Module Practice and Quiz

6.8.1

Packet Tracer - Configure NAT for IPv4

In this Packet Tracer, you will complete the following objectives:

- Configure Dynamic NAT with PAT
- Configure Static NAT

Configure NAT for IPv4

Configure NAT for IPv4

6.8.2

Lab - Configure NAT for IPv4

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure and verify NAT for IPv4
- Part 3: Configure and verify PAT for IPv4
- Part 4: Configure and verify Static NAT for IPv4

Configure NAT for IPv4

6.8.3

What did I learn in this module?

NAT Characteristics

There are not enough public IPv4 addresses to assign a unique address to each device connected to the internet. Private IPv4 addresses cannot be routed over the internet. To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address. NAT provides the translation of private addresses to public addresses. The primary use of NAT is to conserve public IPv4 addresses. It allows networks to use private IPv4 addresses internally and provides translation to a public address only when needed. When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from the NAT pool. In NAT terminology, the inside network is the set of networks that is subject to translation. The outside network refers to all other networks. When determining which type of address is used, it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address:

- **Inside address** - The address of the device which is being translated by NAT.
- **Outside address** - The address of the destination device.

NAT also uses the concept of local or global with respect to addresses:

- **Local address** - A local address is any address that appears on the inside portion of the network.
- **Global address** - A global address is any address that appears on the outside portion of the network.

Types of NAT

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant. Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server. Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses. This is the most common form of NAT for both the home and the enterprise. PAT ensures that devices use a different TCP port number for each session with a server on the internet. PAT attempts to preserve the original source port. However, if the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group. PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol. The most common of these is ICMPv4.

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local address.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network.

NAT Advantages and Disadvantages

Advantages: NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT increases the flexibility of connections to the public network. NAT provides consistency for internal network addressing schemes. NAT hides user IPv4 addresses.

Disadvantages: NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time. The process of two layers of NAT translation is known as Carrier Grade NAT (CGN). End-to-end addressing is lost. Many internet protocols and applications depend on end-to-end addressing from the source to the destination. End-to-end IPv4 traceability is also lost. Using NAT also complicates the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

Static NAT

Static NAT is a one-to-one mapping between an inside address and an outside address. Static NAT allows external devices to initiate connections to internal devices using the statically assigned public address. The first task is to create a mapping between the inside local address and the inside global addresses using the **ip nat inside source static** command. After the mapping is configured, the interfaces participating in the translation are configured as inside or outside relative to NAT using the **ip nat inside** and **ip nat outside** commands. To verify NAT operation use the **show ip nat translations** command. To verify that the NAT translation is working, it is best to clear statistics from any past translations using the **clear ip nat statistics** command before testing.

Dynamic NAT

Dynamic NAT automatically maps the inside local addresses to inside global addresses. Dynamic NAT, like static NAT, requires the configuration of the inside and outside interfaces participating in NAT. Dynamic NAT uses a pool of addresses translating a single inside address to a single outside address. The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come first-served basis. With this type of translation there must be enough addresses in the pool to accommodate all the inside devices needing concurrent access to the outside network. If all addresses in the pool are in use, a device must wait for an available address before it can access the outside network.

To configure dynamic NAT, first define the pool of addresses that will be used for translation using the **ip nat pool** command. The addresses are defined by indicating the starting IPv4 address and the ending IPv4 address of the pool. The **netmask** or **prefix-length** keyword indicates which address bits belong to the network and which bits belong to the host for the range of addresses. Configure a standard ACL to identify (permit) only those addresses that are to be translated. Bind the ACL to the pool, using the following command syntax: Router(config)# **ip nat inside source list** {*access-list-number* | *access-list-name*} **pool** *pool-name*. Identify which interfaces are inside, in relation to NAT. Identify which interfaces are outside, in relation to NAT.

To verify dynamic NAT configurations, The output of the **show ip nat translations** command shown displays all static translations that have been configured and any dynamic translations that have been created by traffic. Adding the **verbose** keyword displays additional information about each translation, including how long ago the entry was created and used. By default, translation entries time out after 24 hours, unless the timers have been reconfigured with the **ip nat translation timeout** *timeout-seconds* command in global configuration mode. To clear dynamic entries before the timeout has expired, use the **clear ip nat translation** privileged EXEC mode command.

PAT

There are two ways to configure PAT, depending on how the ISP allocates public IPv4 addresses. In the first instance, the ISP allocates a single public IPv4 address that is required for the organization to connect to the ISP and in the other, it allocates more than one public IPv4 address to the organization. To configure PAT to use a single IPv4 address, simply add the keyword **overload** to the **ip nat inside source** command. The rest of the configuration is the similar to static and dynamic NAT configuration except that with PAT, multiple hosts can use the same public IPv4 address to access the internet. To configure PAT for a dynamic NAT address pool, simply add the keyword **overload** to the **ip nat inside source** command. Multiple hosts can share an IPv4 address from the pool because PAT is enabled with the keyword **overload**.

To verify PAT configurations us the **show ip nat translations** command. The source port numbers in the NAT table differentiate the transactions. The **show ip nat statistics** command verifies that the NAT-POOL has allocated a single address for multiple translations. Included in the output is information about the number and type of active translations, NAT configuration parameters, the number of addresses in the pool, and how many have been allocated.

NAT64

IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary. However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs). IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but have a different purpose. ULA addresses are meant for only local communications within a site. ULA addresses are not meant to provide additional IPv6 address space, nor to provide a level of security; however, IPv6 does provide for protocol translation between IPv4 and IPv6 known as NAT64. NAT for IPv6 is used in a much different context than NAT for IPv4. The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks. To aid in the move from IPv4 to IPv6, the IETF has developed several transition techniques to accommodate a variety of IPv4-to-IPv6 scenarios, including dual-stack, tunneling, and translation. Dual-stack is when the devices are running protocols associated with both the IPv4 and IPv6. Tunneling for IPV6 is the process of encapsulating an IPv6 packet inside an IPv4 packet. This allows the IPv6 packet to be transmitted over an IPv4-only network. NAT for IPv6 should not be used as a long-term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6.

6.8.4

Module Quiz - NAT for IPv4

1. Which two statements accurately describe an advantage or a disadvantage when deploying NAT for IPv4 in a network? (Choose two.)

☐ NAT causes routing tables to include more information.
☑ NAT introduces problems for some applications that require end-to-end connectivity.
☐ NAT adds authentication capability to IPv4.
☐ NAT improves packet handling.
☐ NAT will impact negatively on switch performance.
☑ NAT provides a solution to slow down the IPv4 address depletion.

2. A network administrator wants to examine the active NAT translations on a border router. Which command would perform the task?

● Router# **show ip nat translations**
○ Router# **clear ip nat translations**
○ Router# **show ip nat statistics**
○ Router# **debug ip nat translations**

3. What are two tasks to perform when configuring static NAT? (Choose two.)

☐ Define the inside global address on the server
☑ Identify the participating interfaces as inside or outside interfaces.
☑ Create a mapping between the inside local and inside global addresses.
☐ Define the outside global address.
☐ Configure a NAT pool.

4. What is a disadvantage of NAT?

○ The costs of readdressing hosts can be significant for a publicly addressed network.
○ The internal hosts have to use a single public IPv4 address for external communication.
● There is no end-to-end addressing.
○ The router does not need to alter the checksum of the IPv4 packets.

5. What is one advantage of using NAT at the edge of the network?

○ NAT enables end-to-end IPv4 traceability, making troubleshooting easier.
○ Dynamic NAT allows devices from outside the local network to easily initiate TCP connections to inside hosts.
● Changing ISPs is simpler because the devices on the inside network do not have to be configured with new addresses when the outside address changes.
○ Performance is significantly increased because the router does not have to perform as many route lookups.

6. What benefit does NAT64 provide?

○ It allows sites to use private IPv4 addresses, and thus hides the internal addressing structure from hosts on public IPv4 networks.
○ It allows sites to use private IPv6 addresses and translates them to global IPv6 addresses.
○ It allows sites to connect multiple IPv4 hosts to the Internet via the use of a single public IPv4 address.
● It allows sites to connect IPv6 hosts to an IPv4 network by translating the IPv6 addresses to IPv4 addresses.

7. What address translation is performed by static NAT?

● An inside local address is translated to a specified inside global address.
○ An inside local address is translated to a specified outside global address.
○ An outside local address is translated to a specified outside global address.
○ An inside local address is translated to a specified outside local address.

8. Using NAT terminology, what is the address of the source host on a private network as seen from inside the network?

○ outside global
○ inside global
● inside local
○ outside local

9. Which statement accurately describes dynamic NAT?

○ It dynamically provides IP addressing to internal hosts.
● It provides an automated mapping of inside local to inside global IP addresses.
○ It always maps a private IP address to a public IP address.
○ It provides a mapping of internal host names to IP addresses.

10. Why is NAT not needed in IPv6?

● Any host or user can get a public IPv6 network address because the number of available IPv6 addresses is extremely large.
○ The problems that are induced by NAT applications are solved because the IPv6 header improves packet handling by intermediate routers.
○ The end-to-end connectivity problems that are caused by NAT are solved because the number of routes increases with the number of nodes that are connected to the Internet.
○ Because IPv6 has integrated security, there is no need to hide the IPv6 addresses of internal networks.

11. A company designs its network so that the PCs in the internal network are assigned IP addresses from DHCP servers, and the packets that are sent to the Internet are translated through a NAT-enabled router. What type of NAT enables the router to populate the translation table from a pool of unique public addresses, as the PCs send packets through the router to the Internet?

○ ARP
● dynamic NAT
○ static NAT
○ PAT

12. What is a security feature of using NAT on a network?

○ denies all packets that originate from private IP addresses
○ allows external IP addresses to be concealed from internal users
○ denies all internal hosts from communicating outside their own network
● allows internal IP addresses to be concealed from external users

13. When dynamic NAT without overloading is being used, what happens if seven users attempt to access a public server on the Internet when only six addresses are available in the NAT pool?

○ No users can access the server.
○ The first user gets disconnected when the seventh user makes the request.
○ All users can access the server.
● The request to the server for the seventh user fails.

14. A company has been assigned the 203.0.113.0/27 block of IP addresses by the ISP. The company has over 6000 internal devices. What type of NAT would be most appropriate for the employee workstations of the company?

○ PAT off the external router interface
○ port forwarding
○ static NAT
○ dynamic NAT
● dynamic NAT overload using the pool of addresses

15. Which version of NAT allows many hosts inside a private network to simultaneously use a single inside global address for connecting to the Internet?

○ dynamic NAT
○ static NAT
● PAT
○ port forwarding

Check

Show Me

Reset