Chapter 5: Network Address Translation for IPv4

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5

5.1 NAT Operation

5.2 Configuring NAT

5.3 Troubleshooting NAT

5.4 Summary

Chapter 5: Objectives

- Describe NAT characteristics.
- Describe the benefits and drawbacks of NAT.
- Configure static NAT using the CLI.
- Configure dynamic NAT using the CLI.
- Configure PAT using the CLI.
- Configure port forwarding using the CLI.
- Configure NAT64.
- Use **`show`** commands to verify NAT operation.

5.1 NAT Operation

Cisco | Networking Academy®
Mind Wide Open™

IPv4 Private Address Space

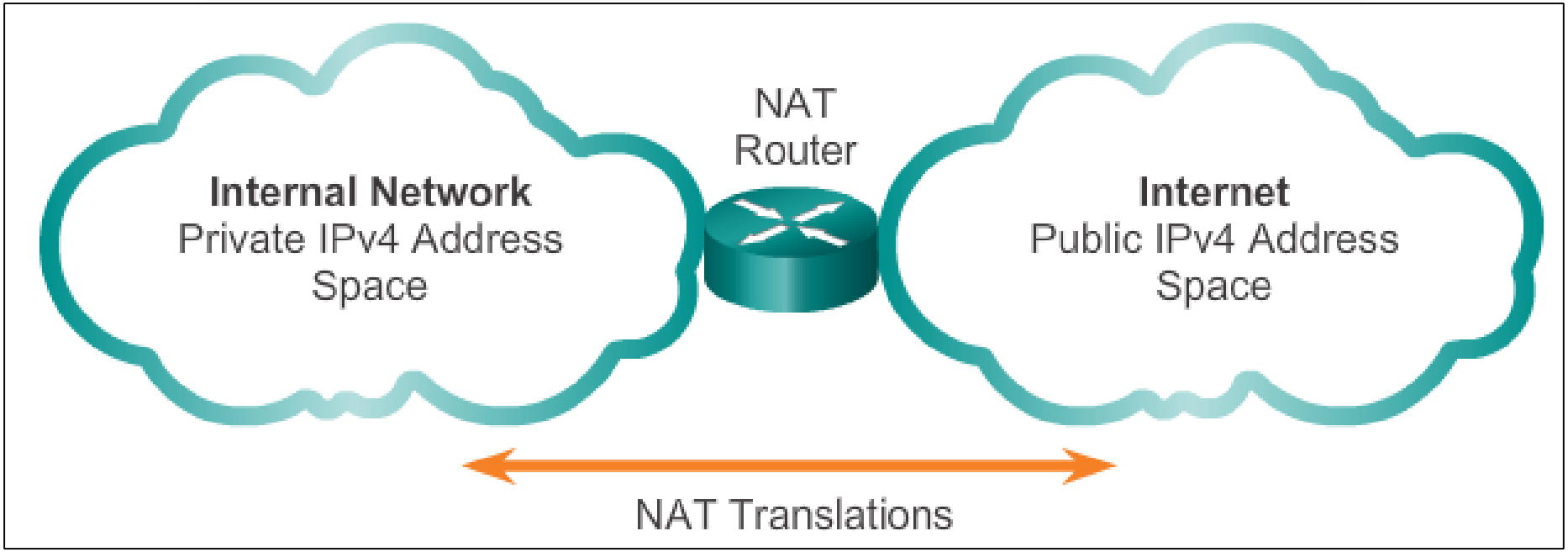
- IPv4 address space is not big enough to uniquely address all the devices that must be connected to the Internet.
- Network private addresses are described in RFC 1918 and are to designed to be used within an organization or site only.
- Private addresses are not routed by Internet routers while public addresses are.
- Private addresses can alleviate IPv4 scarcity, but because they aren't routed by Internet devices, they first need to be translated.
- NAT is process used to perform such translation.

NAT Characteristics

IPv4 Private Address Space

Private Internet addresses are defined in RFC 1918:

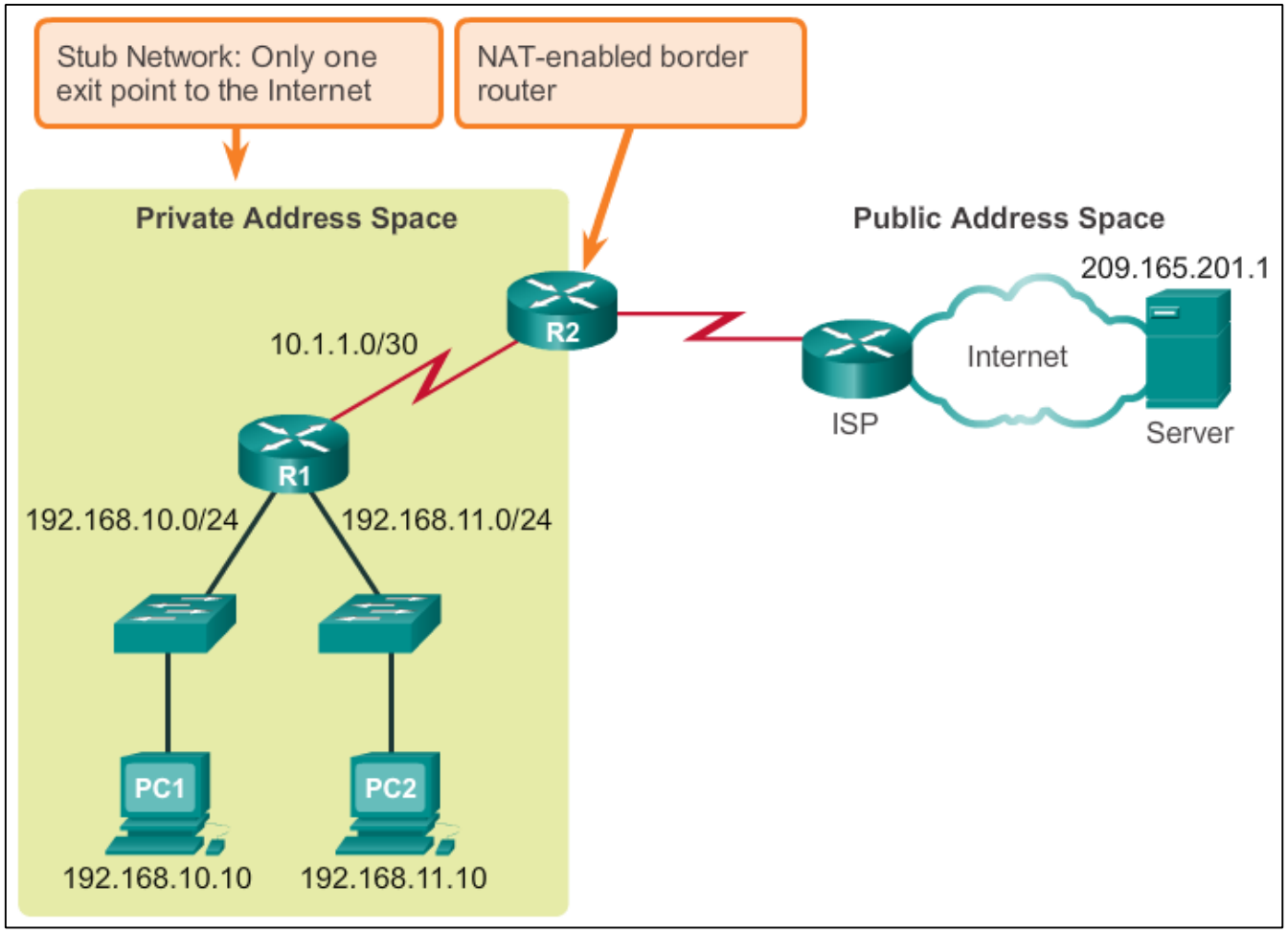
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16



What is NAT?

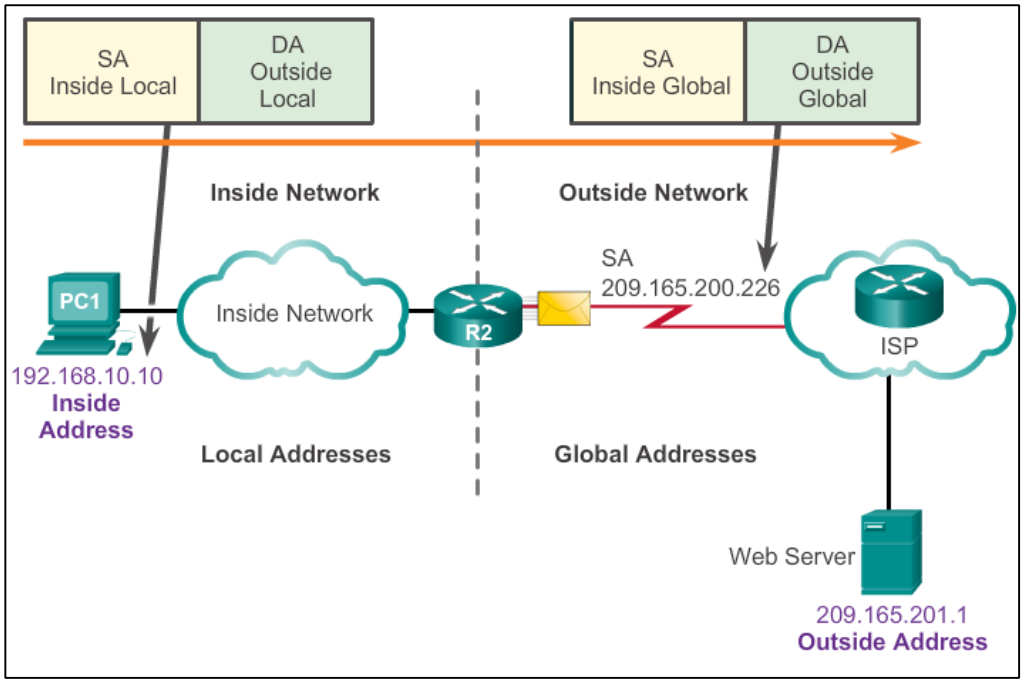
- NAT is a process used to translate network addresses.
- NAT's primary use is to conserve public IPv4 addresses.
- NAT is usually implemented at border network devices, such as firewalls or routers.
- NAT allows the networks to use private addresses internally, only translating to public addresses when needed.
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address.

What is NAT? (cont.)



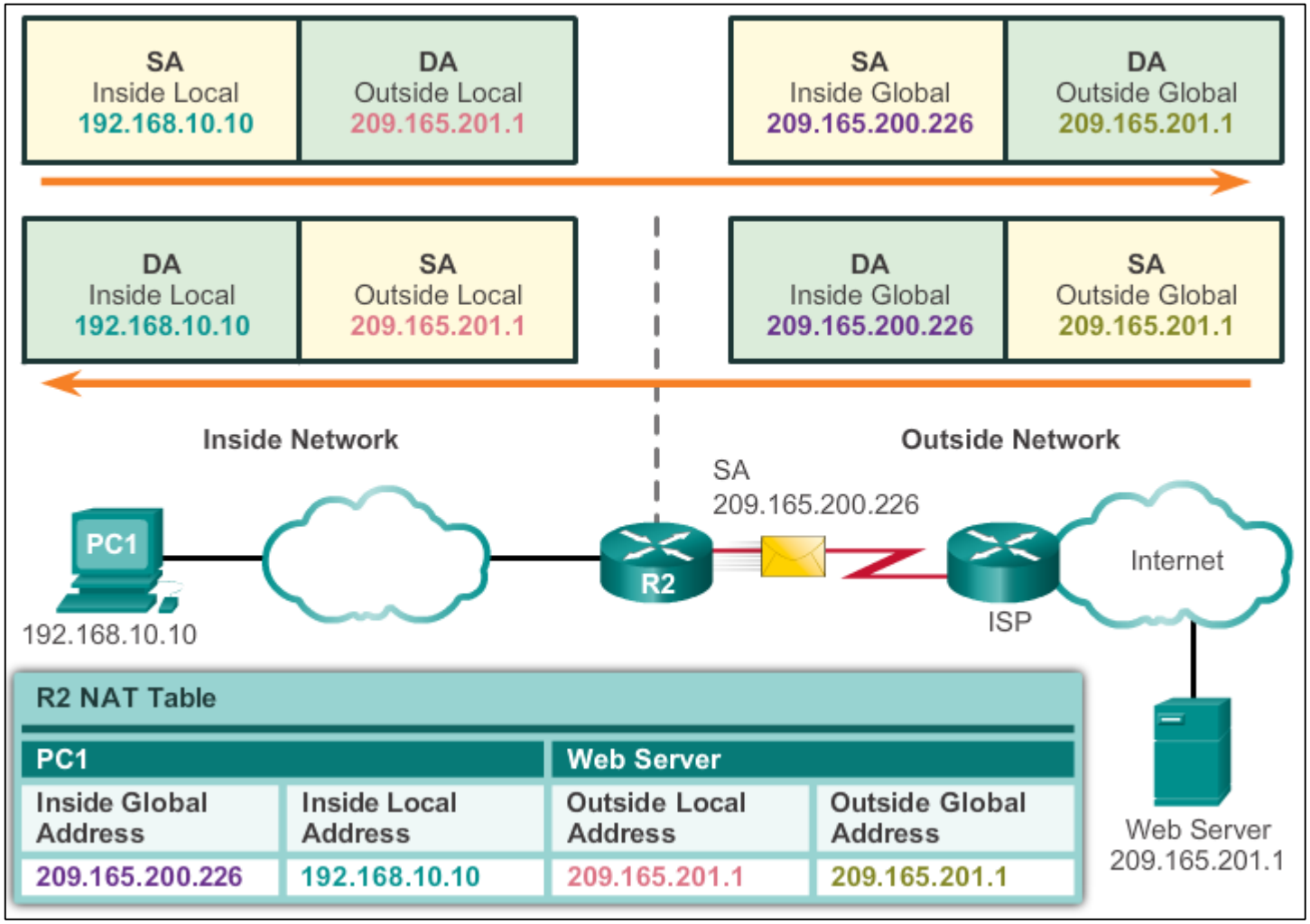
NAT Terminology

- Inside network is the set of devices using private addresses
- Outside network refers to all other networks
- NAT includes four types of addresses:
  - Inside local address
  - Inside global address
  - Outside local address
  - Outside global address



NAT Characteristics

NAT Terminology (cont.)

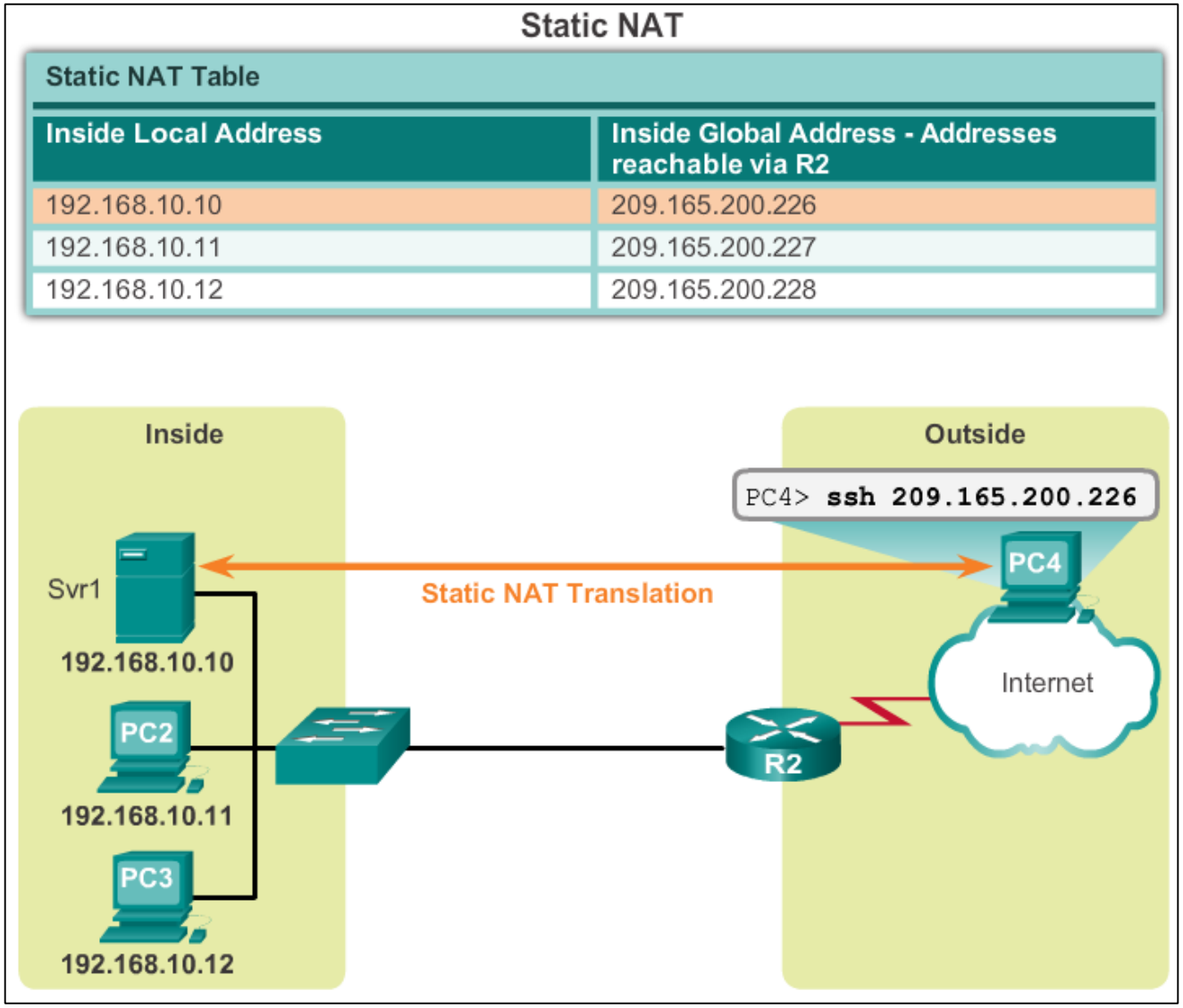


Types of NAT

Static 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 when servers hosted in the inside network must be accessible from the outside network.
- A network administrator can SSH to a server in the inside network by pointing the SSH client to the proper inside global address.

Static NAT (cont.)

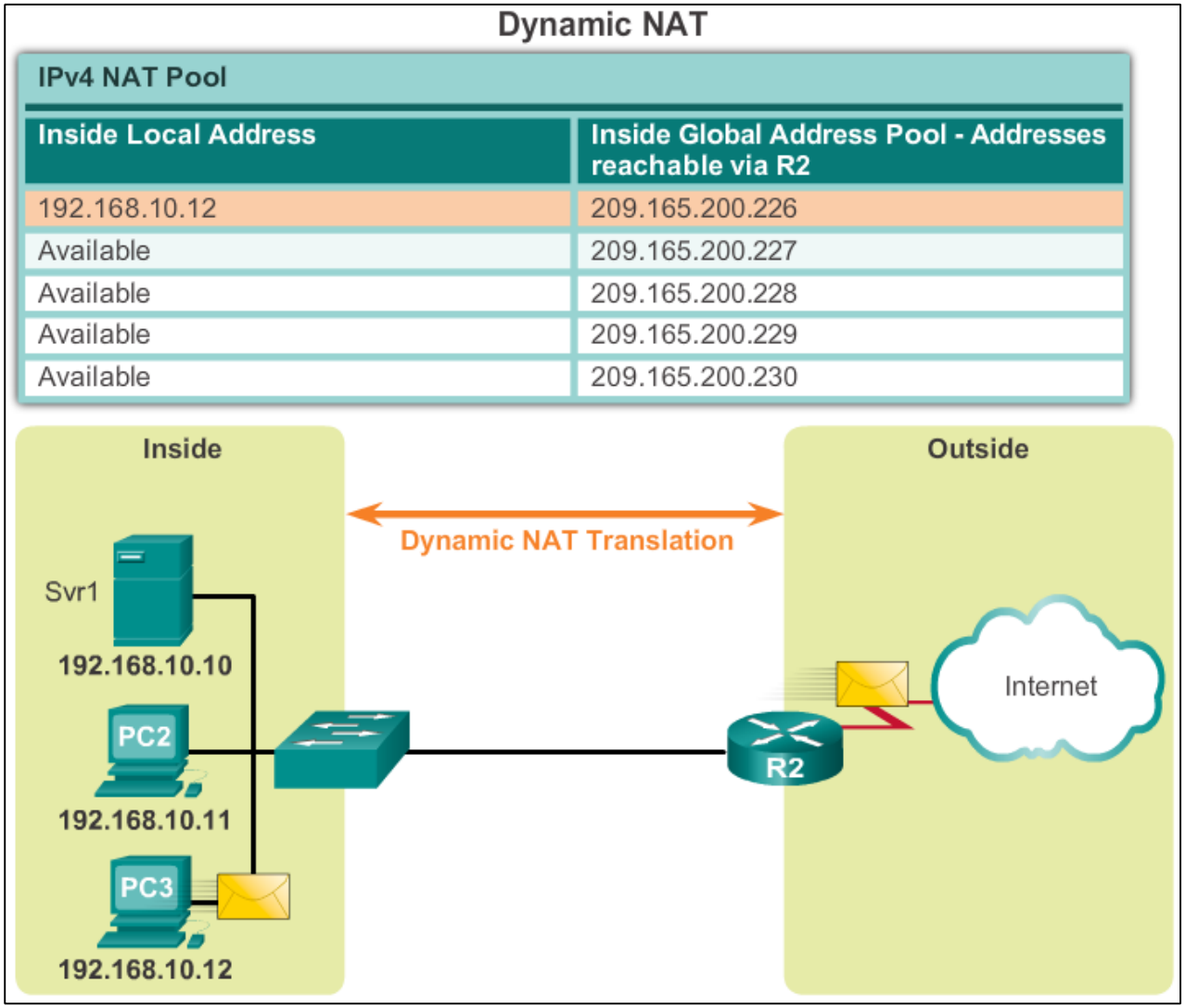


Types of NAT

Dynamic NAT

- 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.
- Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

Dynamic NAT (cont.)



Port Address Translation

- Port Address Translation (PAT) maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- PAT uses the pair source port and source IP address to keep track of what traffic belongs to what internal client.
- PAT is also known as NAT overload.
- By also using the port number, PAT forwards the response packets to the correct internal device.
- The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session.

Comparing NAT and PAT

- NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses.
- PAT modifies both the address and the port number.
- NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address provided by the host on the public network.
- With PAT, there is generally only one or a very few publicly exposed IPv4 addresses.
- PAT is able to translate protocols that do not use port numbers, such as ICMP; each one of these protocols is supported differently by PAT.

Benefits of NAT

- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes
- Provides network security

Disadvantages of NAT

- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted

5.2 Configuring NAT

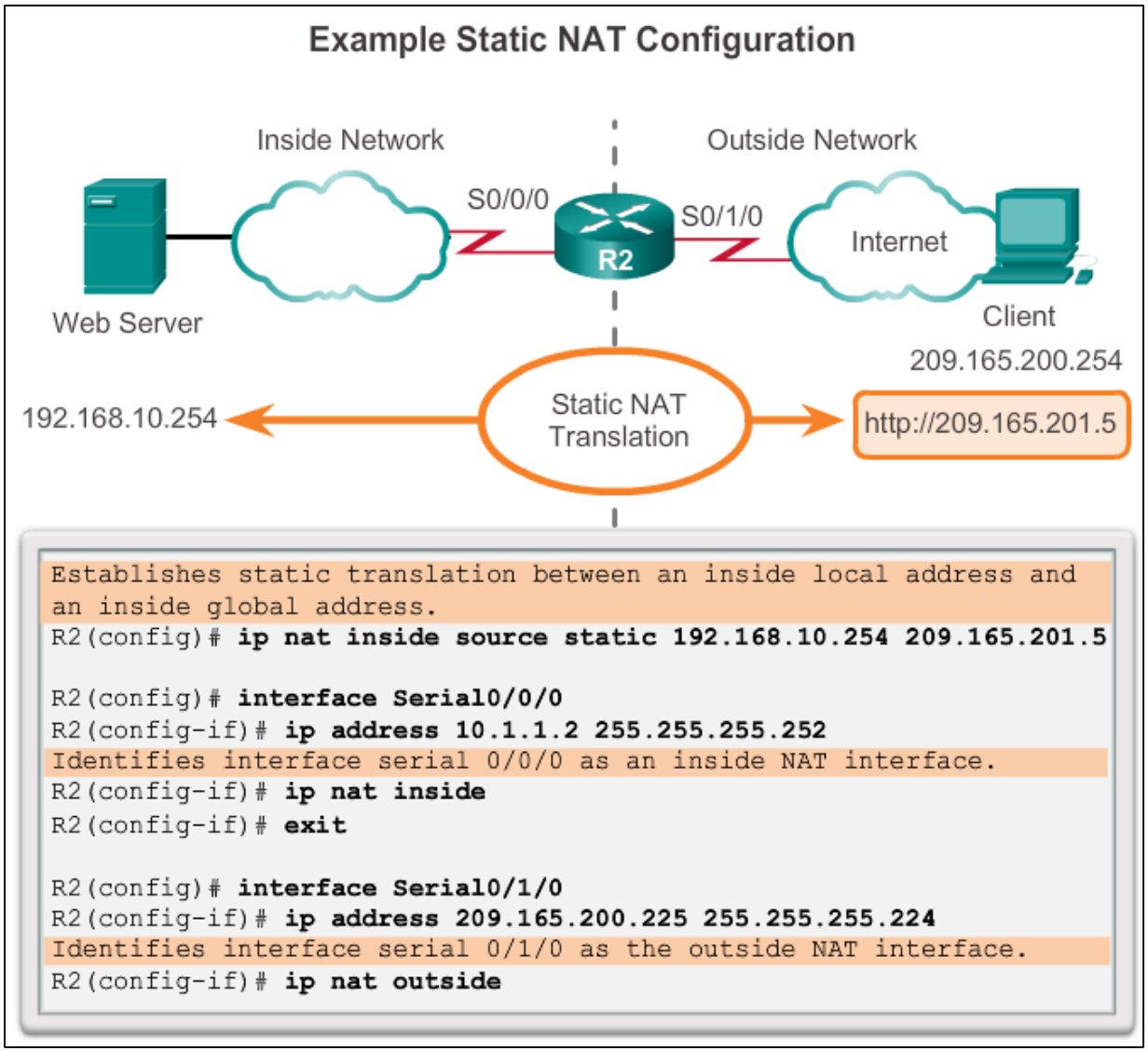
Cisco | Networking Academy®
Mind Wide Open™

Configuring Static NAT

There are two basic tasks to perform when configuring static NAT translations:

- Create the mapping between the inside local and outside local addresses.
- Define which interfaces belong to the inside network and which belong to the outside network.

Configuring Static NAT

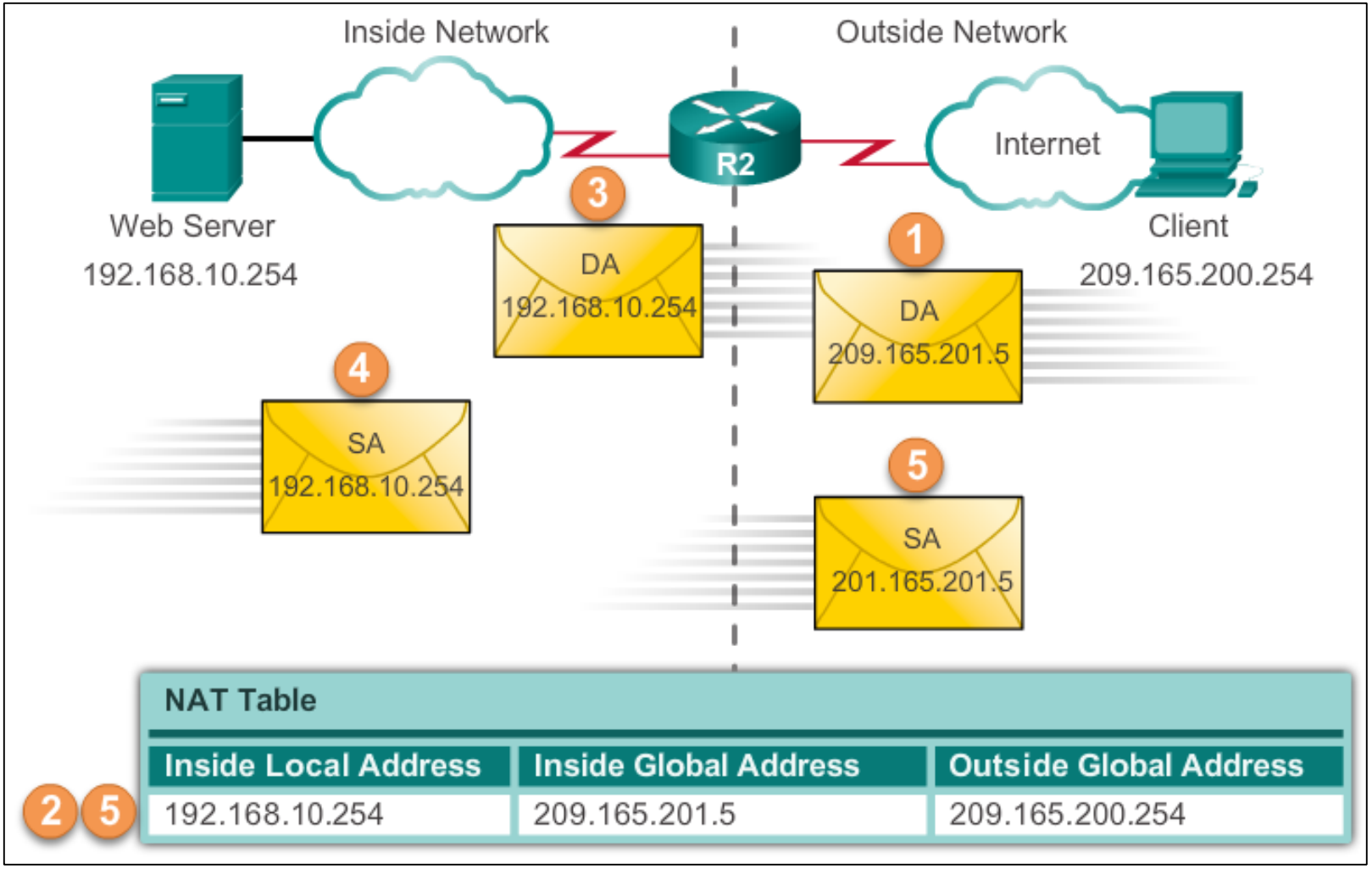



```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Analyzing Static NAT



Verifying Static NAT

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

Configuring Static NAT

Verifying Static NAT (cont.)

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

Dynamic NAT Operation

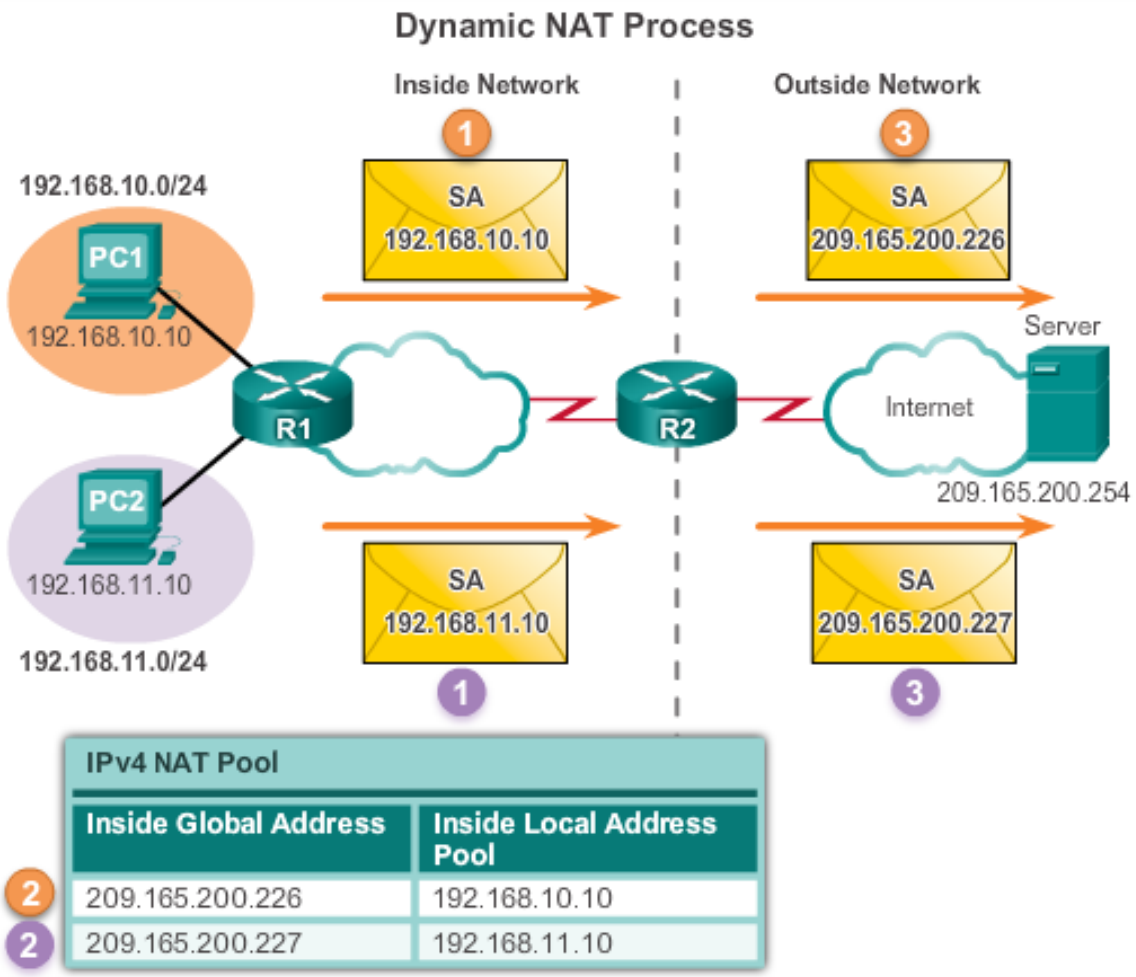
- The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come, first-served basis.
- With dynamic NAT, a single inside address is translated to a single outside address.
- The pool must be large enough to accommodate all inside devices.
- A device is unable to communicate to any external networks if no addresses are available in the pool.

Configuring Dynamic NAT

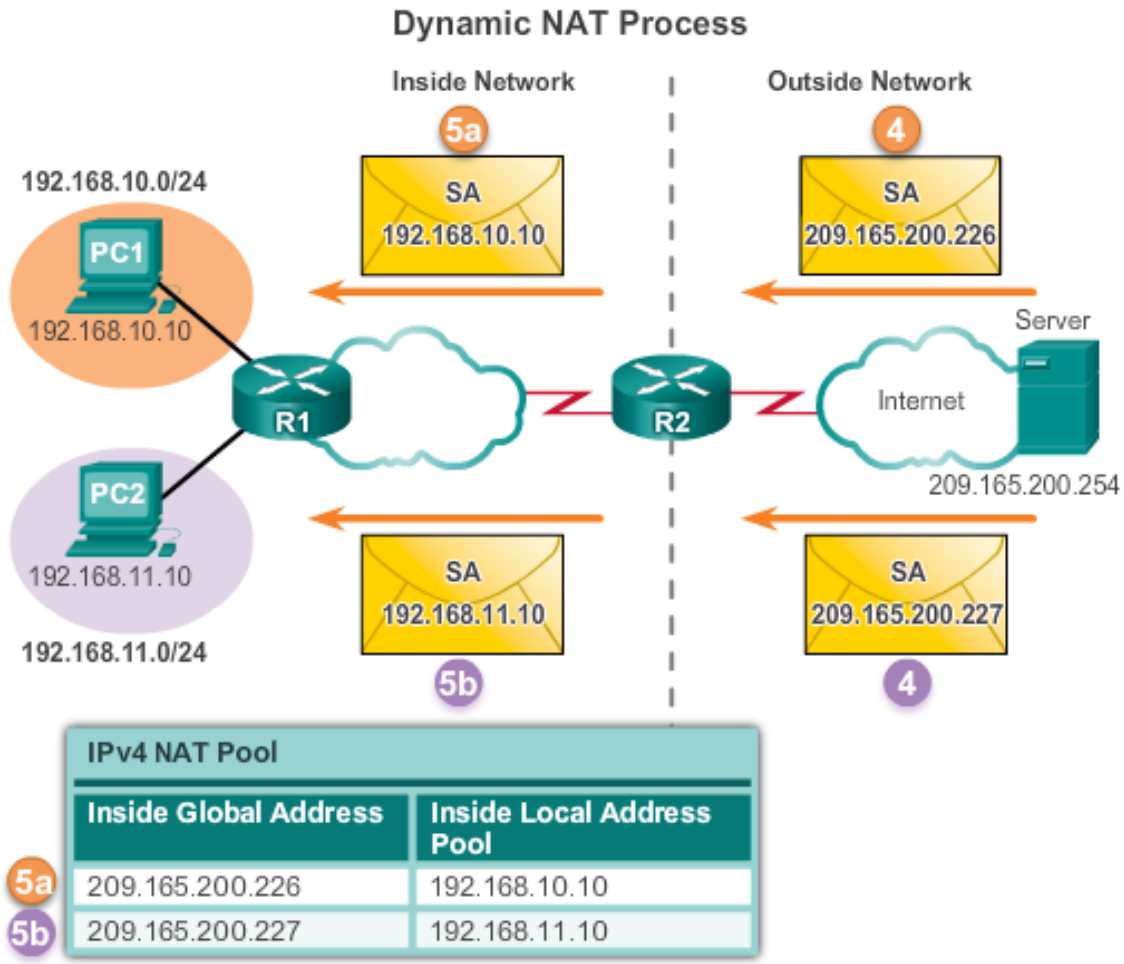
Dynamic NAT Configuration Steps	
Step 1	Define a pool of global addresses to be used for translation. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
Step 2	Configure a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source*[*source-wildcard*]
Step 3	Establish dynamic source translation, specifying the access list and pool defined in prior steps. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 5	Identify the outside interface. **interface** *type number* **ip nat outside**

Configuring Dynamic NAT

Analyzing Dynamic NAT



Analyzing Dynamic NAT



Configuring Dynamic NAT

Verifying Dynamic NAT

Verifying Dynamic NAT with show ip nat translations

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

Configuring Dynamic NAT

Verifying Dynamic NAT

Verifying Dynamic NAT with show ip nat statistics

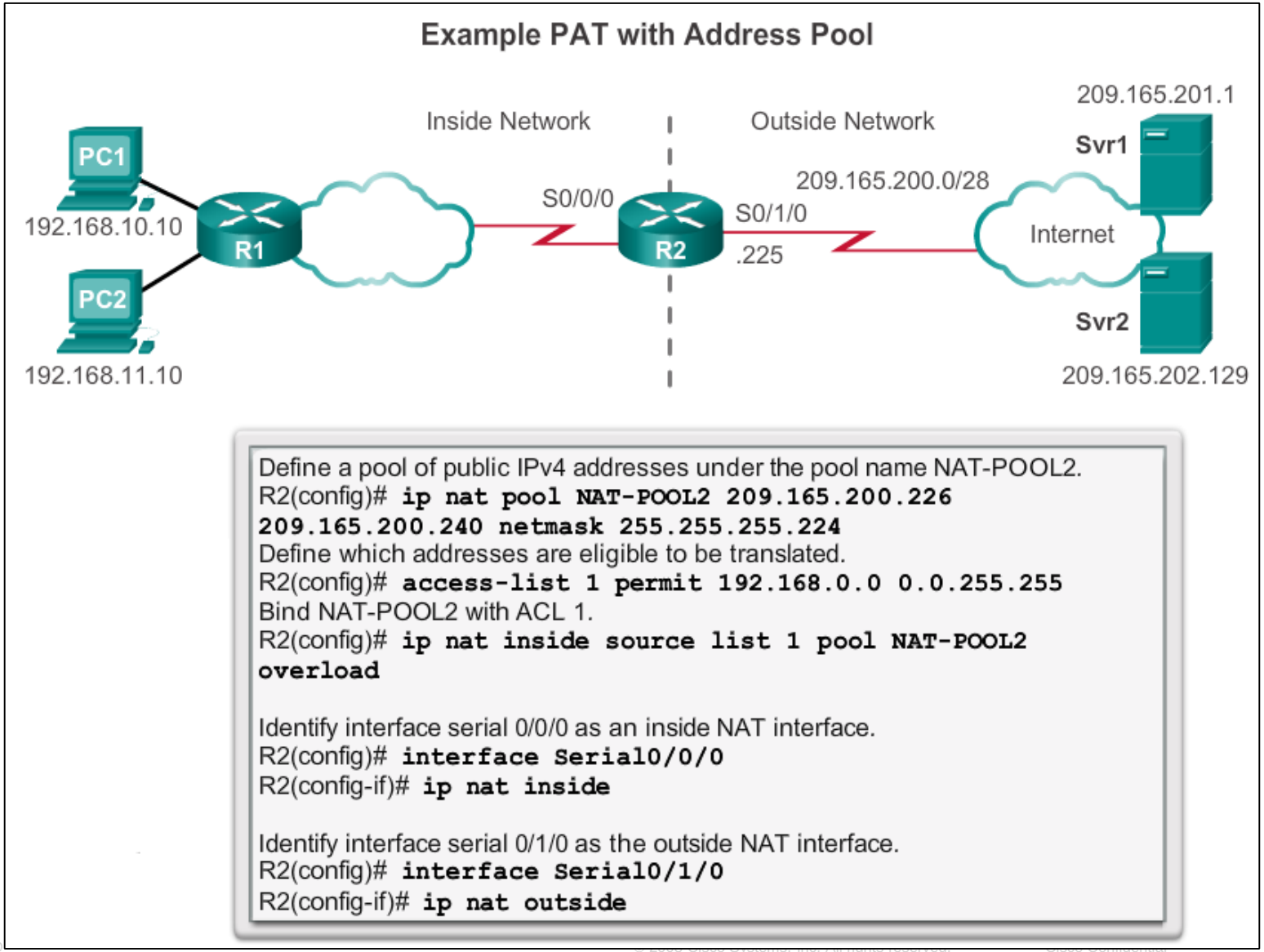
```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Configuring PAT: Address Pool



Define a pool of public IPv4 addresses under the pool name NAT-POOL2.
R2(config)# **ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224**
Define which addresses are eligible to be translated.
R2(config)# **access-list 1 permit 192.168.0.0 0.0.255.255**
Bind NAT-POOL2 with ACL 1.
R2(config)# **ip nat inside source list 1 pool NAT-POOL2 overload**

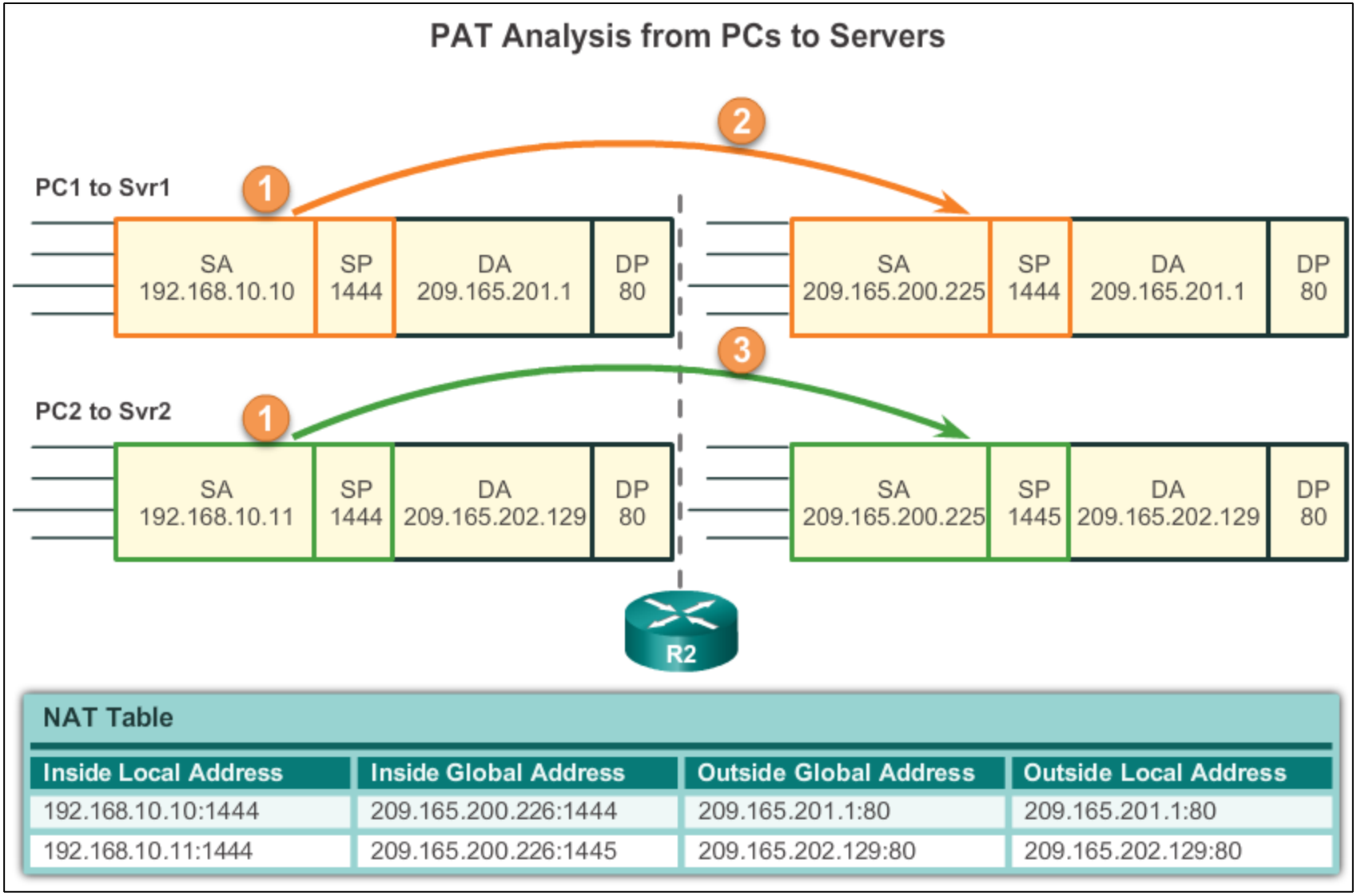
Identify interface serial 0/0/0 as an inside NAT interface.
R2(config)# **interface Serial0/0/0**
R2(config-if)# **ip nat inside**

Identify interface serial 0/1/0 as the outside NAT interface.
R2(config)# **interface Serial0/1/0**
R2(config-if)# **ip nat outside**

Configuring PAT: Single Address

Step 1	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 2	Establish dynamic source translation, specifying the ACL, exit interface and overload options. **ip nat inside source list** *access-list-number* **interface** *type number* **overload**
Step 3	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 4	Identify the outside interface. **interface** *type number* **ip nat outside**

Analyzing PAT

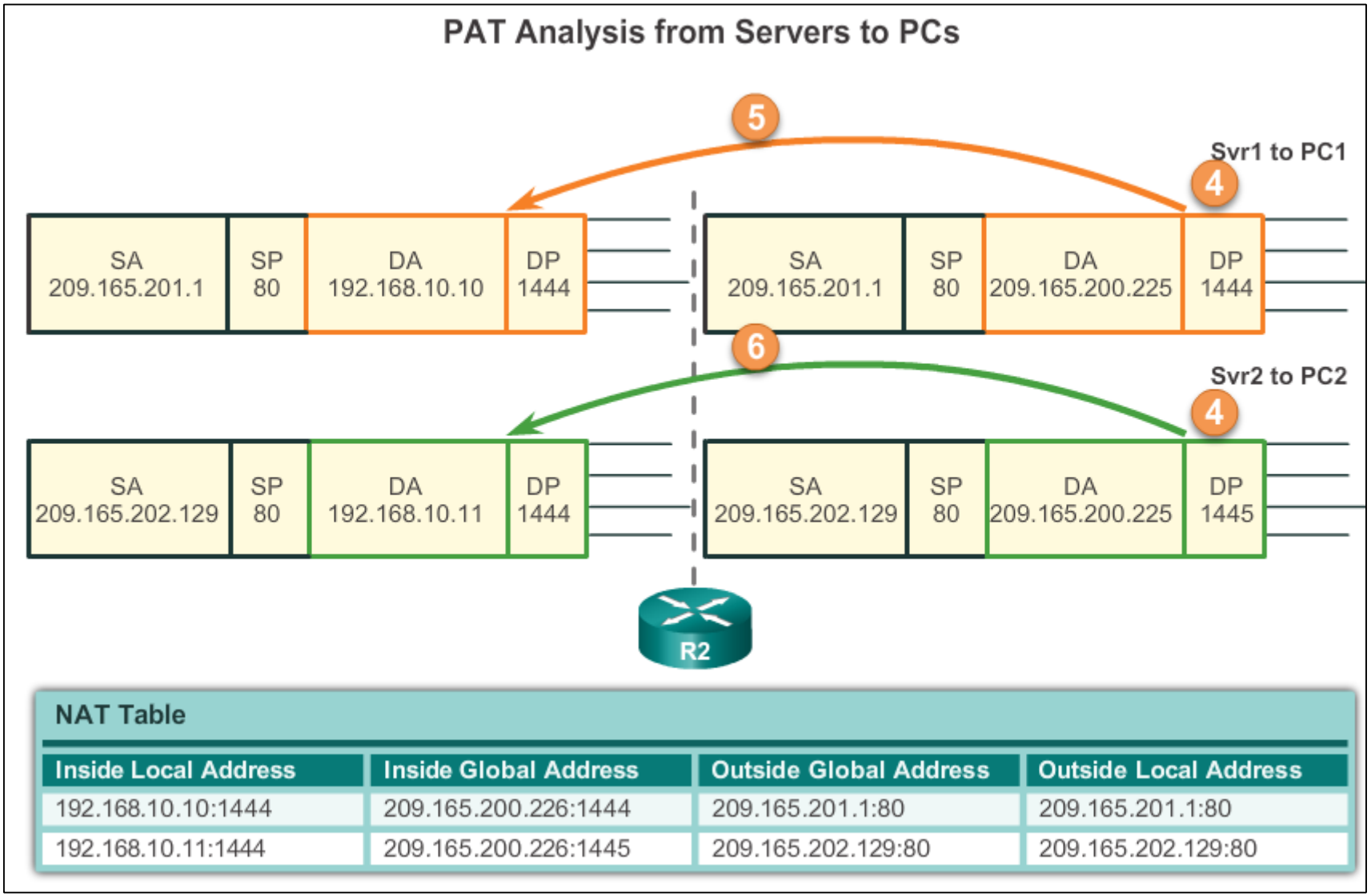


NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Configuring PAT

Analyzing PAT



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Configuring PAT

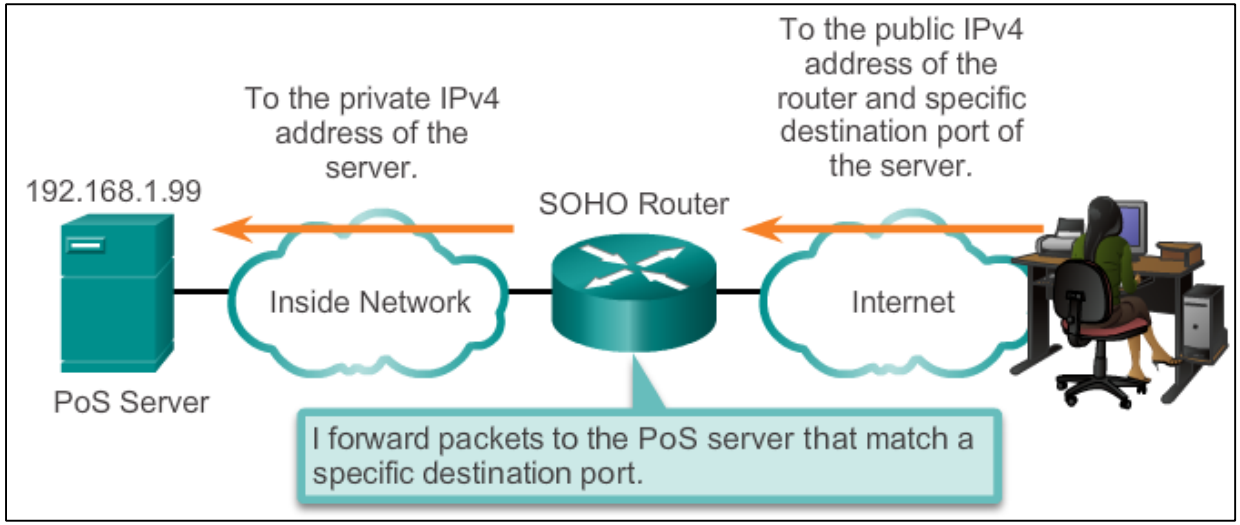
Verifying PAT Translations

Verifying PAT Translations

```
R2# show ip nat translations
Pro  Inside global          Inside local       Outside local      Outside global
tcp  209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80   209.165.201.1:80
tcp  209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80  209.165.202.129:80
R2#
```

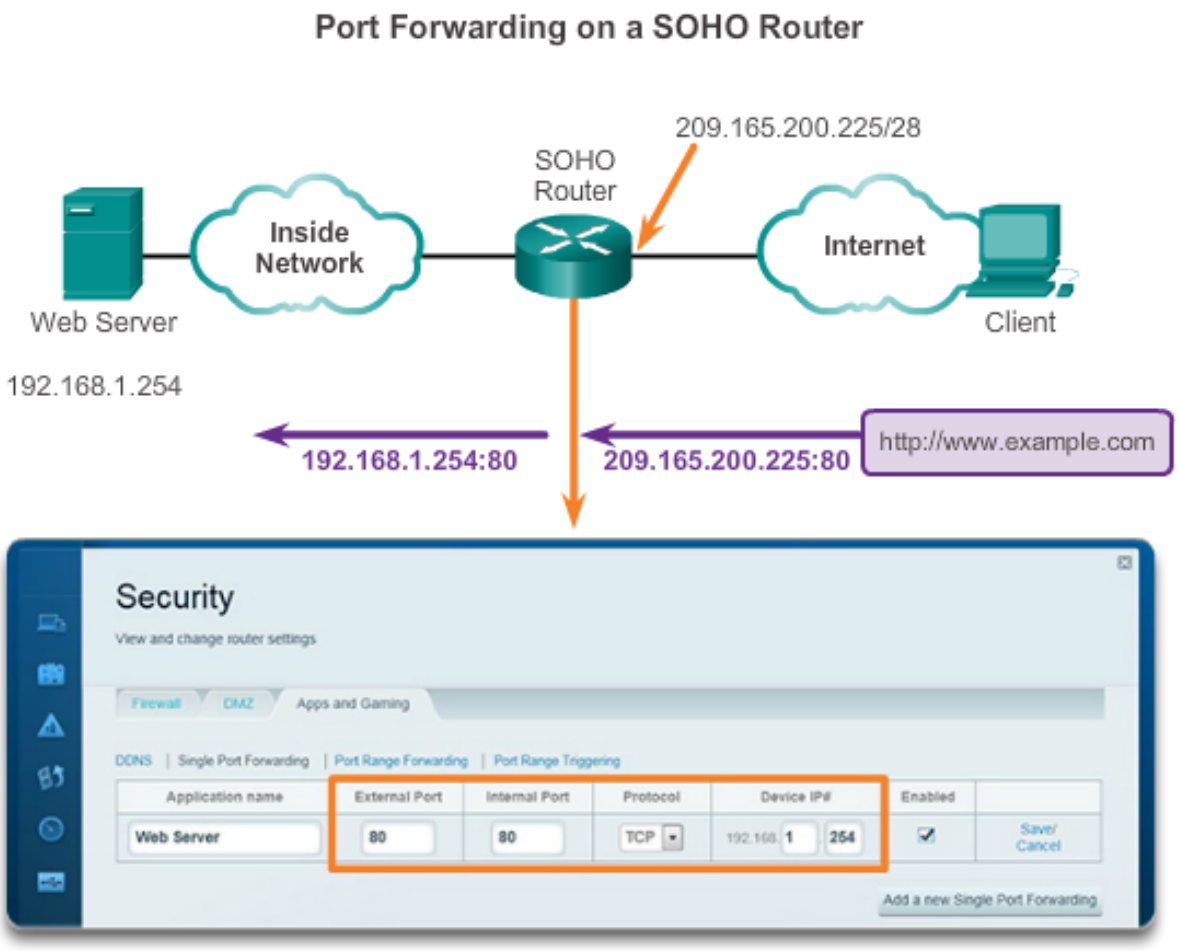
Port Forwarding

- Port forwarding is the act of forwarding a network port from one network node to another.
- A packet sent to the public IP address and port of a router can be forwarded to a private IP address and port in inside network.
- Port forwarding is helpful in situations where servers have private addresses, not reachable from the outside networks.



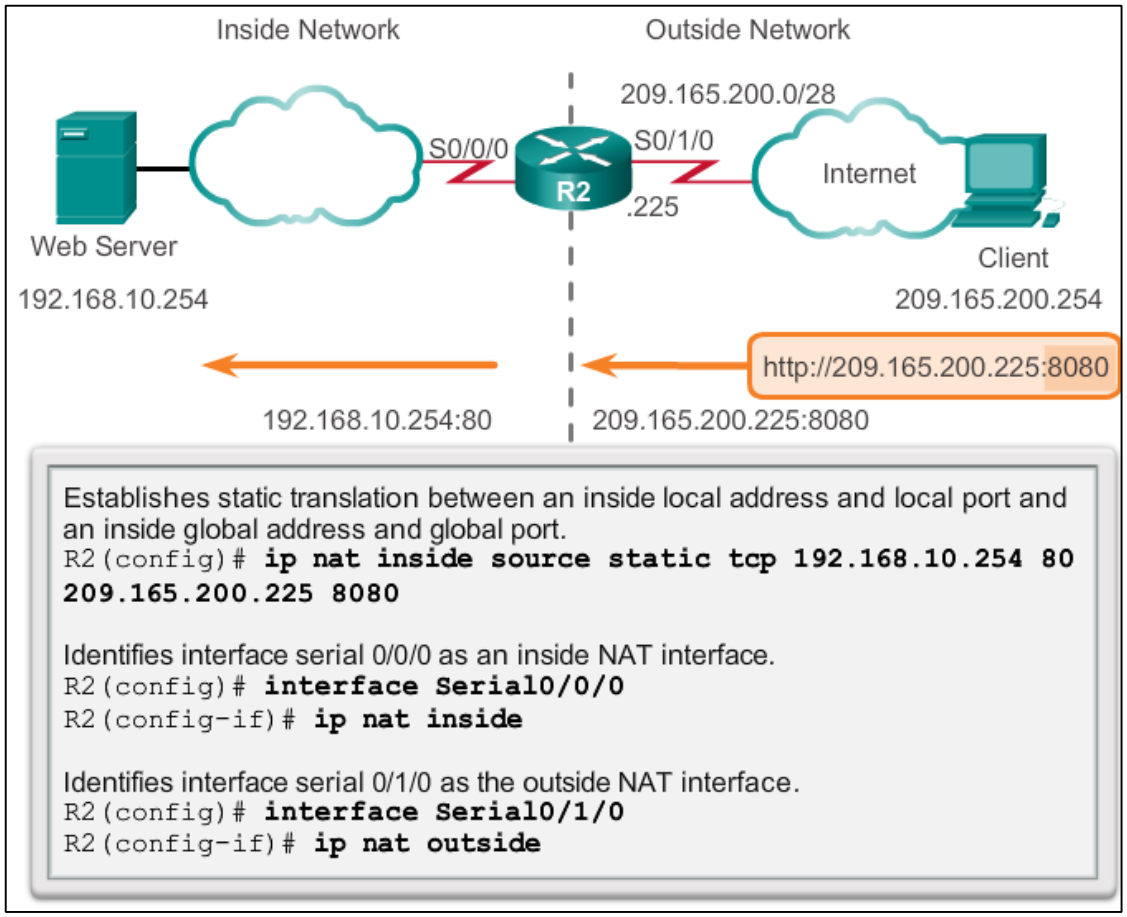
Port Forwarding

SOHO Example



Configuring Port Forwarding with IOS

In IOS, Port forwarding is essentially a static NAT translation with a specified TCP or UDP port number.



Establishes static translation between an inside local address and local port and an inside global address and global port.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as the outside NAT interface.

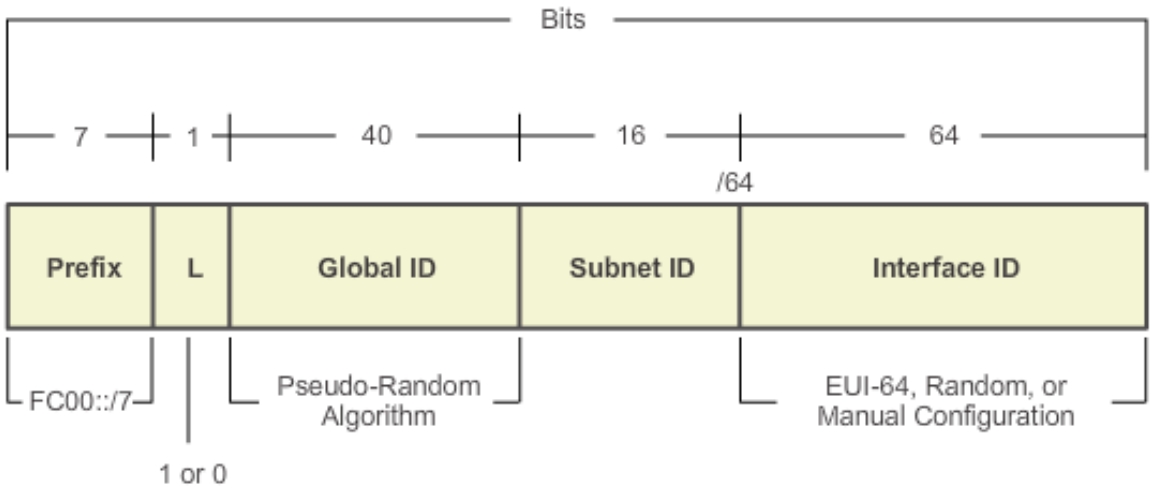
```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

NAT for IPv6?

- NAT is a workaround for IPv4 address scarcity.
- IPv6 with a 128-bit address provides 340 undecillion addresses.
- Address space is not an issue for IPv6.
- IPv6 makes IPv4 public-private NAT unnecessary by design; however, IPv6 does implement a form of private addresses, and it is implemented differently than they are for IPv4.

IPv6 Unique Local Addresses

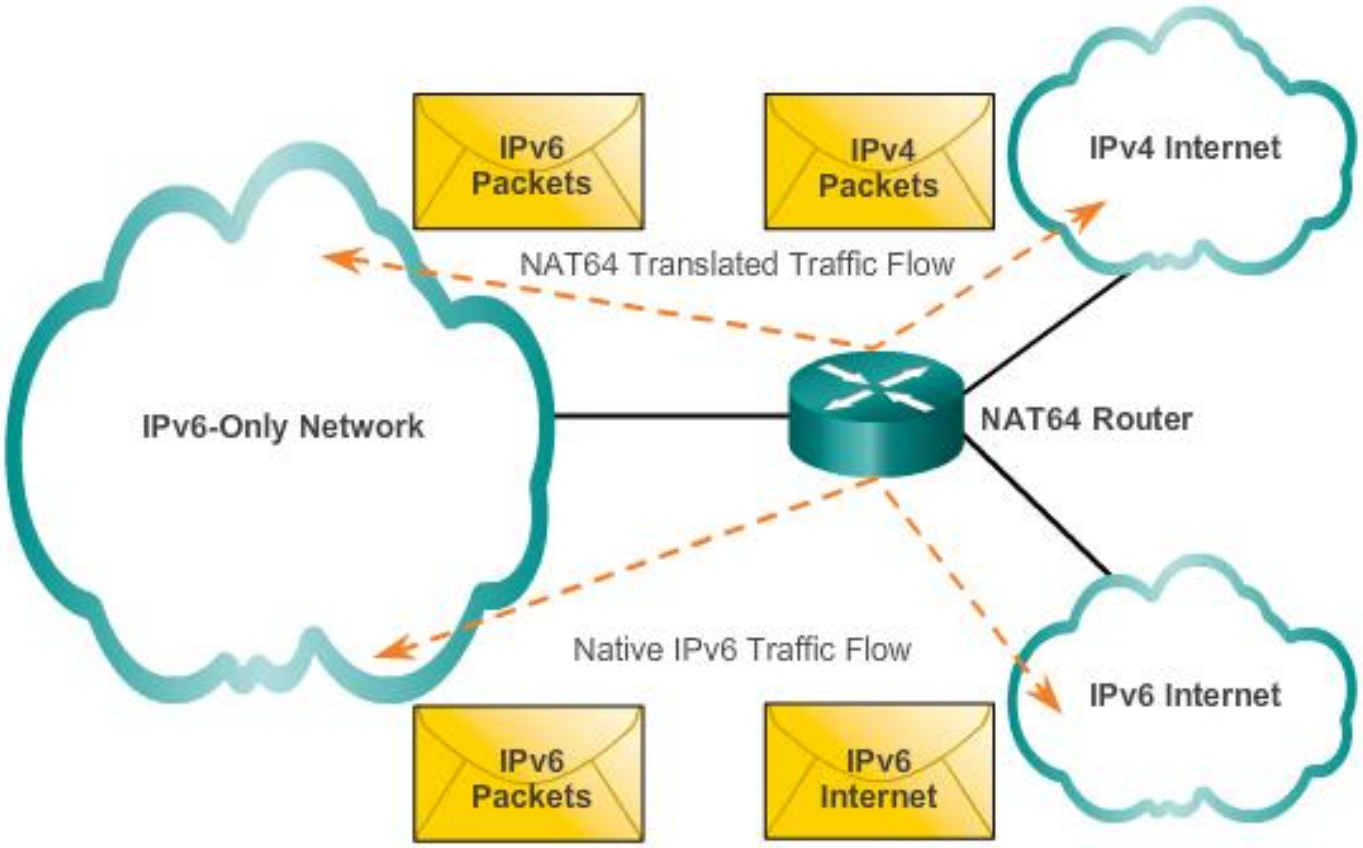
- IPv6 unique local addresses (ULAs) are designed to allow IPv6 communications within a local site.
- ULAs are not meant to provide additional IPv6 address space.
- ULAs have the prefix FC00::/7, which results in a first hextet range of FC00 to FDFF.
- ULAs are also known as local IPv6 addresses (not to be confused with IPv6 link-local addresses).



NAT for IPv6

- IPv6 also uses NAT, but in a much different context.
- In IPv6, NAT is used to provide transparent communication between IPv6 and IPv4.
- NAT64 is not intended to be a permanent solution; it is meant to be a transition mechanism.
- Network Address Translation-Protocol Translation (NAT-PT) was another NAT-based transition mechanism for IPv6, but is now deprecated by IETF.
- NAT64 is now recommended.

NAT for IPv6



5.3 Troubleshooting NAT

Cisco | Networking Academy®
Mind Wide Open™

Troubleshooting NAT: show commands

```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
```

Host 192.168.10.10 telnets to server at 209.165.201.1

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:09 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 31  Misses: 0
CEF Translated packets: 31, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
```

<output omitted>

```
R2# show ip nat translations
Pro Inside global         Inside local         Outside local      Out
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23   209
R2#
```

Troubleshooting NAT: debug command

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2818]
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2819]
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2820]
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4181]
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4182]
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2821]
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4183]
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2822]
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4184]
output omitted
```

Chapter 5: Summary

This chapter has outlined:

- How NAT is used to help alleviate the depletion of the IPv4 address space.
- NAT conserves public address space and saves considerable administrative overhead in managing adds, moves, and changes.
- NAT for IPv4, including:
  - NAT characteristics, terminology, and general operations
  - Different types of NAT, including static NAT, dynamic NAT, and NAT with overloading
  - Benefits and disadvantages of NAT
- The configuration, verification, and analysis of static NAT, dynamic NAT, and NAT with overloading.

Chapter 5: Summary (cont.)

- How port forwarding can be used to access an internal devices from the Internet.
- Troubleshooting NAT using **`show`** and **`debug`** commands.
- How NAT for IPv6 is used to translate between IPv6 addresses and IPv4 addresses.