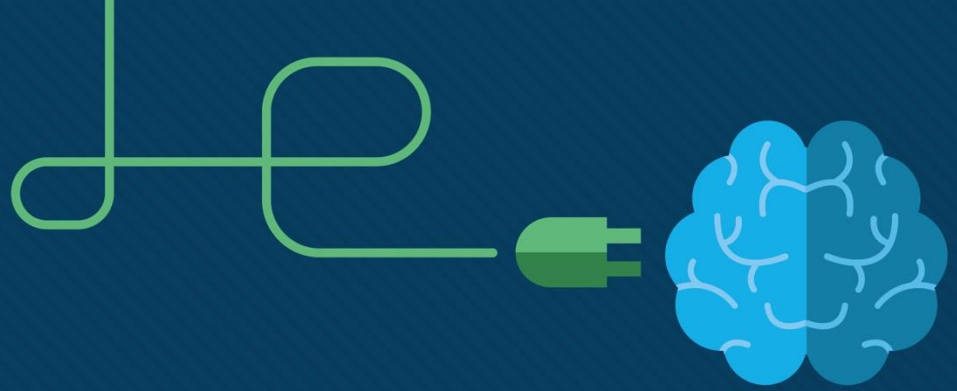


Chapter 9: NAT for IPv4

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 9 - Sections & Objectives

- 9.1 NAT Operation
  - Explain how NAT provides IPv4 address scalability in a small to medium-sized business network
    - Explain the purpose and function of NAT.
    - Explain the operation of different types of NAT.
    - Describe the advantages and disadvantages of NAT.
- 9.2 Configure NAT
  - Configure NAT services on the edge router to provide IPv4 address scalability in a small to medium-sized business network.
    - Configure static NAT using the CLI.
    - Configure dynamic NAT using the CLI.

Chapter 9 - Sections & Objectives (Cont.)

- 9.2 Configure NAT (Cont.)
  - Configure PAT using the CLI.
  - Configure port forwarding using the CLI.
- 9.3 Troubleshoot NAT
  - Troubleshoot NAT issues in a small to medium-sized business network.
  - Troubleshoot NAT

9.1 NAT Operation

IPv4 Private Address Space

- Private IP addresses are used within an organization and home networks.

Did you ever notice how all your labs were based on these addresses?

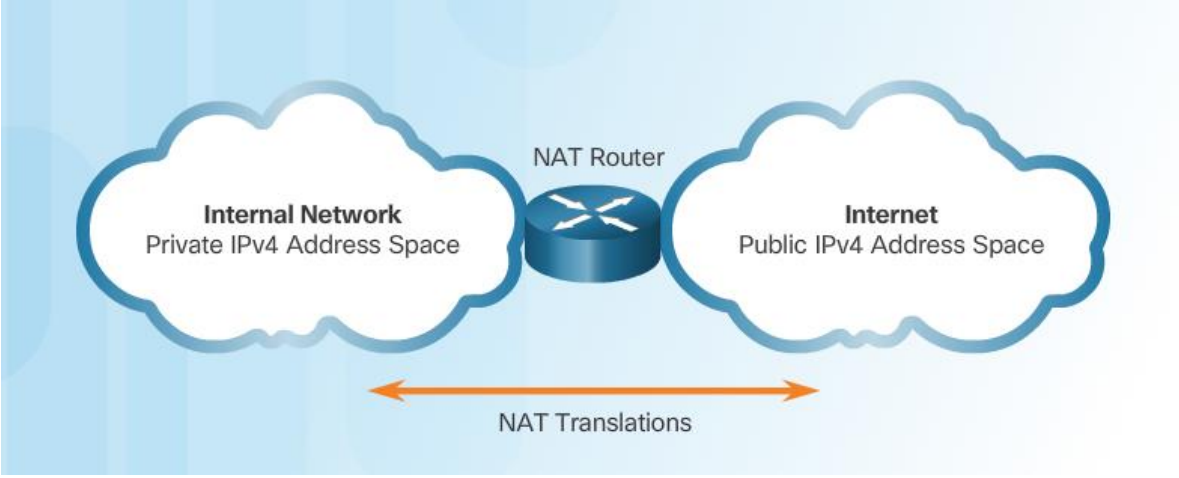
Private Internet Addresses are Defined in RFC 1918

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

These are the IP addresses you will see assigned to company devices.

IPv4 Private Address Space (Cont.)

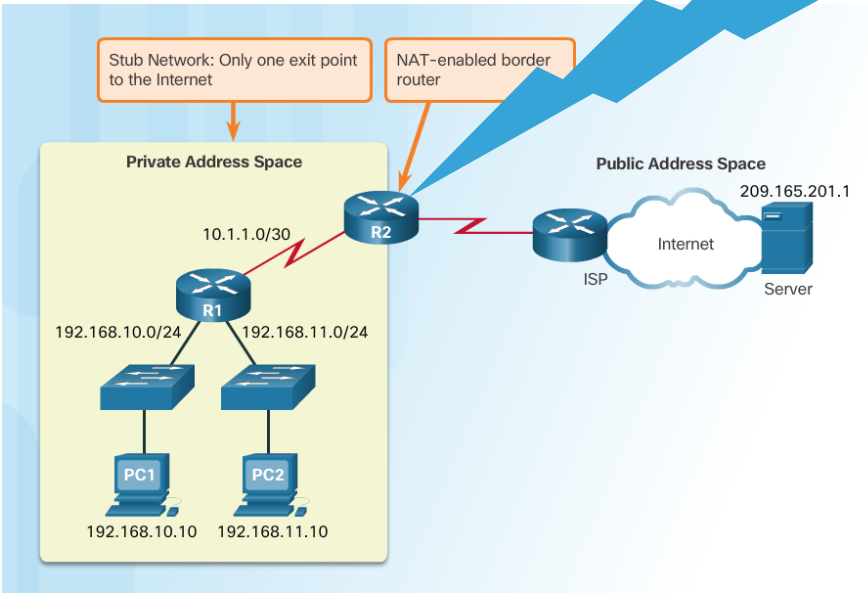
- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses to public addresses that can be routed over the Internet.
- One public IPv4 address can be used for thousands of devices that have private IP addresses.



What is NAT?

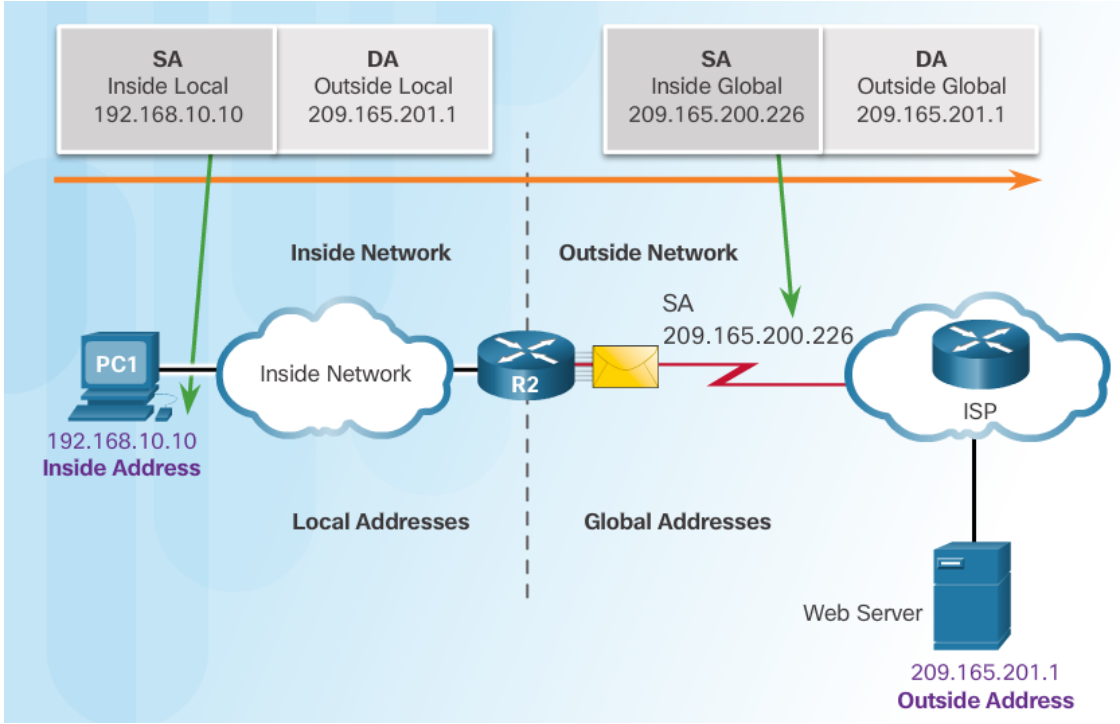
- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses used inside a company to public addresses that can be routed over the Internet.
- NAT hides internal IPv4 addresses from outside networks.
  - Companies use the same private IPv4 addresses so outside devices cannot tell one company's 10.x.x.x network from another company's 10.x.x.x network.
- A NAT-enabled router can be configured with a public IPv4 address.
- A NAT-enabled router can be configured with multiple public IPv4 addresses to be used in a pool or NAT pool for internal devices configured with private addresses.

Important Concept—NAT is enabled on one device (normally the border or edge router)

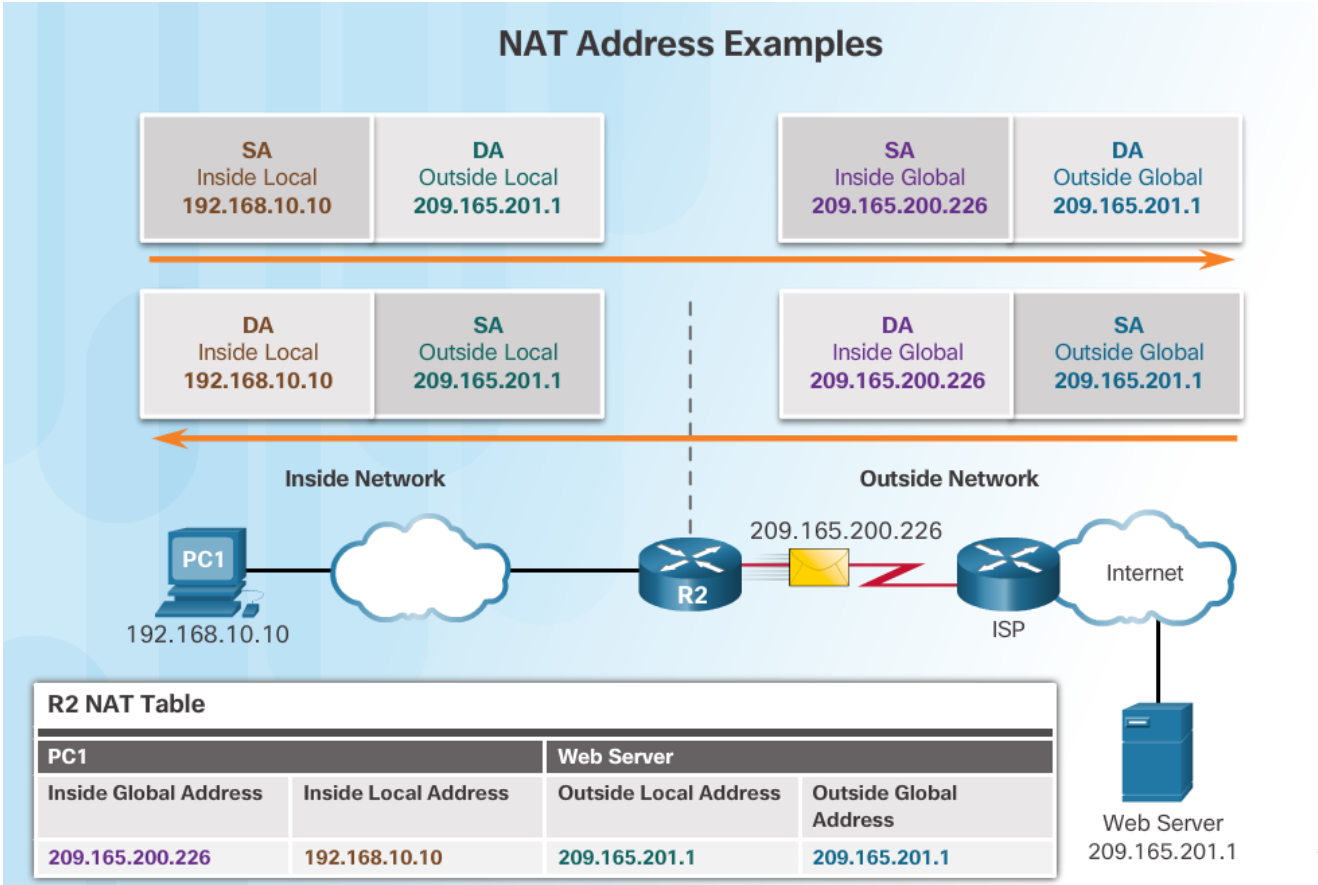


NAT Terminology

- Four types of addresses: inside, outside, local, and global
  - Always consider the device that is having its private address translated to understand this concept.
  - Inside address – address of the company network device that is being translated by NAT
  - Outside address – IP address of the destination device
  - Local address – any address that appears on the inside portion of the network
  - Global address – any address that appears on the outside portion of the network



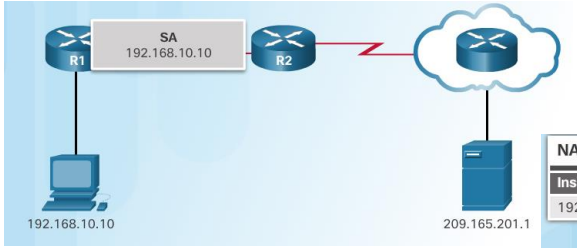
NAT Terminology (Cont.)



R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

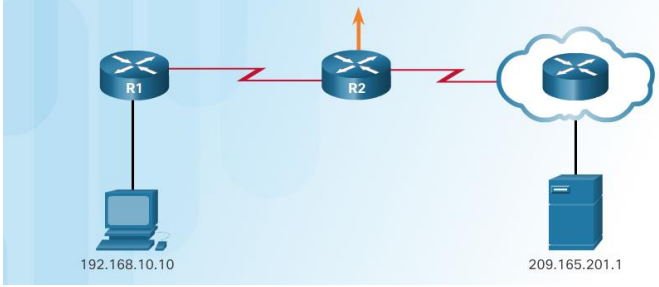
How NAT Works



1. The private (internal) IP address gets translated to a public IP address used to reach the external server.

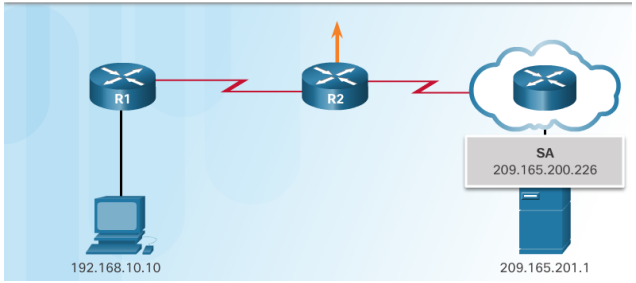
NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

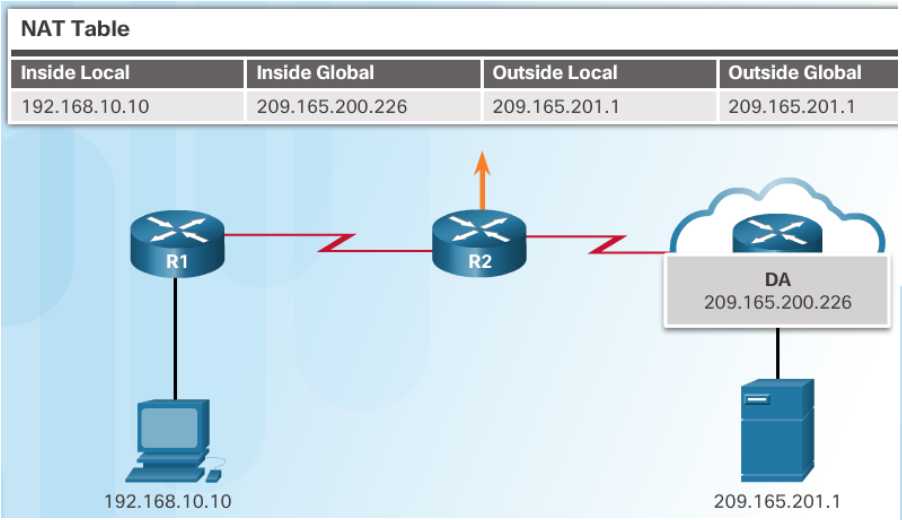


NAT Table

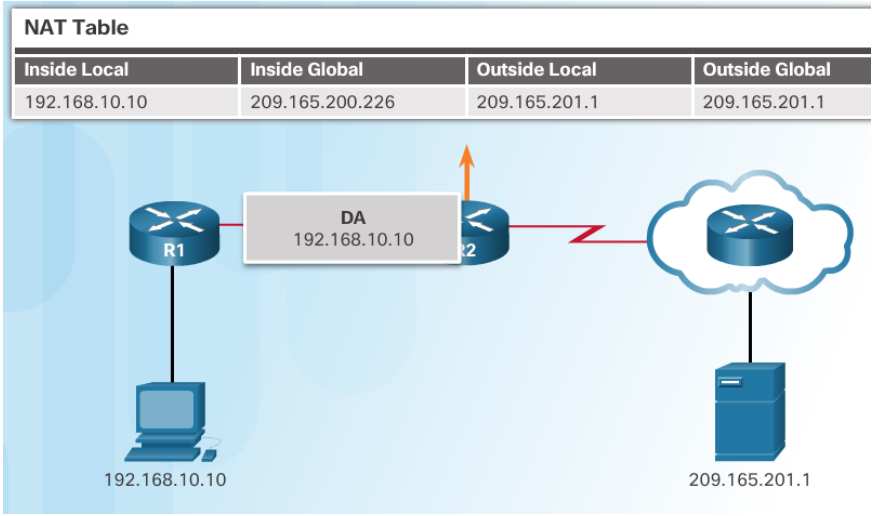
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



How NAT Works (Cont.)



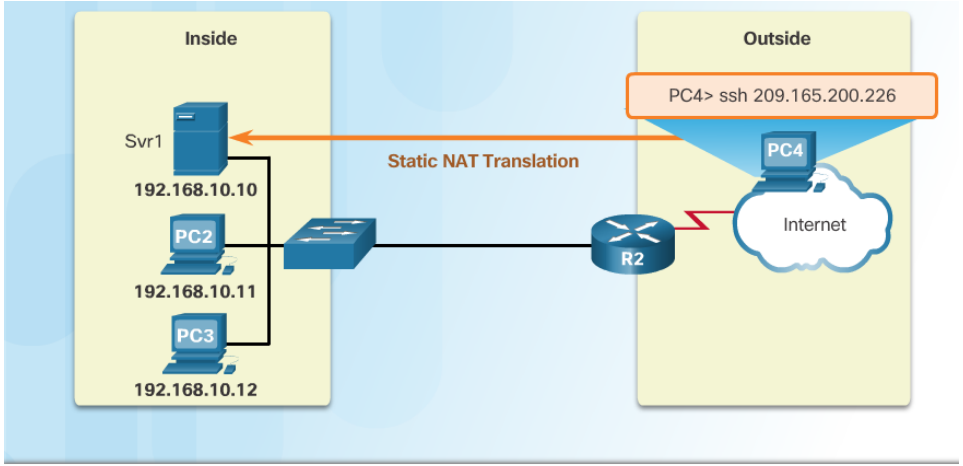
2. The translated public address is used by the server to send the requested information to the device that actually has a private IP address assigned to it.



3. The NAT-enabled router consults the routing table to see what private address requested the data.

Static NAT

- Static address translation (static NAT) assigns one public IP address to one private IP address
- Commonly used for servers that need to be accessed by external devices or for devices that must be accessible by authorized personnel when offsite
- One-to-one address mapping between local and global addresses

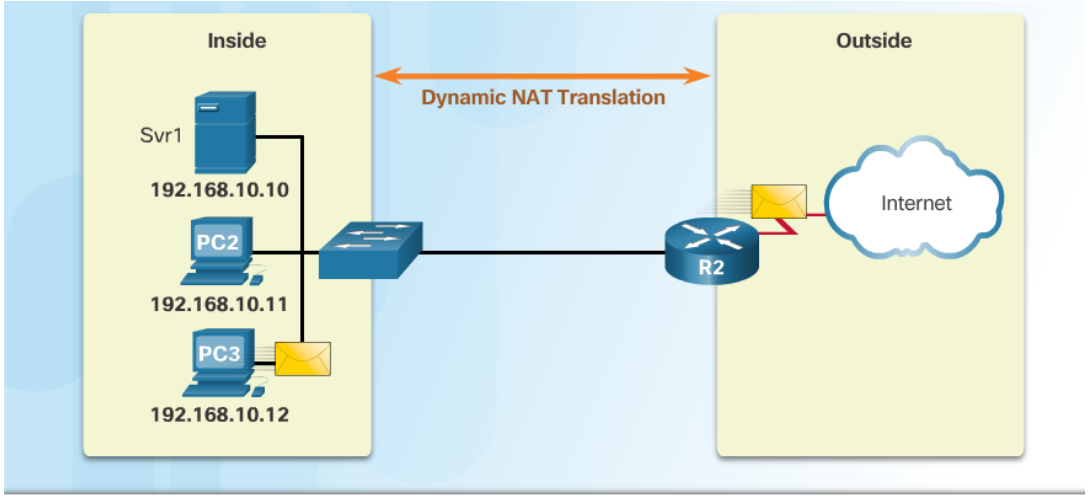


Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Dynamic NAT

- Dynamic NAT assigns a public IP address from a pool of addresses to each packet that originates from a device that has a private IP address assigned when that packet is destined to a network outside the company.
  - Addresses are assigned on a first-come, first serve basis
  - The number of internal devices that can transmit outside the company is limited to the number of public IP addresses in the pool.

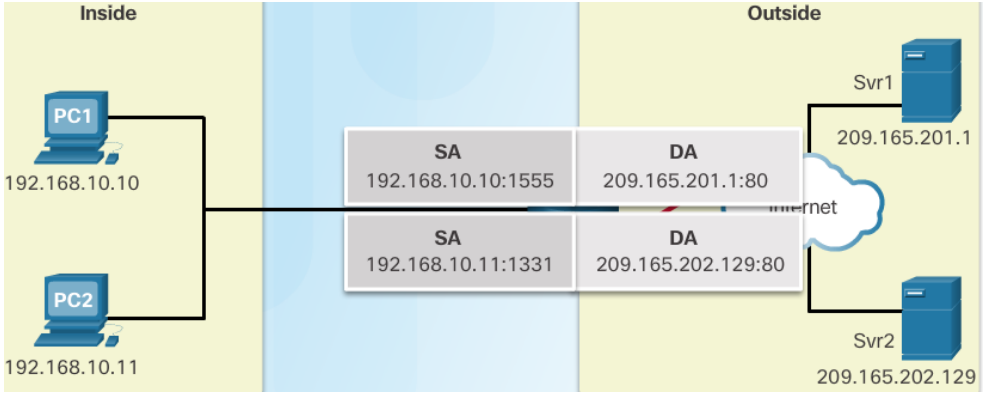


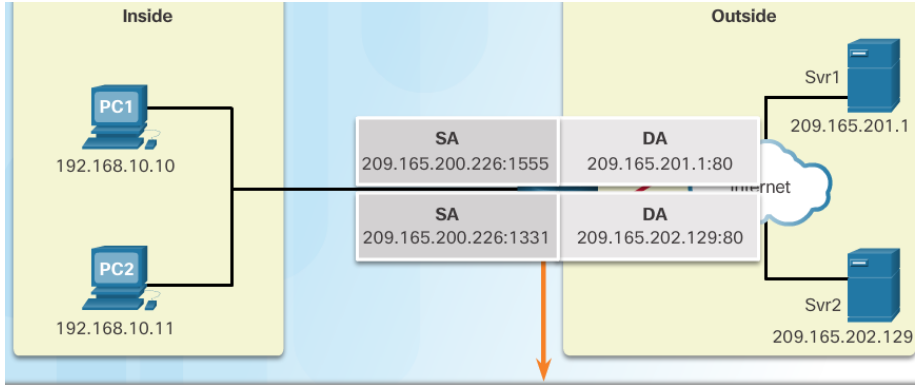
IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Port Address Translation (PAT)

- PAT (otherwise known as NAT overload) can use one public IPv4 address to allow thousand of private IPv4 addresses to communicate with outside network devices.
- Uses port numbers to track the session



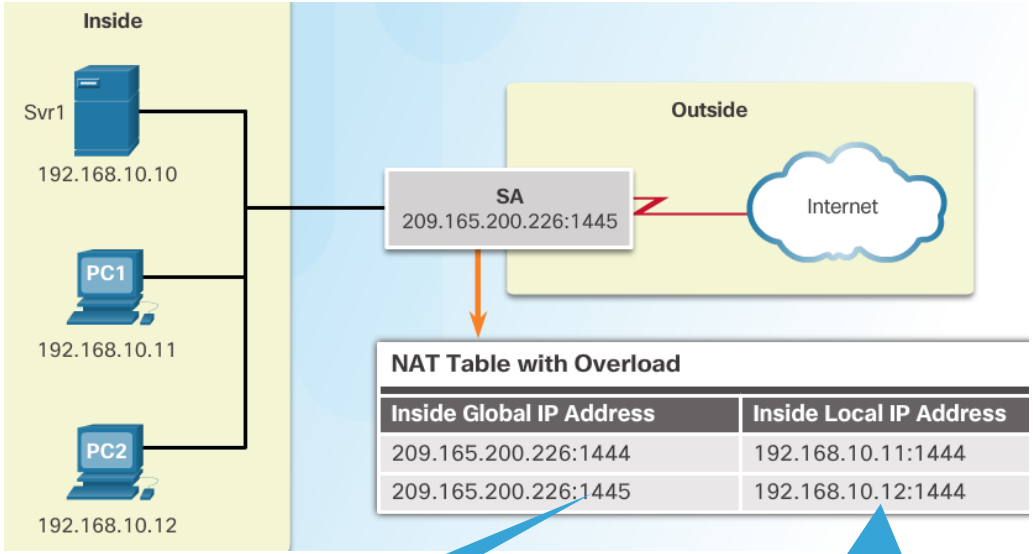


NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Next Available Port

- PAT tries to preserve the original source port number.
  - If that port number is already use, PAT will assign the first available port number for the appropriate port group
    - 0 - 511
    - 512 - 1023
    - 1024 - 65,535
  - When there are no more port numbers available, PAT moves to the next public IP address in the pool if there is one.



Comparing NAT and PAT

NAT

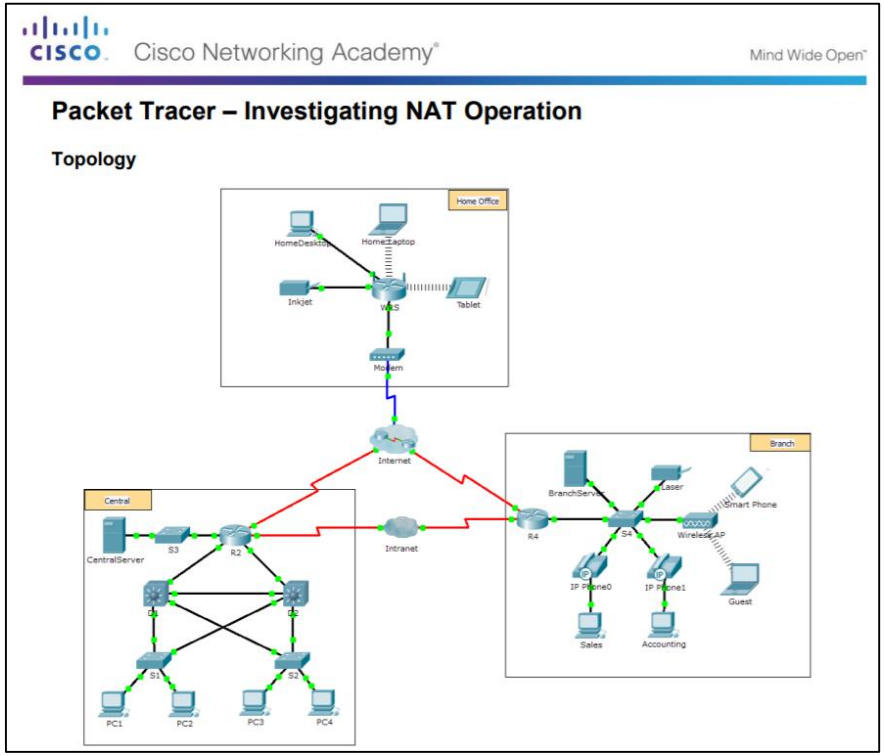
Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

- Static NAT translates address on a 1:1 basis
- PAT uses port numbers so that one public address can be used for multiple privately addressed devices
  - PAT can still function with a protocol such as ICMP that does not use TCP or UDP

Packet Tracer – Investigating NAT Operation



Advantages of NAT

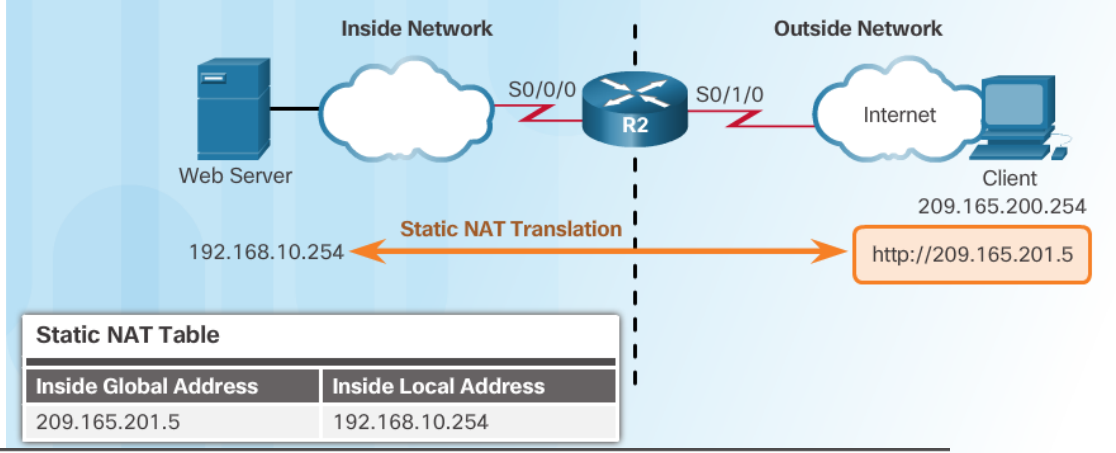
- Conserves the legally registered addressing scheme
  - Every company can use the private IP addresses
- Increases the flexibility of connections to the public network
  - Multiple NAT pools, backup pools, and load-balancing across NAT pools
- Provides consistency for internal network addressing schemes
  - Do not have to readdress the network if a new ISP or public IP address is assigned
- Provides network security
  - Hides user private IPv4 addresses

Disadvantages of NAT

- Performance is degraded.
  - The NAT-enabled border device must track and process each session destined for an external network.
- End-to-end functionality is degraded.
  - Translation of each IPv4 address within the packet headers takes time.
- End-to-end IP traceability is lost.
  - Some applications require end-to-end addressing and cannot be used with NAT.
  - Static NAT mappings can sometimes be used.
  - Troubleshooting can be more challenging.
- Tunneling becomes more complicated.
- Initiating TCP connections can be disrupted.

9.2 Configure NAT

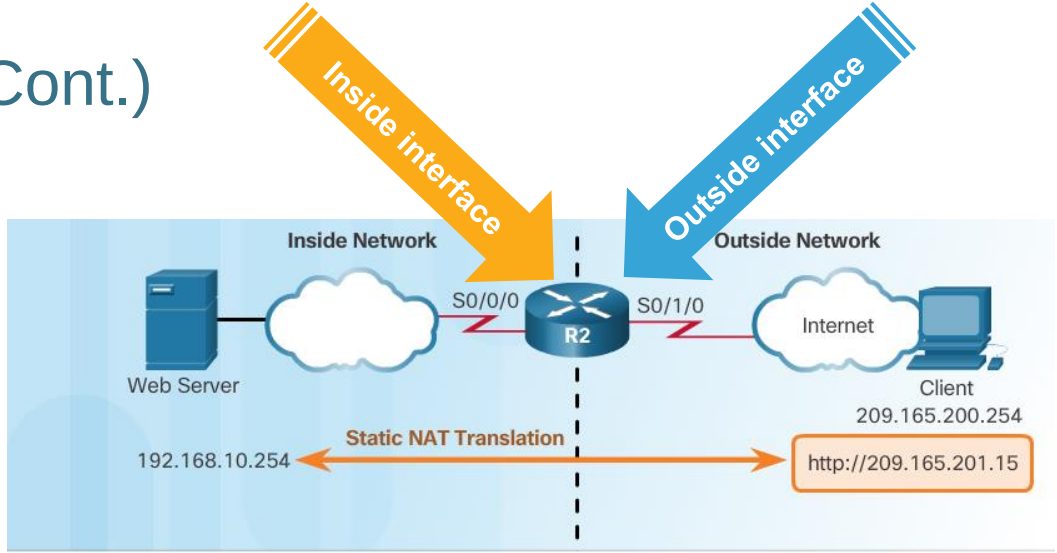
Configure Static NAT



Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. `Router(config)# ip nat inside source static local-ip global-ip`	Enter the **`no ip nat inside source static`** global configuration mode command to remove the dynamic source translation.
2	Specify the inside interface. `Router(config)# interface type number`	Enter the **`interface`** command. The CLI prompt changes from `(config)#` to `(config-if)#`.
3	Mark the interface as connected to the inside. `Router(config-if)# ip nat inside`	
4	Exit interface configuration mode. `Router(config-if)# exit`	
5	Specify the outside interface. `Router(config)# interface type number`	
6	Mark the interface as connected to the outside. `Router(config-if)# ip nat outside`	

Configure Static NAT (Cont.)

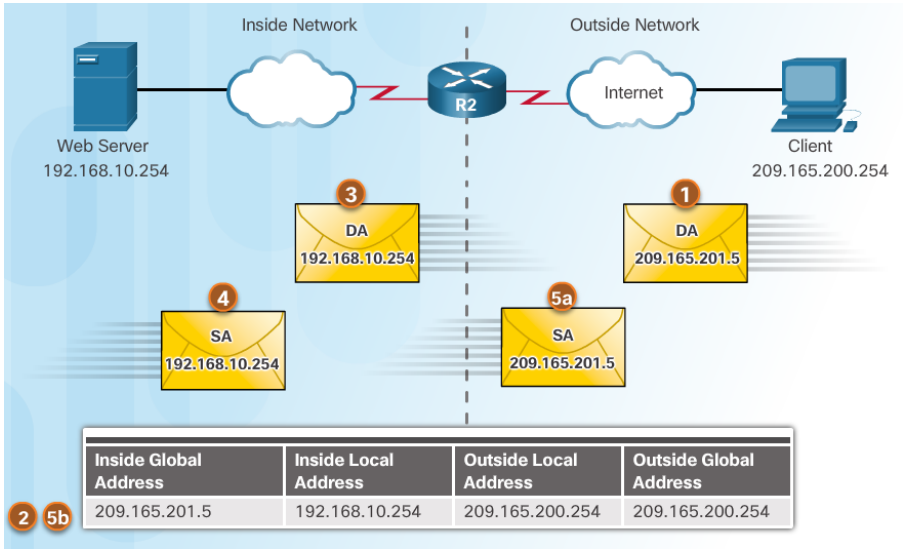
Remember that any interface on the border router that is on the inside network must be configured with the **ip nat inside** command. This is a common mistake for those new to NAT.




```
Establishes static translation between an inside local address and an inside global
address.
R2(config)# ip nat inside source static 192.168.11.99 209.165.201.15

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 209.165.200.1 255.255.255.252
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Analyzing Static NAT

1. Client opens a web browser for a connection to a web server.
2. R2 receives the packet on the outside interface and checks the NAT table.
3. R2 replaces the inside global address with inside local address of 192.168.10.254 (the server's address).
4. Web server responds to the client.
5. (a) R2 receives the packet from the server on the inside address.
   (b) R2 checks NAT table and translates the source address to the inside global address of 209165.201.5 and forwards the packet.
6. The client receives the packet.



Configuring Static NAT
Verifying Static NAT

A best practice is to clear statistics when verifying that NAT is working.

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
---    209.165.201.5     192.168.10.254    ---                ---
R2#
```

Important commands:

- **show ip nat translations**
- **show ip nat statistics**

```
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>
```

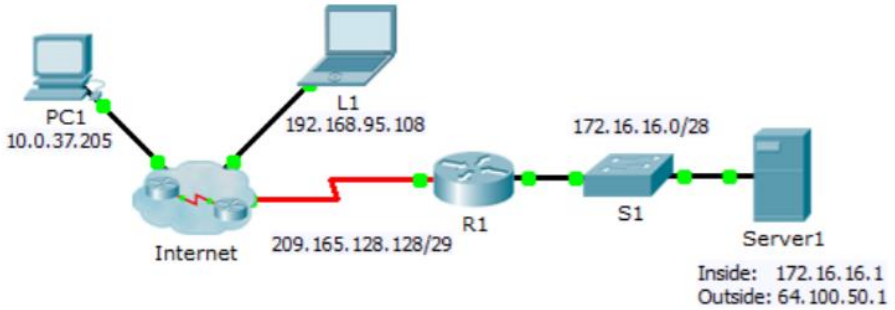
Packet Tracer – Configuring Static NAT

Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Configuring Static NAT

Topology



Objectives

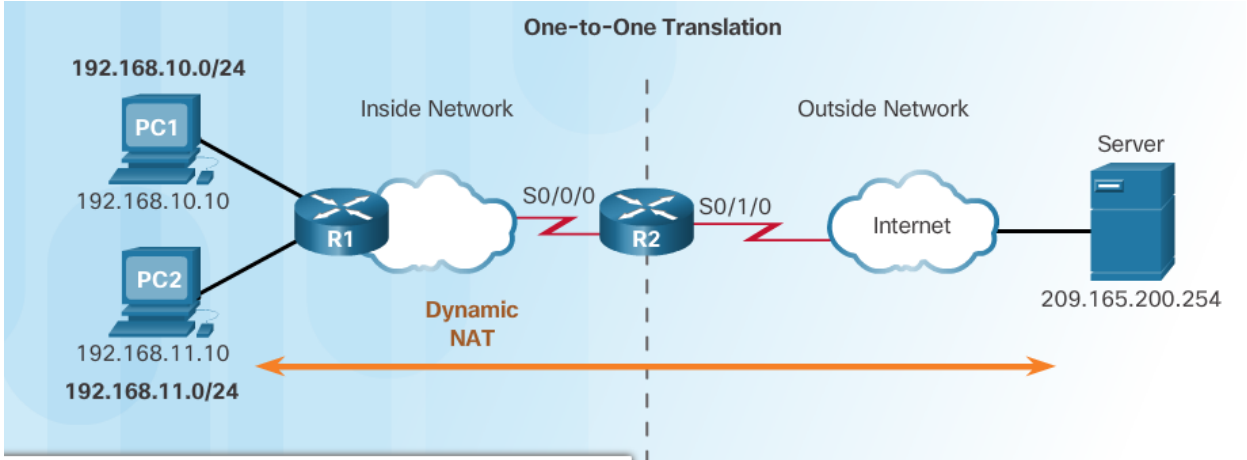
Part 1: Test Access without NAT

Part 2: Configure Static NAT

Part 3: Test Access with NAT

Dynamic NAT Operation

- Remember that dynamic NAT uses a pool of public IPv4 addresses.
- Use the same concepts of inside and outside NAT interfaces as static NAT.



IPv4 NAT Pool

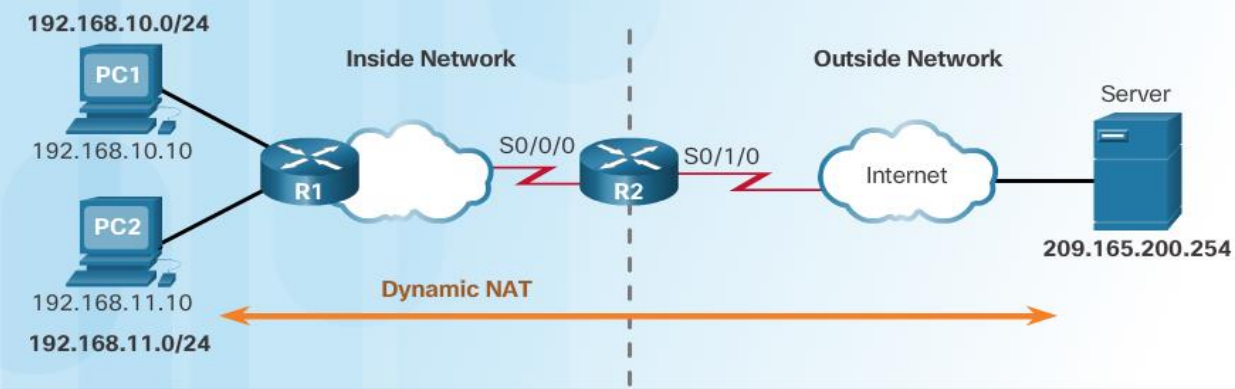
Inside Local Address Pool	Inside Global Address
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227
...	209.165.200.228
...	...
...	209.165.200.240

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**

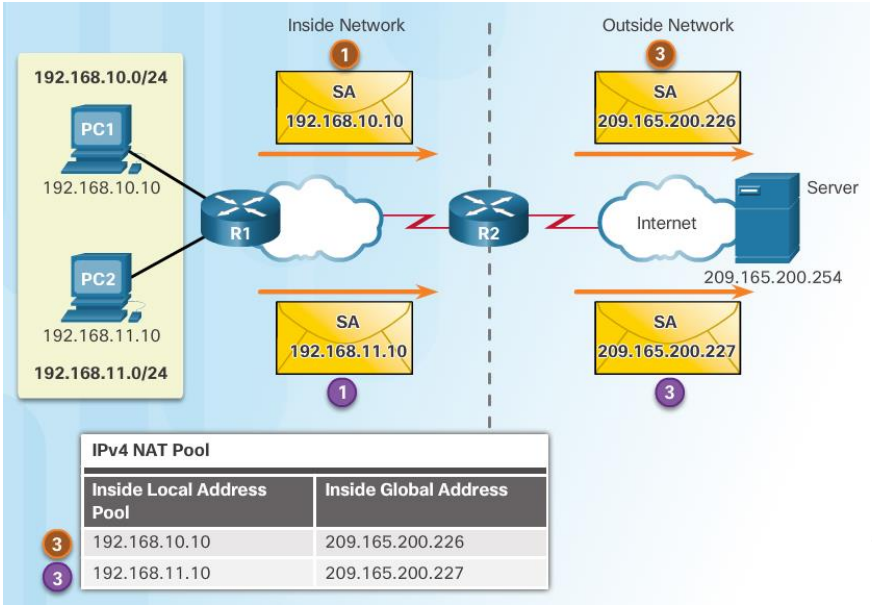
Configuring Dynamic NAT (Cont.)




```
Defines a pool of public IPv4 addresses under the pool name NAT POOL1.
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224

Defines which addresses are eligible to be translated.
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255

Binds NAT-POOL1 with ACL 1.
R2(config)# ip nat inside source list 1 pool NAT-POOL1

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

Analyzing Dynamic NAT

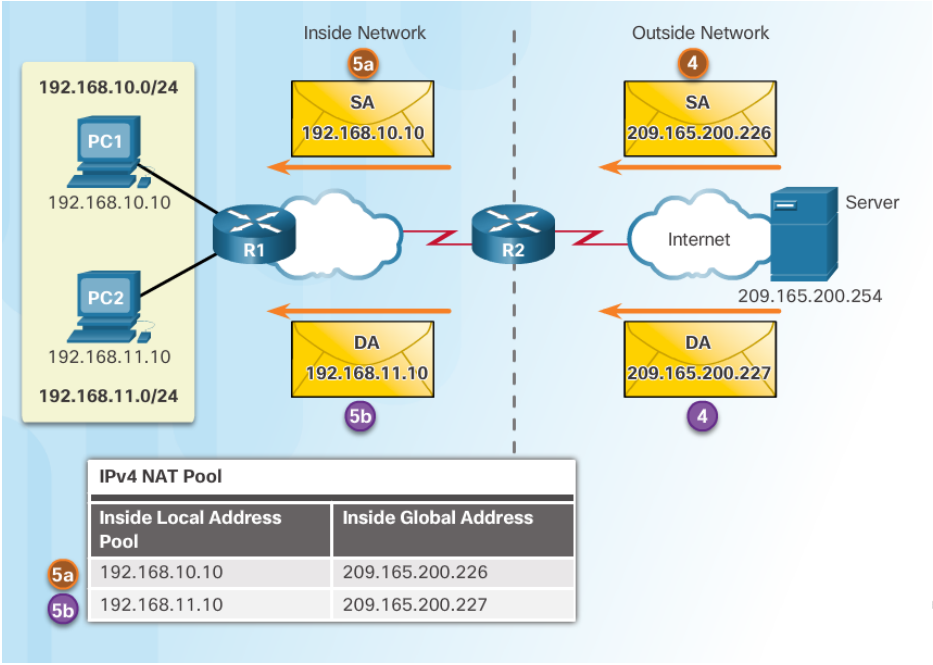
1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns a global address from the NAT pool and creates a NAT table entry for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address from the pool.



Analyzing Dynamic NAT (Cont.)

4. The server responds to PC1 using the destination address of 209.165.200.226 (the NAT-assigned address) and to PC2 using the destination address of 209.165.200.227.

5. (a and b) R2 looks up each received packet and forwards based on the private IP address found in the NAT table for each of the destination addresses.



Verifying Dynamic NAT

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

Command	Description
`clear ip nat translation *`	Clears all dynamic address translation entries from the NAT translation table.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Clear a simple dynamic translation entry containing an inside translation or both inside and outside translation.
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local port global-ip global-port*]	Clears an extended dynamic translation entry.

Verifying Dynamic NAT (Cont.)

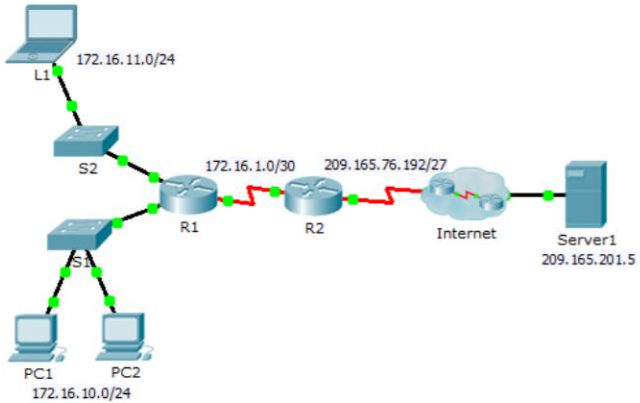
```
R2# clear ip nat statistics

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#
```

Packet Tracer – Configuring Dynamic NAT

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Configuring Dynamic NAT

Topology

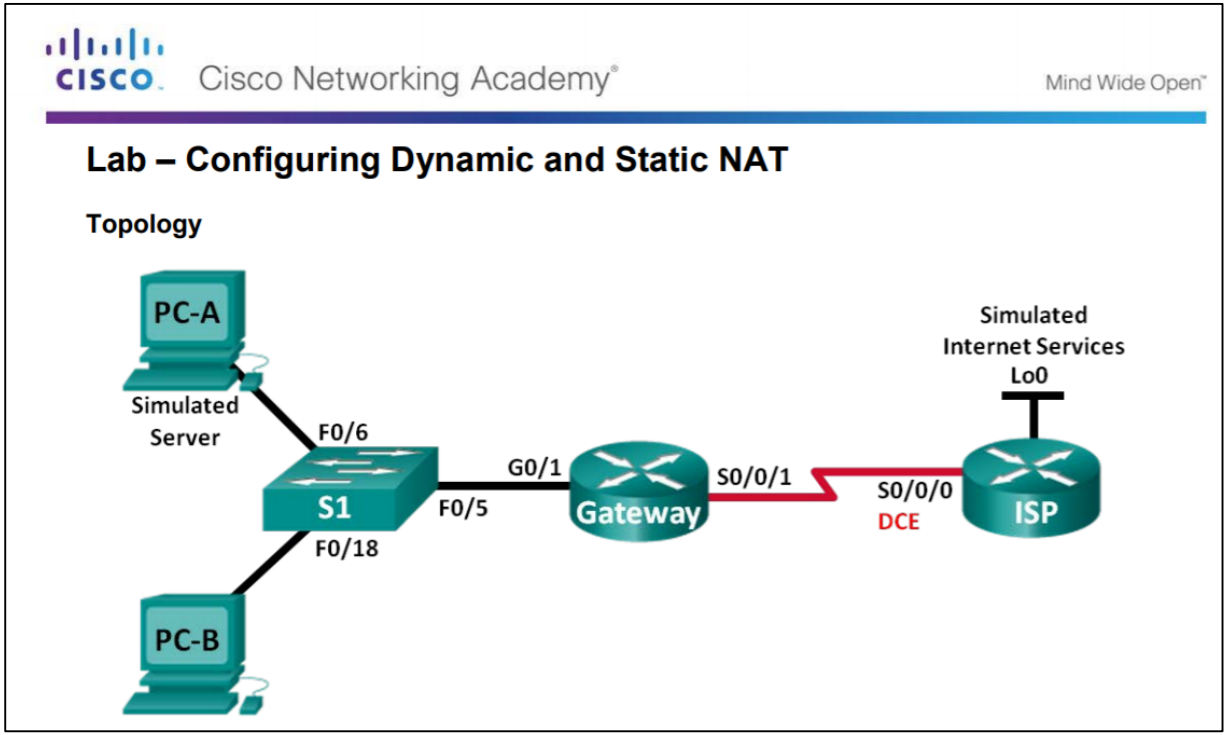


Objectives

Part 1: Configure Dynamic NAT

Part 2: Verify NAT Implementation

Configuring Dynamic and Static NAT



Configuring PAT: Address Pool

The pool contains the public addresses.

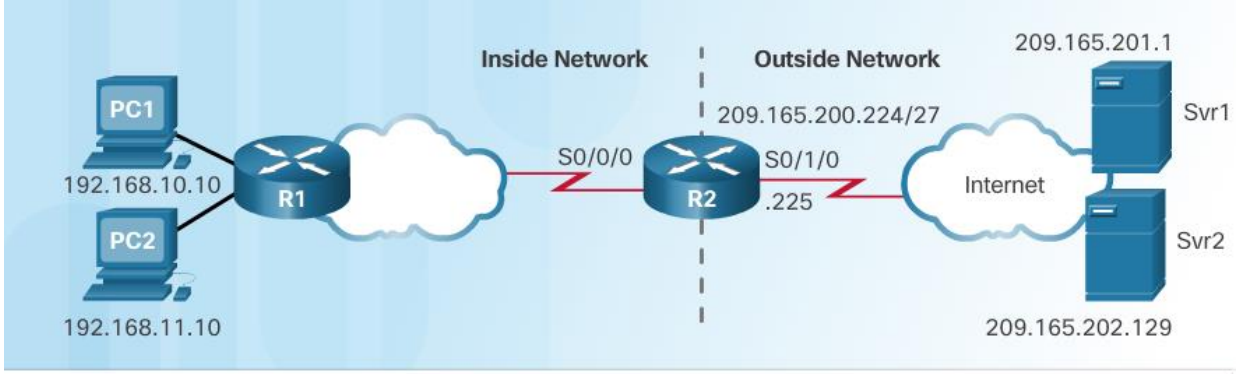
The ACL defines which private IP addresses gets translated.

The **ip nat inside source list** *acl#* **pool** *name* **overload** command ties Step 1 with Step 2.

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

The **overload** command is what allows the router to track port numbers (and do PAT instead of dynamic NAT).

Configuring PAT: Address Pool (Cont.)



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.

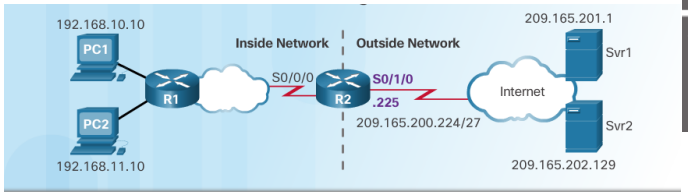
```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Configuring PAT: Single Address

- When a public address is assigned to the external interface on the border router, that public address can be used for PAT and translate internal private IP addresses to the public IP address.

Still need an ACL to define which private IP addresses gets translated.

Instead of associating an ACL with a pool, the ACL is associated with an interface that has a public IP address assigned.



NAT Table

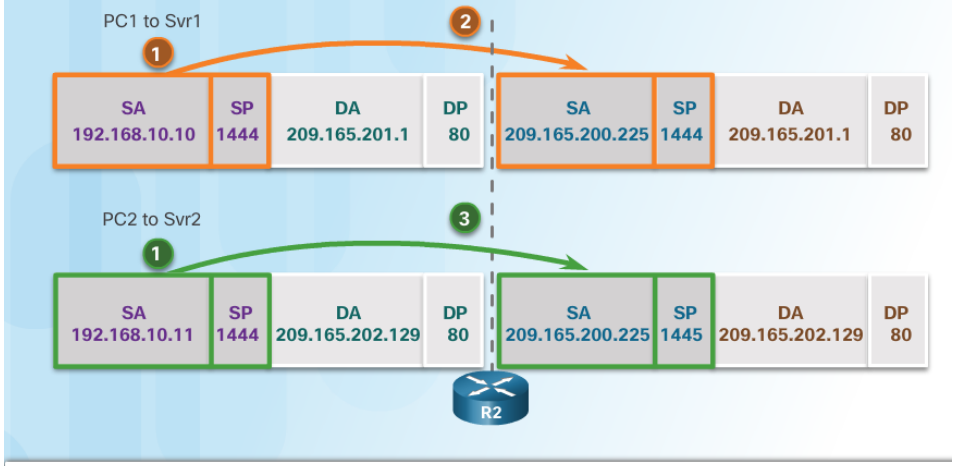
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

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**

The overload command is always needed for PAT.

Analyzing PAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns the IP address of the outside interface, adds a port number, and creates a NAT table entry for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address.



NAT Table

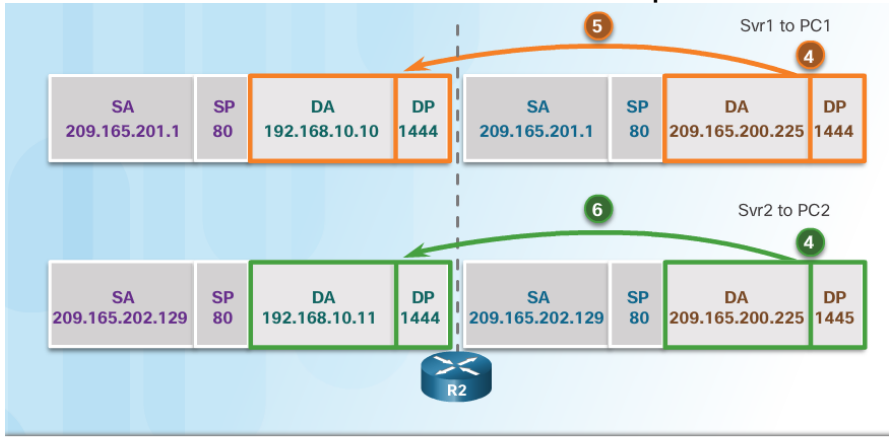
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Analyzing PAT (Cont.)

4. Each server responds to PC1 and PC2 using the destination address of the public address assigned to the external interface on the border router.

5. R2 looks up the received packet and forwards to PC1 because that is the private IP address found in the NAT table for the destination address and port number.

6. R2 looks up the received packet and forwards to PC2 because that is the private IP address found in the NAT table for the destination address and port number.



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Verifying PAT

```
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#
```

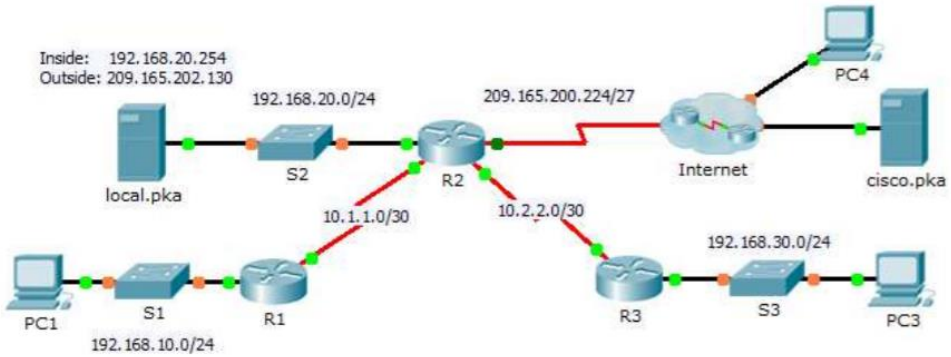
```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
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

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

Packet Tracer – Implementing Static and Dynamic NAT

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Implementing Static and Dynamic NAT

Topology



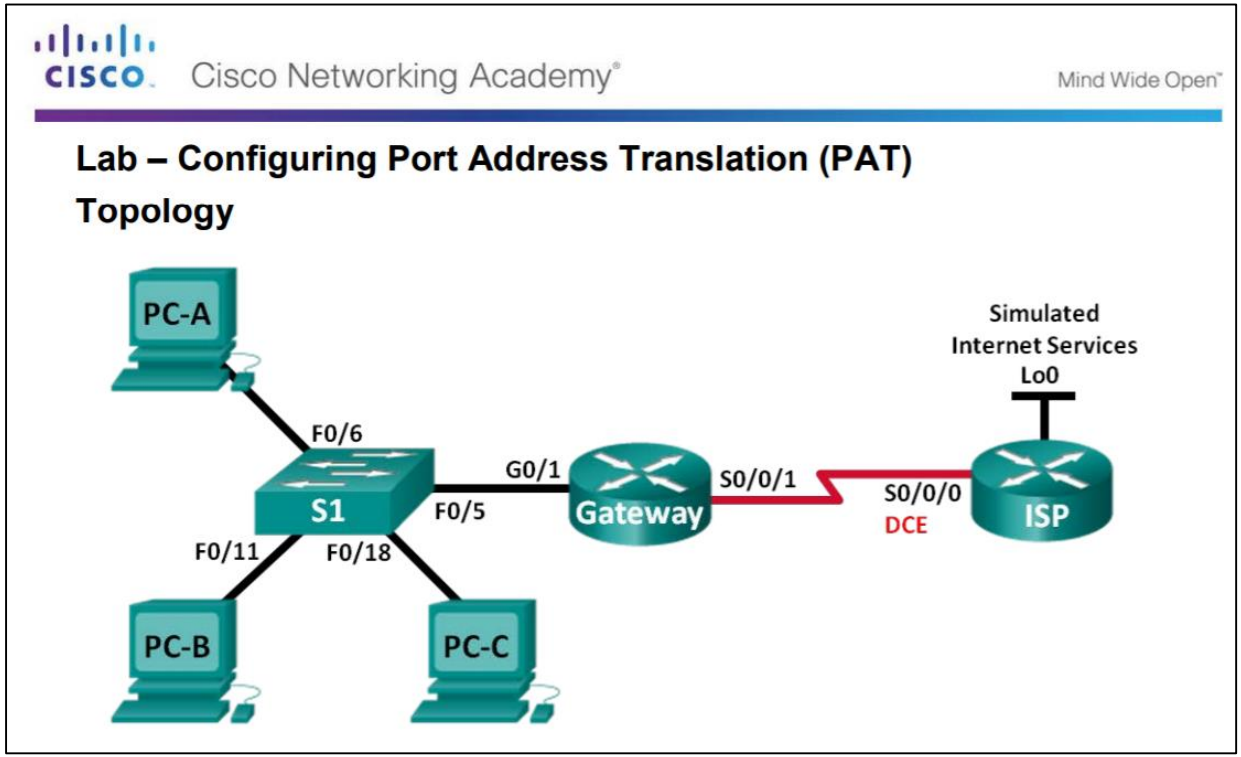
Objectives

Part 1: Configure Dynamic NAT with PAT

Part 2: Configure Static NAT

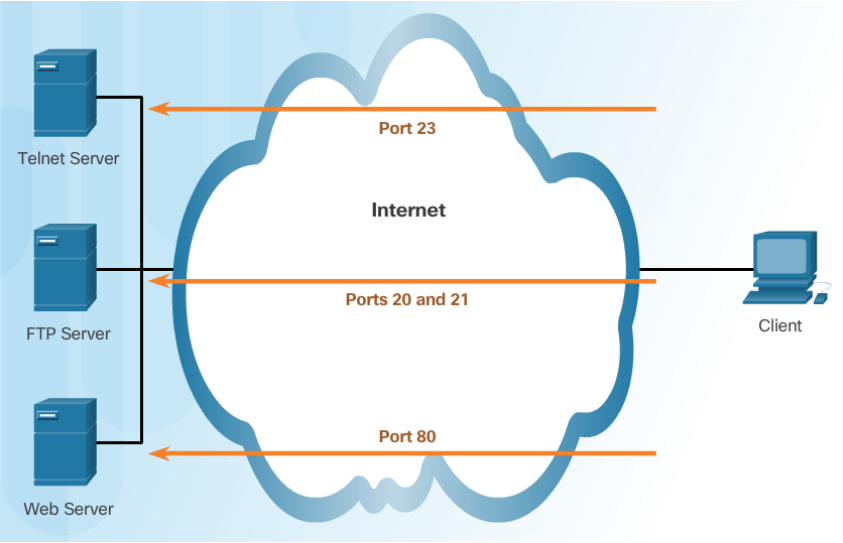
Part 3: Verify NAT Implementation

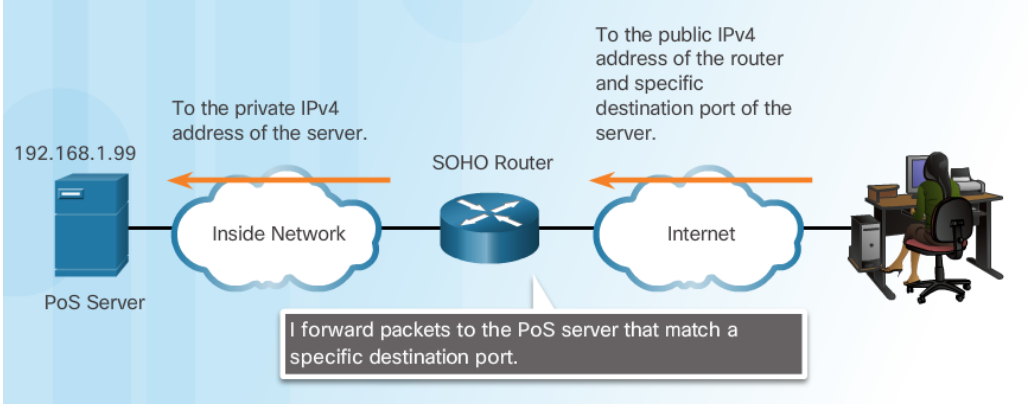
Configuring Port Address Translation (PAT)



Port Forwarding

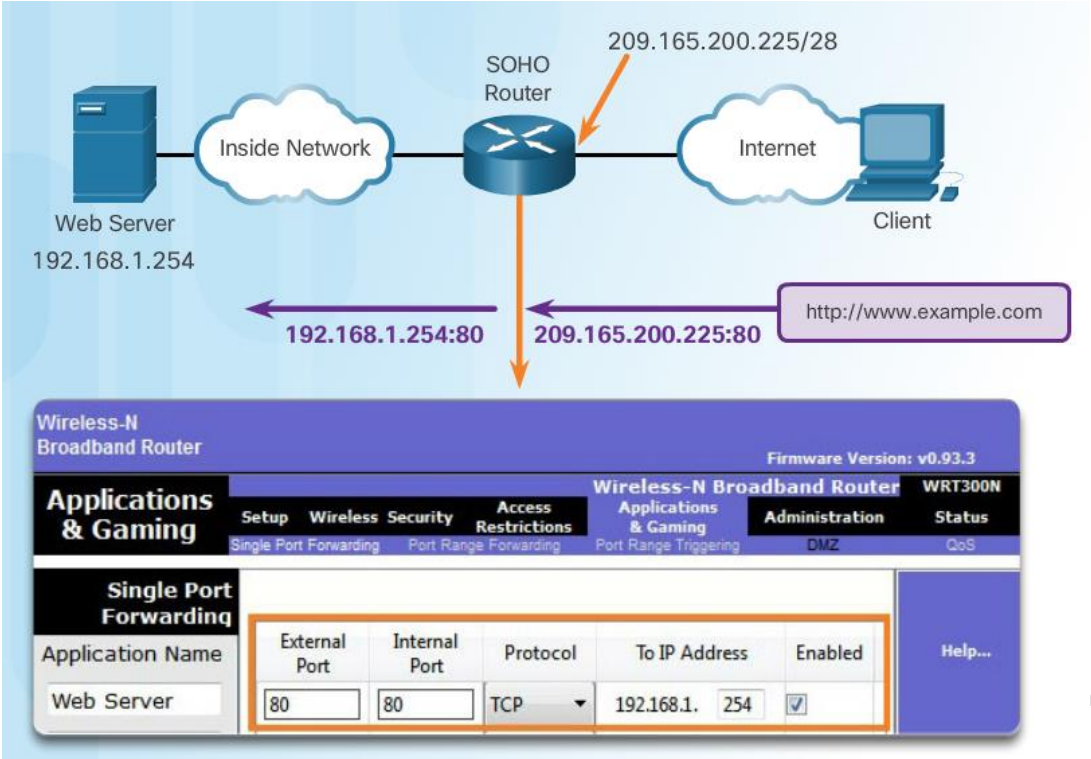
- Port forwarding allows an external device to reach a device on a specific port number and the device is located on an internal (private) network.
  - Required for some peer-to-peer file-sharing programs and operations such as web serving and outgoing FTP
  - Solves the problem of NAT only allowing translations for traffic destined for external networks at the request of internal devices.



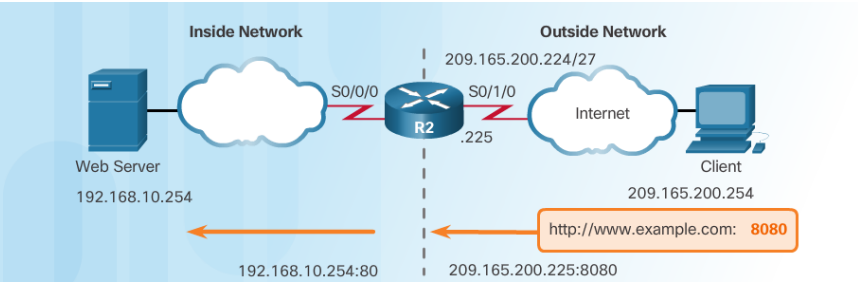


Wireless Router Example

- Port forwarding can be enabled for specific applications
  - Must specify the inside local address that requests should be forwarded to



Configuring Port Forwarding with IOS



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
```

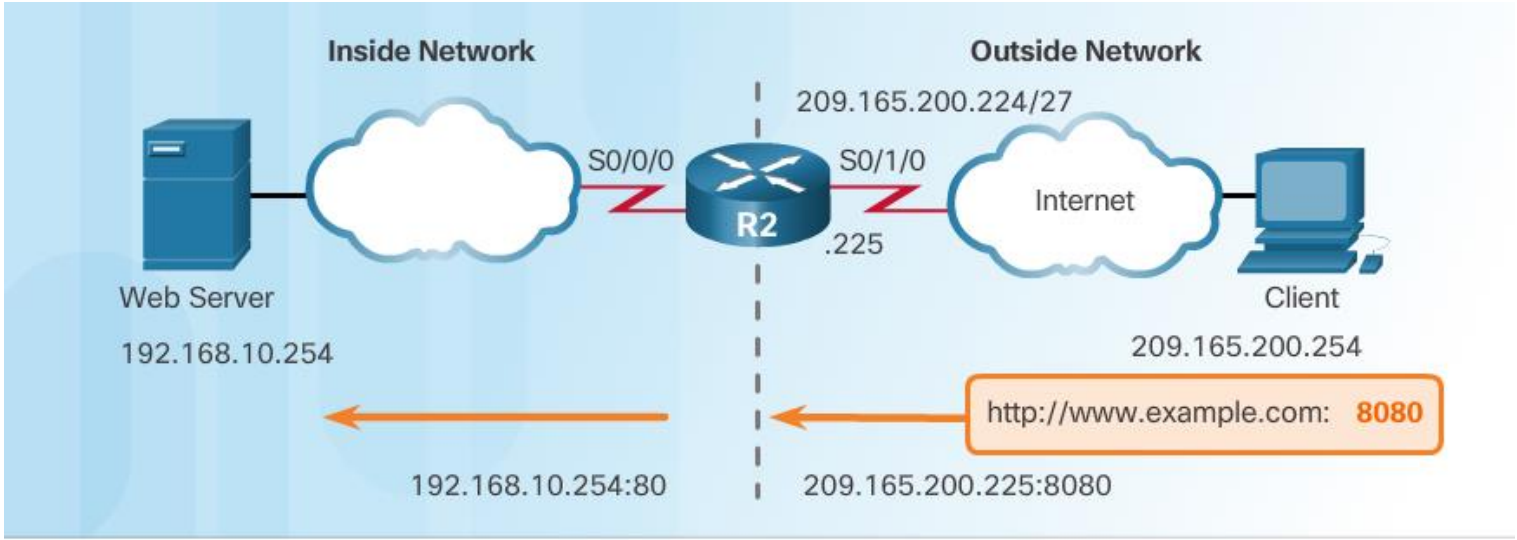
Identifies interface serial 0/1/0 as the outside NAT interface.

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

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```

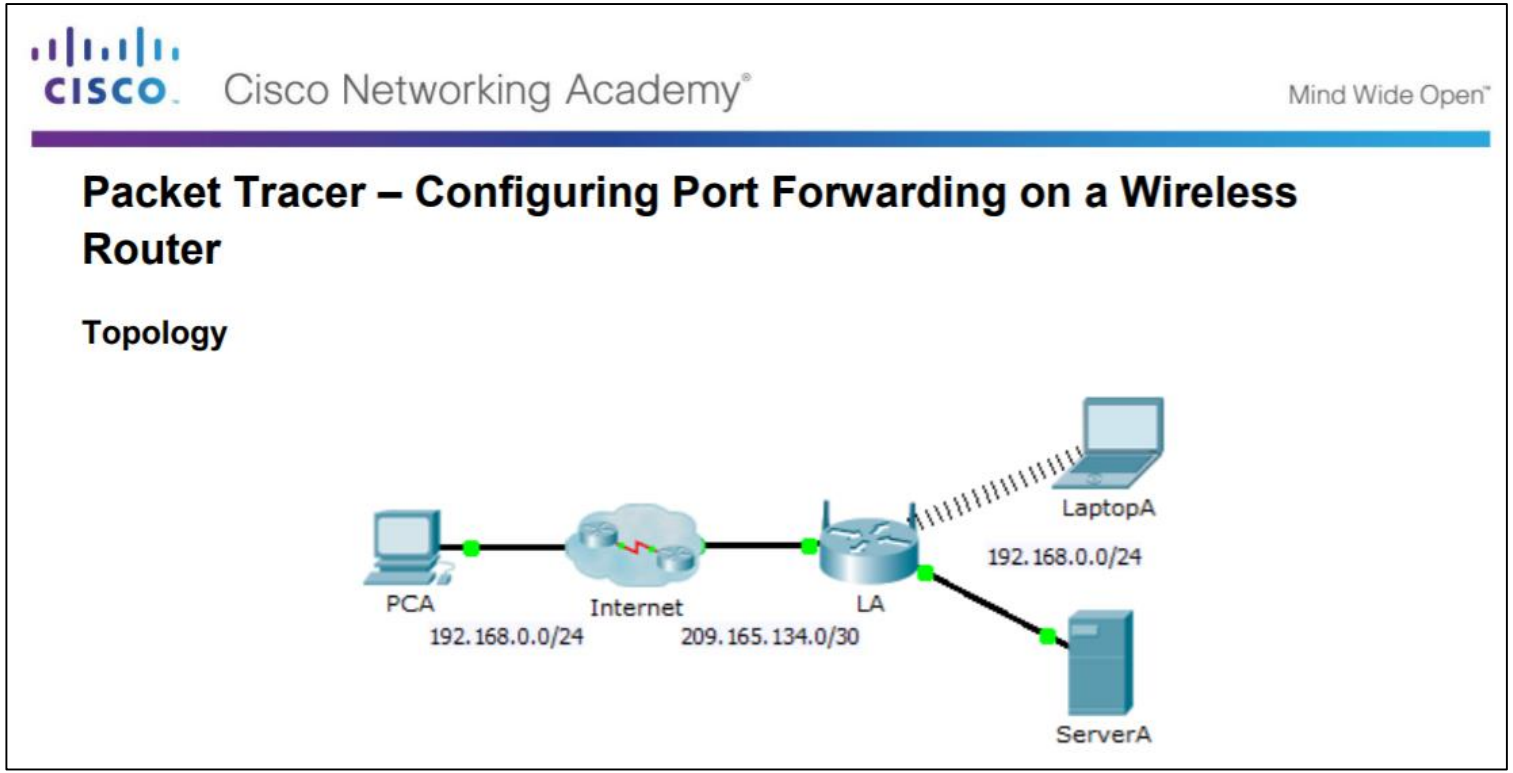
Parameter	Description
tcp or **udp**	Indicates if this is a TCP or UDP port number.
local-ip	This is the IPv4 address assigned to the host on the inside network, typically from RFC 1918 private address space.
local-port	Sets the local TCP/UDP port in a range from 1 – 65,535. This is the port number the server is listening on.
global-ip	This is the IPv4 globally unique IP address of an inside host. This is the IP address the outside clients will use to reach the internal server.
global-port	Sets the global TCP/UDP port in a range from 1 – 65,535. This is the port number the outside client will use to reach the internal server.
extendable	The **extendable** option is applied automatically. The **extendable** keyword allows the user to configure several ambiguous static translations, where ambiguous translations are translations with the same local or global address. It allows the router to extend the translation to more than one port if necessary.

Configuring Port Forwarding with IOS (Cont.)



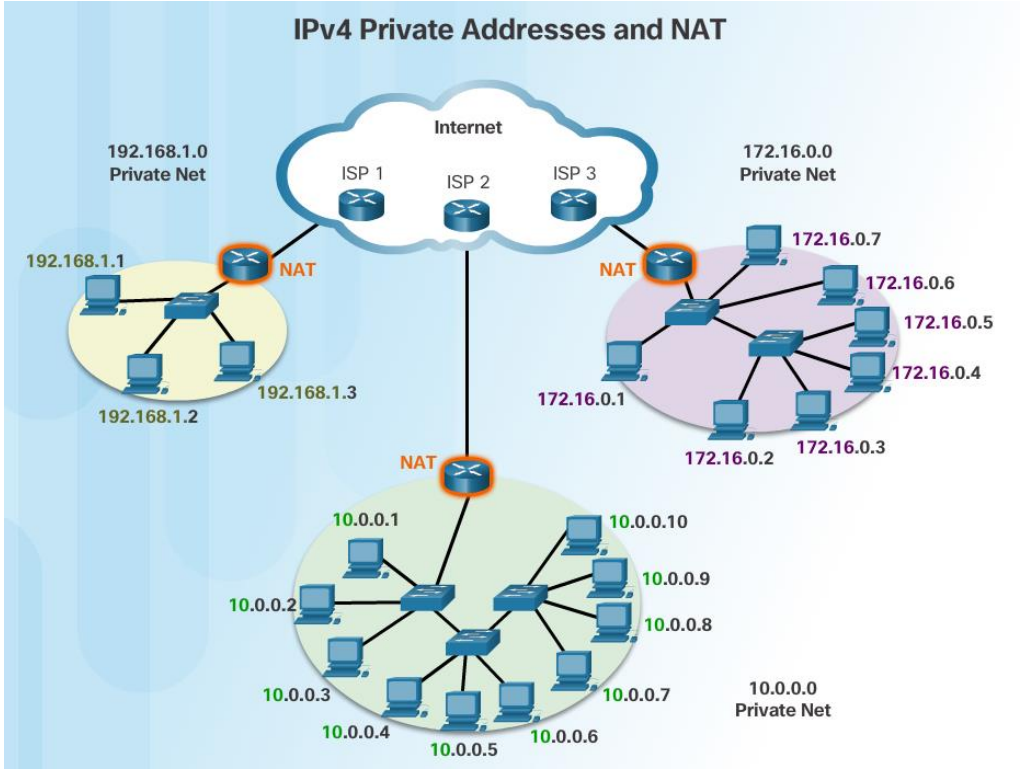

```
R2# show ip nat translations
Pro Inside global         Inside local       Outside local          Outside global
tcp 209.165.200.225:8080 192.168.10.254:80  209.165.200.254:46088 209.165.200.254:46088
tcp 209.165.200.225:8080 192.168.10.254:80  ---                    ---
R2#
```

Packet Tracer – Configuring Port Forwarding on a Wireless Router



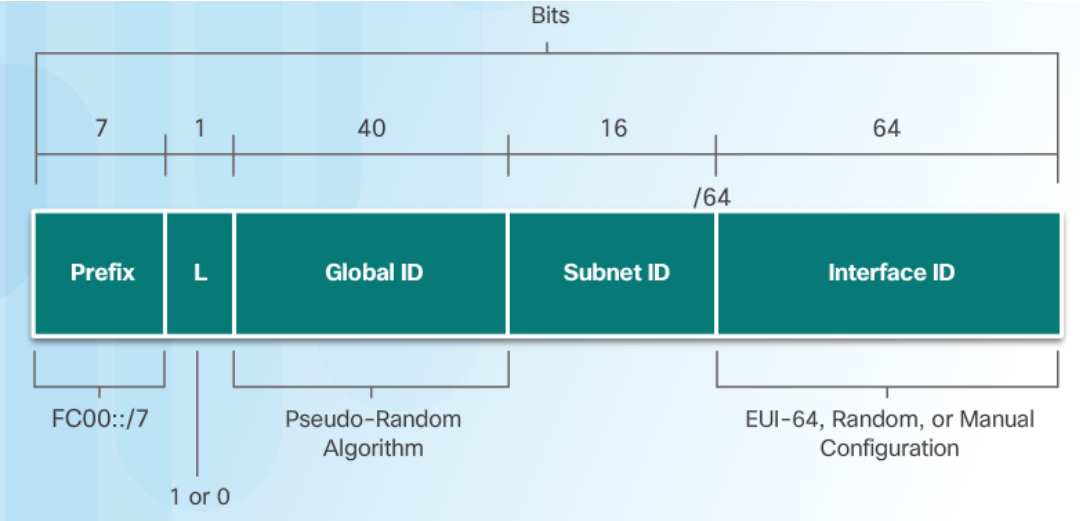
NAT for IPv6?

- IPv6 was developed with the intention of making NAT for IPv4 unnecessary
- IPv6 does have its own form of NAT
  - IPv6 has its own private address space



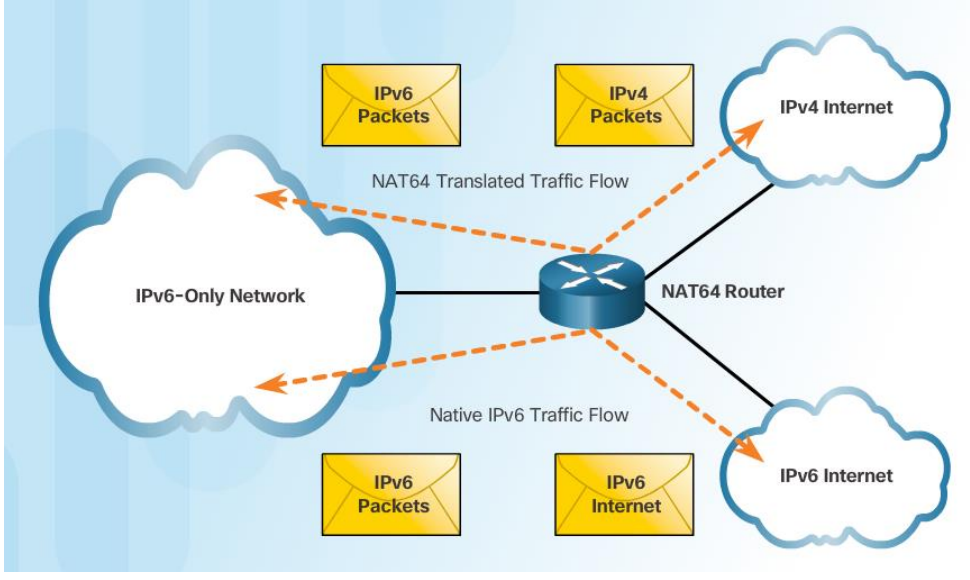
IPv6 Unique Local Addresses

- IPv6 unique local addresses (ULAs) are similar to IPv4 private addresses
  - ULAs are to provide IPv6 address space for communications within a local site.
  - First 64 bits of a ULA
    - Prefix of FC00::/7 (FC00 to FDFF)
    - Next bit is a 1 if the prefix is locally assigned
    - Next 40 bits define a global ID
    - Next 16 bits is a subnet ID
  - Last 64 bits of a ULA is the interface ID or host portion of the address
- Allows sites to be combined without address conflicts
- Allows internal connectivity
- Not routable on the Internet



NAT for IPv6

- Provide access between IPv6-only and IPv4-only networks (not translating private address to public addresses as NAT for IPv4 was)
- Techniques available
  - Dual-stack – both devices run protocols for both IPv4 and IPv6
  - Tunneling – Encapsulate the IPv6 packet inside an IPv4 packet for transmission over an IPv4-only network
  - NAT for IPv6 (translation)
    - Should not be used as a long term strategy
    - The older Network Address Translation-Protocol Translation (NAT-PT)
    - NAT64

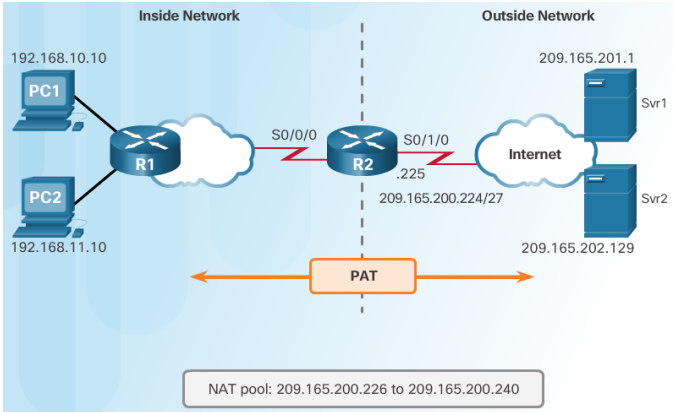


9.3 Troubleshoot NAT

NAT Troubleshooting Commands

The show ip nat Commands

1. Determine what NAT is supposed to achieve and compare with configuration. This may reveal a problem with the configuration.
2. Verify translations using the **show ip nat translations** command.
3. Use the **clear** and **debug** commands to verify NAT.
4. Review what is happening to the packet and verify routing.



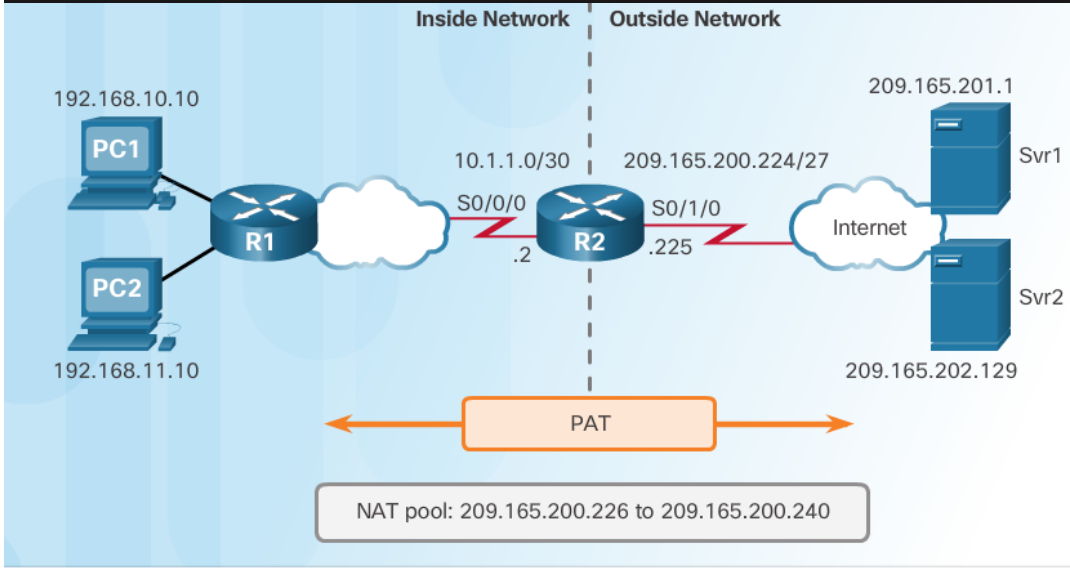

```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
<output omitted>

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      Outside global
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23   209.165.201.1:23
```

NAT Troubleshooting Commands

The debug ip nat Commands

- Common commands
  - **debug ip nat**
  - **debug ip nat detailed**
- Output symbols and values
  - * - The translation is occurring in the fast-switched path
  - **s=** - Source IPv4 address
  - **a.b.c.d--->w.x.y.z** – Source a.b.c.d is translated to w.x.y.z.
  - **d=** - Destination IPv4 address
  - **[xxxx]** - IPv4 identification number
- Check the ACL to ensure the correct private addresses are designated.

```
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>
```



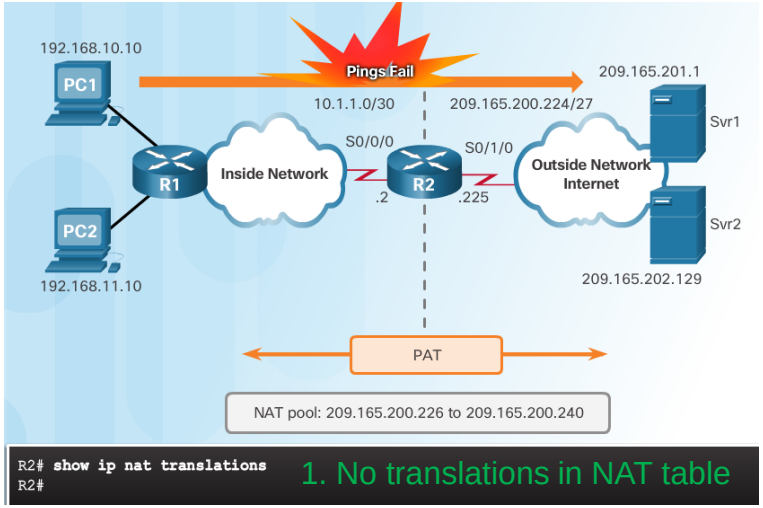

```
R2# show access-lists
Standard IP access list 1
  10 permit 192.168.0.0, wildcard bits 0.0.255.255 (29 matches)
```

NAT Troubleshooting Scenario

- Internal hosts cannot contact external servers.

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

R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```

2. Outside and inside interfaces are reversed




```
R2# show ip nat translations
R2#
```

1. No translations in NAT table

```
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
R2#

R2(config)# no access-list 1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

3. Incorrect ACL

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:37:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 20  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 1
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      Outside global
icmp 209.165.200.226:38 192.168.10.10:38  209.165.201.1:38   209.165.201.1:38
R2#
```

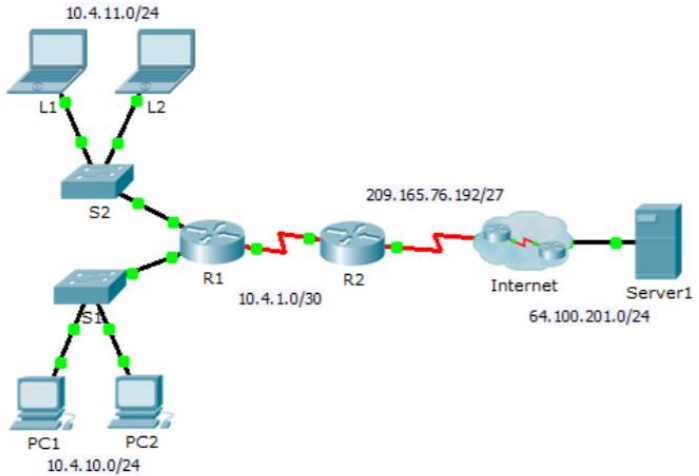
Translations working!

Packet Tracer – Verifying and Troubleshooting NAT Configurations

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Verifying and Troubleshooting NAT Configurations

Topology



Troubleshooting NAT Configurations

Cisco Networking Academy® Mind Wide Open™

Lab - Troubleshooting NAT Configurations

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Objectives

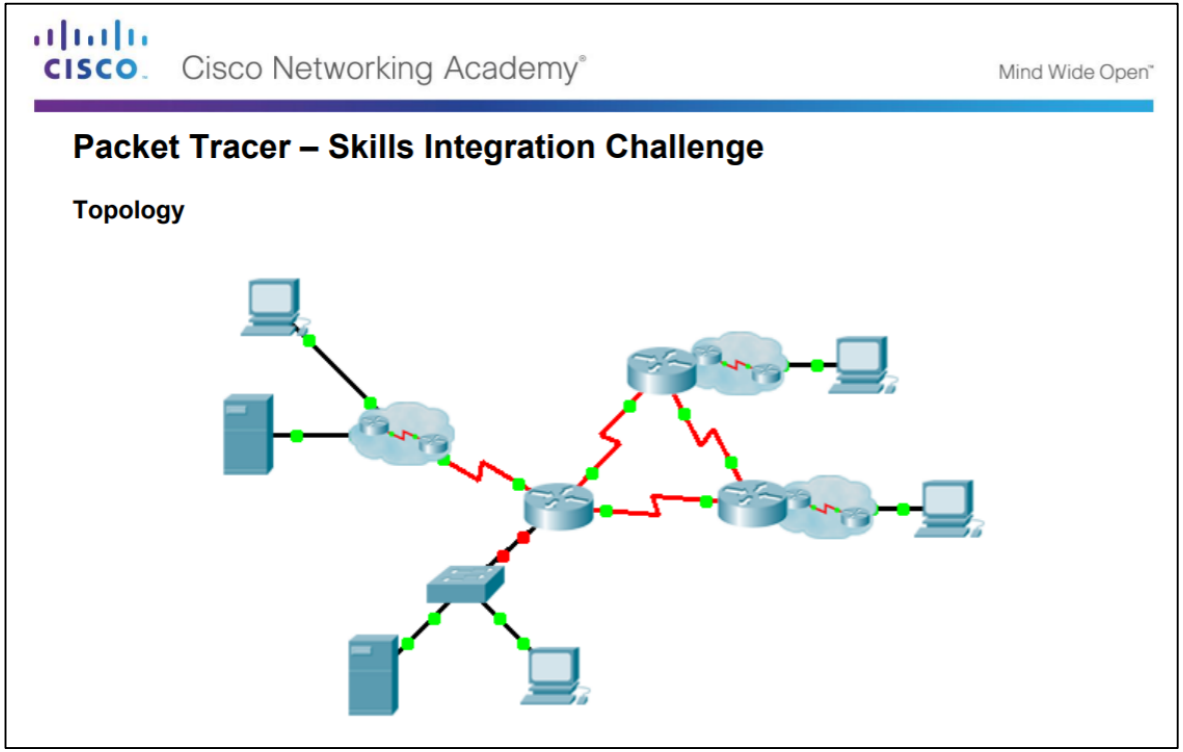
Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Static NAT

Part 3: Troubleshoot Dynamic NAT

9.4 Chapter Summary

Packet Tracer - Skills Integration Challenge



Chapter 9: NAT for IPv4

- Explain how NAT provides IPv4 address scalability in a small to medium-sized business network.
- Configure NAT services on the edge router to provide IPv4 address scalability in a small to medium-sized business network.
- Troubleshoot NAT issues in a small to medium-sized business network.


CISCO