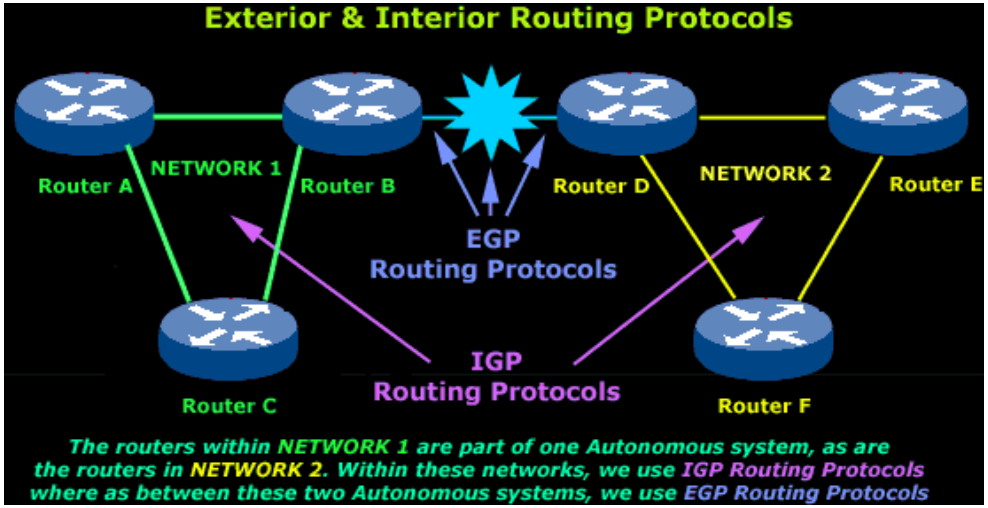
CIS 3210
Network Address Translation



NAT Operation

Internet Concerns

- There are not enough public IPv4 addresses to assign a unique address to each device connected to the Internet.
  - In 1990, the IETF was concerned with this limited supply of IPv4 addresses.

- Therefore the IETF developed several solutions to help stave off this depletion of global IPv4 addresses:
  - Subnetting
  - Variable-length subnet masking (VLSM)
  - Classless interdomain routing (CIDR)
  - Route summarization
  - Private addressing and NAT
  - Long term solution: IP version 6 (IPv6)

Private Addresses

- The IETF developed RFC 1918 which identified three IPv4 address ranges that were deemed as “Private”.

- Specifically, RFC 1918 identified these three ranges:

Class	RFC 1918 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

Private Addresses

- Private addresses are used within an organization to allow devices to communicate locally.
- However, private IPv4 addresses can't be routed over the Internet.
  - Private addresses have no global significance.
  - Internet routers filter private addresses and drop the traffic.
- So how do internal computers access the Internet?

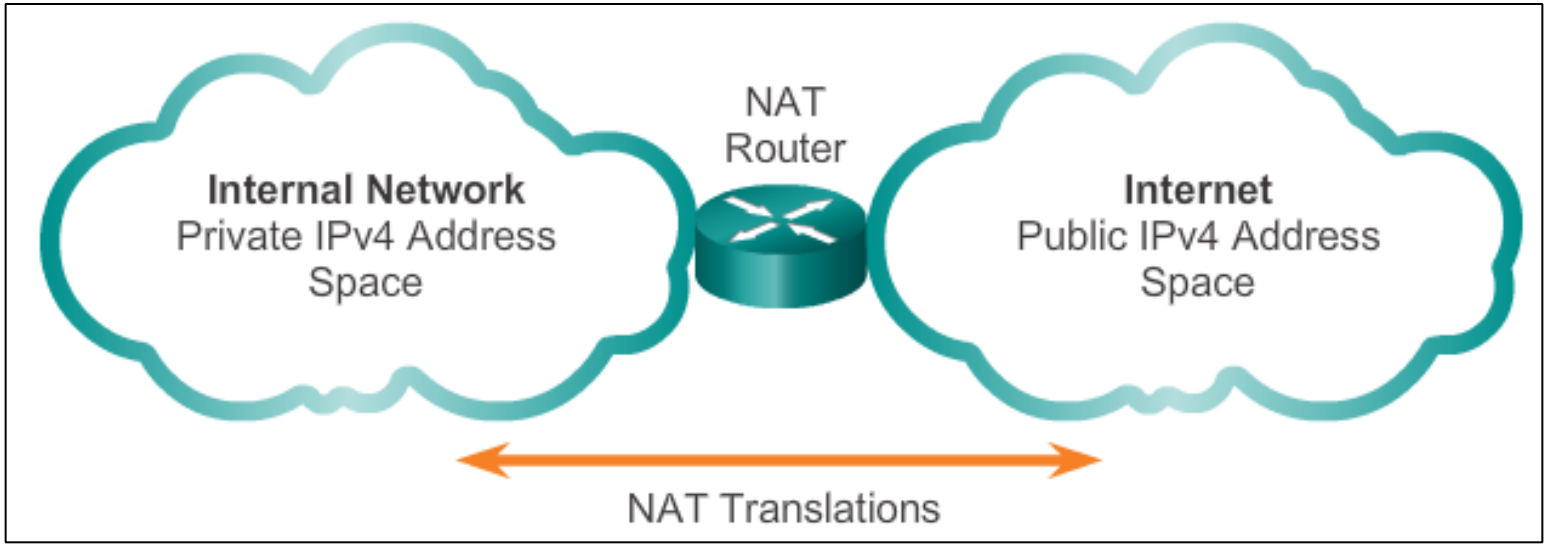
Network Address Translation (NAT)

- To provide Internet access to private hosts, the IETF developed RFC 1631: *The IP Network Address Translator (NAT)*.

- NAT and private addresses helped IPv4 fight off address depletion.
  - Without NAT, the exhaustion of the IPv4 address space would have occurred by the year 2000.

Network Address Translation (NAT)

- NAT translates the internal private address into a valid external public address.
  - Used to provide corporate hosts access to the Internet.
  - Also used to provide Internet access to home networks.



- NAT swaps the private source IP address for a public IP address.

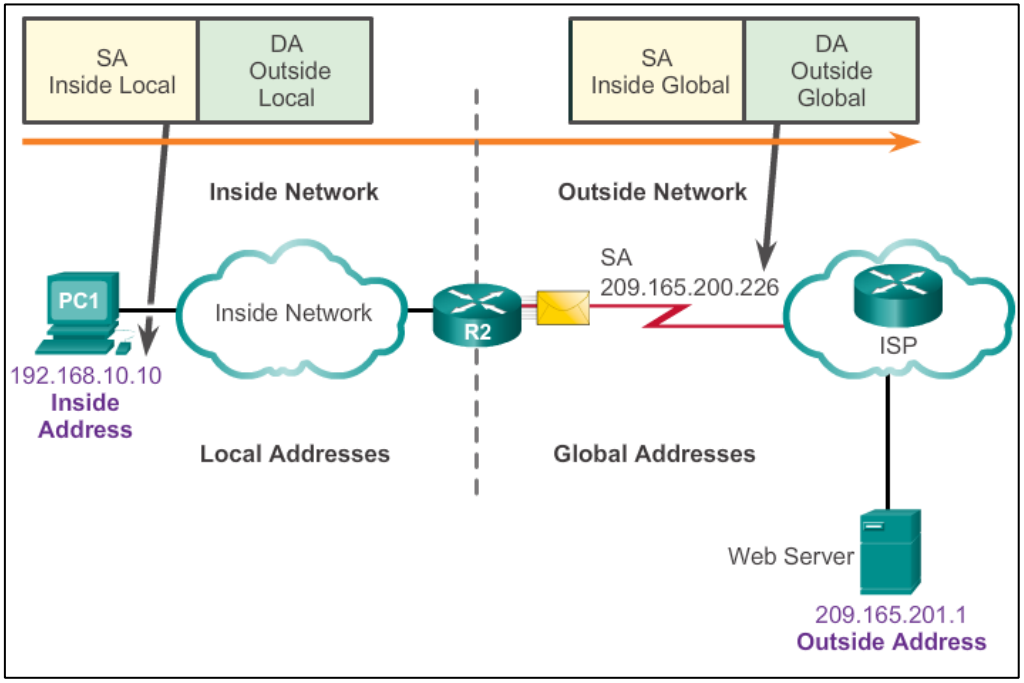
NAT Advantages / Disadvantages

Advantages	Disadvantages
Conserves legally registered addresses	Translation may introduce switching path delays
Increases flexibility when connecting to Internet	Loss of end-to-end IP traceability
Hides IP addresses inside the network from outside users	Certain applications will not function with NAT enabled
Can handle network with overlapping addresses	Requires memory to maintain translation table
Eliminates address renumbering as network changes	

NAT Terminology

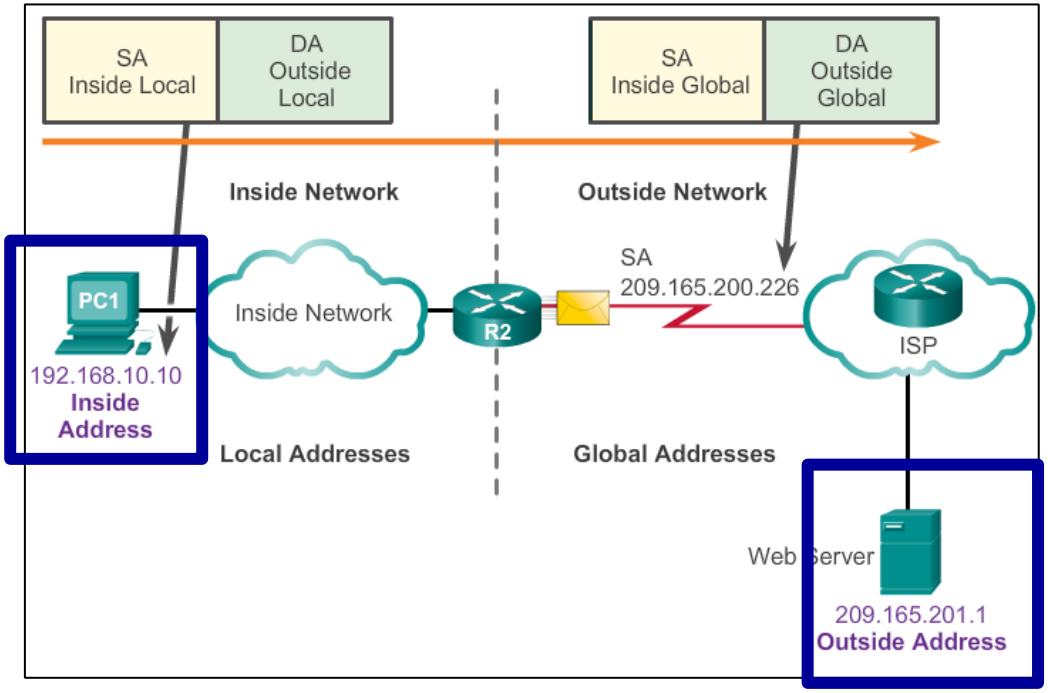
NAT Terminology

- **Inside network** is the set of devices using private addresses



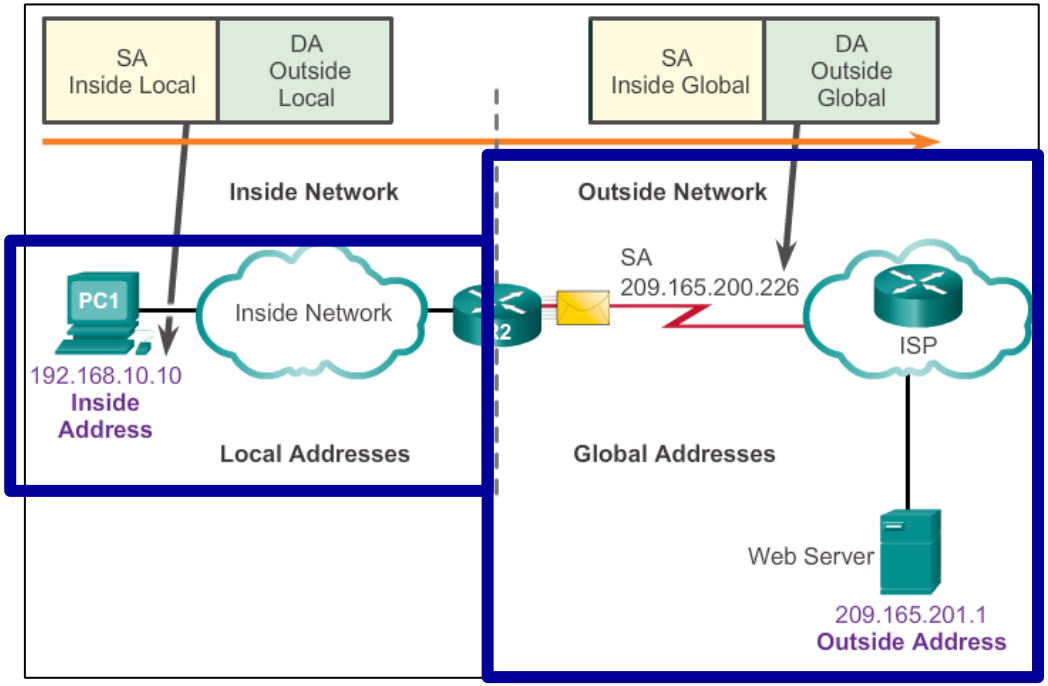
- **Outside network** refers to all other networks

NAT Terminology



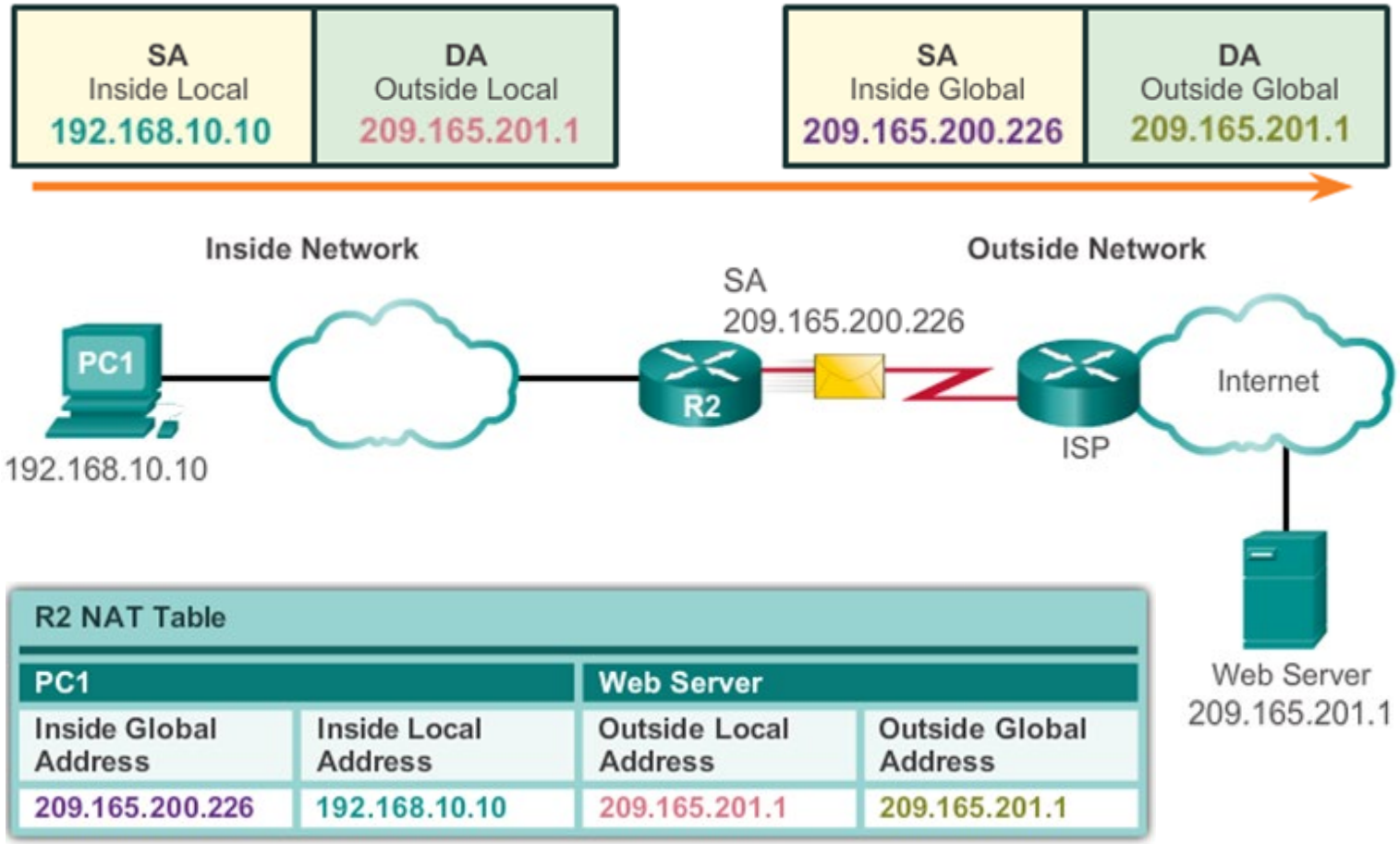
- NAT terminology is always applied from the perspective of the device with the translated address:
  - **Inside address**: The address of the device which is being translated by NAT.
  - **Outside address**: The address of the destination device.

NAT Terminology



- NAT also uses the concept of local or global with respect to addresses:
  - **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.

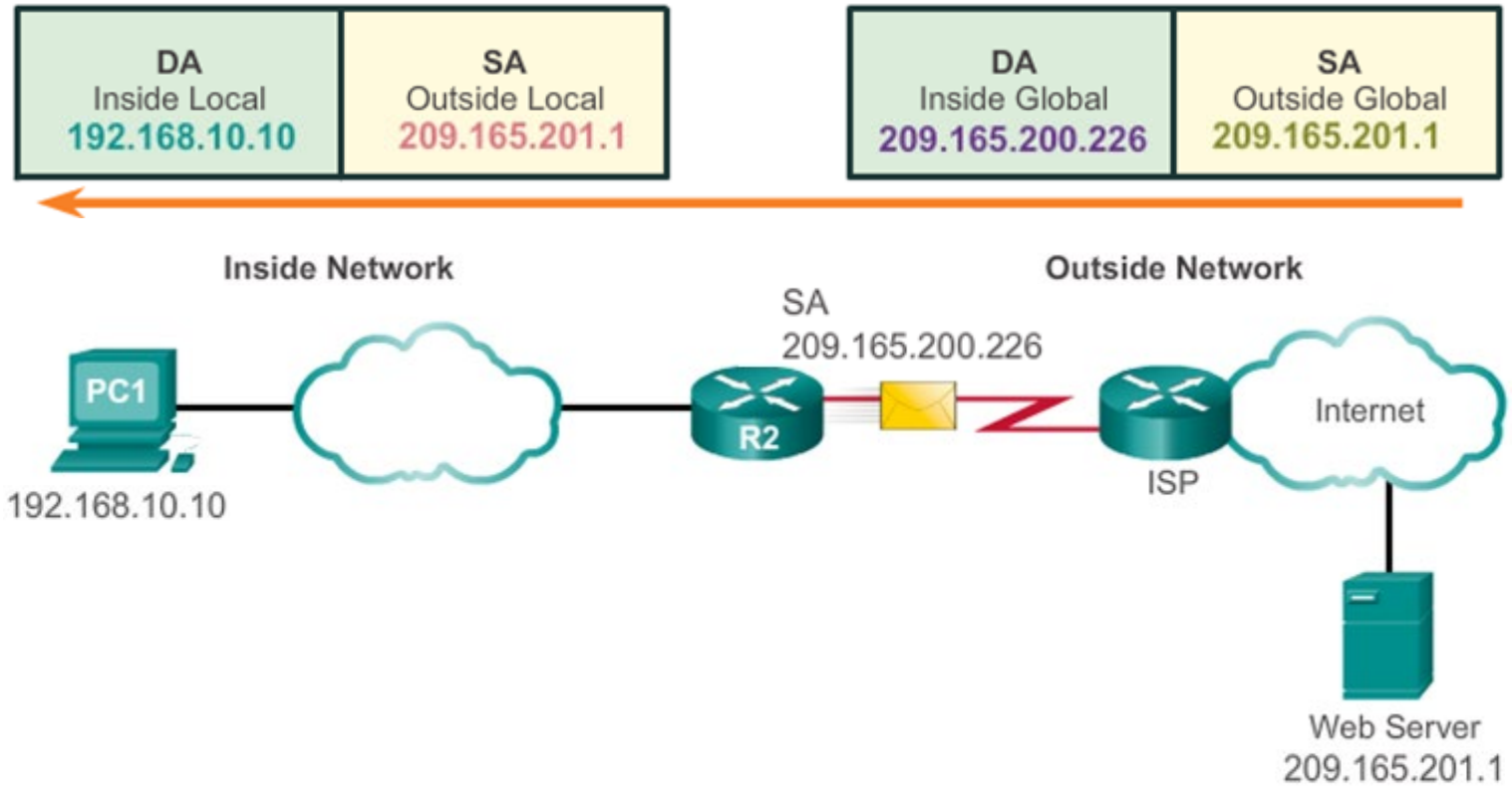
NAT Terminology Example



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

NAT Terminology Example



Three Types of NAT Applications

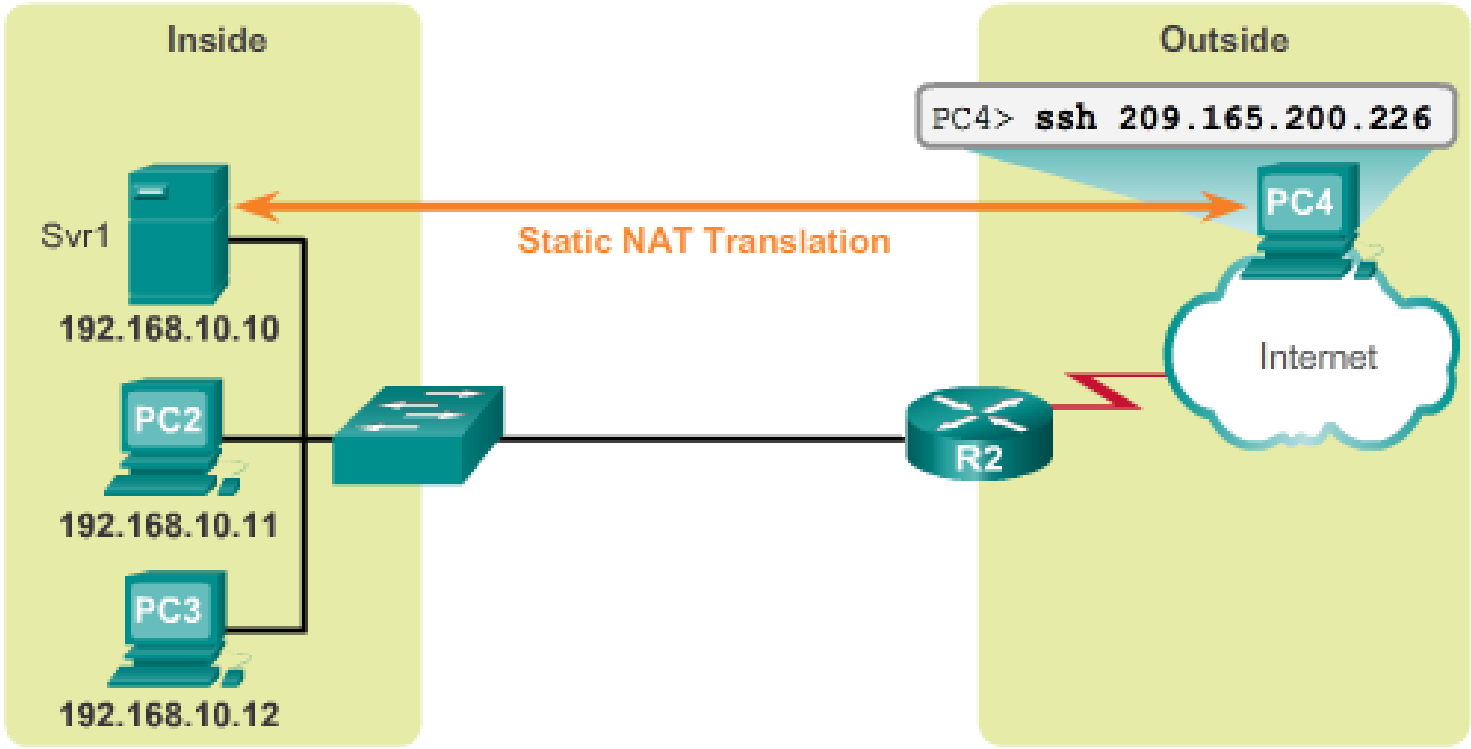
- **Static address translation (static NAT)**:
  - One-to-one address mapping between local and global addresses.
- **Dynamic address translation (dynamic NAT)**:
  - Many-to-many address mapping between local and global addresses.
- **Port Address Translation (PAT)**:
  - Many-to-one address mapping between local and global addresses.
  - This method is also known as overloading (NAT overloading).

Static NAT

Static NAT

- Permanently bind an inside local address to an inside global address.
- Mappings are configured by the administrator and remain constant.
- Typically used to configure an internal server that must be accessed from the outside world.

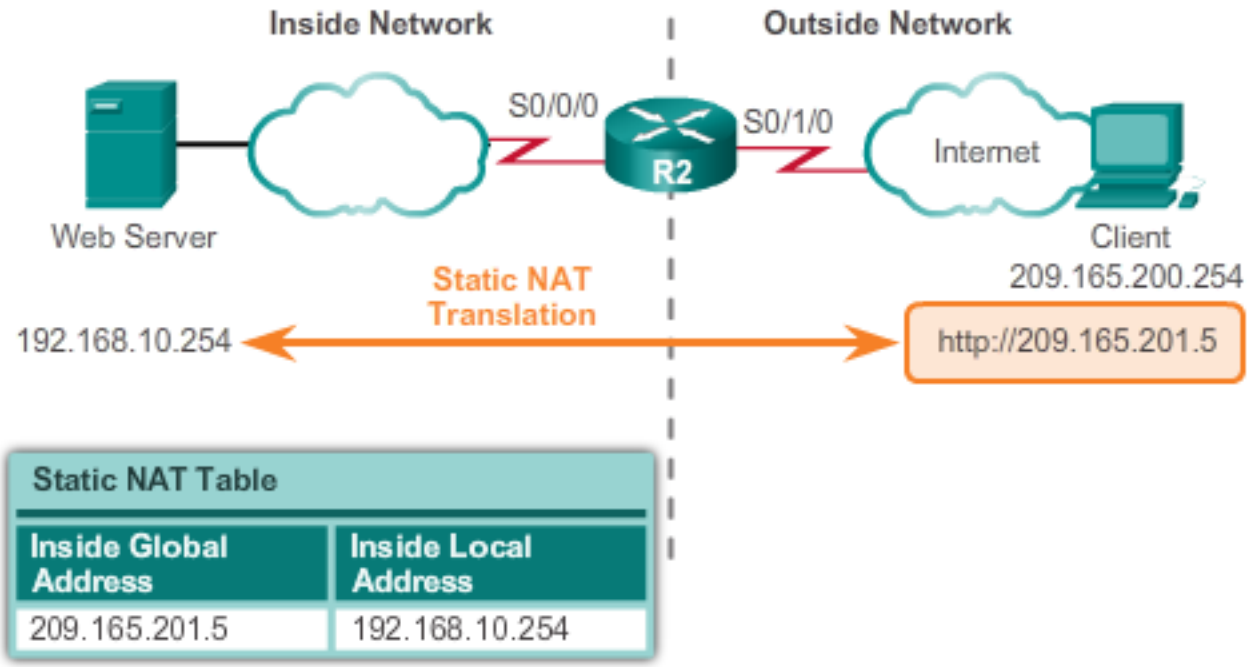
Static NAT



Static NAT Table

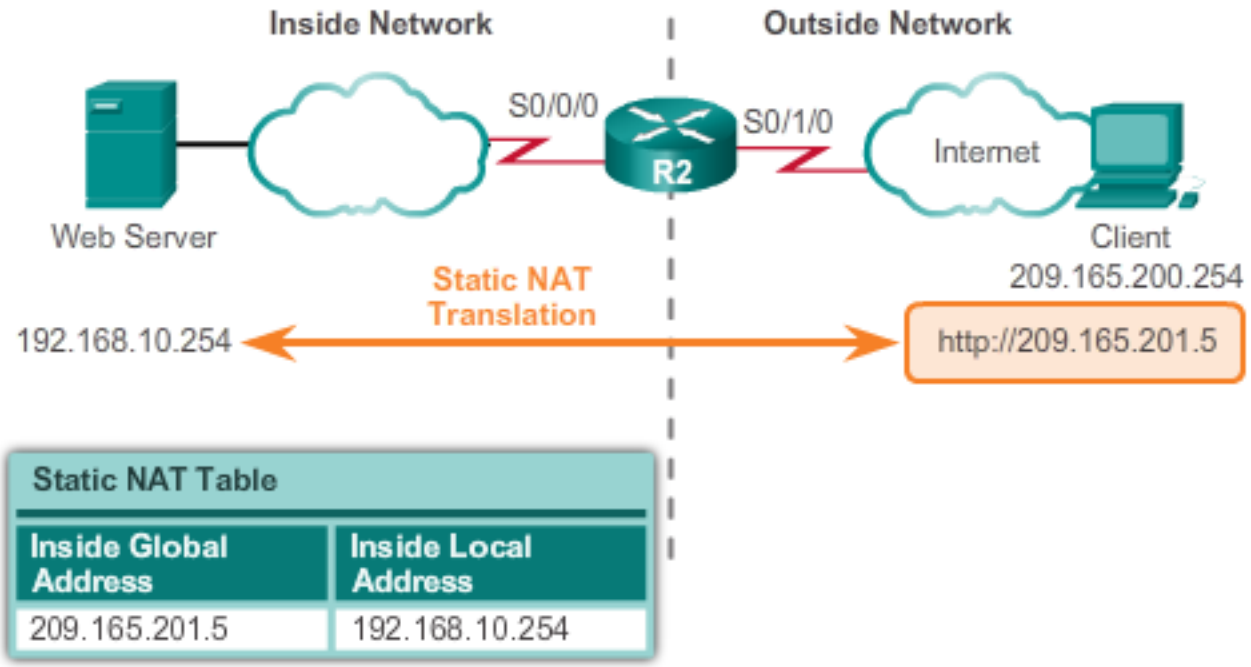
Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Configuring Static NAT Example




```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
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
R2(config-if)# ip nat outside
R2(config-if)#
```

Verifying Static NAT Example




```
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#
```

Verifying Static NAT Example

```
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

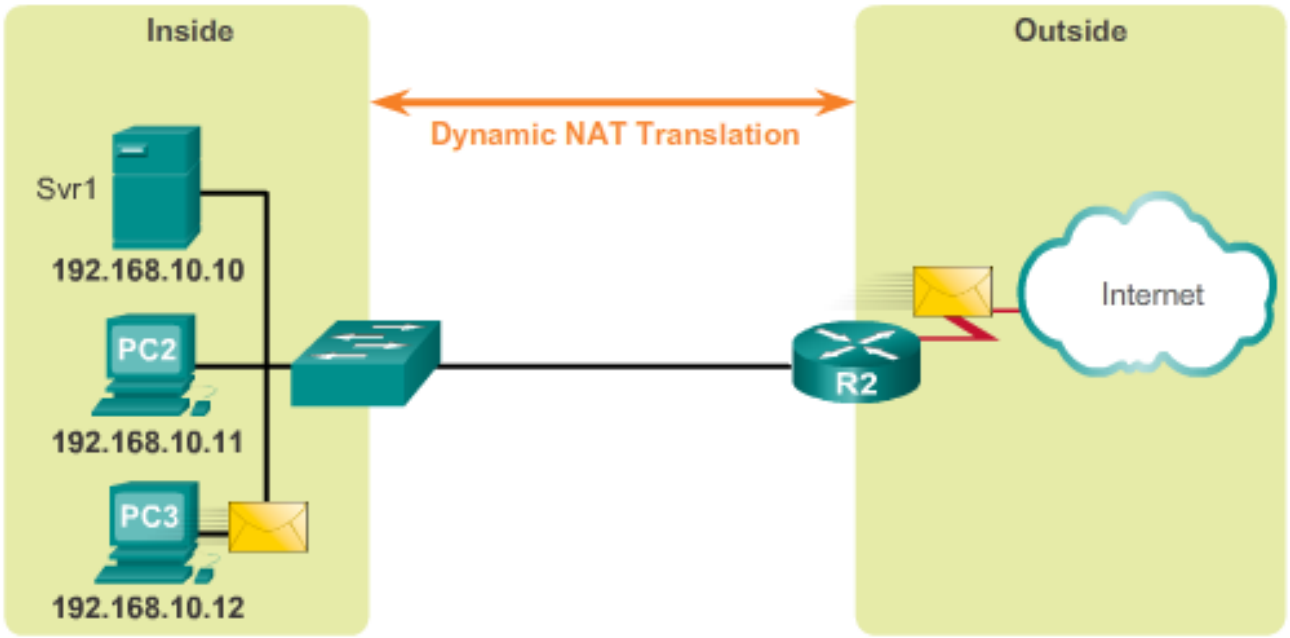
```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0

<Output omitted>
```

Dynamic NAT

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 the inside local address an inside global address from a pool of addresses.

Dynamic NAT Example



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

Dynamic NAT Configuration Steps

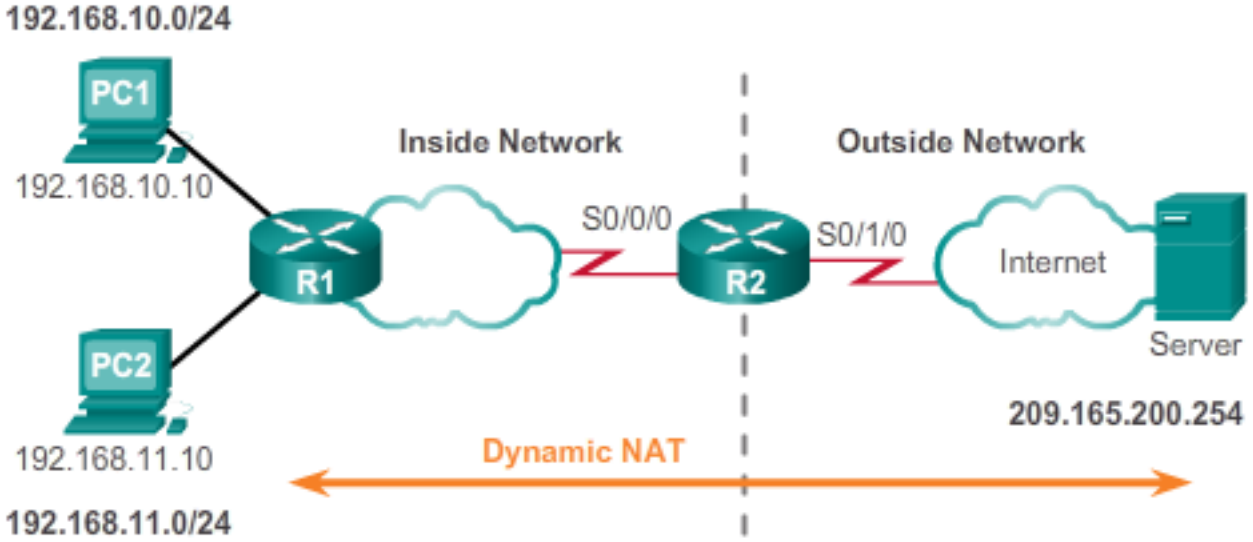
1. Define the pool of addresses that will be used for translation.
   - Configured using the **`ip nat pool`** *`pool-name start-ip end-ip`* {**`netmask`** *`netmask`* | **`prefix-length`** *`prefix-length`*} global configuration command.

2. Configure a standard ACL to identify (permit) only those addresses that are to be translated.

3. Bind the ACL to the pool.
   - Configured using the **`ip nat inside source list`** *`acl-#`* **`pool`** *`pool-name`* global config command.

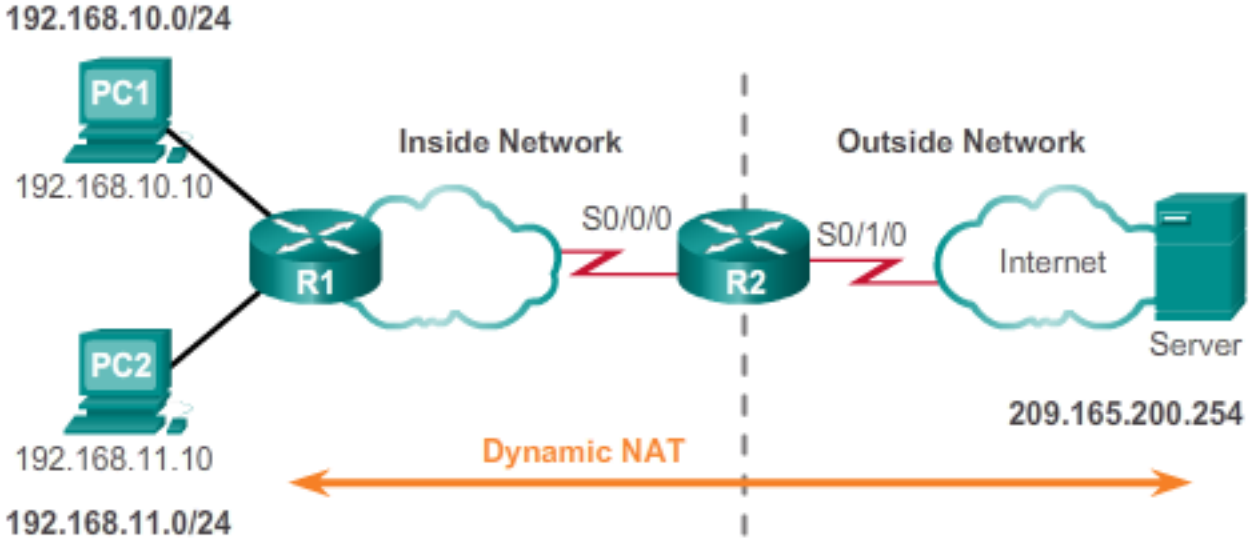
4. Identify the inside and outside NAT interfaces.
   - Configured using the **`ip nat inside`** and **`ip nat outside`** interface configuration commands.

Configuring Dynamic NAT Example




```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask
255.255.255.224
R2(config)#
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)#
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Verifying Dynamic NAT Example




```
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#
```

Verifying Dynamic NAT Example

```
R2# clear ip nat statistics
R2#
<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#
```

Dynamic NAT Timeout

```
Router(config)# ip nat translation timeout sec
Router(config)# ip nat translation timeout 120
```

It is useful to use the **clear ip nat translations *** before verifying translations.

- Dynamic translations are temporary, and will eventually time out (default 24 hours).
  - Timeout can be configured.
    - It is important for translation table entries to time out so that addresses in the pool become available for other hosts.
    - If translation table entries do not time out fast enough, the entire pool of addresses could be in use.

Address Port Address Translation (PAT)

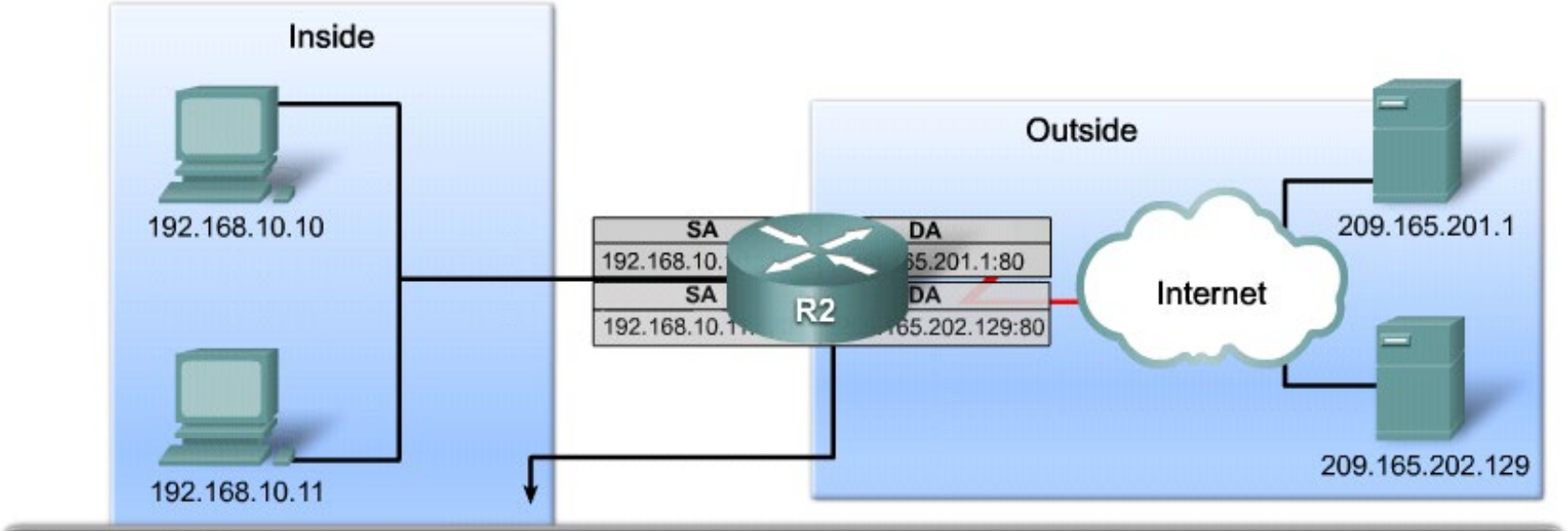
NAT Overload (PAT)

- PAT (also called NAT overload) allows the router to use one inside global address for many inside local addresses.
  - With address overloading, many privately addressed nodes can access the Internet using a single global address.

- There are two ways to configure PAT:
  - ISP allocates a single public IPv4 address
  - ISP allocates more than one public IPv4 address

- **Note**:
  - Over 65,000 inside addresses can theoretically map to a single outside address.
  - However, 4000 local addresses per global address is more realistic.
  - Each NAT translation consumes about 160 bytes of router DRAM.

NAT Overload (PAT)



NAT Table with Overload			
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address	Outside Local 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

- The NAT router keeps track of the different conversations by mapping TCP and UDP port numbers in the translation table.
  - Called an extended table entry.

Steps for Configuring PAT Using a Pool

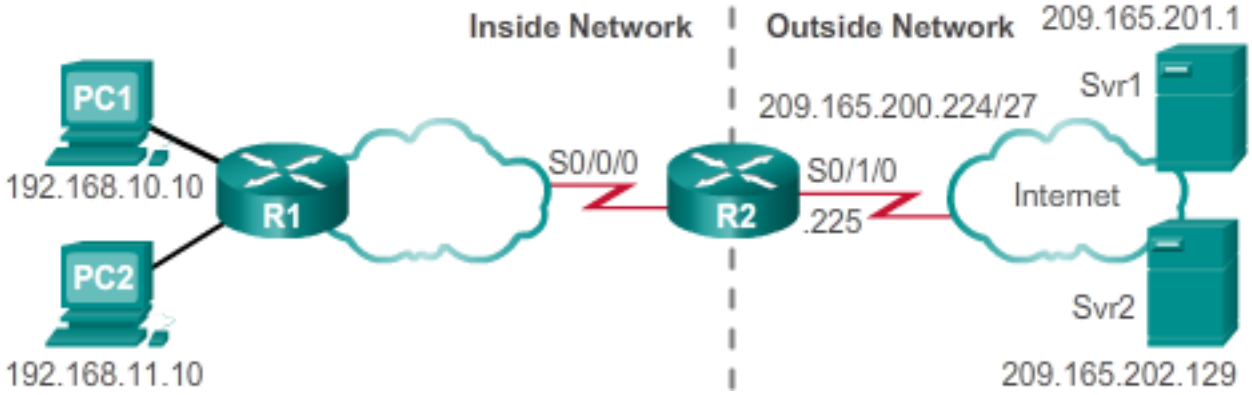
1. Define the pool of addresses that will be used for translation.
   - Configured using the **`ip nat pool`** *`pool-name start-ip end-ip`* {**`netmask`** *`netmask`* | **`prefix-length`** *`prefix-length`*} global configuration command.

2. Configure a standard ACL to identify (permit) only those addresses that are to be translated.

3. Bind the ACL to the pool.
   - Configured using the **`ip nat inside source list`** *`acl-#`* **`pool`** *`pool-name`* **`overload`** global config command.

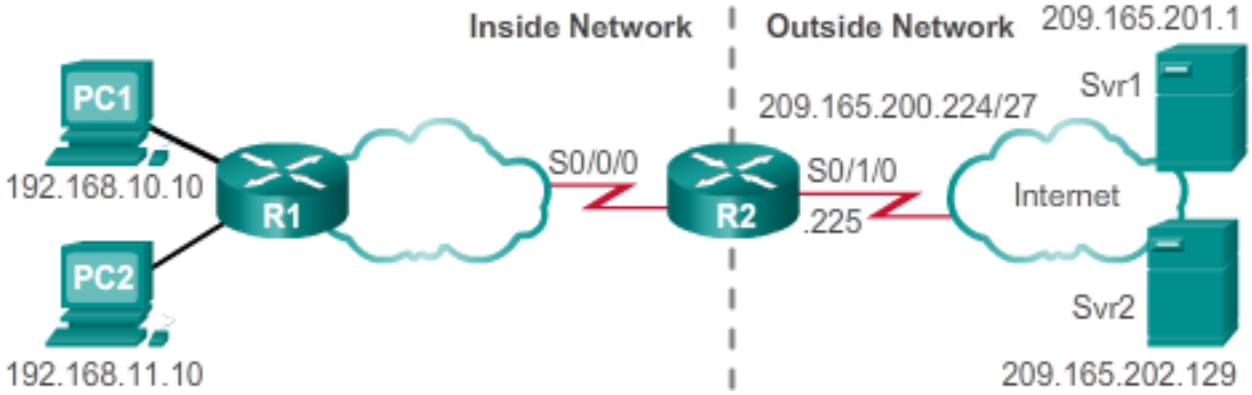
4. Identify the inside and outside NAT interfaces.
   - Configured using the **`ip nat inside`** and **`ip nat outside`** interface configuration commands.

Configuring PAT Using a Pool Example




```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 prefix-
length 27
R2(config)#
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)#
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)#
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Verifying PAT Using a Pool Example

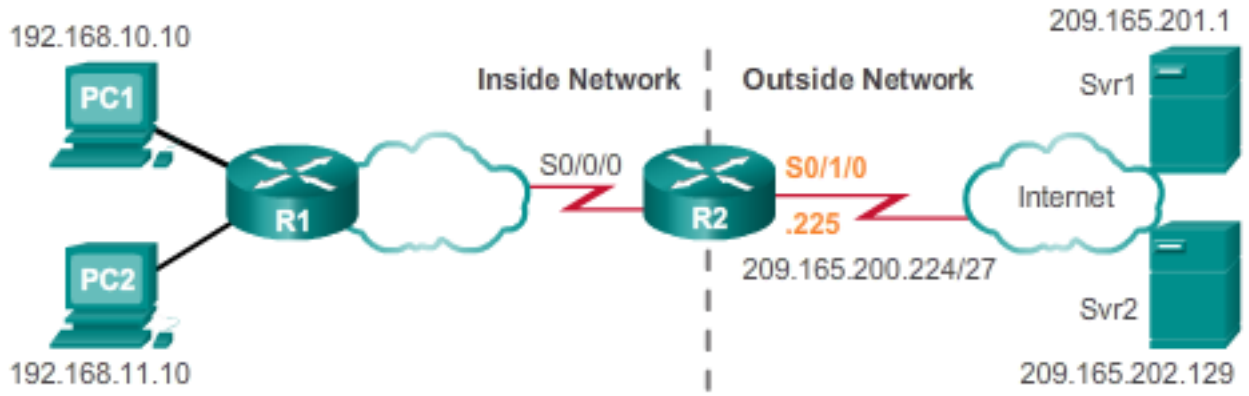



```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local       Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80    209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80
209.165.202.129:80
R2#
```

Verifying PAT Using an Address Example

```
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#
```

Configuring PAT Using an Address Example

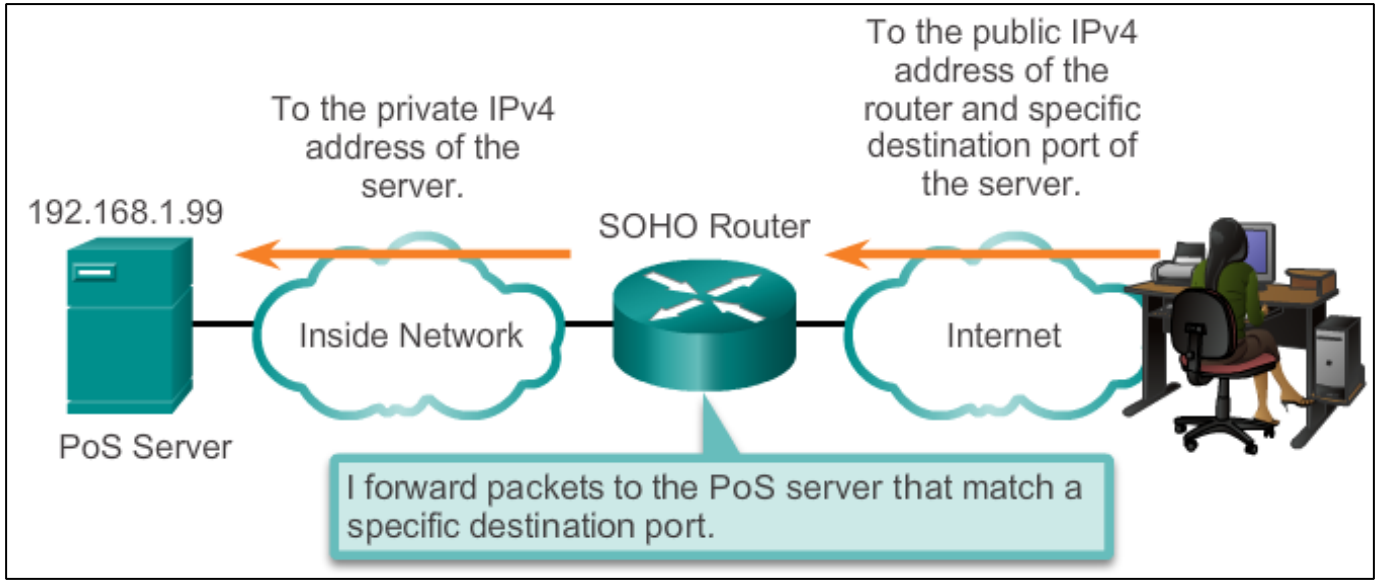



```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)#
R2(config)# ip nat source list 1 interface serial 0/1/0 overload
R2(config)#
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

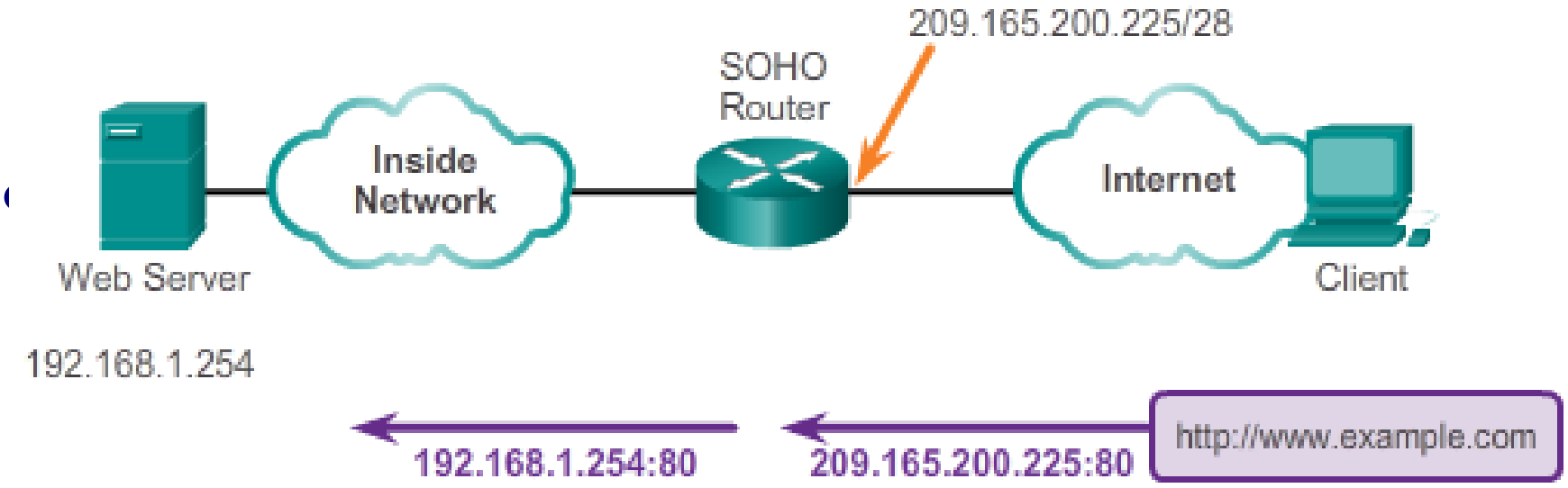
Port Forwarding

Port Forwarding

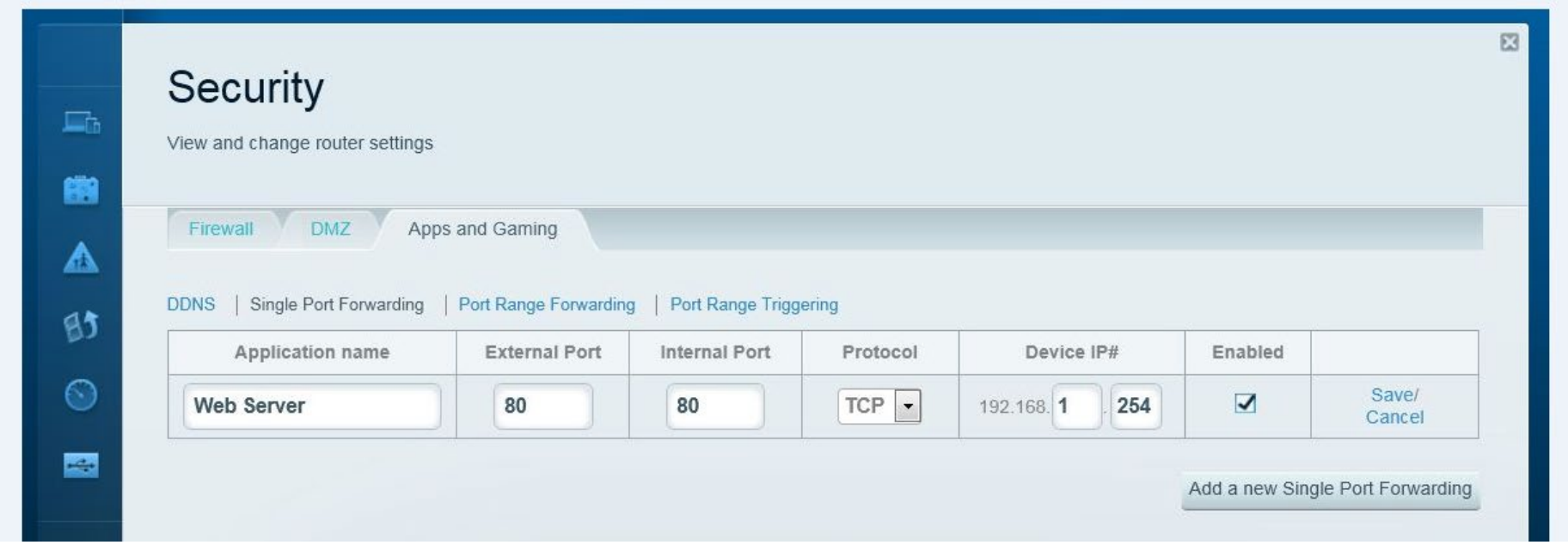
- Port forwarding (sometimes referred to as *tunneling*) is the act of forwarding traffic addressed to a specific a network port from one network node to another.
  - Helpful in situations where servers have private addresses, not reachable from the outside networks.
  - Port forwarding can be enabled for applications by specifying the inside local address that requests should be forwarded to.



Port Forwarding Example



Port Forwarding Example



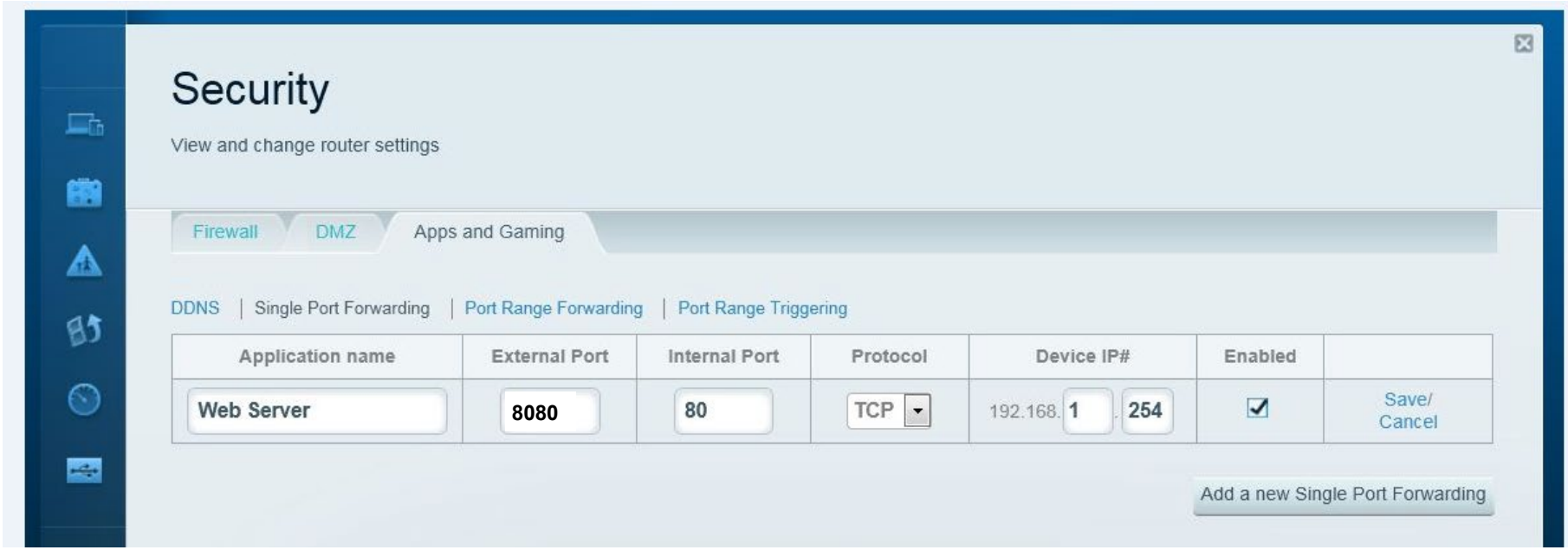
- The Linksys router is configured to redirect the HTTP requests to the internal web server at 192.168.1.254 using the default port number 80.

Using Non-Default Port Numbers

- A port other than the default can be specified.
  - For instance, in the previous example, the default HTTP port 80 can be changed to something else.
- Useful if you want to “hide” the service from others.
- However, the external user would have to know the specific port number to use.

Using Non-Default Port Numbers

- To specify a different port, the value of the External Port in the Single Port Forwarding window would be modified.



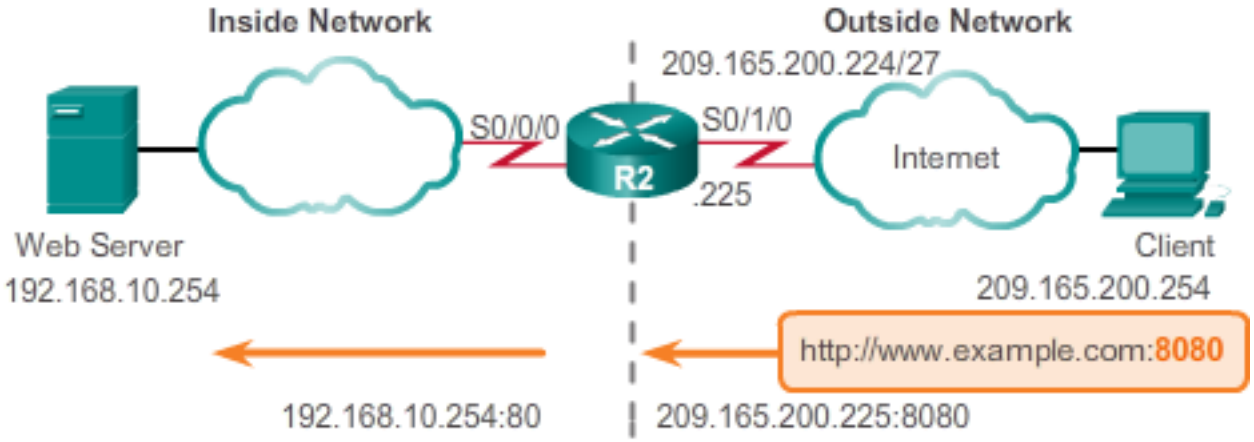
- External users would now have to use the outside web address with ":8080" appended to it.
  - E.g., **http://209.165.200.225:8080**

Configuring Port Forwarding with IOS

- In IOS, Port forwarding is essentially a static NAT translation with a specified TCP or UDP port number.
  - Configured using the **ip nat inside source** {**static** {**tcp** | **udp** *local-ip local-port global-ip global-port*} [**extendable**] global configuration command.

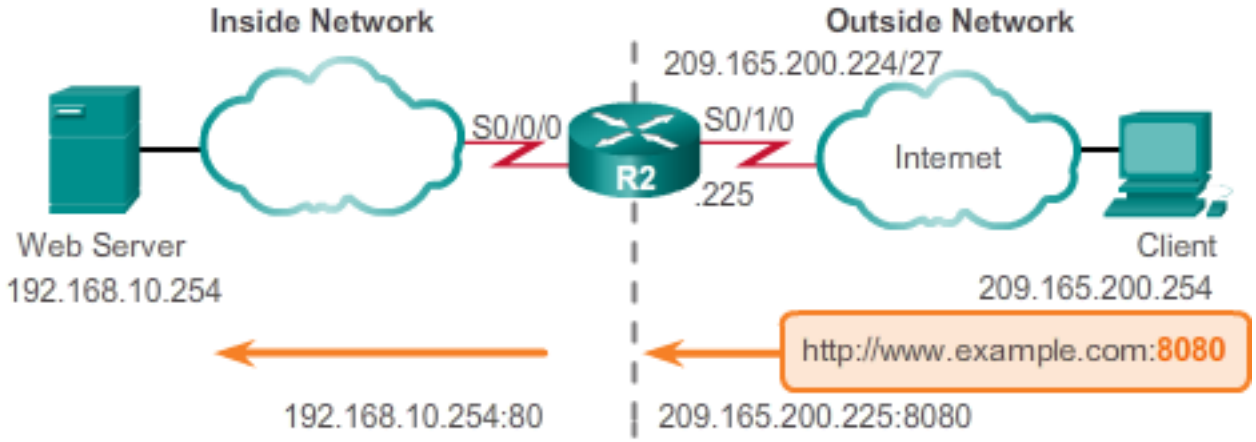
Parameter	Description
tcp or **udp**	• Indicates if this is a TCP or UDP port number.
local-ip	• This is the IPv4 address assigned to the inside host (typically a private address).
local-port	• Sets the local TCP/UDP port in a range from 1-65535. • This is the port number the server is listening on.
global-ip	• Sets the global TCP/UDP port in a range from 1-65535. • This is the port number the outside client will use to reach the internal server.
extendable	• The option is applied by default and allows the router to extend the translation to more than one port if necessary.

IOS Port Forwarding Example




```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
R2(config)#
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

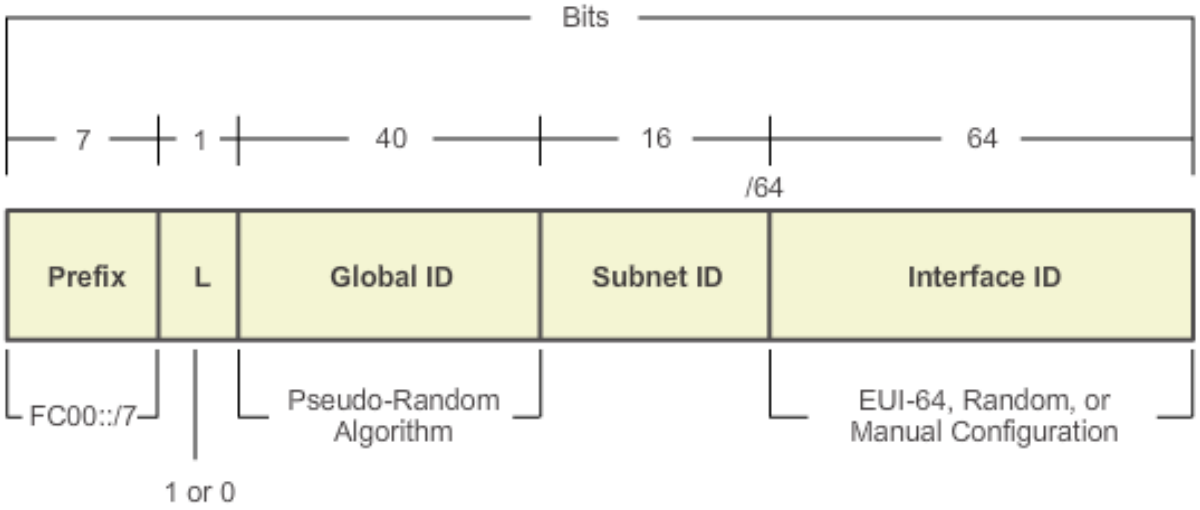
IOS Port Forwarding Example




```
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#
```

Configuring NAT and IPv6

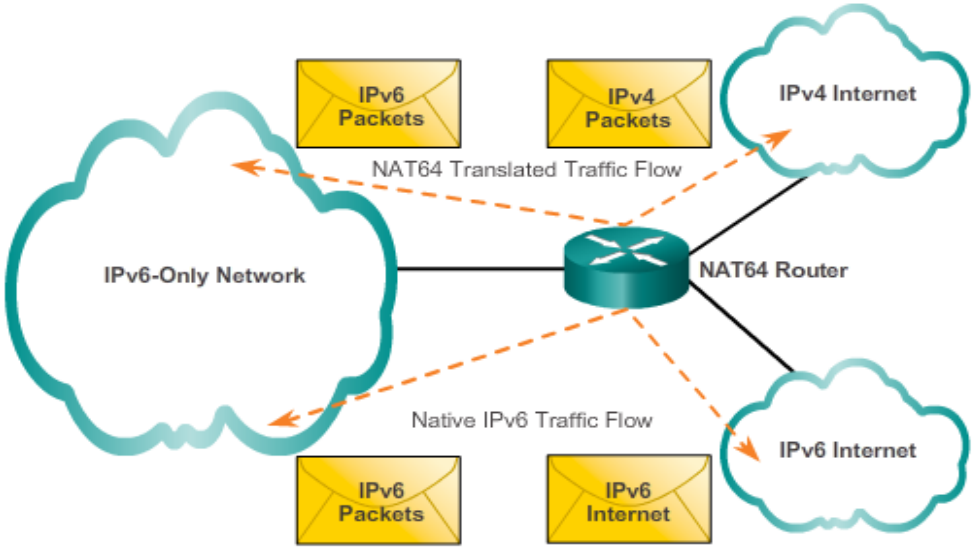
IPv6 Unique Local Addresses – NOT for translation to GUA public address!



- IPv6 has identified unique local addresses (ULAs) which are *similar to private addresses* and are designed to allow IPv6 communications within a local site.
  - ULAs are also known as local IPv6 addresses (not to be confused with IPv6 link-local addresses).

- ULAs have the prefix FC00::/7, which results in a first hextet range of FC00 to FDFF.

NAT for IPv6



- IPv6 can still use NAT but in a much different context.
- In IPv6, NAT64 was developed to provide transparent communication between IPv6 and IPv4.