7.3.5 NAT Facts

Network address translation (NAT) allows you to connect a private network to the internet without obtaining registered addresses for every host. This lesson covers:

- How NAT works
- Implementing NAT
- Reserved private IP addresses

How NAT Works

NAT works by translating private addresses to the public address of the NAT router.

- Hosts on the private network share the IP address of the NAT router or a pool of addresses assigned for the network.
- The NAT router maps port numbers to private IP addresses. Responses to internet requests include the port number appended by the NAT router. This allows the NAT router to forward responses back to the correct private host.
- Technically speaking, NAT translates one address to another. Port address translation (PAT) associates a port number with the translated address.
  - With only NAT, you would need a public address for each private host. NAT associates a single public address with a single private address.
  - PAT allows multiple private hosts to share a single public address. Each private host is associated with a unique port number on the NAT router.
  - Because virtually all NAT routers perform PAT, you normally use PAT, and not just NAT, when you use a NAT router. (NAT is usually synonymous with PAT.)

Implementing NAT

When you implement NAT, be aware of the following:

- NAT supports a limit of 5,000 concurrent connections.
- NAT provides some security for the private network because it translates or hides private addresses.
- A NAT router can act as a limited-function DHCP server, assigning addresses to private hosts.
- A NAT router can forward DNS requests to the internet.

The following table describes three types of NAT implementation.

Type	Description
Dynamic NAT	Dynamic NAT automatically maps internal IP addresses with a dynamic port assignment. On the NAT device, the internal device is identified by the public IP address and the dynamic port number. Dynamic NAT allows internal (private) hosts to contact external (public) hosts, but not vice versa—external hosts cannot initiate communications with internal hosts. This implementation is also sometimes called many-to-one NAT because many internal private IP address are mapped to one public IP address on the NAT router.
Static NAT (SNAT)	Static NAT maps a single private IP address to a single public IP address on the NAT router. Static NAT is used to take a server on the private network (such as a web server) and make it available on the internet. Using a static mapping allows external hosts to contact internal hosts—external hosts contact the internal server using the public IP address and the static port. This implementation is called one-to-one NAT because one private IP address is mapped to one public IP address. In addition to static NAT, the term SNAT also means source NAT, stateful NAT, and secure NAT. Although the terms vary, the function is the same. One commonly used implementation of static NAT is called port forwarding. Port forwarding allows incoming traffic addressed to a specific port to move through the firewall and be transparently forwarded to a specific host on the private network. Inbound requests are addressed to the port used by the internal service on the router's public IP address (such as port 80 for a web server). This is often called the public port. Port forwarding associates the inbound port number with the IP address and port of a host on the private network. This port is often called the private port. Based on the public port number, incoming traffic is redirected to the private IP address and port of the destination host on the internal network. Port forwarding is also called destination network address translation, or DNAT.
Dynamic and Static NAT	Dynamic and static NAT, where two IP addresses are given to the public NAT interface (one for dynamic NAT and one for static NAT), allows traffic to flow in both directions.

Reserved Private IP Addresses

When connecting a private network to the internet through NAT, IP addresses on the private network are commonly those reserved by the Internet Assigned Numbers Authority (IANA) for that purpose. These address ranges are guaranteed not to be used on the internet and do not need to be registered. The private IPv4 address ranges are:

- 10.0.0.1 to 10.255.255.254
- 172.16.0.1 to 172.31.255.254
- 192.168.0.1 to 192.168.255.254