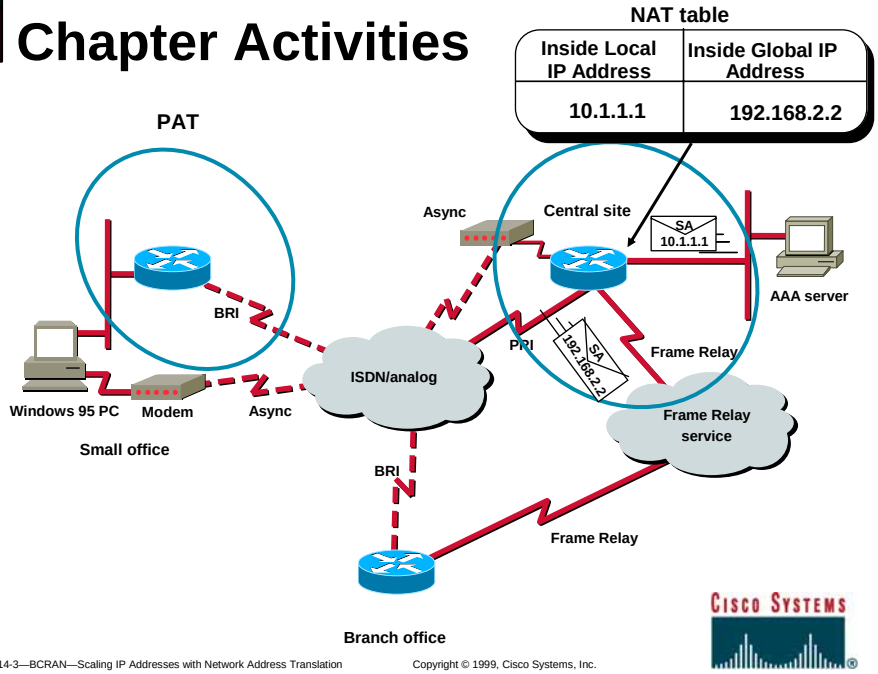
Chapter 11. NAT

Objectives

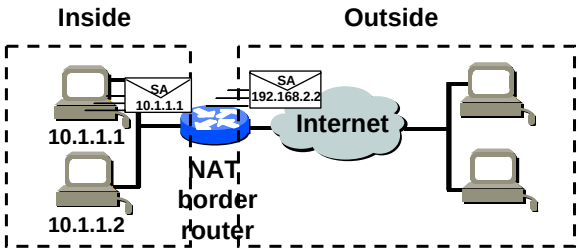
Upon completion of this chapter, you will be able to perform the following tasks:

- **Identify how NAT and PAT solve the limited IP address problem and describe how they operate**
- **Configure NAT and PAT**
- **Verify NAT and PAT**

Chapter Activities



Why Use NAT?



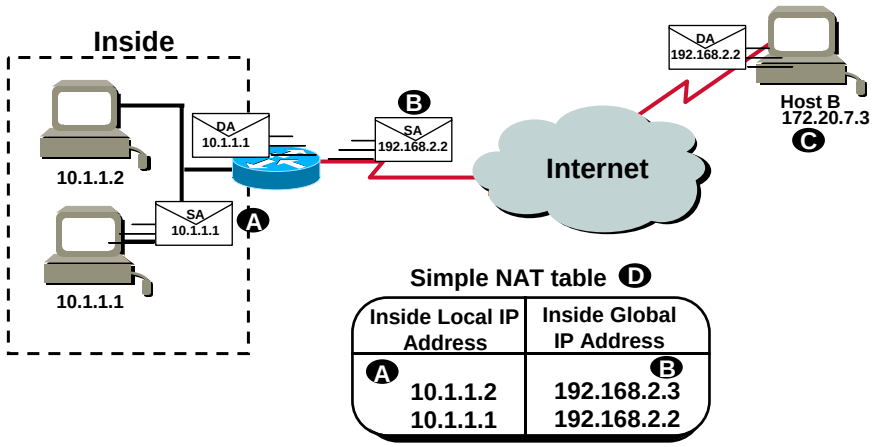
Use NAT if:

- You need to connect to the Internet and your hosts do not have globally unique IP addresses
- You change over to a new ISP that requires you to renumber your network
- Two intranets with duplicate addresses merge
- You want to support basic load sharing

NAT Implementation Considerations

Advantages	Disadvantages
Conserves legally registered addresses	Translation introduces switching path delays
Reduces address overlap occurrence	Loss of end-to-end IP traceability
Increases flexibility when connecting to Internet	Certain applications will not function with NAT enabled
Eliminates address renumbering as network changes	

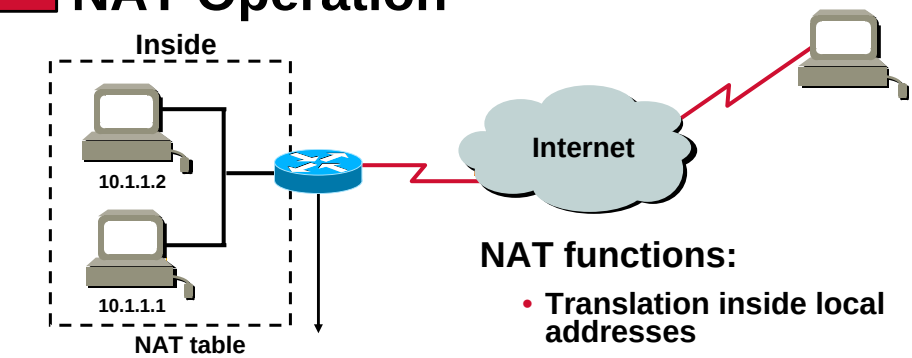
NAT Overview and Terminology



Simple NAT table D

Inside Local IP Address	Inside Global IP Address
A 10.1.1.2	B 192.168.2.3
10.1.1.1	192.168.2.2

NAT Operation



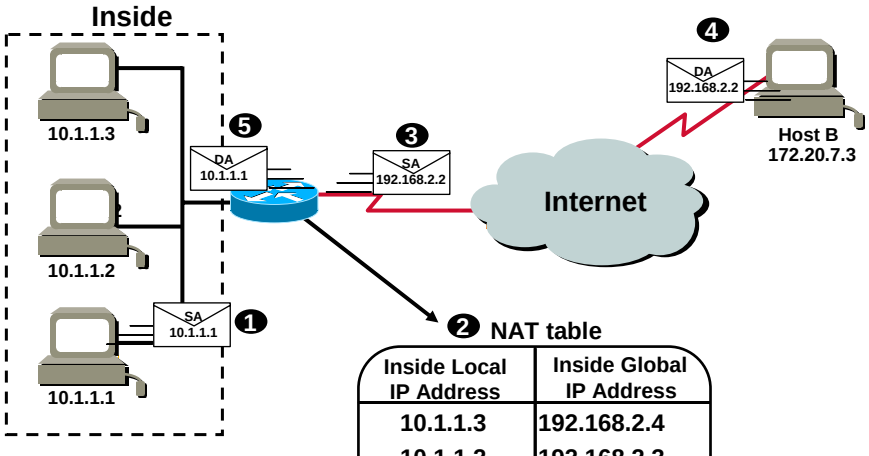
NAT table

Inside Local IP Address	Inside Global IP Address
10.1.1.1	192.168.2.2
10.1.1.2	192.168.2.3

NAT functions:

- Translation inside local addresses
- Overloading inside global addresses
- TCP load distribution
- Handling overlapping networks

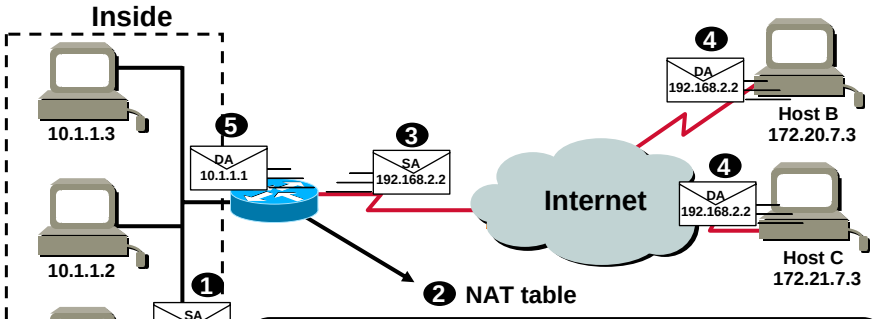
Translating Inside Local Addresses



2 NAT table

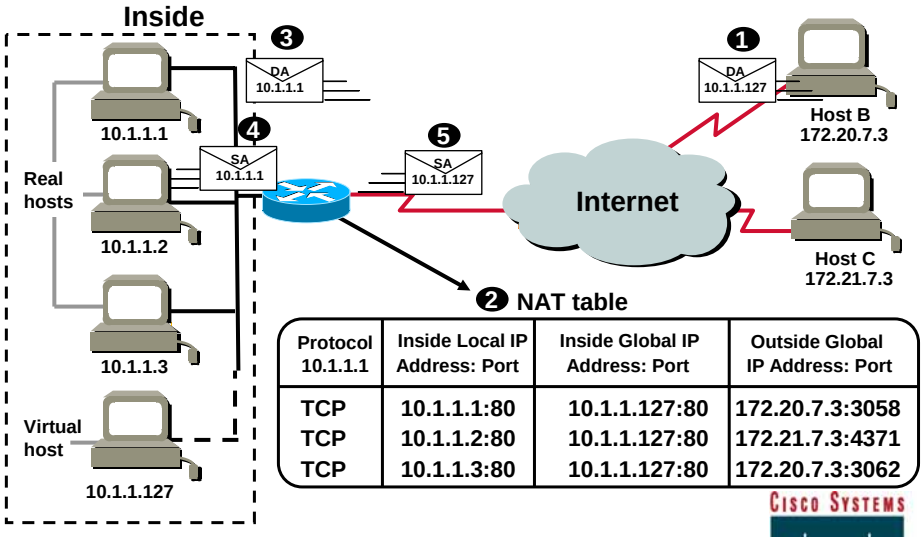
Inside Local IP Address	Inside Global IP Address
10.1.1.3	192.168.2.4
10.1.1.2	192.168.2.3
10.1.1.1	192.168.2.2

Overloading Inside Global Addresses



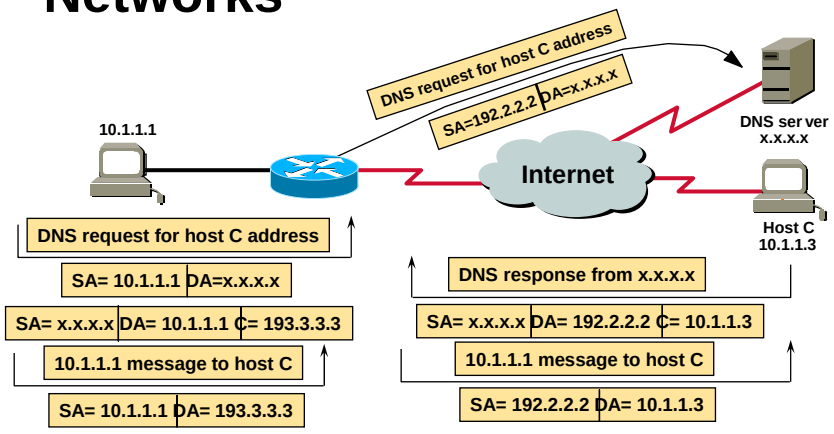
Protocol 10.1.1.1	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port
TCP	10.1.1.3:1723	192.168.2.2:1492	172.21.7.3:23
TCP	10.1.1.2:1723	192.168.2.2:1723	172.21.7.3:23
TCP	10.1.1.1:1024	192.168.2.2:1024	172.20.7.3:23

TCP Load Distribution



Protocol 10.1.1.1	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port
TCP	10.1.1.1:80	10.1.1.127:80	172.20.7.3:3058
TCP	10.1.1.2:80	10.1.1.127:80	172.21.7.3:4371
TCP	10.1.1.3:80	10.1.1.127:80	172.20.7.3:3062

Handling Overlapping Networks



NAT table

Inside Local IP Address	Inside Global IP Address	Outside Global IP Address	Outside Local IP Address
10.1.1.1	192.2.2.2	10.1.1.3	193.3.3.3

Static NAT Configuration Example

```
ip nat inside source static 10.1.1.1 192.168.2.2
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
```

This interface connected to the inside network.

This interface connected to the outside world.

Maps the inside local address to the inside global address.

Dynamic NAT Configuration

```
ip nat pool dyn-nat 192.168.2.1 192.168.2.254
    netmask 255.255.255.0
ip nat inside source list 1 pool dyn-nat
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
```

This interface connected to the inside network.

This interface connected to the outside world.

Translate between inside hosts addressed from 10.1.1.0/24 to the globally unique 192.168.2.0/24 network.

Configuring Inside Global Address Overloading

```
ip nat pool ovrld-nat 192.168.2.1 192.168.2.2
      netmask 255.255.255.0
ip nat inside source list 1 pool ovrld-nat overload
!
interface Ethernet0/0
 ip address 10.1.1.10 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

Configuring TCP Load Distribution

```
ip nat pool real-hosts 10.1.1.1 10.1.1.126 prefix-length 24
       type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial0
 ip address 192.168.1.129 255.255.255.224
 ip nat outside
!
interface ethernet0
 ip address 10.1.1.254 255.255.255.0
 ip nat inside
!
access-list 2 permit 10.1.1.127
```


Configuring NAT to Translate Overlapping Addresses

```
ip nat pool net-2 192.2.2.1 192.2.2.254 prefix-length 24
ip nat pool net-10 10.0.1.1 10.0.1.254 prefix-length 24
ip nat outside source list 1 pool net-2
ip nat inside source list 1 pool net-10
!
interface Serial0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface Ethernet0
 ip address 10.1.1.254 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.1.1.0 0.0.0.255
```


Verifying NAT

Basic IP address translation

```
Router#show ip nat trans
Pro Inside global  Inside local  Outside local  Outside global
---192.2.2.1       10.1.1.1      ---            ---
---192.2.2.2       10.1.1.2      ---            ---
```

IP address translation with overloading

```
Router#sh ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.2.1:11003  10.1.1.1:11003     172.16.2.2:23      172.16.2.2:23
tcp 192.168.2.1:1067   10.1.1.1:1067      172.16.2.3:23      172.16.2.3:23
```

Unique TCP port numbers are used to distinguish between hosts.

A translation for a Telnet is still active.
Two different inside hosts appear on the outside with a single IP address.

Troubleshooting NAT

```
Router#debug ip nat
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [0]
NAT: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [0]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [1]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [2]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [3]
NAT*: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [1]
NAT: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [1]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [4]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [5]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [6]
NAT*: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [2]
```

An example address translation inside-to-outside.

A reply to the packet sent.

An example TCP conversation, inside-to-outside.

*** Indicates translation was in the fast path.**

Clearing NAT Translation Entries

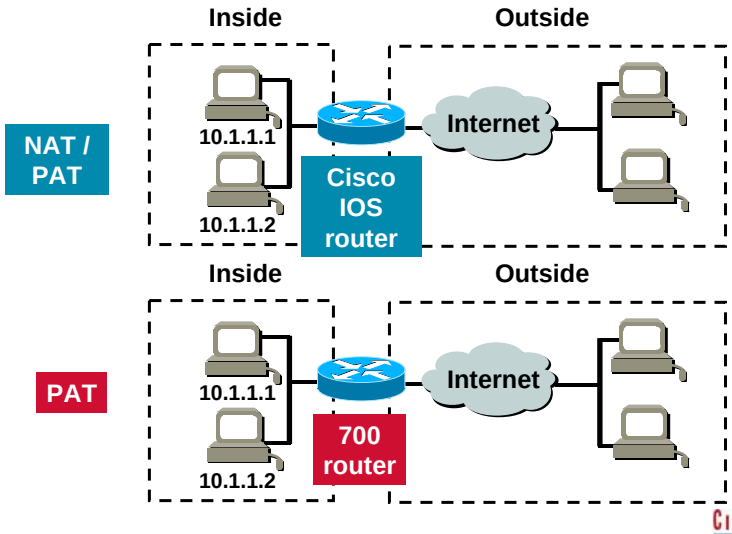
```
Router#sh ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.2.1:11003  10.1.1.1:11003     172.16.2.2:23      172.16.2.2:23
tcp 192.168.2.1:1067   10.1.1.1:1067      172.16.2.3:23      172.16.2.3:23
router#clear ip nat trans *
router#
router#show ip nat trans
```

All entries are cleared.

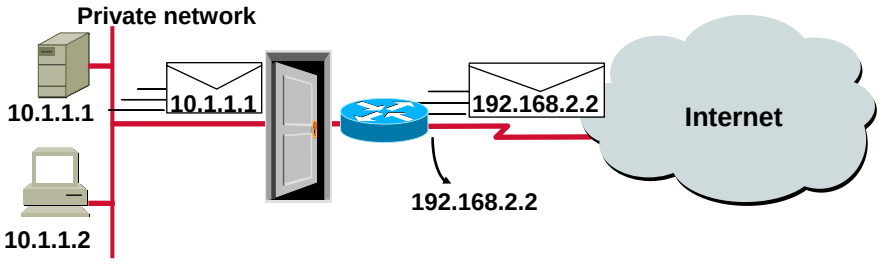
```
router#show ip nat transPro Inside global              Inside local    Outside
local               Outside global
udp 192.168.2.2:1220 10.1.1.2:1120   171.69.2.132:53    171.69.2.132:53
tcp 192.168.2.1:1100310.1.1.1:11003 172.16.2.2:23       172.16.2.2:23
tcp 192.168.2.1:1067 10.1.1.1:1067  172.16.2.3:23       172.16.2.3:23
router#clear ip nat trans udp inside 192.168.2.2 10.1.1.2 1220
171.69.2.132 53 171.69.2.132 53
router#show ip nat trans
Pro Inside global     Inside local    Outside local      Outside global
tcp 192.168.2.1:11003  10.1.1.1:11003     172.16.2.2:23      172.16.2.2:23
tcp 192.168.2.1:1067   10.1.1.1:1067      172.16.2.3:23      172.16.2.3:23
```

192.168.2.2 is cleared.

PAT Overview

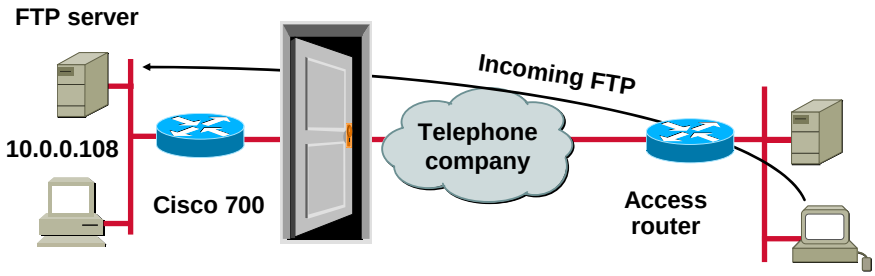


PAT Overview (cont.)



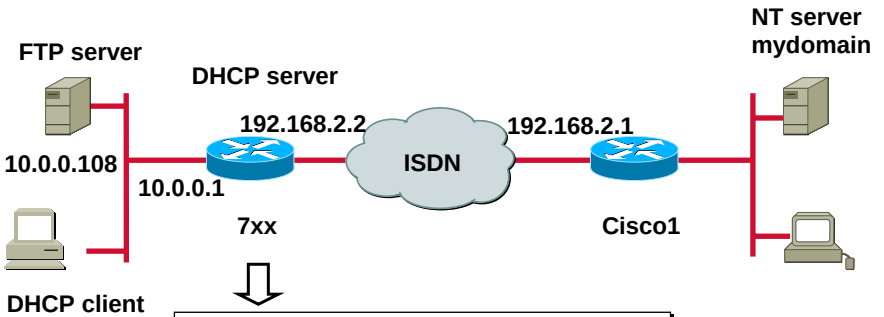
- Enables hosts on private networks to communicate over public networks
- Conserves IP addresses

PAT Porthandler Operation



- Only packets destined for the server (by type) are allowed through

Configuring PAT



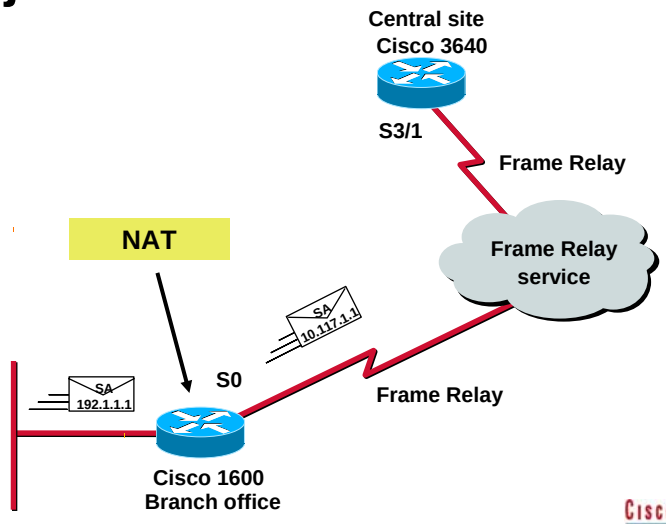

```
>SEt SYStem 7xx
7XX>SEt USer Cisco1
7xx:Cisco1>SEt IP PAT ON
7xx:Cisco1>cd
7xx>SEt IP PAT POrt FTP 10.0.0.108
```


Monitoring PAT

```
7xx:Cisco1>show ip pat
Dropped - icmp 0, udp 0, tcp 0, map 0, frag 0
Timeout - udp 5 minutes, tcp 30 minutes
Port handlers [no default]:

Port     Handler         Service
-------------------------------------
21       10.0.0.108      FTP
23       Router          TELNET
67       Router          DHCP Server
68       Router          DHCP Client
69       Router          TFTP
80       Router          HTTP
161      Router          SNMP
162      Router          SNMP-TRAP
520      Router          RIP
```

Laboratory Exercise: Visual Objective



Summary

After completing this chapter, you should be able to perform the following tasks:

- **Identify how NAT and PAT solve the limited IP address problem and describe how they operate**
- **Configure NAT and PAT**
- **Verify NAT and PAT**

Review Questions

- **What is the difference between a simple translation entry and an extended translation entry? State how each is used.**
- **Give one or more examples when NAT could be used.**
- **Your networks are addressed using 10.1.1.0/24 subnets. Your ISP provides you a globally unique address of 192.1.1.0/24. What commands do you use to translate from 10.1.1.0/24 to 192.1.1.0/24?**
- **When viewing the output of the *show ip nat translations* command, how can you determine when an inside global address is being used for overloading inside global addresses?**

Blank Page For IG pagination