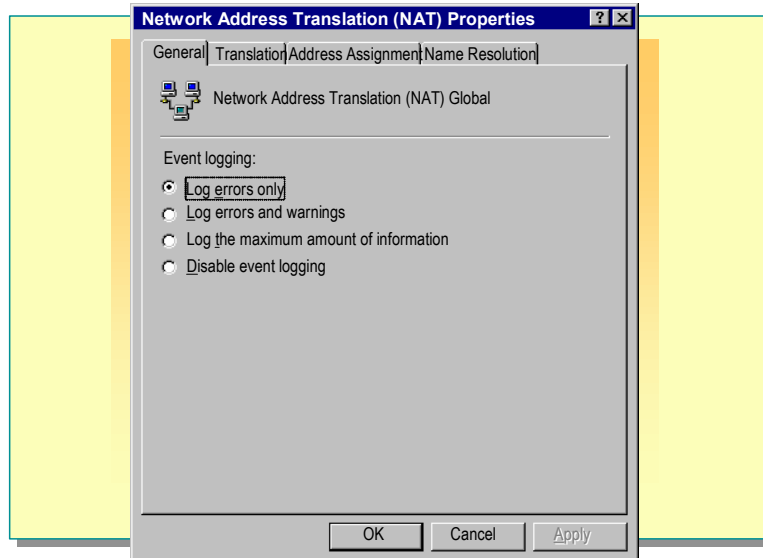
Configuring NAT

Topic Objective

To illustrate the user interface for configuring NAT.

Lead-in

After you install NAT, you must configure the router to use NAT.



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

Delivery Tip

Explain the procedure for configuring the router to use NAT, and describe the tabs and settings in the **Network Address Translation (NAT) Properties** dialog box.

After you have installed the NAT routing protocol, you must configure the router to use NAT. You can configure NAT by using Routing and Remote Access. Double-click the name of the server that you want to configure, and then expand **IP Routing**. Right-click **Network Address Translation (NAT)**, and then click **Properties**.

The following table describes the options that you can configure in the **Network Address Translation (NAT) Properties** dialog box.

Tab	Description
General	Enables you to configure event logging, which specifies the type and amount of information that is logged in the system log in Event Viewer. The default setting is Log errors only .
Translation	Enables you to configure the following settings: • Remove TCP mappings after. Sets the number of minutes that a dynamic mapping for a TCP session remains in the translation table for the router. The default setting is 1,440 minutes (24 hours). • Remove UDP mappings after. Sets the number of minutes that a UDP message remains in the translation table for the router. The default setting is one minute. • Reset Defaults. Restores the default settings of the time-out values for dynamic mapping of TCP traffic and UDP traffic. Enables you to configure the following settings: • Click Applications to configure special applications on your private network that communicate with other applications that are running on computers on the Internet and that you want to make available to users on the Internet. These applications include those that send response traffic from a port other than the port used by the initial incoming traffic from the Internet client.

(continued)

Tab	Description
Address Assignment	Enables you to configure the computer running NAT to act as a DHCP server and assign IP addresses to clients. • If your network does not contain a DHCP server, select the Automatically assign IP addresses by using DHCP check box, and then in the IP address and Mask boxes, configure the IP address range that the DHCP allocator will use to assign IP addresses. Click Exclude to exclude IP addresses from the range, such as the internal IP address of the computer or any static IP addresses that are assigned to computers in your network. The default network address range is based on the network 192.168.0.0 with a subnet mask of 255.255.255.0. • If your network contains one or more DHCP servers, clear the Automatically assign IP addresses by using DHCP check box.
Name Resolution	Enables you to configure the computer running NAT to appear as a DNS server to clients and to provide name resolution for these clients. • If your network does not contain a DNS server, select the Resolve IP addresses for clients using Domain Name System (DNS) check box. Even though the computer running NAT is not a DNS server, it appears as a DNS server to clients. When the computer running NAT receives a DNS query, it forwards the query to a DNS server and forwards the reply that it receives from the DNS server to the client. • To specify whether the NAT server makes a connection by using a demand-dial interface to resolve DNS names, select the Connect to the public network when a name needs to be resolved check box, and then, under Demand-dial interface, select an interface from the list.

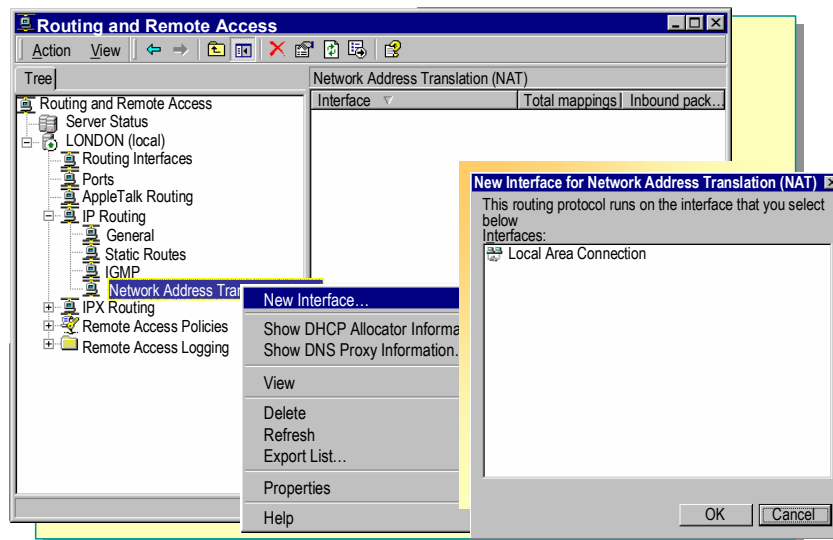
Installing the Router Interface for NAT

Topic Objective

To illustrate the user interface for installing the router interface for NAT.

Lead-in

You must add and configure the router interface for NAT to ensure that the computer running NAT translates packets properly.



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

To enable NAT, you must add to the NAT routing protocol the interface on the Windows 2000-based router that connects to the Internet.

Note Enable NAT translation only on interfaces that are connected to the Internet.

Adding the Router Interface

To add an interface to the NAT routing protocol:

1. Open Routing and Remote Access.
2. In the console tree, expand **IP Routing**, and then click **Network Address Translation (NAT)**.
3. Right-click **Network Address Translation (NAT)**, and then click **New Interface**.
4. In the **New Interface for Network Address Translation (NAT)** dialog box, click the interface you want to add, and then click **OK**.
5. On the **General** tab of the **Network Address Translation Properties** dialog box for the interface, select one of the following options:
 - If this interface connects to the Internet, click **Public interface connected to the Internet**, and then select the **Translate TCP/UDP headers** check box.
 - If this interface connects to the small-office or home network, click **Private interface connected to private network**.
6. Click **OK**.

Delivery Tip

Explain the procedure for adding the router interface.

Configuring the Router Interface

Delivery Tip

Explain the procedure for configuring the router interface, and describe the tabs and settings in the **Properties** dialog box for the connection.

After you have added the interface, you must configure it by using the Routing and Remote Access administrative tool. In the console tree, click **Network Address Translation (NAT)**. In the details pane, right-click the connection that you want to configure, and then click **Properties**. The following table describes the tabs and associated options that you can configure in the **Properties** dialog box for the connection.

Tab	Description
General	Enables you to configure the following settings: • Private interface connected to private network. Specifies that the interface is a private interface that is connected to the private network. • Public interface connected to the Internet. Specifies that the interface is the public interface that is connected to the Internet. • Translate TCP/UDP headers (recommended). Specifies whether the router performs TCP port and UDP port translation in addition to IP address translation. If you only have a single public IP address, you must select this check box. Otherwise, network traffic from hosts on the private network cannot be properly translated to Internet traffic.
Address Pool	Lists the configured ranges of public IP addresses that your ISP assigned to your network. • Click Add to add IP ranges to the address pool. In the Add Address Pool dialog box, type the start and end addresses of the address pool and the subnet mask of the subnet to which the range of addresses belongs. You can add multiple address ranges per interface. • Click Reservations to reserve public IP addresses for specific internal clients. Reservations enable computers to always use the same public IP address. In the Add Reservations dialog box, type the public IP address that you want to reserve, and the private IP address of the computer that will receive packets that are sent to the public IP address. Select the Allow incoming sessions to this address check box to make the internal computer accessible from the Internet.
Special Ports	Enables you to map incoming sessions to specific ports and addresses on your private network. In the Protocol box, select TCP or UDP, and then click Add. In the Add Special Port dialog box, under Public address, click: • On this interface to specify that the mapping applies to all addresses on this external interface. • On this address pool entry to specify that the mapping applies to a single address in the address pool. In the Incoming port box, type the number of the TCP or UDP port to which computers on the Internet connect. In the Private address box, type the IP address of the internal computer to which the NAT server will forward packets. In the Outgoing port box, type the TCP or UDP port on the internal computer to which the NAT server will forward packets.

Lab A: Configuring Internet Access by Using NAT

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure a computer as a NAT client, configure a computer as a NAT server, and configure NAT for incoming connections.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure a computer as a NAT client.
- Configure a computer as a NAT server.
- Configure NAT for incoming connections.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how NAT enables shared network access.
- Experience configuring TCP/IP properties.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller
- A partner with a similarly configured computer
- Microsoft Internet Explorer configured to use your local network connection

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.

Important In this lab, you will work with a partner. One computer will be the NAT server and the other will be the NAT client. The computer of the student with the lower student number will act as the NAT server; the computer of the student with the higher student number will act as the NAT client. Before starting the lab, determine the role that your computer will play.

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 ISP has assigned a few IP addresses to your organization. You need to ensure that all of the users in your organization have access to the Internet. You also need to ensure that business partners can access information on select computers that are on your internal network.

Estimated time to complete this lab: 30 minutes

Exercise 1

Configuring a NAT Client

Scenario

Because your organization has a limited number of public IP addresses, you need to configure client computers to access the Internet by using NAT.

Goal

In this exercise, you will configure a NAT client.

Task	Detailed Steps
 Perform the following procedure only on the computer that will be the NAT client.	
1. Configure your computer to use your partner's PartnerNet network adapter as the default gateway, and then disable the Classroom network connection.	a. Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. b. Right-click My Network Places, and then click Properties. c. In Network and Dial-up Connections, right-click PartnerNet, and then click Properties. d. Click Internet Protocol (TCP/IP), and then click Properties. e. In the Default gateway box, type the IP address of your partner's PartnerNet connection, and then click OK. f. Click OK to close the PartnerNet Properties dialog box. g. Right-click Classroom, and then click Disable. h. Minimize Network and Dial-up Connections.

Exercise 2

Configuring a NAT Server

Scenario

Because your company uses a private IP addressing scheme, and to control the security of your network, all access to the Internet from your organization must go through a NAT server.

Goal

In this exercise, you will configure a computer to become the NAT server for your organization.

Tasks	Detailed Steps
	Perform the following procedure only on the computer that will be the NAT server. If your computer will be the NAT client, observe while your partner configures the server.
	1. Use Routing and Remote Access to configure your computer as NAT server. Configure the Classroom network connection as the Internet connection. a. Log on as <code>administrator@domain.nwtraders.msft</code> (where <i>domain</i> is the name of your domain) with a password of password. b. Open Routing and Remote Access from the Administrative Tools menu. c. 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. d. In the Routing and Remote Access wizard, click Next. e. On the Common Configurations page, verify that Internet connection server is selected, and then click Next. f. On the Internet Connection Server Setup page, verify that Set up a router with the Network Address Translation (NAT) routing protocol is selected, and then click Next. g. On the Internet Connection page, verify that Use the selected Internet connection is selected, click Classroom, click Next, and then click Finish. h. In Routing and Remote Access, in the console tree, expand <i>server</i>, expand IP Routing, and then click Network Address Translation (NAT).
	Perform the following procedure on the computer that is the NAT client only. Do not start this procedure until your partner has completed the preceding procedure.

(continued)

Tasks	Detailed Steps
2. Test network communications with the instructor's computer.	a. At a command prompt, type ping london.nwtraders.msft and then press ENTER.  <i>You should see four replies to the ping command, even though your computer's connection to the Classroom network is disabled. Network traffic to the instructor's computer goes through the NAT server.</i> b. At the command prompt, type net view \\london.nwtraders.msft and then press ENTER. c. Confirm that you can see the shared folders on the instructor's computer, and then close the command prompt window. d. Open Internet Explorer. e. In the Address box, type http://london.nwtraders.msft and then click Go.  <i>If a Web site is configured on your partner's computer, a Web page is displayed. If no Web site is configured, a page titled Under Construction is displayed.</i>
 Perform the following procedure on the computer that is the NAT server. Do not start this procedure until your partner has completed the preceding procedure.	
3. Review NAT activity and port mappings on your computer.	a. In Routing and Remote Access, right-click Network Address Translation (NAT), and then click Refresh.  <i>The Classroom network connection displays data for port mappings and packets that NAT translated as a result of your partner's actions. The PartnerNet network connection shows no activity.</i> b. In the details pane, right-click Classroom, and then click Show Mappings.  <i>The Network Address Translation Session Mapping Table shows all client connections to the NAT server and the resulting external connections, including the IP addresses and the ports used.</i> c. Close the server - Network Address Translation Session Mapping Table window.

Exercise 3

Configuring NAT Settings

Scenario

Users on your network use a network-based application that requires a server on the Internet to initiate a TCP connection with a client. Also, business partners need to access, from the Internet, information on a Web server that is located on your internal network.

Goal

In this exercise, you will configure the NAT server to allow external computers to establish TCP connections with a NAT client on TCP port 27960. You will also allow external users to access an internal Web server.

Tasks	Detailed Steps
 Perform the following procedures on the NAT server only.	
1. Configure NAT to allow an application called Seismic Activity Monitor to establish connections with a NAT client on port 27960.	a. In the console tree, right-click Network Address Translation (NAT), and then click Properties. b. In the Network Address Translation (NAT) Properties dialog box, on the Translation tab, click Applications. c. In the Network Application Settings dialog box, click Add. d. In the Internet Connection Sharing Application dialog box, in the Name of application box, type Seismic Activity Monitor e. In the Remote server port number box, type 27960 f. Click UDP. g. In the UDP box, type 27960 and then click OK. h. Click OK to close the Network Applications Settings dialog box. i. In the Network Address Translation (NAT) Properties dialog box, on the Address Assignment tab, verify that the Automatically assign IP addresses by using DHCP check box is not selected. j. On the Name Resolution tab, verify that the Clients using Domain Name System (DNS) check box is not selected, and then click OK.

(continued)

Tasks	Detailed Steps
2. Configure NAT to allow external computers to connect to a Web server on your partner's computer, and then test the connection.	a. In the details pane, right-click Classroom, and then click Properties. b. In the Classroom Properties dialog box, on the Special Ports tab, in the Protocol box, ensure that TCP is selected, and then click Add. c. In the Add Special Port dialog box, in the Incoming port box, type 8080 d. In the Private address box, type the IP address of your partner's PartnerNet connection, and in the Outgoing port box, type 80 and then click OK twice. e. Ask the instructor or a student who is not your partner to open Internet Explorer and connect to http://192.168.z.x:8080 (where <i>z</i> is the third octet of the Classroom connection and <i>x</i> is your student number).  <i>If a Web site is configured on your partner's computer, a Web page is displayed. If no Web site is configured, a page Under Construction is displayed.</i>

Exercise 4

Removing NAT

Scenario

After you have tested NAT for your organization, you must remove all NAT configuration from your test network.

Goal

In this exercise, you will restore all settings on the NAT client and the NAT server.

Tasks	Detailed Steps
 Perform the following procedures only on the computer that is the NAT server.	
1. Disable Routing and Remote Access.	- 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 all open windows, and then log off.
 Perform the following procedure only on the computer that is the NAT client. Do not start this procedure until your partner has finished the preceding procedure.	
2. Restore your original TCP/IP configuration.	- Restore Network and Dial-up Connections. - Right-click PartnerNet, and then click Properties. - Click Internet Protocol (TCP/IP), and then click Properties. - Clear the Default Gateway check box, and then click OK. - Click OK to close the PartnerNet Properties dialog box. - Right-click Classroom, and then click Enable. - Close Network and Dial-up Connections. - At a command prompt, type ping london.nwtraders.msft and then press ENTER. <i>If you receive four replies, your network configuration has been correctly reconfigured. If you do not receive four replies after using the ping command several times, tell your instructor.</i> - Close all open windows, and then log off.

If Time Permits

Configuring a Second NAT Server

Reverse roles with your partner and repeat all of the exercises in this lab so that the computer that you configured as a NAT client the first time that you completed the exercise is now configured as a NAT server.

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.

- Options for Connecting a Network to the Internet
- Configuring Internet Access by Using a Router
- Configuring Internet Access by Using NAT

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

1. How does NAT help to reduce IP address registration costs and protect against unauthorized access to your network?

NAT translates private IP addresses to external, public IP addresses. This reduces IP address registration costs because you can use unregistered IP addresses internally and translate them to a small number of registered IP addresses that are used to communicate with external networks, such as the Internet. NAT also hides internal IP addresses from external networks, which protects against unauthorized access to your network. The only IP address that is visible to the Internet is the IP address of the computer running NAT.

2. What are the two connectivity options that are available for configuring Internet access by using a router?

You can configure Routing and Remote Access to create a permanent connection from your network to the Internet by using a dedicated, private, point-to-point connection. You can also configure Routing and Remote Access for demand-dial routing, which enables you to configure a connection that becomes active only when data is sent to the remote site.

3. What must you do to configure Internet access by using NAT?

To configure the computer running NAT, you must first install and enable Routing and Remote Access on a computer that is connected both to your intranet and the Internet. You must then add and configure the NAT routing protocol on the router, by using Routing and Remote Access in MMC.

