[Previous] [Next]

Chapter 12

Supporting Network Address Translation (NAT)

About This Chapter

Network address translation (NAT) is a protocol that allows a network with private addresses to access information on the Internet through an Internet Protocol (IP) translation process. In this chapter, you will learn how to configure your home network or small office network to share a single connection to the Internet with NAT.

Before You Begin

To complete the lessons in this chapter, you must have

- Completed Chapter 10

[Previous] [Next]

Lesson 1: Introducing NAT

NAT enables private IP addresses to be translated into public IP addresses for traffic to and from the Internet. This keeps traffic from passing directly to the internal network, while saving the small office or home office user the time and expense of getting and maintaining a public address range. This lesson provides an overview of NAT.

After this lesson, you will be able to

- Describe the purpose of NAT
- Identify the components of NAT
- Describe how NAT works

Estimated lesson time: 45 minutes

Network Address Translation

Microsoft Windows 2000 Network Address Translation (NAT) allows computers on a small network, such as a small office or home office, to share a single Internet connection with only a single public IP address. The computer on which NAT is installed can act as a network address translator, a simplified DHCP server, a Domain Name System (DNS) proxy, and a Windows Internet Name Service (WINS) proxy. NAT allows host computers to share one or more publicly registered IP addresses, helping to conserve public address space.

Understanding Network Address Translation

With NAT in Windows 2000, you can configure your home network or small office network to share a single connection to the Internet. NAT consists of the following components:

- **Translation component.** The Windows 2000 router on which NAT is enabled, hereafter called the NAT computer, acts as a network address translator, translating the IP addresses and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port numbers of packets that are forwarded between the private network and the Internet.

- **Addressing component.** The NAT computer provides IP address configuration information to the other computers on the home network. The addressing component is a simplified DHCP server that allocates an IP address, a subnet mask, a default gateway, and the IP address of a DNS server. You must configure computers on the home network as DHCP clients to receive the IP configuration automatically. The default TCP/IP configuration for computers running Windows 2000, Windows NT, Windows 95, and Windows 98 is as a DHCP client.

- **Name resolution component.** The NAT computer becomes the DNS server for the other computers on the home network. When name resolution requests are received by the NAT computer, it forwards the name resolution requests to the Internet-based DNS server for which it is configured, and returns the responses to the home network computer.

Routed and Translated Internet Connections

There are two types of connections to the Internet: routed and translated. When planning for a routed connection, you will need a range of IP addresses from your Internet service provider (ISP) to use on the internal portion of your network, and they will also give you the IP address of the DNS server you need to use. You can either statically configure the IP address configuration of each computer or use a DHCP server.

The Windows 2000 router needs to be configured with a network adapter for the internal network (10 or 100BaseT Ethernet, for example). It also needs to be configured with an Internet connection such as an analog or Integrated Services Digital Network (ISDN) modem, xDSL modem, cable modem, or a fractional T1 line.

The translated method, or NAT, gives you a more secure network because the addresses of your private network are completely hidden from the Internet. The connection shared computer, which uses NAT, does all of the translation of Internet addresses to your private network, and vice versa. However, be aware that the NAT computer does not have the ability to translate all payloads. This is because some applications use IP addresses in other fields besides the standard TCP/IP header fields.

The following protocols do not work with NAT:

- Kerberos

- IP Security Protocol (IPSec)

The DHCP allocator functionality in NAT enables all DHCP clients in the network to automatically obtain an IP address, subnet mask, default gateway, and DNS server address from the NAT computer. If you have any non-DHCP computers on the network, then statically configure their IP address configuration.

To keep resource costs to a minimum on a small network, only one server running Windows 2000 is needed. Depending on whether you are running a translated or routed connection, this single server can suffice for NAT, Automatic Private IP Addressing (APIPA), Routing and Remote Access, and DHCP.

Public and Private Addresses

If your intranet is not connected to the Internet, any IP addressing can be deployed. If direct (routed) or indirect (proxy or translator) connectivity to the Internet is desired, there are two types of addresses you can use: public addresses and private addresses.

Public Addresses

Public addresses are assigned by the Internet Network Information Center (InterNIC), and consist of class-based network IDs or blocks of Classless Inter-Domain Routing (CIDR)-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet. When the public addresses are assigned, routes are programmed into the routers of the Internet so that traffic to the assigned public addresses can reach its location. Traffic to destination public addresses is reachable on the Internet.

Private Addresses

Each IP node requires an IP address that is globally unique to the IP internetwork. In the case of the Internet, each IP node on a network connected to the Internet requires an IP address that is globally unique to the Internet. As the Internet grew, organizations connecting to the Internet required a public address for each node on their intranets. This requirement placed a huge demand on the pool of available public addresses.

When analyzing the addressing needs of organizations, the designers of the Internet noted that for many organizations, most of the hosts on the organization's intranet did not require direct connectivity to Internet hosts. Those hosts that did require a specific set of Internet services, such as World Wide Web access and e-mail, typically accessed the Internet services through application-layer gateways such as proxy servers and e-mail servers. The result was that most organizations only required a small amount of public addresses for those nodes (such as proxies, routers, firewalls, and translators) that were directly connected to the Internet.

For the hosts within the organization that do not require direct access to the Internet, IP addresses that do not duplicate already assigned public addresses are required. To solve this addressing problem, the Internet designers reserved a portion of the IP address space and named this space the private address space. Private IP addresses are never assigned as public addresses. Because the public and private address spaces do not overlap, private addresses never duplicate public addresses. The following private IP address ranges are specified by Internet Request for Comments (RFC) 1918:

- **10.0.0.0 through 10.255.255.255.** The 10.0.0.0 private network is a class A network ID that allows the following range of valid IP addresses: 10.0.0.1 to 10.255.255.254. The 10.0.0.0 private network has 24 host bits that can be used for any subnetting scheme within the private organization.

- **172.16.0.0 through 172.31.255.255.** The 172.16.0.0 private network can be interpreted either as a block of 16 class B network IDs or as a 20-bit assignable address space (20 host bits) that can be used for any subnetting scheme within the private organization. The 172.16.0.0 private network allows the following range of valid IP addresses: 172.16.0.1 to 172.31.255.254.

- **192.168.0.0 through 192.168.255.255.** The 192.168.0.0/16 private network can be interpreted either as a block of 256 class C network IDs or as a 16-bit assignable address space (16 host bits) that can be used for any subnetting scheme within the private organization. The 192.168.0.0 private network allows the following range of valid IP addresses: 192.168.0.1 to 192.168.255.254.

Private addresses are not reachable on the Internet. Therefore, Internet traffic from a host that has a private address must either send its requests to an application-layer gateway (such as a proxy server), which has a valid public address, or have its private address translated into a valid public address by a network address translator before it is sent on the Internet.

How NAT Works

A network address translator is an IP router defined in RFC 1631 that can translate IP addresses and TCP/UDP port numbers of packets as they are being forwarded. Consider a small business network with multiple computers connecting to the Internet. A small business would normally have to obtain an ISP-allocated public IP address for each computer on its network. With NAT, however, the small business can use private addressing (as described in RFC 1597) and have the NAT map its private addresses to a single or to multiple public IP addresses as allocated by its ISP. For example, if a small business is using the 10.0.0.0 private network for its intranet and has been granted the public IP address of 198.200.200.1 by its ISP, the NAT maps (using static or dynamic mappings) all private IP addresses being used on network 10.0.0.0 to the public IP address of 198.200.200.1.

Static and Dynamic Address Mapping

NAT can use either static or dynamic mapping. A static mapping is configured so that traffic is always mapped a specific way. You could map all traffic to and from a specific private network location to a specific Internet location. For instance, to set up a Web server on a computer on your private network, you create a static mapping that maps [Public IP Address, TCP Port 80] to [Private IP Address, TCP Port 80].

Dynamic mappings are created when users on the private network initiate traffic with Internet locations. The NAT service automatically adds these mappings to its mapping table and refreshes them with each use. Dynamic mappings that are not refreshed are removed from the NAT mapping table after a configurable amount of time. For TCP connections, the default time-out is 24 hours. For UDP traffic, the default time-out is 1 minute.

Proper Translation of Header Fields

By default, a NAT translates IP addresses and TCP/UDP ports. These modifications to the IP datagram require the modification and recalculation of the following fields in the

IP, TCP, and UDP headers:

- Source IP address
- TCP, UDP, and IP checksum
- Source port

If the IP address and port information is only in the IP and TCP/UDP headers—for example, with Hypertext Transfer Protocol (HTTP) or World Wide Web traffic—the application protocol can be translated transparently. There are applications and protocols, however, that carry IP or port addressing information within their headers. File Transfer Protocol (FTP), for example, stores the dotted-decimal representation of IP addresses in the FTP header for the FTP port command. If the NAT does not properly translate the IP address, connectivity problems can occur. Additionally, in the case of FTP, because the IP address is stored in dotted-decimal format, the translated IP address in the FTP header can be a different size. Therefore, the NAT must also modify TCP sequence numbers to ensure that no data is lost.

NAT Editors

In the case where the NAT component must additionally translate and adjust the payload beyond the IP, TCP, and UDP headers, a NAT editor is required. A NAT editor is an installable component that can properly modify otherwise nontranslatable payloads so that they can be forwarded across a NAT. Windows 2000 includes built-in NAT editors for the following protocols:

- FTP
- Internet Control Message Protocol (ICMP)
- Point-to-Point Tunneling Protocol (PPTP)
- NetBIOS over TCP/IP

Additionally, the NAT routing protocol includes proxy software for the following protocols:

- H.323
- Direct Play
- Lightweight Directory Access Protocol (LDAP)-based Internet Locator Service (ILS) registration
- Remote procedure call

NOTE

IPSec traffic is not translatable.

A NAT Example

If a small business is using the 192.168.0.0 private network ID for its intranet and has been granted the public address of w1.x1.y1.z1 by its ISP, then NAT maps all private addresses on 192.168.0.0 to the IP address of w1.x1.y1.z1. If multiple private addresses are mapped to a single public address, NAT uses dynamically chosen TCP and UDP ports to distinguish one intranet location from another. Figure 12.1 shows an example of using NAT to transparently connect an intranet to the Internet.

> **NOTE**
>
> The use of w1.x1.y1.z1 and w2.x2.y2.z2 is intended to represent valid public IP addresses as allocated by InterNIC or an ISP.

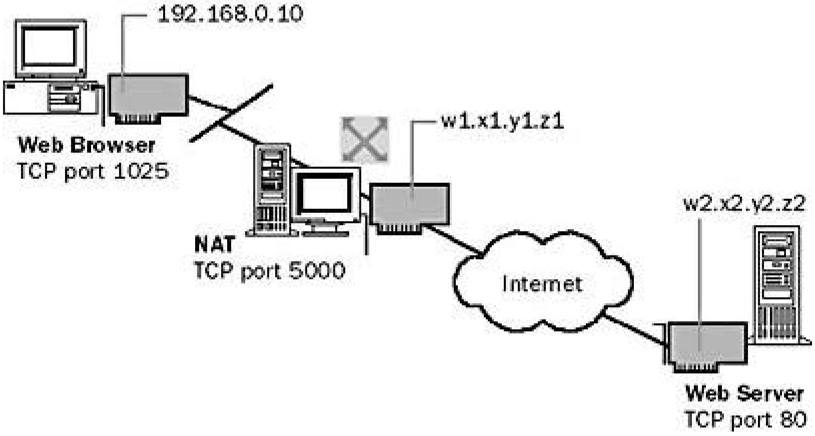


Figure 12.1 *Using NAT to transparently connect an intranet to the Internet*

NAT Processes in Windows 2000 Routing and Remote Access

For Windows 2000 Routing and Remote Access, the NAT component can be enabled by adding NAT as a routing protocol in the Routing and Remote Access snap-in.

> **NOTE**
>
> NAT services are also available with the Internet connection sharing feature available from the Network and Dial-Up Connections folder, as explained in Lesson 2. Internet connection sharing performs the same function as the NAT routing protocol in Routing and Remote Access but it allows very little configuration flexibility. For information about configuring Internet connection sharing and why you would choose Internet connection sharing over the NAT routing protocol of Routing and Remote Access, see Windows 2000 Server Help.

Installed with the NAT routing protocol are a series of NAT editors. NAT consults the editors when the payload of the packet being translated matches one of the installed editors. The editors modify the payload and return the result to the NAT component. NAT interacts with the TCP/IP protocol in two important ways:

- To support dynamic port mappings, the NAT component requests unique TCP and UDP port numbers from the TCP/IP protocol stack when needed.
- With TCP/IP, so that packets being sent between the private network and the

Internet are first passed to the NAT component for translation.

Figure 12.2 shows the NAT components and their relation to TCP/IP and other router components.

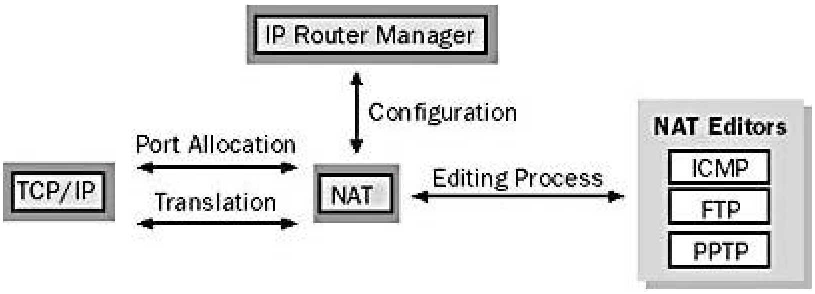


Figure 12.2 *NAT components*

Outbound Internet Traffic

For traffic from the private network that is outbound on the Internet interface, NAT first assesses whether or not an address/port mapping, whether static or dynamic, already exists for the packet. If not, a dynamic mapping is created. The NAT creates a mapping depending on whether there are single or multiple public IP addresses available.

- If a single public IP address is available, the NAT requests a new unique TCP or UDP port for the public IP address and uses that as the mapped port.

- If multiple public IP addresses are available, the NAT performs private-IP-address-to-public-IP-address mapping. For these mappings, the ports are not translated. When the last public IP address is needed, the NAT switches to performing address and port mapping, as it would in the case of the single public IP address.

After mapping, the NAT checks for editors and invokes one if necessary. After editing, the NAT modifies the IP and TCP or UDP headers and forwards the packet using the Internet interface. Figure 12.3 shows NAT processing for outbound Internet traffic.

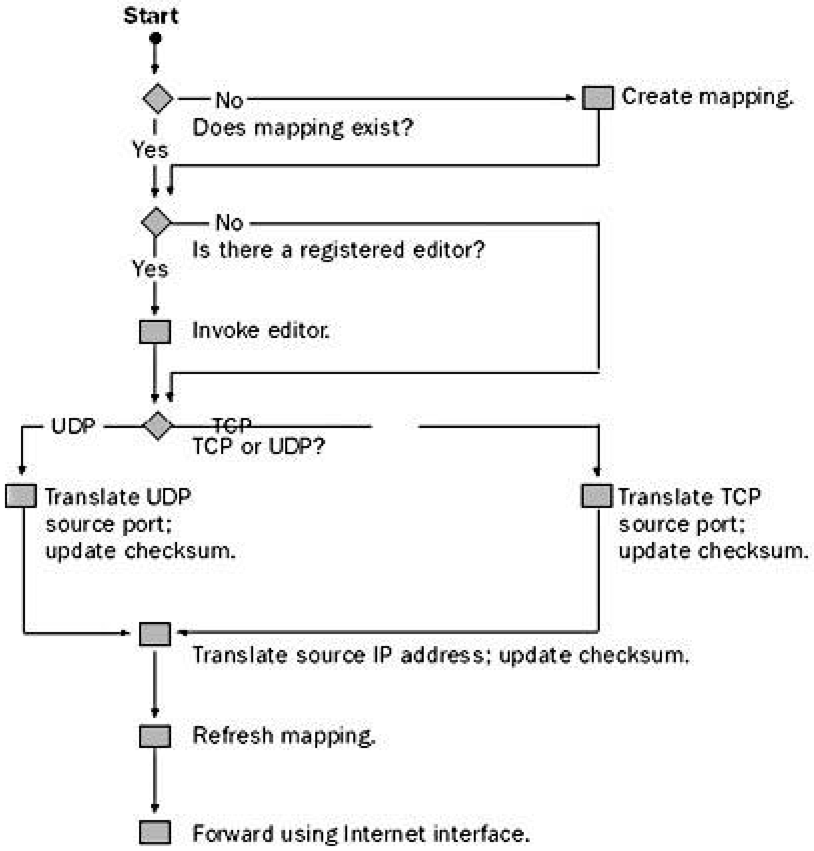

Start
No
Create mapping.
Does mapping exist?
Yes
No
Is there a registered editor?
Yes
Invoke editor.
UDP
TCP
TCP or UDP?
Translate UDP source port; update checksum.
Translate TCP source port; update checksum.
Translate source IP address; update checksum.
Refresh mapping.
Forward using Internet interface.

Figure 12.3 *NAT processing of outbound Internet traffic*

Inbound Internet Traffic

For traffic from the private network that is inbound on the Internet interface, the NAT first assesses whether an address/port mapping, whether static or dynamic, exists for the packet. If a mapping does not exist for the packet, it is silently discarded by the NAT.

This behavior protects the private network from malicious users on the Internet. The only way that Internet traffic is forwarded to the private network is either in response to traffic initiated by a private network user that created a dynamic mapping, or because a static mapping exists so that Internet users can access specific resources on the private network.

After mapping, the NAT checks for editors and invokes one if necessary. After editing, the NAT modifies the TCP, UDP, and IP headers and forwards the frame using the private network interface. Figure 12.4 shows NAT processing for inbound Internet traffic.

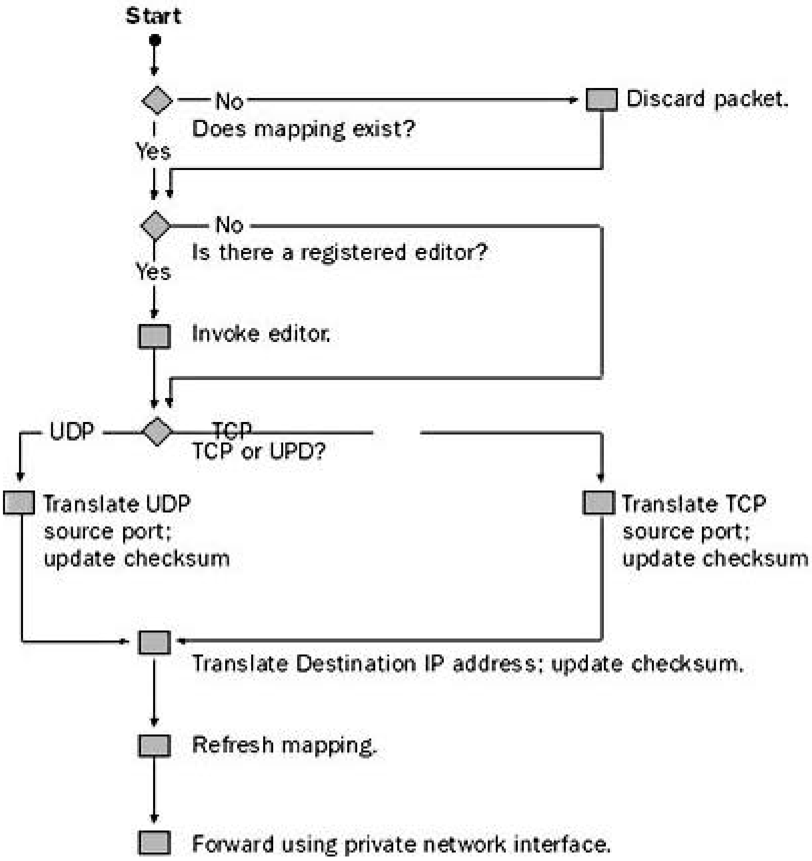

Start
No
Does mapping exist?
Yes
Discard packet.
No
Is there a registered editor?
Yes
Invoke editor.
UDP
TCP
TCP or UPD?
Translate UDP source port; update checksum
Translate TCP source port; update checksum
Translate Destination IP address; update checksum.
Refresh mapping.
Forward using private network interface.

Figure 12.4 *NAT processing of inbound Internet traffic*

Additional NAT Routing Protocol Components

To help simplify the configuration of small networks connecting to the Internet, the NAT routing protocol for Windows 2000 also includes a DHCP allocator and a DNS proxy.

DHCP Allocator

The DHCP allocator component provides IP address configuration information to the other computers on the network. The DHCP allocator is a simplified DHCP server that allocates an IP address, a subnet mask, a default gateway, and the IP address of a DNS server. You must configure computers on the DHCP network as DHCP clients to receive the IP configuration automatically. The default TCP/IP configuration for Windows 2000, Windows NT, Windows 95, and Windows 98 computers is as a DHCP client.

Table 12.1 lists the DHCP options in the DHCPOFFER and DHCPACK messages issued by the DHCP allocator during the DHCP lease configuration process. You cannot modify these options or configure additional DHCP options.

Table 12.1 *DHCP Lease Configuration Options*

Option Number	Option Value	Description
1	255.255.0.0	Subnet mask

3	IP address of private interface	Router (default gateway)
6	IP address of private interface	DNS server (only issued if DNS proxy is enabled)
58 (0x3A)	5 minutes	Renewal time
59 (0x3B)	5 days	Rebinding time
51	7 days	IP address lease time
15 (0x0F)	Primary domain name of NAT computer	DNS domain

The DHCP allocator only supports a single scope of IP addresses as configured from the Address Assignment tab in the Properties Of The Network Address Translation (NAT) Routing Protocol dialog box in the Routing and Remote Access snap-in. The DHCP allocator does not support multiple scopes, superscopes, or multicast scopes. If you need this functionality, you should install a DHCP server and disable the DHCP allocator component of the NAT routing protocol.

DNS Proxy

The DNS proxy component acts as a DNS server to the computers on the network. DNS queries sent by a computer to the NAT server are forwarded to the DNS server. Responses to DNS queries computers receive via the NAT server are re-sent to the original small office or home office computer.

Lesson Summary

NAT enables private IP addresses to be translated into public IP addresses for traffic to and from the Internet. This keeps the internal network secure from the Internet, while saving the user the time and expense of acquiring and maintaining a public address range. A small business would normally have to obtain an ISP-allocated public IP address for each computer on its network. With the NAT, however, the small business can use private addressing and have the NAT map its private addresses to a single or to multiple public IP addresses as allocated by its ISP.

[Previous] [Next]

Lesson 2: Installing Internet Connection Sharing

Internet Connection Sharing (ICS) is a feature of Network and Dial-Up Connections that allows you to use Windows 2000 to connect your home network or small office network to the Internet. For example, you might have a home network that connects to the Internet by using a dial-up connection. In this lesson, you will learn how to install ICS in Windows 2000.

After this lesson, you will be able to

- Enable the ICS feature of Windows 2000
- Configure Internet options for ICS

Estimated lesson time: 35 minutes

Internet Connection Sharing

Internet Connection Sharing (ICS) is a simple package consisting of DHCP, NAT, and DNS. You can use ICS to easily connect your entire network to the Internet. Because ICS provides a translated connection, all of the computers on the network can access Internet resources such as e-mail, Web sites, and FTP sites. ICS provides the following:

- Ease of configuration
- Single public IP address
- Fixed address range for hosts
- DNS proxy for name resolution
- Automatic IP addressing

ICS provides many more features than just address translation. Microsoft has added many features to make the configuration of Internet connections as simple as possible. ICS can be fully configured and administered from the Routing and Remote Access Manager. For a simple home network, a Connection Sharing Wizard can also be launched from Control Panel Connections. The wizard does not allow configuration of any options but can get a home network up on the Internet in minutes. What simplifies the configuration is automatic addressing and automatic name resolution through the DHCP allocator, DNS proxy, and WINS proxy components. Each of these components provides a simplified configuration over the full version of DHCP, DNS, and WINS servers.

By enabling ICS on the computer that uses the dial-up connection, you are providing NAT, addressing, and name resolution services for all computers on your home network. After ICS is enabled and users verify their networking and Internet options, home network or small office network users can use applications such as Microsoft Internet Explorer and Microsoft Outlook Express as if they were directly connected to the ISP. The ICS computer then dials the ISP and creates the connection so that the user can reach the specified Web address or resource. To use the ICS feature, users on your home office or small office network must configure TCP/IP on their local area connection to obtain an IP address automatically.

Enabling Internet Connection Sharing

Before you enable ICS, consider the following:

- You should not use the ICS feature in a network with other Windows 2000 Server domain controllers, DNS servers, gateways, DHCP servers, or systems configured for static IP.
- When you enable ICS, the network adapter connected to the home or small office

network is given a new IP address configuration. Existing TCP/IP connections on the ICS computer are lost and need to be reestablished.

- To use the ICS feature, users on your home office or small office network must configure TCP/IP on their local area connection to obtain an IP address automatically.

- If the ICS computer is using ISDN or a modem to connect to the Internet, you must select the Enable On-Demand Dialing check box.

- **To enable ICS on a network connection**

1. Click Start, point to Settings, then click Network And Dial-Up Connections.

2. Right-click the dial-up, virtual private network (VPN), or incoming connection you want to share, then click Properties.

3. In the Sharing tab, select the Enable Internet Connection Sharing For This Connection check box.

4. If you want this connection to dial automatically when another computer on your home network attempts to access external resources, select the Enable On-Demand Dialing check box.

Installing Connection Sharing

Connection Sharing is configured from within the Routing and Remote Access Manager.

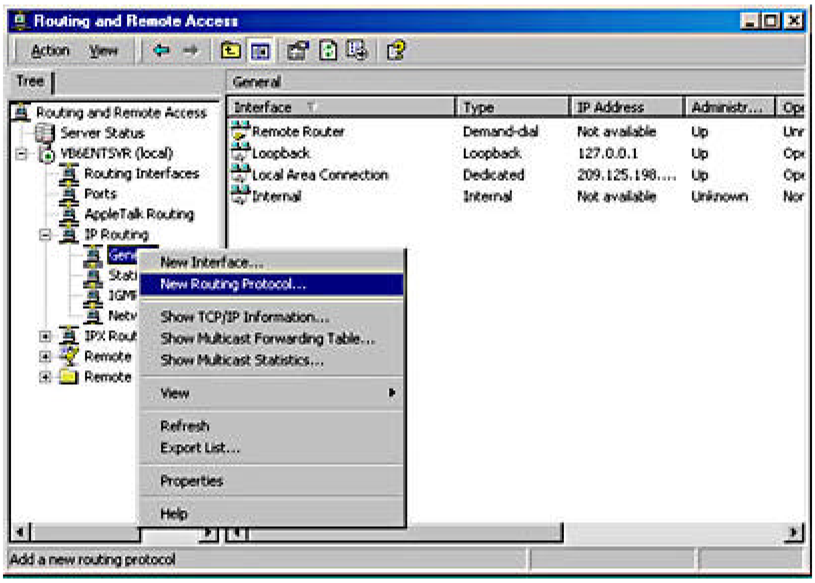
- **To install Connection Sharing**

1. In the Routing and Remote Access Manager, open the IP Routing folder and right-click on General.

2. Click New Routing Protocol, as illustrated in Figure 12.5.

   The Select Routing Protocol dialog box appears.

3. In the Select Routing Protocol dialog box, click Connection Sharing.



Interface	Type	IP Address	Administr...	Op
Remote Router	Demand-dial	Not available	Up	Unr
Loopback	Loopback	127.0.0.1	Up	Op
Local Area Connection	Dedicated	209.125.198....	Up	Op
Internal	Internal	Not available	Unknown	Nor

Add a new routing protocol

Figure 12.5 *Routing and Remote Access Manager IP Routing menu*

Configuring Internet Options for Internet Connection Sharing

If you have not previously established an Internet connection, complete the following steps.

- **To establish an Internet connection**

1. Open Internet Explorer.
2. Click I Want To Set Up My Internet Connection Manually or I Want To Connect Through A Local Area Network (LAN), then click Next.
3. Click I Connect Through A Local Area Network (LAN), then click Next.
4. Clear the Automatic Discovery Of Proxy Server [Recommended] check box, then click Next.
5. If you want to set up an Internet mail account now, and know your connection information, click Yes, and provide the e-mail account information for which the wizard prompts you. If you do not want to set up an Internet mail account, click No, click Next, then click Finish.

If you have previously established an Internet connection, you will be prompted to complete the following steps.

- **To configure Internet options for ICS**

1. From the Tools menu, click Internet Options.
2. In the Connections tab, click Never Dial A Connection, then click LAN Settings.
3. In Automatic Configuration, clear the Automatically Detect Settings and Use Automatic Configuration Script check boxes.

4. In Proxy Server, clear the Use A Proxy Server check box.

Internet Connection Sharing and NAT

To connect a small office or home office network to the Internet, you can use either a routed or translated connection. For a routed connection, the computer running Windows 2000 Server acts as an IP router that forwards packets between the internal network and the public Internet. Although conceptually simple, a routed connection requires knowledge of IP addressing and routing. However, routed connections allow for all IP traffic between internal hosts and the public Internet. For more information, see the Small Office/Home Office (SOHO) Network to the Internet online help topic.

For a translated connection, the computer running Windows 2000 Server acts as a network address translator. Translated connections that use computers running Windows 2000 Server require less knowledge of IP addressing and routing, and provide a simplified configuration for hosts and the Windows 2000 router. However, translated connections may not allow all IP traffic between SOHO hosts and Internet hosts.

In Windows 2000 Server, you can configure a translated connection to the Internet by using either the ICS feature of Network and Dial-Up Connections or the NAT routing protocol provided with Routing and Remote Access. Both ICS and NAT provide translation, addressing, and name resolution services to SOHO hosts.

As described in the previous section, ICS is designed to provide a single step of configuration (a single check box) on the computer running Windows 2000 to provide a translated connection to the Internet for all of the hosts on the network. However, once enabled, ICS does not allow further configuration beyond the configuration of applications and services. For example, ICS is designed for a single IP address obtained from an ISP and does not allow you to change the range of IP addresses allocated to hosts.

As you learned in Lesson 1, the NAT routing protocol is designed to provide maximum flexibility in the configuration of the computer running Windows 2000 Server to provide a translated connection to the Internet. NAT requires additional configuration steps; however, each step of the configuration is customizable. The NAT protocol allows for ranges of IP addresses from the ISP and the configuration of the range of IP addresses allocated to hosts.

Table 12.2 summarizes the features and capabilities of ICS and NAT.

Table 12.2 *ICS and NAT Features*

ICS	NAT
Single check box configuration	Manual configuration
Single public IP address	Multiple public IP addresses
Fixed address range for internal hosts	Configurable address range for internal hosts
Single internal interface	Multiple internal interfaces

ICS and NAT are features of Windows 2000 Server that are designed to connect SOHO networks to the Internet. ICS and NAT are not designed to

- Directly connect separate private networks together
- Connect networks within an intranet
- Directly connect branch office networks to a corporate network
- Connect branch office networks to a corporate network over the Internet

Troubleshooting Connection Sharing (NAT)

You can answer the following questions to troubleshoot configuration problems with Connection Sharing (NAT):

- **Are all of your interfaces (public and private) added to the Connection Sharing (NAT) routing protocol?** You must add both public (Internet) and private (small office or home office) interfaces to the Connection Sharing (NAT) routing protocol.
- **Is translation enabled on the Internet (external) interface?** You need to verify that the interface on the Windows router that connects to the Internet is configured for translation. The Enable Translation Across This Interface option in the General tab of the Properties Of The Internet Interface dialog box should be selected.
- **Is Connection Sharing enabled on the private (internal) interface?** You need to verify that the interface on the Windows router that connects to the internal network is configured for Connection Sharing. The Allow Clients On This Interface To Access Any Shared Networks option in the General tab of the Properties Of The Home Network Interface dialog box should be selected.
- **Is TCP/UDP port translation enabled?** If you only have a single public IP address, you need to verify that the Translate TCP/UDP Headers check box in the General tab of the Properties Of The External Interface dialog box is selected.
- **Is your range of public addresses set correctly?** If you have multiple public IP addresses, you need to verify that they are properly entered in the Address Pool tab of the Properties Of The Internet Interface dialog box. If your address pool includes an IP address that was not allocated to you by your ISP, then inbound Internet traffic that is mapped to that IP address may be routed by the ISP to another location.
- **Is the protocol being used by a program translatable?** If you have some programs that do not seem to work through the NAT, you can try running them from the NAT computer. If they work from the NAT computer and not from a computer on the private network, then the payload of the program may not be translatable. You can check the protocol being used by the program against the list of supported NAT editors.
- **Is Connection Sharing addressing enabled on the home office network?** If

static addresses are not configured on the private network, verify that Connection Sharing addressing is enabled on the interfaces corresponding to the private network. To verify, click Interfaces in the Addressing tab of the Properties Of The Connection Sharing Object dialog box.

Lesson Summary

ICS is a feature of Network and Dial-Up Connections that allows you to use Windows 2000 to connect your home network or small office network to the Internet. ICS can be fully configured and administered from the Routing and Remote Access Manager. By enabling ICS on the computer that uses the dial-up connection, you are providing NAT, addressing, and name resolution services for all computers on your home network.

[Previous] [Next]

Lesson 3: Installing and Configuring NAT

The main intent of NAT is to save on the diminishing IP address space. A secondary benefit of NAT is providing network connectivity without the need to understand IP routing or IP routing protocols. The NAT can be used without the knowledge or cooperation of an ISP. Contacting the ISP for the addition of static routes is not required. In this lesson, you will learn how to install and configure NAT.

After this lesson, you will be able to

- Describe some design issues you should consider before implementing NAT
- Enable NAT addressing
- Configure interface IP address ranges
- Configure interface special ports
- Configure NAT network applications

Estimated lesson time: 20 minutes

Network Address Translation Design Considerations

A common use for NAT is Internet connectivity from a home or small network. To prevent problems, there are certain design issues you should consider before you implement NAT. For example, when using a NAT, private addresses are normally used on the internal network. As described in Lesson 1, private addresses are intended for internal networks, meaning those not directly connected to the Internet. It is recommended that you use these addresses instead of picking addresses at random to avoid potentially duplicating IP address assignment. Additionally, you should consider routing instead of a NAT because routing is fast and efficient, and IP was designed to be routed. However, routing requires valid IP addresses and considerable knowledge to be implemented.

IP Addressing Issues

You should use the following IP addresses from the InterNIC private IP network IDs: 10.0.0.0 with a subnet mask of 255.0.0.0, 172.16.0.0 with a subnet mask of 255.240.0.0, and 192.168.0.0 with a subnet mask of 255.255.0.0. By default, NAT uses the private network ID 192.168.0.0 with the subnet mask of 255.255.255.0 for the private network.

If you are using public IP networks that have not been allocated by the InterNIC or your ISP, then you may be using the IP network ID of another organization on the Internet. This is known as illegal or overlapping IP addressing. If you are using overlapping public addresses, then you cannot reach the Internet resources of the overlapping addresses. For example, if you use 1.0.0.0 with the subnet mask of 255.0.0.0, then you cannot reach any Internet resources of the organization that is using the 1.0.0.0 network. You can also exclude specific IP addresses from the configured range. Excluded addresses are not allocated to private network hosts.

- **To configure the NAT server**

1. Install and enable Routing and Remote Access.

   In the Routing and Remote Access Server Setup Wizard, choose the options for ICS and to set up a router with the NAT routing protocol. After the wizard is finished, all of the configuration for NAT is complete. You do not need to complete steps 2 through 8. If you have already enabled Routing and Remote Access, then complete steps 2 through 8, as needed.

2. Configure the IP address of the home network interface.

3. For the IP address of the LAN adapter that connects to the home network, you need to configure the following:

   - IP address: 192.168.0.1
   - Subnet mask: 255.255.255.0
   - No default gateway

   NOTE

   The IP address in the preceding configuration for the home network interface is based on the default address range of 192.168.0.0 with a subnet mask of 255.255.255.0, which is configured for the addressing component of NAT. If you change this default address range, you should change the IP address of the private interface for the NAT computer to be the first IP address in the configured range. Using the first IP address in the range is a recommended practice, not a requirement of the NAT components.

4. Enable routing on your dial-up port.

   If your connection to the Internet is a permanent connection that appears in Windows 2000 as a LAN interface (such as DDS, T-Carrier, frame relay, permanent ISDN, xDSL, or cable modem), or if you are connecting your computer running Windows 2000 to another router before the connection to the

Internet, and the LAN interface is configured with an IP address, subnet mask, and default gateway either statically or through DHCP, skip to step 6.

5. Create a demand-dial interface to connect to your ISP.

   You must create a demand-dial interface that is enabled for IP routing and uses your dial-up equipment and the credentials that you use to dial your ISP.

6. Create a default static route that uses the Internet interface.

   For a default static route, you need to select the demand-dial interface (for dial-up connections) or LAN interface (for permanent or intermediate router connections) that is used to connect to the Internet. The destination is 0.0.0.0 and the network mask is 0.0.0.0. For a demand-dial interface, the gateway IP address is not configurable.

7. Add the NAT routing protocol.

   Instructions for adding the NAT routing protocol are described in the next procedure.

8. Add your Internet and home network interfaces to the NAT routing protocol.

9. Enable NAT addressing and name resolution.

- **To add NAT as a routing protocol**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing and Remote Access.

2. In the console tree, click General under Routing And Remote Access\Server Name\IP Routing.

3. Right-click General, then click New Routing Protocol.

4. In the Select Routing Protocol dialog box, click Network Address Translation, then click OmK.

- **To enable NAT addressing**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.

2. In the console tree, click NAT.

3. Right-click NAT, then click Properties.

4. In the Address Assignment tab, select the Automatically Assign IP Addresses By Using DHCP check box.

5. If applicable, in IP Address And Mask, configure the range of IP addresses to allocate to DHCP clients on the private network.

6. If applicable, click Exclude, configure the addresses to exclude from allocation to DHCP clients on the private network, then click OK.

Single or Multiple Public Addresses

If you are using a single public IP address allocated by your ISP, no other IP address configuration is necessary. If you are using multiple IP addresses allocated by your ISP, then you must configure the NAT interface with your range of public IP addresses. For the range of IP addresses given to you by your ISP, you must determine whether the range of public IP addresses can be expressed by using an IP address and a mask.

If you are allocated a number of addresses that have a power of 2 (2, 4, 8, 16, and so on), you can express the range by using a single IP address and mask. For example, if you are given the four public IP addresses 200.100.100.212, 200.100.100.213, 200.100.100.214, and 200.100.100.215 by your ISP, then you can express these four addresses as 200.100.100.212 with a mask of 255.255.255.252. If your IP addresses are not expressible as an IP address and a subnet mask, you can enter them as a range or series of ranges by indicating the starting and ending IP addresses.

- **To configure interface IP address ranges**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.

2. In the console tree, click NAT.

3. In the details pane, right-click the interface you want to configure, then click Properties.

4. In the Address Pool tab, click Add.

   If you are using a range of IP addresses that can be expressed with an IP address and a subnet mask, in Start Address, type the starting IP address, and in Mask, type the subnet mask. However, if you are using a range of IP addresses that cannot be expressed with an IP address and a subnet mask, in Start Address, type the starting IP address, and in End Address, type the ending IP address.

Allowing Inbound Connections

Normal NAT usage from a home or small business allows outbound connections from the private network to the public network. Programs such as Web browsers that run from the private network create connections to Internet resources. The return traffic from the Internet can cross the NAT because the connection was initiated from the private network. To allow Internet users to access resources on your private network, you must do the following:

- Configure a static IP address configuration on the resource server including IP address (from the range of IP addresses allocated by the NAT computer), subnet mask (from the range of IP addresses allocated by the NAT computer), default gateway (the private IP address of the NAT computer), and DNS server (the private IP address of the NAT computer).

- Exclude the IP address being used by the resource computer from the range of IP addresses being allocated by the NAT computer.

- Configure a special port. A special port is a static mapping of a public address and port number to a private address and port number. A special port maps an inbound connection from an Internet user to a specific address on your private network. By using a special port, you can create a Web server on your private network that is accessible from the Internet.

- **To configure interface special ports**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.
2. In the details pane, right-click the interface you want to configure, and then click Properties.
3. In the Special Ports tab, in Protocol, click either TCP or UDP, then click Add.
4. In Incoming Port, type the port number of the incoming public traffic.
5. If a range of public IP addresses is configured, click On This Address Pool Entry, and then type the public IP address of the incoming public traffic.
6. In Outgoing Port, type the port number of the private network resource.
7. In Private Address, type the private address of the private network resource.

Configuring Applications and Services

You may need to configure applications and services to work properly across the Internet. For example, if users on your small office or home office network want to play the Diablo game with other users on the Internet, NAT must be configured for the Diablo application.

- **To configure NAT network applications**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.
2. In the console tree, click NAT.
3. Right-click NAT, then click Properties.
4. In the Translation tab, click Applications.
5. To add a network application, in the Applications dialog box, click Add.
6. In the Add Application dialog box, type the settings for the network application, then click OK.

NOTE

You can also edit or remove an existing NAT network application by clicking Edit or Remove in the Applications dialog box.

Virtual Private Network Connections from a Translated Network

To access a private intranet using a VPN connection from a translated network, you can use the PPTP and create a VPN connection from a host on the internal network to the VPN server within the second private intranet. The NAT routing protocol has a NAT editor for PPTP traffic. Layer 2 Tunneling Protocol (L2TP) over IPSec connections do not work across the NAT server.

Virtual Private Networks and NATs

Not all traffic can by translated by the NAT. Some applications may have embedded IP addresses (not in the IP header) or may be encrypted. For these applications one can tunnel through the NAT using PPTP. PPTP does require an editor, which has been implemented in the NAT. Only the IP and Generic Routing Encapsulation (GRE) headers are edited or translated. The original IP datagram is not affected. This allows for encryption or otherwise unsupported applications to go through the NAT.

The source of the PPTP packets will be translated to a NAT address. The encapsulated IP packet will have a source address assigned by the PPTP server. When the packet is beyond the PPTP server, the encapsulation is removed and the source address will be the one assigned by the PPTP server. If the PPTP server is using a pool of valid Internet addresses, the client now has a valid address and can go anywhere on the Internet. Any application will work, as the original IP datagram is not translated. Only the encapsulation or wrapper is translated by the NAT.

NOTE

L2TP does not require a NAT editor. However, L2TP with IPSec cannot be translated by the NAT. There cannot be a NAT editor for IPSec.

This method of NAT bypass is only useful if there is a PPTP server to tunnel to. This will be good for branch offices or home users tunneling to a corporate network, as illustrated in Figure 12.6.

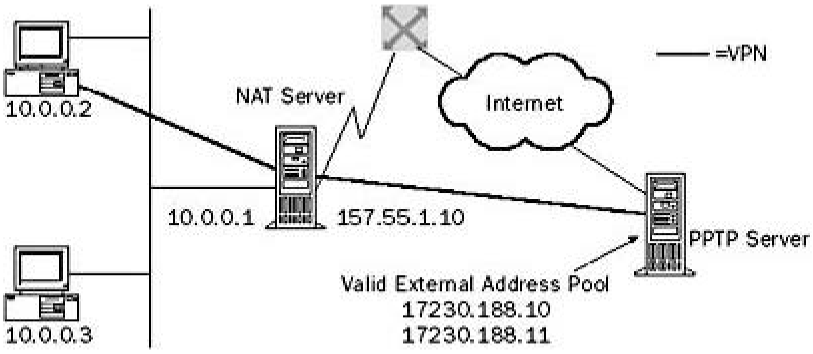


Figure 12.6 *Implementing a VPN through a NAT server*

Lesson Summary

When using a NAT, private addresses are normally used on the internal network. It is recommended that you use these addresses on a private network instead of picking addresses at random because they are potentially duplicate addresses not valid on the Internet. To prevent problems, you should identify design issues before you implement NAT. Normal NAT usage from a home or small business allows outbound connections from the private network to the public network. You may need to configure applications and services to work properly across the Internet. In addition, remember that not all traffic can by translated by the NAT because some applications may have embedded IP addresses or may be encrypted. For these applications you can tunnel through the NAT using PPTP.

[Previous] [Next]

Review

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What is the purpose of NAT?

2. What are the components of NAT?

3. If a small business is using the 10.0.0.0 private network for its intranet and has been granted the public IP address of 198.200.200.1 by its ISP, to what public IP address does NAT map all private IP addresses being used on network 10.0.0.0?

4. What must you do to allow Internet users to access resources on your private network?

Answers