5.6.4 NAT Facts

A *Network Address Translation* (NAT) router translates multiple private addresses into a single registered IP address. NAT helps address the shortage of registered IPv4 addresses.

- The internet is classified as a *public* network. All devices on the public network must have a registered IP address; this address is assigned by an ISP.
- An internal network is classified as a *private* network. All devices on the private network use private IP addresses internally, but share a single public IP address when accessing the internet.
- NAT is typically implemented on a default gateway router.
- A router running NAT modifies the source IP addresses contained within the IP packet, replacing private addresses in the packet with a public IP address.
- The private network can use IPv4 addresses in the following ranges that have been reserved for private use (meaning they will not be used by hosts on the internet).
  - 10.0.0.0 to 10.255.255.255 (known as class A private network addresses)
  - 172.16.0.0 to 172.31.255.255 (known as class B private network addresses)
  - 192.168.0.0 to 192.168.255.255 (known as class C private network addresses)
- IPv6 reserves all addresses beginning with a binary 1111 1110 11 (hexadecimal FEC0::/48) for private IP networks. This address range is called the site-local address range.

  Most routers recognize addresses in these ranges as private IP address and do not route them.

- NAT translates a host's private IP address into a public IP address that can be used by the internet or other public networks.
  - The NAT router uses *Port Address Translation* (PAT) to associate a port number with a request from a private host.
  - Returning data is sent to the port number specified in the request.
  - The NAT router uses its translation table to determine the private host associated with that port number and forwards the data to the appropriate host.
  - Most routers that are configured with NAT are really performing PAT. NAT is typically used synonymously with PAT.
- NAT can be implemented in one of three ways:
  - Network Address and Port Translation (also referred to as *Dynamic NAT, Many-to-One NAT,* and *IP Masquerade*) supports multiple private hosts on one public IP address.
    - Dynamic NAT allows internal (private) hosts to contact external (public) hosts, but not vice versa. External hosts cannot initiate communications with internal hosts.
    - This is the implementation of NAT that is most frequently used.
  - *Static* NAT (also referred to as *One-to-One NAT* and *Port Forwarding*) maps an internal IP address to a static port assignment or even to a specific public IP address.
    - Using static mapping allows external hosts to contact internal hosts.
    - Static NAT is typically used to make a server on the private network (such as a web server) available on the internet.
    - External hosts contact the internal server using the public IP address and the static port.
    - On a Windows system, the public IP address is *reserved* for a specific host on the private network.
  - Dynamic and Static NAT, in which 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.

Be aware of the following NAT facts:

- NAT should not be considered an acceptable form of network security, although it provides some security for the private network by hiding the private addresses. For a more secure solution, combine NAT with packet filters or firewalls.
- NAT does not provide improved throughput for traffic. To improve throughput for traffic, implement a solution like a proxy server.
- NAT supports a limit of 5,000 concurrent connections.
- NAT routers operate at the Network layer of the OSI Model.
- 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.
- Because NAT changes packet headers, IPSec might not work correctly through NAT. IPSec detects changes to packet headers as part of the security process.