# Network Address Translation

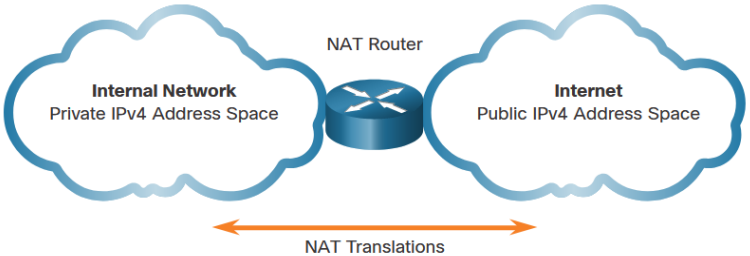
Dr. Md. Shohrab Hossain
Professor, CSE, BUET

Source: Cisco Networking

# IPv4 Address Space

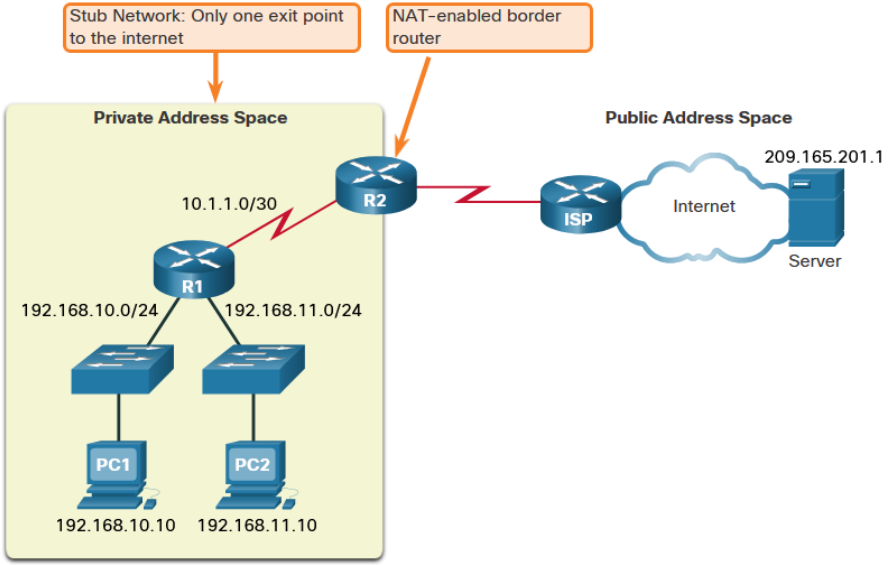
- Networks are commonly implemented using private IPv4 addresses, as defined in RFC 1918.
- Private IPv4 addresses cannot be routed over the internet and are used within an organization or site to allow devices to communicate locally.
- To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address.
- NAT provides the translation of private addresses to public addresses.

| Class | Activity Type | Activity Name |
|---|---|---|
| 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

- The primary use of NAT is to conserve public IPv4 addresses.
- NAT allows networks to use private IPv4 addresses internally and translates them to a public address when needed.
- A NAT router typically operates at the border of a stub network.
- When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router which performs the NAT process, translating the internal private address of the device to a public, outside, routable address.



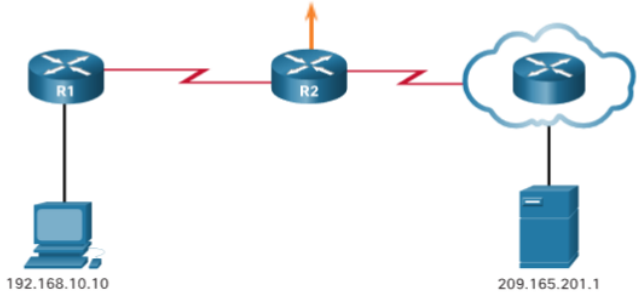
# How NAT Works

PC1 wants to communicate with an outside web server with public address 209.165.201.1.

1. PC1 sends a packet addressed to the web server.
2. R2 receives the packet and reads the source IPv4 address to determine if it needs translation.
3. R2 adds mapping of the local to global address to the NAT table.
4. R2 sends the packet with the translated source address toward the destination.
5. The web server responds with a packet addressed to the inside global address of PC1 (209.165.200.226).
6. R2 receives the packet with destination address 209.165.200.226. R2 checks the NAT table and finds an entry for this mapping. R2 uses this information and translates the inside global address (209.165.200.226) to the inside local address (192.168.10.10), and the packet is forwarded toward PC1.

**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 Terminology

NAT includes four types of addresses:

- Inside local address
- Inside global address
- Outside local address
- Outside global address

NAT terminology is always applied from the perspective of the device with the translated address:

- **Inside address** - The address of the device which is being translated by NAT.
- **Outside address** - The address of the destination device.
- **Local address** - A local address is any address that appears on the inside portion of the network.
- **Global address** - A global address is any address that appears on the outside portion of the network.

# NAT Terminology (Cont.)

**Inside local address**

The address of the source as seen from inside the network. This is typically a private IPv4 address. The inside local address of PC1 is 192.168.10.10.

**Inside global addresses**

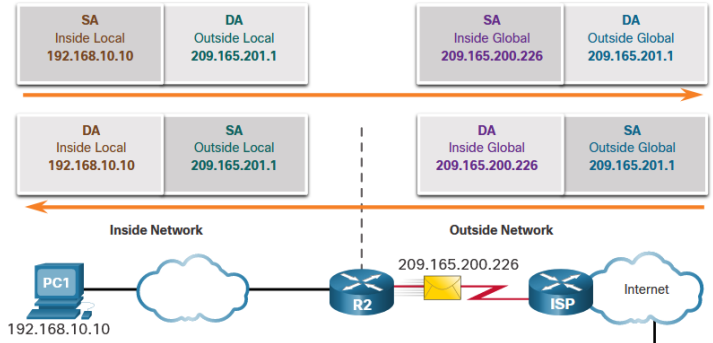
The address of source as seen from the outside network. The inside global address of PC1 is 209.165.200.226

**Outside global address**

The address of the destination as seen from the outside network. The outside global address of the web server is 209.165.201.1

**Outside local address**

The address of the destination as seen from the inside network. PC1 sends traffic to the web server at the IPv4 address 209.165.201.1. While uncommon, this address could be different than the globally routable address of the destination.



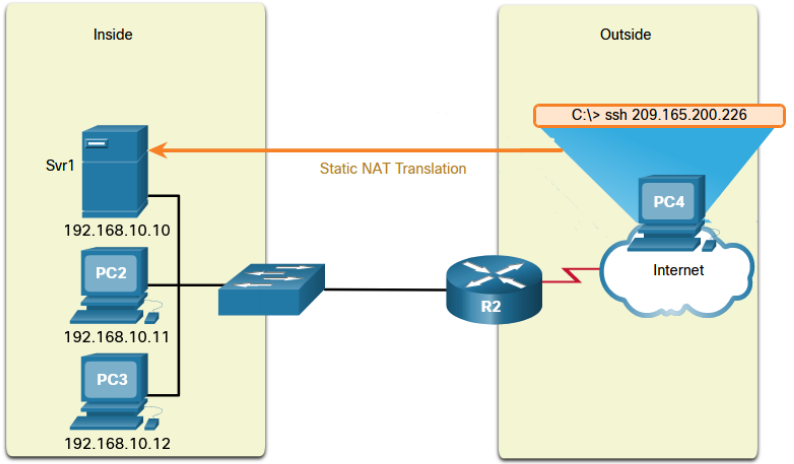

| R2 NAT Table | | | |
|---|---|---|---|
| **PC1** | | **Web Server** | |
| **Inside Global Address** | **Inside Local Address** | **Outside Local Address** | **Outside Global Address** |
| **209.165.200.226** | **192.168.10.10** | **209.165.201.1** | **209.165.201.1** |

# Types of NAT

# Static NAT

Static NAT uses a one-to-one mapping of local and global addresses configured by the network administrator that remain constant.

- Static NAT is useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server.
- It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the internet.




**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 |

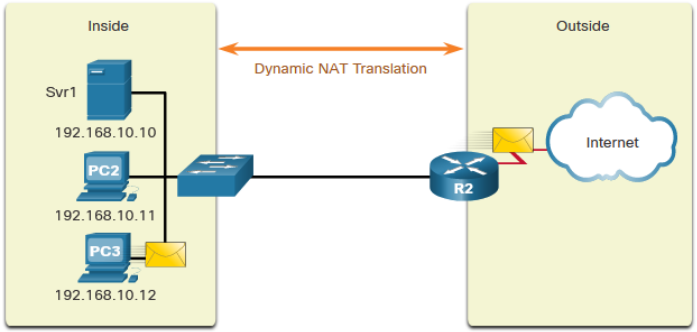
**Note**: Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

# 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.
- The other addresses in the pool are still available for use.

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

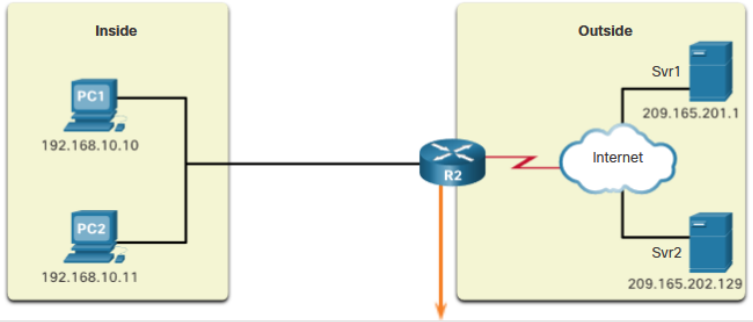



| IPv4 NAT Pool | |
|---|---|
| **Inside Local Address** | **Inside Global Address Pool - Addresses reachable via R2** |
| 192.168.10.12 | 209.165.200.226 |
| Available | 209.165.200.227 |
| Available | 209.165.200.228 |
| Available | 209.165.200.229 |
| Available | 209.165.200.230 |

# Port Address Translation

Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.

- With PAT, when the NAT router receives a packet from the client, it uses the source port number to uniquely identify the specific NAT translation.
- PAT ensures that devices use a different TCP port number for each session with a server on the internet.



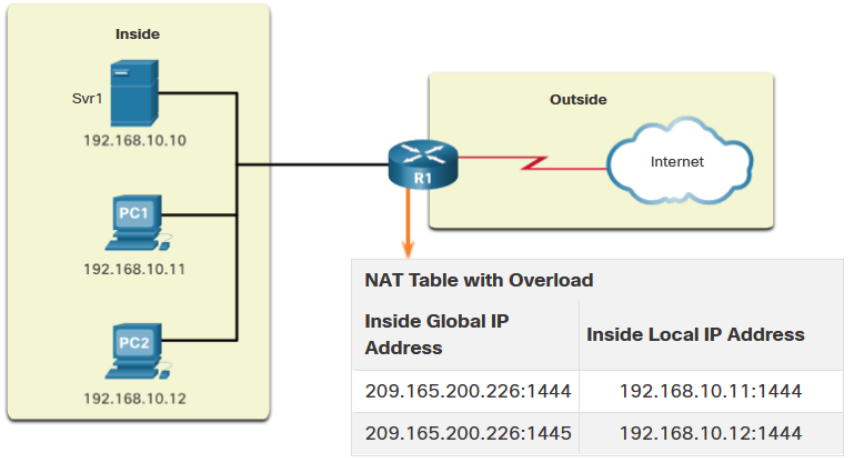

**NAT Table with Overload**

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

# Next Available Port

PAT attempts to preserve the original source port. If the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0-511, 512-1,023, or 1,024-65,535.

- When there are no more ports available and there is more than one external address in the address pool, PAT moves to the next address to try to allocate the original source port.
- The process continues until there are no more available ports or external IPv4 addresses in the address pool.



# NAT and PAT Comparison

Summary of the differences between NAT and PAT.

**NAT** - Only modifies the IPv4 addresses

| Inside Global Address | Inside Local Address |
|---|---|
| 209.165.200.226 | 192.168.10.10 |

**PAT** - PAT modifies both the IPv4 address and the port number.

| Inside Global Address | Inside Local Address |
|---|---|
| 209.165.200.226:2031 | 192.168.10.10:2031 |

| NAT | PAT |
|---|---|
| One-to-one mapping between Inside Local and Inside Global addresses. | One Inside Global address can be mapped to many Inside Local addresses. |
| Uses only IPv4 addresses in translation process. | Uses IPv4 addresses and TCP or UDP source port numbers in translation process. |
| A unique Inside Global address is required for each inside host accessing the outside network. | A single unique Inside Global address can be shared by many inside hosts accessing the outside network. |

# Advantages of NAT

NAT provides many benefits:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.
- NAT conserves addresses through application port-level multiplexing.
- NAT increases the flexibility of connections to the public network.
- NAT provides consistency for internal network addressing schemes.
- NAT allows the existing private IPv4 address scheme to remain while allowing for easy change to a new public addressing scheme.
- NAT hides the IPv4 addresses of users and other devices.

# Disadvantages of NAT

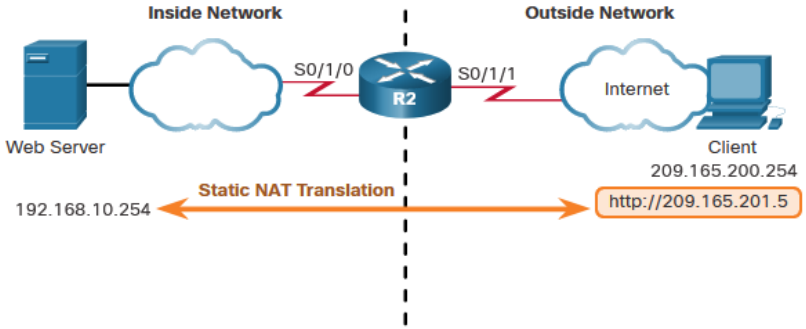
NAT does have drawbacks:

- NAT increases forwarding delays.
- End-to-end addressing is lost.
- End-to-end IPv4 traceability is lost.
- NAT complicates the use of tunneling protocols, such as IPsec.
- Services that require the initiation of TCP connections from the outside network, or stateless protocols, such as those using UDP, can be disrupted.

# Static NAT

# Static NAT Scenario

- Static NAT is a one-to-one mapping between an inside address and an outside address.
- Static NAT allows external devices to initiate connections to internal devices using the statically assigned public address.
- For instance, an internal web server may be mapped to a specific inside global address so that it is accessible from outside networks.



# Configure Static NAT

There are two basic tasks when configuring static NAT translations:

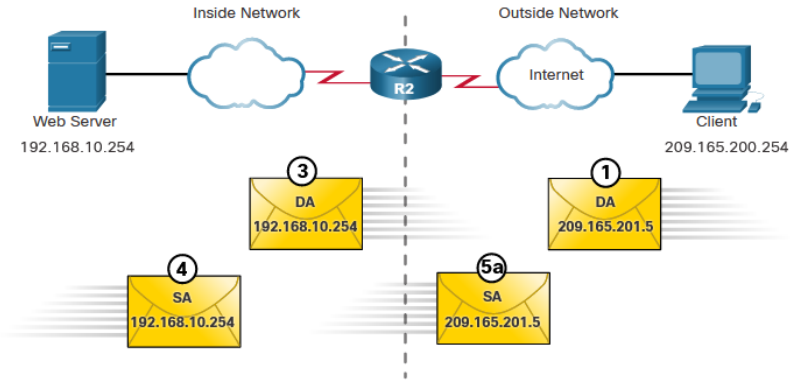
- **Step 1** - Create a mapping between the inside local address and the inside global addresses using the **ip nat inside source static** command.
- **Step 2** - The interfaces participating in the translation are configured as inside or outside relative to NAT with the **ip nat inside** and **ip nat outside** commands.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

# Analyze Static NAT

The static NAT translation process between the client and the web server:

1. The client sends a packet to the web server.
2. R2 receives packets from the client on its NAT outside interface and checks its NAT table.
3. R2 translates the inside global address of to the inside local address and forwards the packet towards the web server.
4. The web server receives the packet and responds to the client using its inside local address.
5. (a) R2 receives the packet from the web server on its NAT inside interface with source address of the inside local address of the web server and (b) translates the source address to the inside global address.




| | Inside Local Address | Inside Global Address | Outside Local Address | Outside Global Address |
|---|---|---|---|---|
| 2 5b | 192.168.10.254 | 209.165.201.5 | 209.165.200.254 | 209.165.200.254 |

# Verify Static NAT

To verify NAT operation, issue the **show ip nat translations** command.

- This command shows active NAT translations.
- Because the example is a static NAT configuration, the translation is always present in the NAT table regardless of any active communications.
- If the command is issued during an active session, the output also indicates the address of the outside device.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local     Outside global
---  209.165.201.5       192.168.10.254     ---               ---
Total number of translations: 1
```

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local         Outside global
tcp  209.165.201.5       192.168.10.254     209.165.200.254       209.165.200.254
---  209.165.201.5       192.168.10.254       ---                   ---
Total number of translations: 2
```

# Verify Static NAT (Cont.)

Another useful command is **show ip nat statistics.**

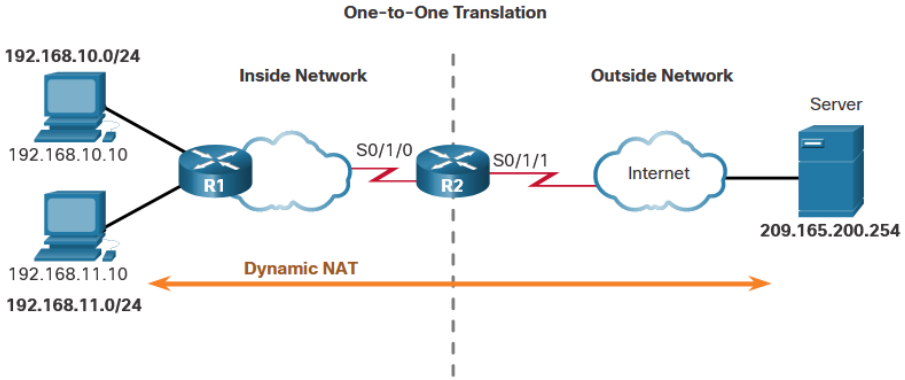
- It displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number of addresses that have been allocated.
- To verify that the NAT translation is working, it is best to clear statistics from any past translations using the **clear ip nat statistics** command before testing.

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 1
(output omitted)
```

# Dynamic NAT

# Dynamic NAT Scenario

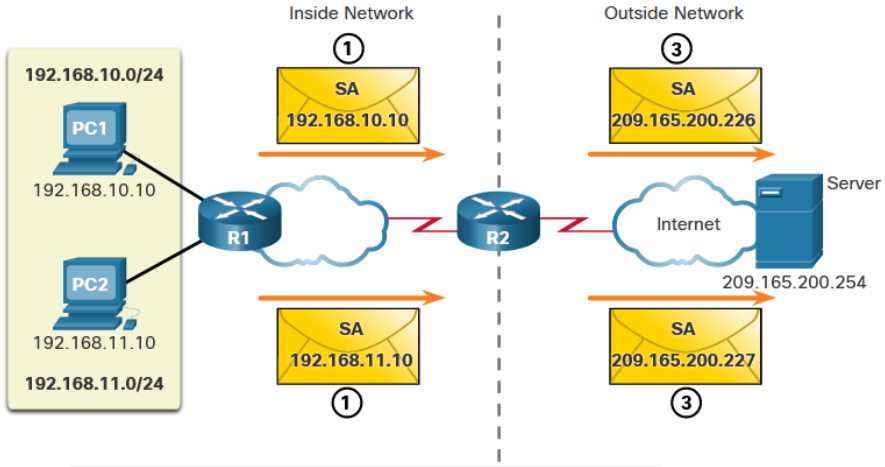
- Dynamic NAT automatically maps inside local addresses to inside global addresses.
- Dynamic NAT uses a pool of inside global addresses.
- The pool of inside global addresses is available to any device on the inside network on a first-come first-served basis.
- If all addresses in the pool are in use, a device must wait for an available address before it can access the outside network.



# Analyze Dynamic NAT – Inside to Outside

Dynamic NAT translation process:

1. PC1 and PC2 send packets requesting a connection to the server.
2. R2 receives the first packet from PC1, checks the ALC to determine if the packet should be translated, selects an available global address, and creates a translation entry in the NAT table.
3. R2 replaces the inside local source address of PC1, 192.168.10.10, with the translated inside global address of 209.165.200.226 and forwards the packet. (The same process occurs for the packet from PC2 using the translated address of 209.165.200.227.)




| 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 |

# Configure Dynamic NAT

There are five tasks when configuring dynamic NAT translations:

- **Step 1** - Define the pool of addresses that will be used for translation using the **ip nat pool** command.
- **Step 2** - Configure a standard ACL to identify (permit) only those addresses that are to be translated.
- **Step 3** - Bind the ACL to the pool, using the **ip nat inside source list** command.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

# Configure Dynamic NAT (Cont.)

There are five tasks when configuring dynamic NAT translations:

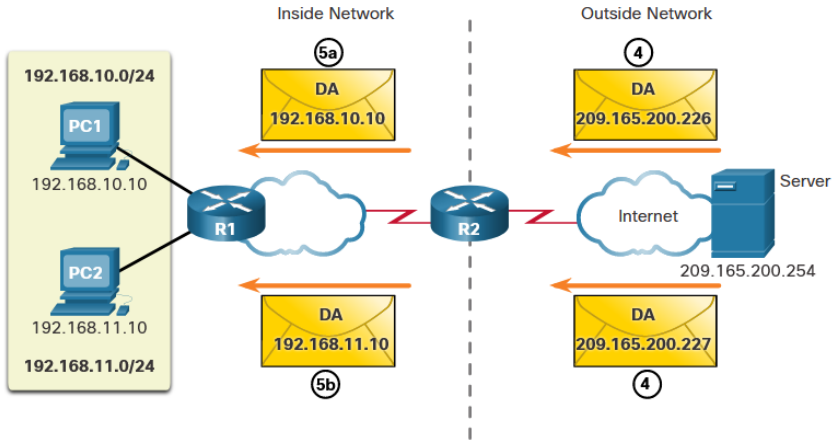
- **Step 4** - Identify which interfaces are inside.
- **Step 5** - Identify which interfaces are outside.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

# Analyze Dynamic NAT – Outside to Inside

## Dynamic NAT translation process:

4. The server receives the packet from PC1 and responds using the destination address of 209.165.200.226. The server receives the packet from PC2, it responds to using the destination address of 209.165.200.227.
5. (a) When R2 receives the packet with the destination address of 209.165.200.226; it performs a NAT table lookup and translates the address back to the inside local address and forwards the packet toward PC1.
   (b) When R2 receives the packet with the destination address of 209.165.200.227; it performs a NAT table lookup and translates the address back to the inside local address 192.168.11.10 and forwards the packet toward PC2.




| | IPv4 NAT Pool | |
|---|---|---|
| | **Inside Local Address Pool** | **Inside Global Address** |
| 5a | 192.168.10.10 | 209.165.200.226 |
| 5b | 192.168.11.10 | 209.165.200.227 |

# Verify Dynamic NAT

The output of the **show ip nat translations** command displays all static translations that have been configured and any dynamic translations that have been created by traffic.

```
R2# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.228    192.168.10.10      ---                ---
--- 209.165.200.229    192.168.11.10      ---                ---
R2#
```

# Verify Dynamic NAT (Cont.)

By default, translation entries time out after 24 hours, unless the timers have been reconfigured with the **ip nat translation timeout** *timeout-seconds* command in global configuration mode. To clear dynamic entries before the timeout has expired, use the **clear ip nat translation** privileged EXEC mode command.

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

| 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*] | Clears 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. |

# PAT

# Configure PAT to Use a Single IPv4 Address

To configure PAT to use a single IPv4 address, add the keyword **overload** to the **ip nat inside source** command.

In the example, all hosts from network 192.168.0.0/16 (matching ACL 1) that send traffic through router R2 to the internet will be translated to IPv4 address 209.165.200.225 (IPv4 address of interface S0/1/1). The traffic flows will be identified by port numbers in the NAT table because the **overload** keyword is configured.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/1
R2(config-if)# ip nat outside
```

# Configure PAT to Use an Address Pool

An ISP may allocate more than one public IPv4 address to an organization. In this scenario the organization can configure PAT to use a pool of IPv4 public addresses for translation.

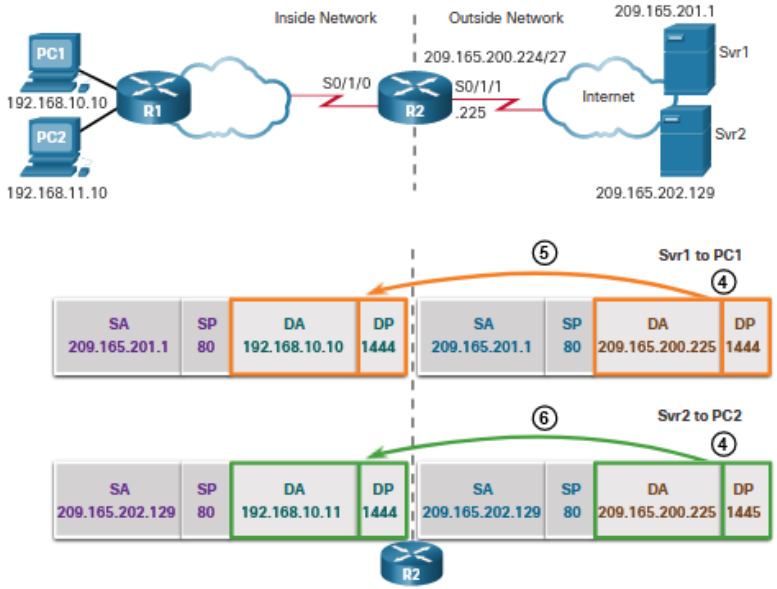
To configure PAT for a dynamic NAT address pool, simply add the keyword **overload** to the **ip nat inside source** command.

In the example, NAT-POOL2 is bound to an ACL to permit 192.168.0.0/16 to be translated. These hosts can share an IPv4 address from the pool because PAT is enabled with the keyword **overload**.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial0/1/0
R2(config-if)# ip nat outside
```

# Analyze PAT – Server to PC

1. PC1 and PC2 send packets to Svr1 and Svr2.
2. The packet from PC1 reaches R2 first. R2 modifies the source IPv4 address to 209.165.200.225 (inside global address). The packet is then forwarded towards Svr1.
3. The packet from PC2 arrives at R2. PAT changes the source IPv4 address of PC2 to the inside global address 209.165.200.225. PC2 has the same source port number as the translation for PC1. PAT increments the source port number until it is a unique value in its table. In this instance, 1445.

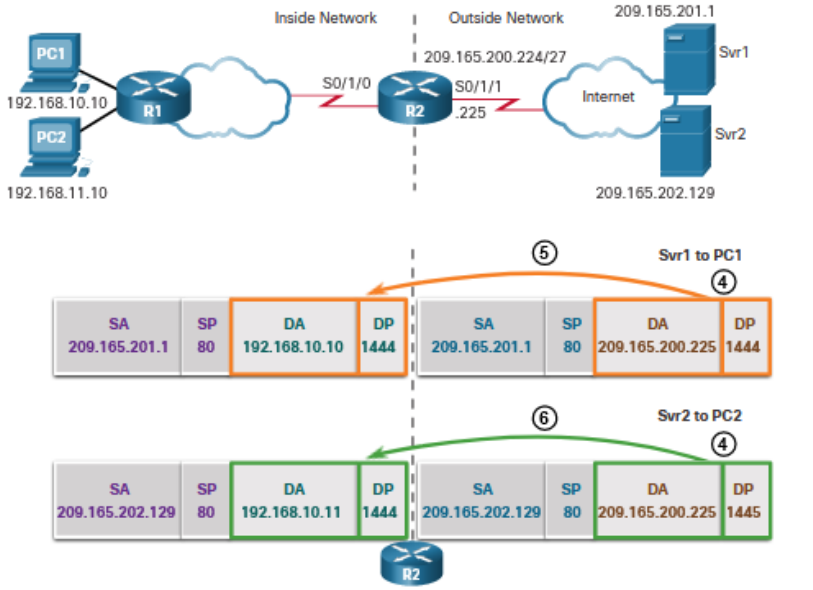



**NAT Table**

| 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 | 209.165.201.129:80 | 209.165.202.129:80 |

# Analyze PAT – PC to Server

1. PC1 and PC2 send packets to Svr1 and Svr2.
2. The packet from PC1 reaches R2 first. R2 modifies the source IPv4 address to 209.165.200.225 (inside global address). The packet is then forwarded towards Svr1.
3. The packet from PC2 arrives at R2. PAT changes the source IPv4 address of PC2 to the inside global address 209.165.200.225. PC2 has the same source port number as the translation for PC1. PAT increments the source port number until it is a unique value in its table. In this instance, it is 1445.

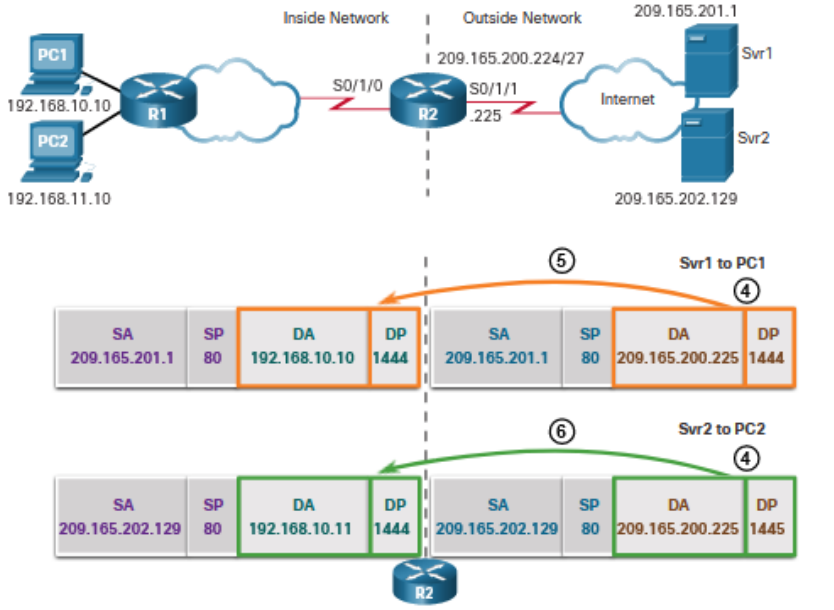



**NAT Table**

| 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 | 209.165.201.129:80 | 209.165.202.129:80 |

# Analyze PAT – Server to PC

1. The servers use the source port from the received packet as the destination port, and the source address as the destination address for the return traffic.
2. R2 changes the destination IPv4 address of the packet from Srv1 from 209.165.200.225 to 192.168.10.10, and forwards the packet toward PC1.
3. R2 changes the destination address of packet from Srv2. from 209.165.200.225 to 192.168.10.11. and modifies the destinations port back to its original value of 1444. The packet is then forwarded toward PC2.




**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 | 209.165.201.129:80 | 209.165.202.129:80 |

# Verify PAT

The same commands used to verify static and dynamic NAT are used to verify PAT. The **show ip nat translations** command displays the translations from two different hosts to different web servers. Notice that two different inside hosts are allocated the same IPv4 address of 209.165.200.226 (inside global address). The source port numbers in the NAT table differentiate the two transactions.

```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local      Outside global
tcp 209.165.200.225:1444  192.168.10.10:1444  209.165.201.1:80   209.165.201.1:80
tcp 209.165.200.225:1445  192.168.11.10:1444  209.165.202.129:80 209.165.202.129:80
R2#
```