Network Services
Network Address Translation

- **Network address translation (NAT)**
  - Defined in RFC 3022
    - Describes methods for connecting private (internal) IP addresses to the Internet
- **NAT uses a one-to-one mapping or one-to-many mapping method**
  - To allow one or more private IP clients to gain access to the Internet by mapping the private IP addresses to public IP addresses
Network Address Translation (continued)

<table>
<thead>
<tr>
<th>Class</th>
<th>Private Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.x.x.x</td>
</tr>
<tr>
<td>B</td>
<td>172.16.x.x – 172.31.x.x</td>
</tr>
<tr>
<td>C</td>
<td>192.168.x.x</td>
</tr>
</tbody>
</table>

*Table 9-1*  RFC 1918 private address ranges
Network Address Translation (continued)

• Advantages
  – Conserves public IP addresses
  – Hides your internal IP addressing scheme from the outside world, greatly enhancing network security
  – Allows for easy renumbering of your IP addresses

• Disadvantages
  – Introduces a small amount of delay into your network
    • Because the NAT router has to create and maintain the NAT table
  – End-to-end IP traceability is lost
  – Some applications fail due to NAT
Network Address Translation (continued)

• NAT is available in three forms:
  – Static NAT
  – Dynamic NAT
  – Port address translation (PAT)
Static NAT

• **Static NAT**
  – The simplest form of NAT
  – A single private IP address is mapped to a single public IP address

• NAT router must maintain a table in memory
  – Table maps internal IP addresses to addresses presented to the Internet
Figure 9-1  Static NAT table
Static NAT (continued)

• The network configuration for NAT is quite simple in a small network
  – The NAT router will be the default gateway for all clients
• In a larger network, the NAT router might be one of many routers
  – Routers would have to be configured to use the NAT router for Internet communications
• NAT should be configured on the border router of a large network
Dynamic NAT

- **Dynamic NAT**
  - The NAT router automatically maps a group of valid local IP addresses to a group of Internet IP addresses, as needed
- The network administrator is not concerned about which IP address the internal clients use
- Any private IP address will automatically be translated to one of the available Internet IP addresses by the NAT router
  - Addresses for dynamic NAT are pulled out of a predefined pool of public addresses
Port Address Translation

• **Port address translation (PAT)**
  – Also known as *overloading*
  – Is a special form of dynamic NAT
  – Allows multiple internal, private IP addresses to use a single external registered address

• To differentiate between the connections, PAT uses multiple public TCP and UDP ports
  – To create unique sockets that map to internal IP addresses
Port Address Translation (continued)

<table>
<thead>
<tr>
<th>Host</th>
<th>Source Local Socket</th>
<th>Source Translated Socket</th>
<th>Destination Remote Socket</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>192.168.0.1:1025</td>
<td>209.86.192.198:1025</td>
<td>209.120.178.205:80</td>
</tr>
<tr>
<td>B</td>
<td>192.168.0.2:1027</td>
<td>209.86.192.198:1026</td>
<td>209.120.178.205:80</td>
</tr>
<tr>
<td>C</td>
<td>192.168.0.3:1025</td>
<td>209.86.192.198:1027</td>
<td>209.120.178.205:80</td>
</tr>
<tr>
<td>D</td>
<td>192.168.0.4:1512</td>
<td>209.86.192.198:1049</td>
<td>64.247.37.221:21</td>
</tr>
<tr>
<td>D</td>
<td>192.168.0.4:1513</td>
<td>209.86.192.198:1050</td>
<td>64.247.37.221:20</td>
</tr>
<tr>
<td>E</td>
<td>192.168.0.5:1025</td>
<td>209.86.192.198:1029</td>
<td>64.46.108.24:80</td>
</tr>
<tr>
<td>Internal</td>
<td>192.168.0.100:80</td>
<td>209.86.192.198:80</td>
<td>72.13.15.24:1099</td>
</tr>
<tr>
<td>Web server</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 9-2  NAT mapping table
Port Address Translation (continued)

• The NAT server uses **port forwarding**
  – To send connections from external clients to the Web server on the internal network

• **Overlapping**
  – Occurs when:
    • The internal network has been incorrectly configured for an IP range that actually exists on the Internet *or*
    • Two companies merge and each company was using the same private IP address range
  – Can be solved using NAT because NAT hides the incorrectly configured internal IP scheme
Configuring Network Address Translation

- You can configure NAT as static NAT, dynamic NAT, or PAT
Configuring Static NAT

• Configuring static NAT is a two-step process:
  – Define the static mapping between the inside address and the outside address
  – Define the NAT router’s interfaces as inside or outside

• The static mapping is defined with the following command:

  ip nat inside source static [inside ip] [outside ip]
  ip nat [inside | outside]
  show ip nat translations
Configuring Dynamic NAT

• Steps:
  – Configure a standard access control list to define what internal traffic will be translated
  – Define a pool of addresses to be used for dynamic NAT allocation
  – Link the access list to the NAT pool
  – Define interfaces as either inside or outside

• To define the standard access list, you must use the following syntax:

  RouterA(config)#access-list [1-99] permit [inside IP network(s)] [wildcard mask]
Configuring Dynamic NAT (continued)

- The syntax for defining the NAT pool is:
  
  \[
  \text{ip nat pool} \ [\text{pool name}] \ [\text{start ip}] \ [\text{end ip}] \\
  \text{netmask} \ [\text{netmask}] \\
  \]

- The pool must then be linked to the access list with the following command:
  
  \[
  \text{ip nat inside source list} \ [\text{access list number}] \\
  \text{pool} \ [\text{pool name}] \\
  \]

- Finally, you must define the interfaces as either inside or outside
Configuring Dynamic NAT (continued)

• Steps for configuring PAT:
  – Configure a standard access list to define what internal traffic will be translated
  – Link the access list to the interface to be used for PAT
  – Define interfaces as either inside or outside

Router A(config)#access-list 1 permit 192.168.0.0 0.0.0.255
Router A(Config)#ip nat inside source list 1 interface serial 0/1 overload
Figure 9-2  Port address translation example
Domain Name Service

- Domain Name Service (DNS)
  - A popular and important naming service
  - Based on the client/server model, DNS translates names into IP addresses
- Use the `ip host` command to manually provide name resolution on a Cisco router
- Lookup
  - By default, a Cisco router will try several times to find an IP address for a name if you enter one
Domain Name Service (continued)

RouterA#SwitchA
Translating "SwitchA"...domain server (255.255.255.255)

Translating "SwitchA"...domain server (255.255.255.255)
(255.255.255.255)
Translating "SwitchA"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Figure 9-3   Output with no name server configured
Domain Name Service (continued)

• Configuring DNS Lookup
  – The command to configure a DNS lookup on a Cisco router is `ip name-server`
  • The `ip domain-lookup` command enables DNS if it has previously been disabled

```plaintext
RouterA(config)#ip domain-lookup
RouterA(config)#ip name-server 10.0.0.3
RouterA(config)#ip domain-name cannon.com
RouterA#SwitchA
Trying SwitchA (10.0.0.2)... Open
SwitchA>
```

**Figure 9-4**  Output when name server is configured
Dynamic Host Configuration Protocol

• Dynamic Host Configuration Protocol (DHCP)
  – Provides IP configuration information to hosts on bootup
  – This functionality is much like that provided by older protocols RARP and BOOTP
• DHCP manages addressing by leasing the IP information to the hosts
  – This leasing allows the information to be recovered when not in use and reallocated when needed
Dynamic Host Configuration Protocol (continued)

![DHCP process diagram]

**Figure 9-5** DHCP process
Dynamic Host Configuration Protocol (continued)

• You can configure your Cisco router to be a DHCP server

• **DHCP relay**
  – The router can forward the request to other DHCP servers if it cannot satisfy a DHCP request

• Configuring the router to be a DHCP server
  – Enable the service using the `service dhcp` command at the global configuration mode prompt
  – Configure DHCP bindings and decide where to store the DHCP bindings database
Dynamic Host Configuration Protocol (continued)

• Configuring the router to be a DHCP server (continued)
  – Define the pool of addresses
  – Configure any optional IP configuration parameters
  – Exclude any statically configured addresses

• Monitoring DHCP
  – The best way to check the bindings is to execute the `show ip dhcp binding` command on the router
  – For information on the specific DHCP address pool, use the `show ip dhcp pool` command
RouterA>en
RouterA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#ip dhcp pool RouterA
RouterA(dhcp-config)#network 10.0.0.0 255.255.255.0
RouterA(dhcp-config)# default-router 10.0.0.1
RouterA(dhcp-config)#domain-name cannon
RouterA(dhcp-config)#dns-server 10.0.0.3
RouterA(dhcp-config)#netbios-name-server 10.0.0.3
RouterA(dhcp-config)#ip dhcp excluded-address 10.0.0.1 10.0.0.3
RouterA(config)#^Z
RouterA#

Figure 9-6  DHCP service on RouterA
Dynamic Host Configuration Protocol (continued)

RouterA#show ip dhcp binding
Bindings from all pools not associated with VRF:
<table>
<thead>
<tr>
<th>IP address</th>
<th>Client-ID/</th>
<th>Lease expiration</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.4</td>
<td>0100.e0b8.cbff</td>
<td>Mar 02 1993 12:21 AM</td>
<td>Automatic</td>
</tr>
</tbody>
</table>

**Figure 9-7**  Output from the show ip dhcp binding command

RouterA#show ip dhcp pool

Pool RouterA:

- Utilization mark (high/low) : 100 / 0
- Subnet size (first/next) : 0 / 0
- Total addresses : 254
- Leased addresses : 1
- Pending event : none

1 subnet is currently in the pool:

<table>
<thead>
<tr>
<th>Current index</th>
<th>IP address range</th>
<th>Leased addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.5</td>
<td>10.0.0.1 - 10.0.0.254</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 9-8**  Output from the show ip dhcp pool command
Security Device Manager

- Cisco’s new Security Device Manager (SDM)
  - Web-based tool for advanced configuration on Cisco routers
  - SDM can be used to configure the NAT, DNS, and DHCP services
- These services are relatively easy to configure using the command-line interface
Security Device Manager (continued)

- Using SDM to Configure NAT
  - Using SDM to configure static NAT
    - See Figure 9-9
  - Using SDM to configure dynamic NAT
    - See Figures 9-10 and 9-11
  - Using SDM to configure PAT
    - See Figure 9-12
Figure 9-9  Using SDM to configure static NAT
Figure 9-10  Using SDM to create an access list for dynamic NAT
Figure 9-11  Using SDM to create an access list for dynamic NAT
Figure 9-12  Using SDM to configure PAT
Security Device Manager (continued)

• Using SDM to configure DNS
  – See Figure 9-13
• Using SDM to configure DHCP
  – See Figure 9-14
Security Device Manager (continued)

Figure 9-13  Using SDM to point to DNS servers on the network
Figure 9-14  Using SDM to configure DHCP