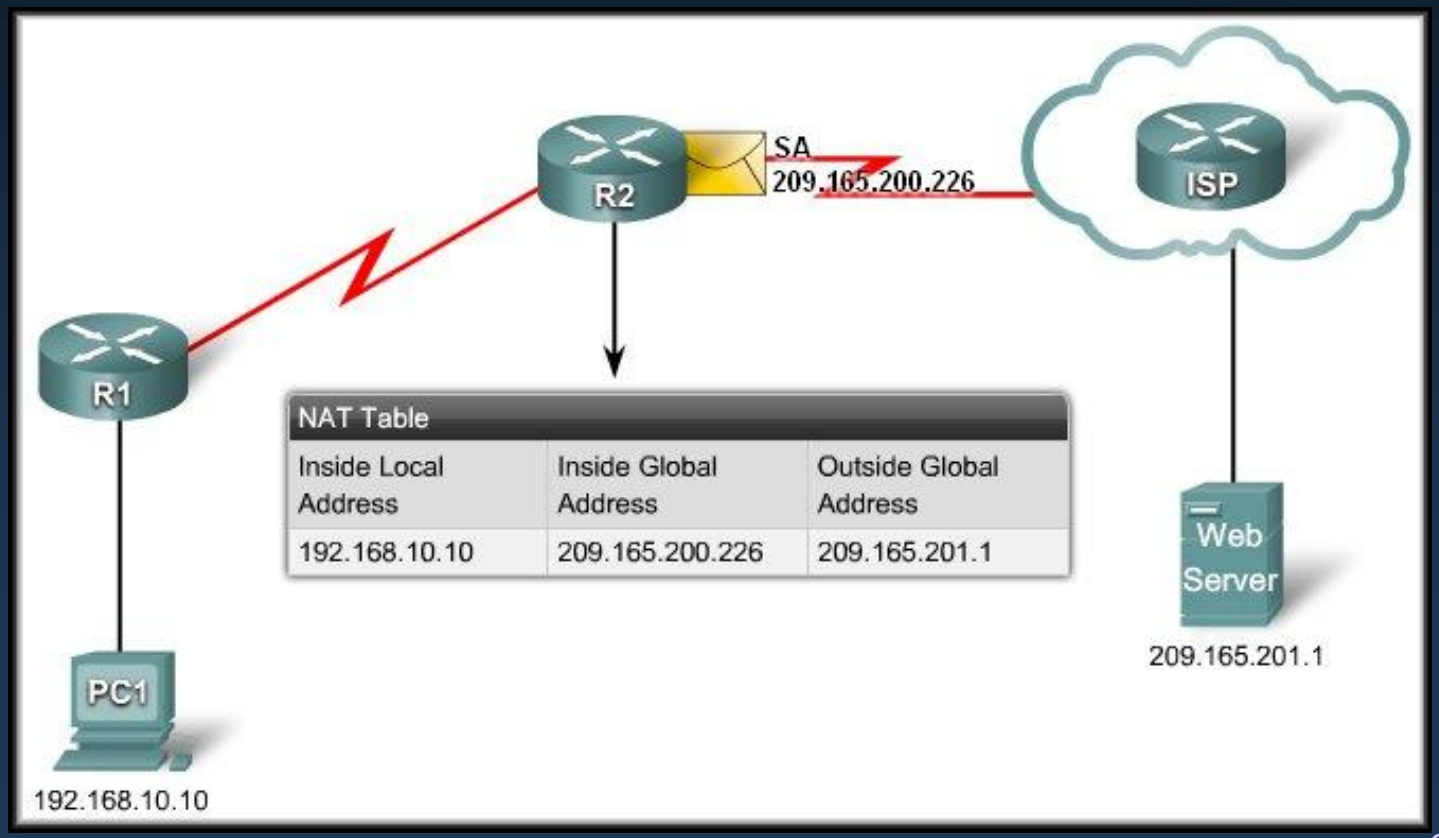
IPv4 Services
NAT/PAT

IP Addressing Services

Scaling Networks With Network Address Translation (NAT)



Scaling Networks With NAT

- All public Internet addresses must be registered with a Regional Internet Registry (RIR).
- Organizations can lease public addresses from an ISP.
- Only the registered holder of a public Internet address can assign that address to a network device.

Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AfriNIC

Scaling Networks With NAT

- Private Internet Addresses:
  - These are reserved private Internet addresses drawn from three blocks.
  - These addresses are for private, internal network use only.
  - RFC 1918 specifies that private addresses are not to be routed over the Internet.

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

Scaling Networks With NAT

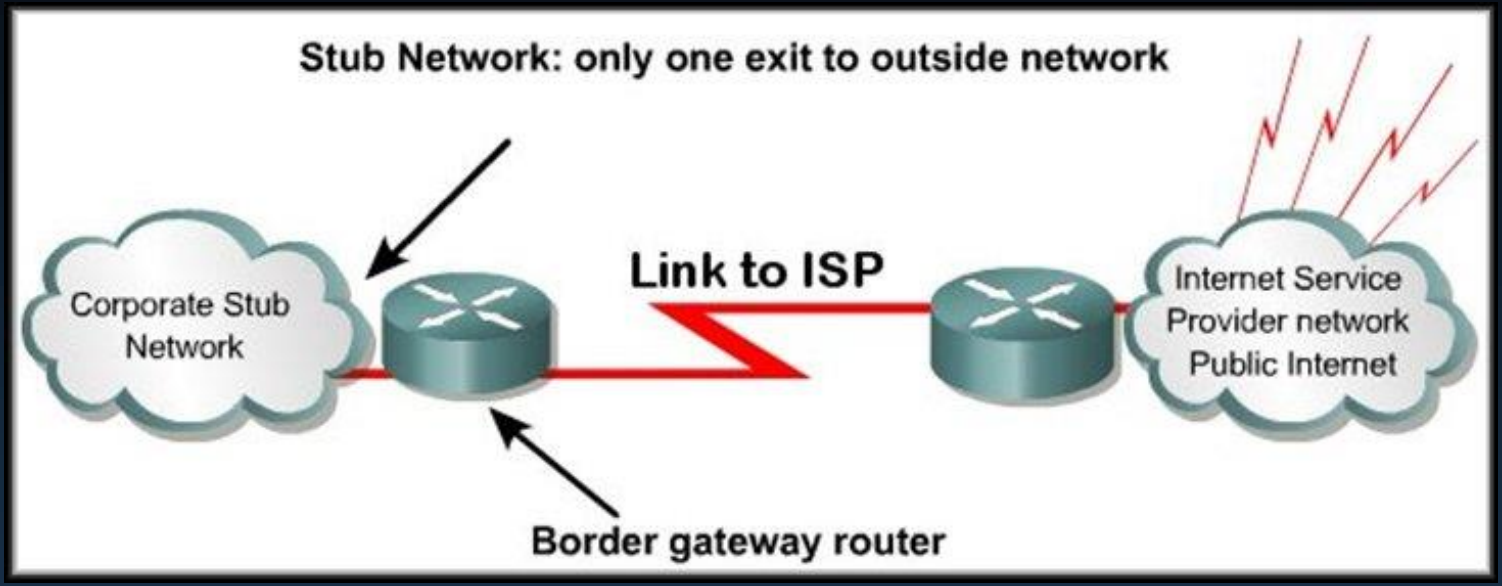
- Private Internet Addresses:
  - Two Issues:
    - You cannot route private addresses over the Internet.
    - There are not enough public addresses to allow organizations to provide one to every one of their hosts.
  - Networks need a mechanism to translate private addresses to public addresses at the edge of their network that works in both directions.
  - Solution – NAT.

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

What is NAT?

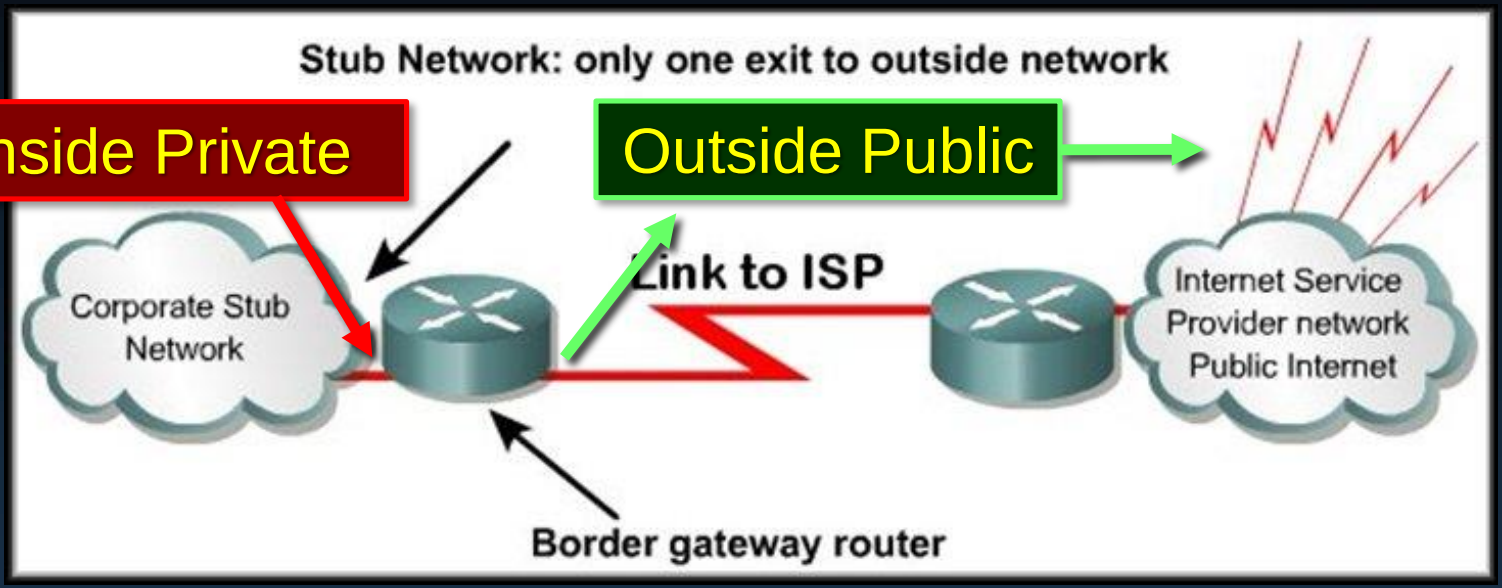
- The DHCP server assigns IP dynamic addresses to devices inside the network.
- NAT-enabled routers retain one or many valid Internet IP addresses outside of the network.
- When the client sends packets out of the network, NAT translates the internal IP address of the client to an external address.
- *To outside users, all traffic coming to and going from the network has the same IP address or is from the same pool of addresses.*

What is NAT?



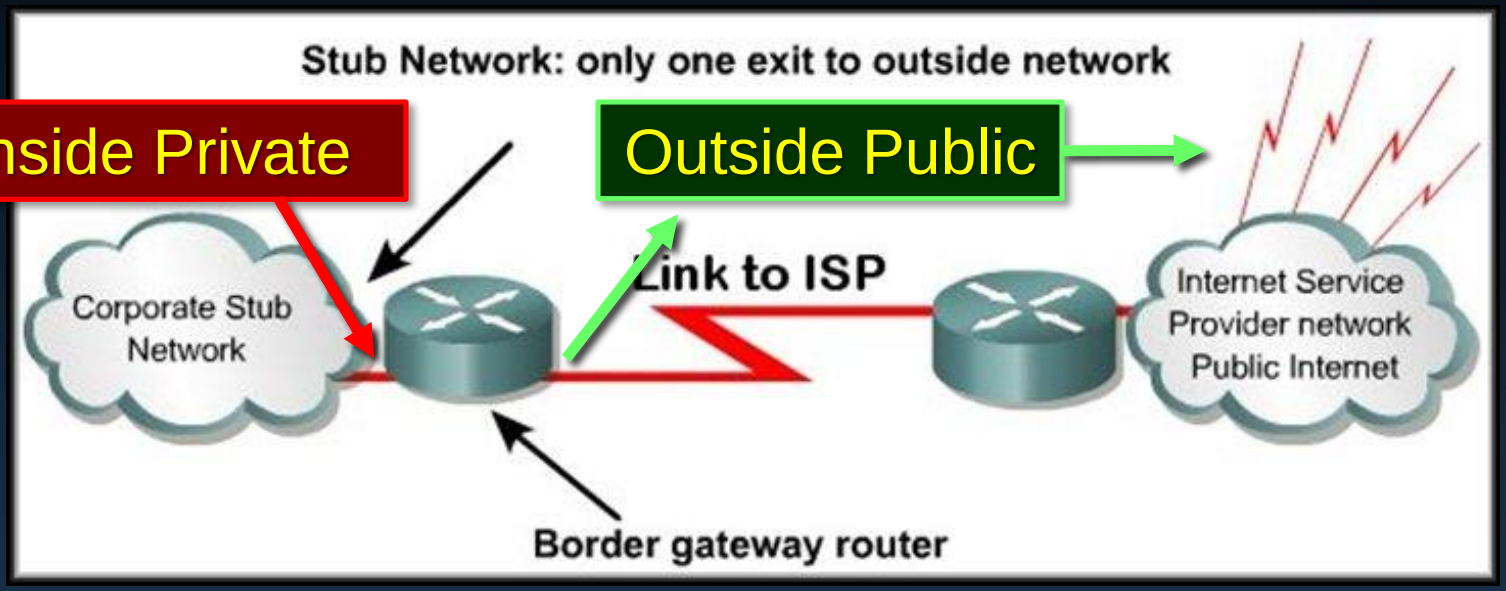
- A NAT enabled device typically operates at the border of a stub network.
- A stub network is a network that has a single connection to its neighbor network.

What is NAT?



- When a host on the inside network wants to access a host on the outside network, the packet is sent to the border gateway router.
- The border gateway router performs the NAT process, translating the inside private address to an outside public address.

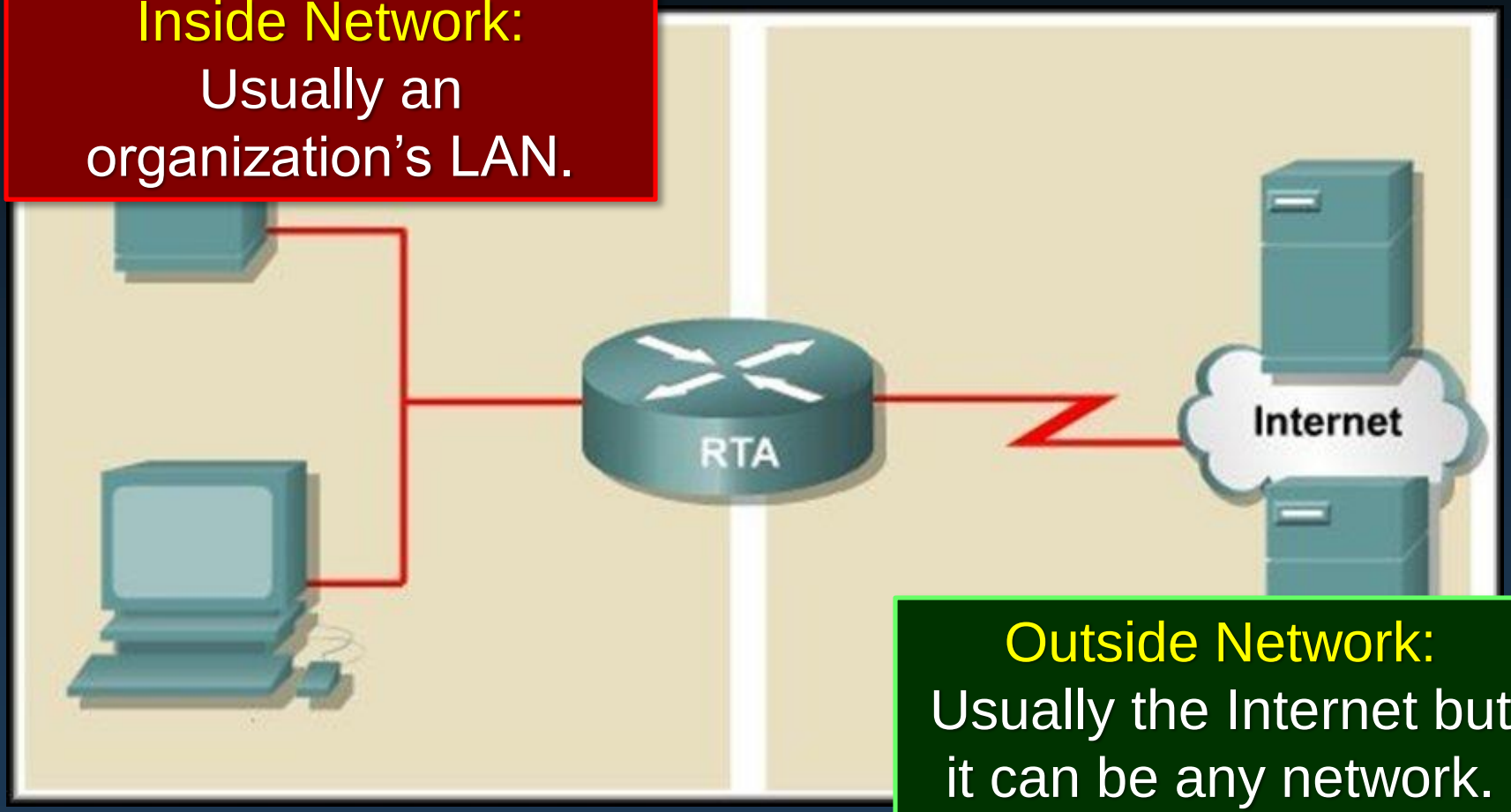
What is NAT?



- The translation process uses an internal translation table.
- The contents of the table will vary depending on the type of network translation being implemented.
- We will be looking at the use of static NAT, dynamic NAT and Port Address Translation (PAT).

NAT Terminology

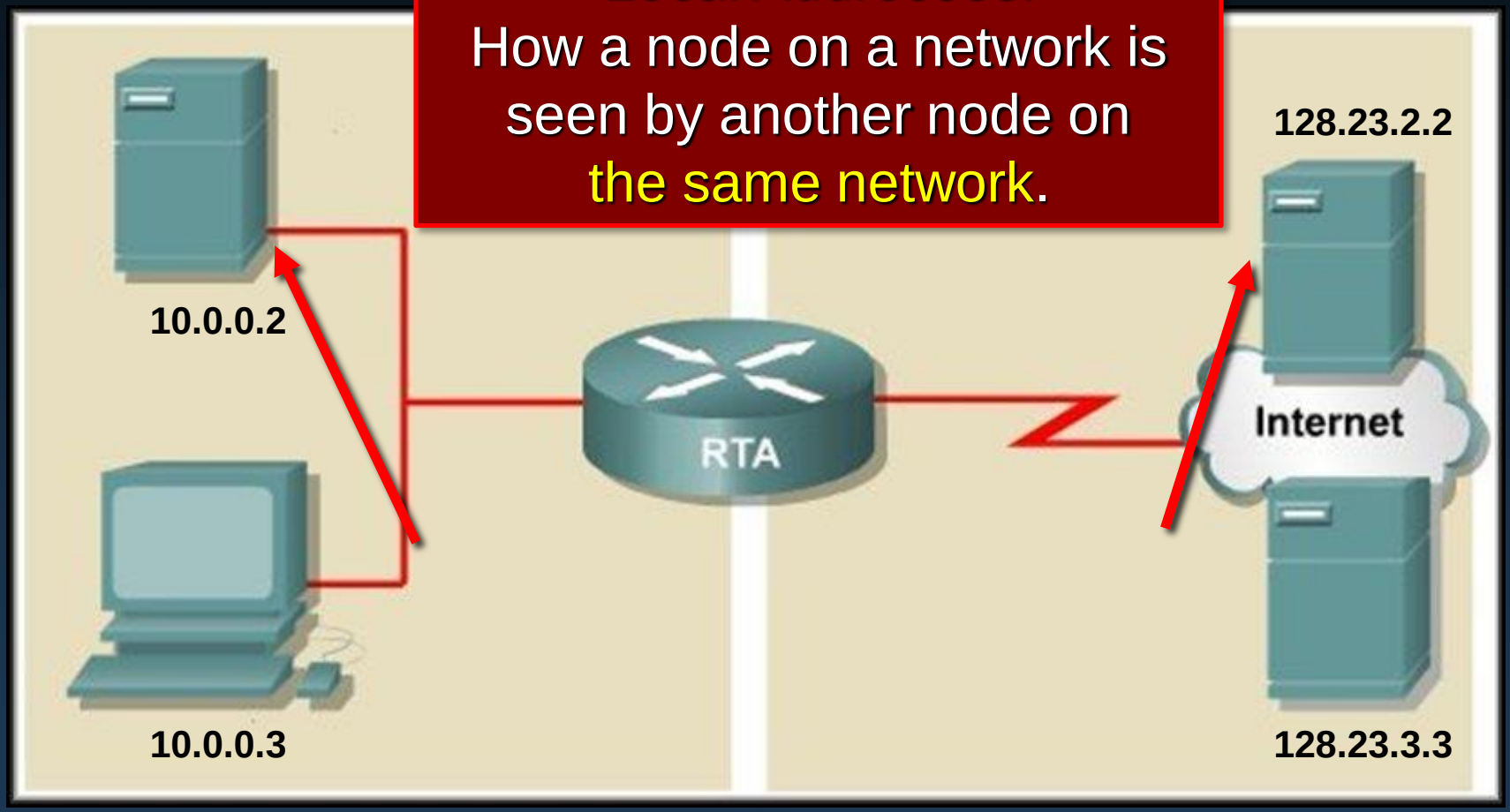
Inside Network:
Usually an organization's LAN.



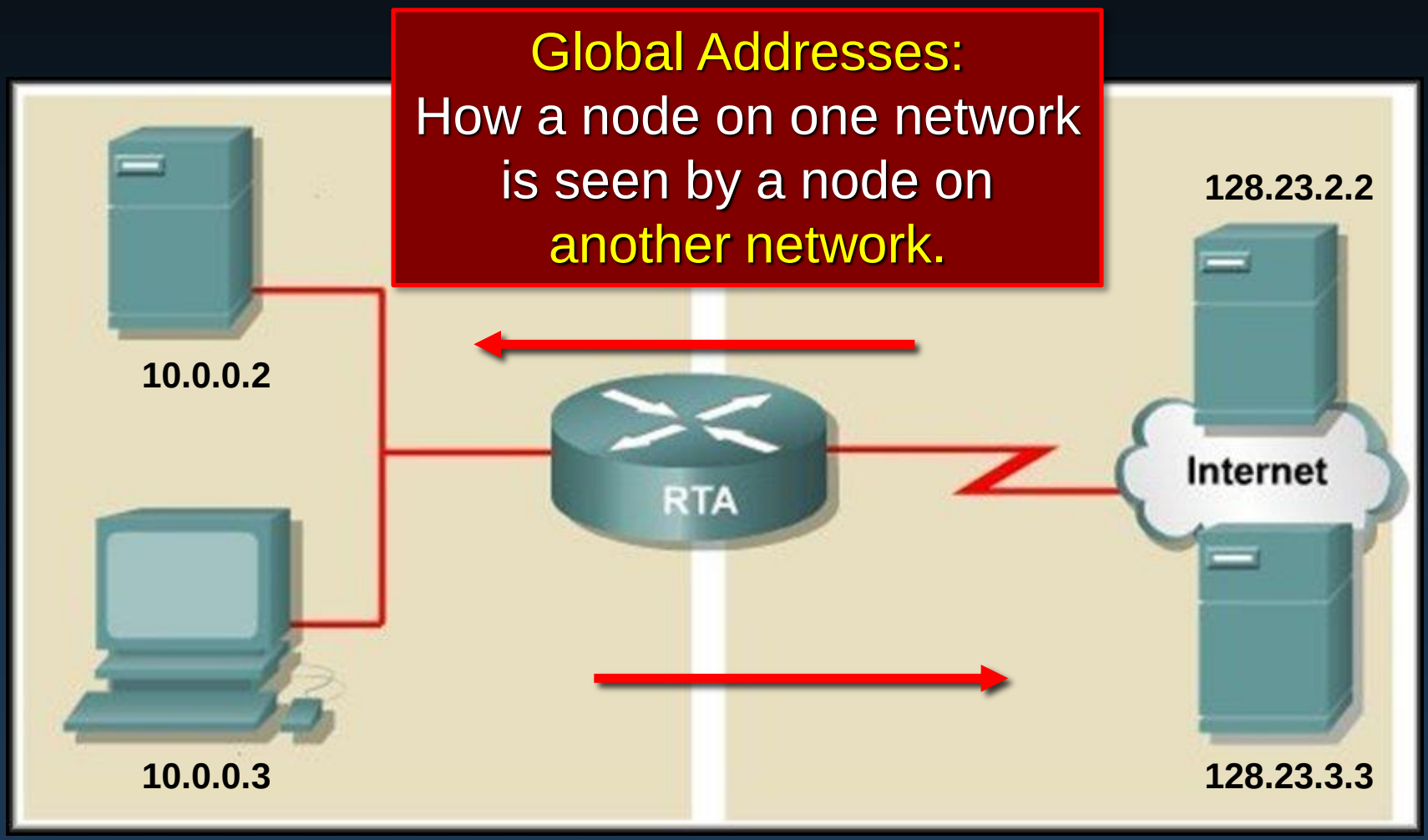
Outside Network:
Usually the Internet but it can be any network.

NAT Terminology

Local Addresses:
How a node on a network is seen by another node on the same network.



NAT Terminology



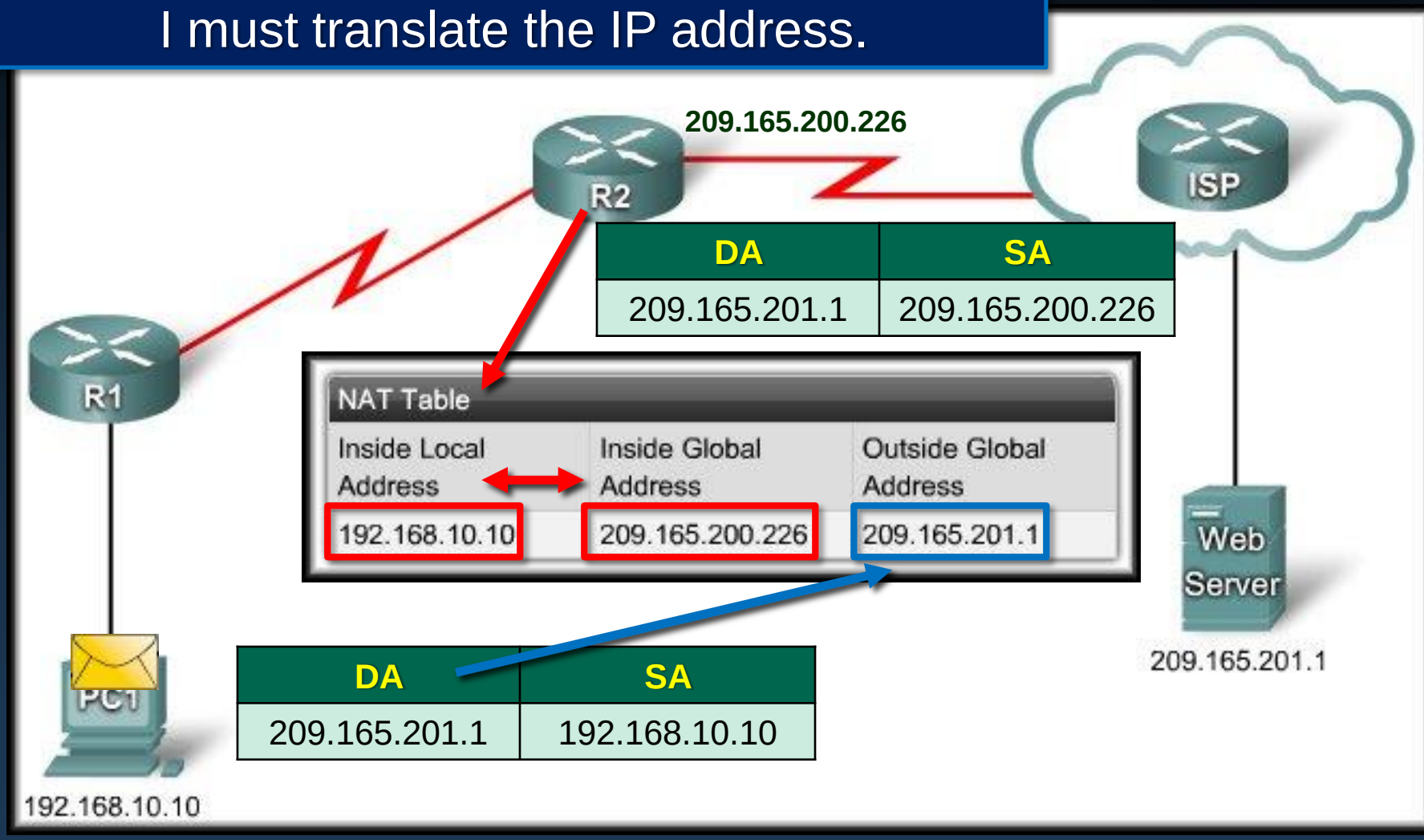
NAT Terminology

- Inside Local Address: 
  - An RFC 1918 address assigned to a host on an inside network.
- Inside Global Address: 
  - A valid public address that the host on the inside network is assigned as it exits the router.
- Outside Global Address: 
  - A reachable IP address assigned to a host on the Internet.
- *Outside Local Address:*
  - A local address assigned to a host on an outside network.
  - *(Use beyond the scope of this course).*

How Does NAT Work?

R2: I have a packet for the outside network. I must translate the IP address.

Send

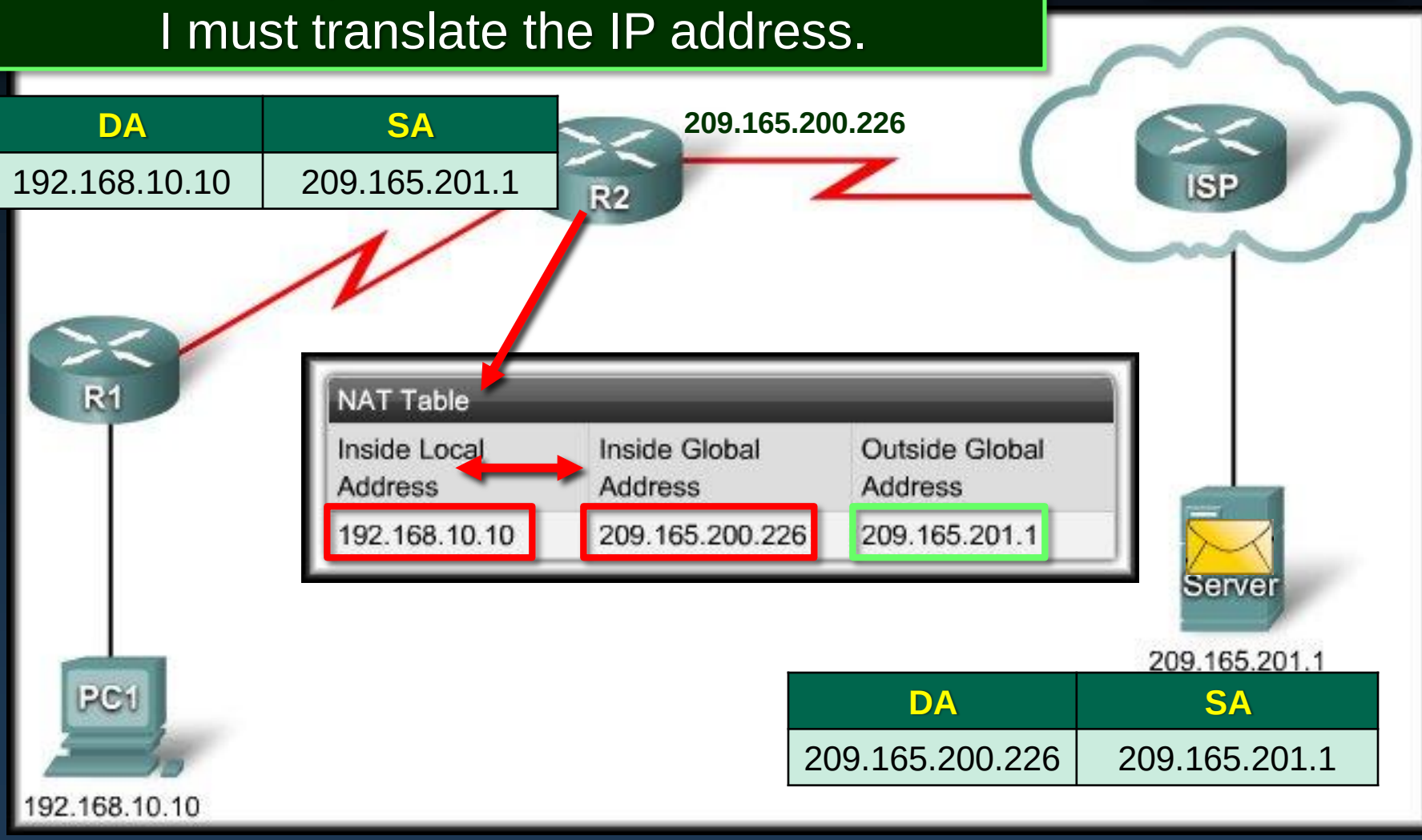


How Does NAT Work?

R2: I have a packet for the inside network.
I must translate the IP address.

Receive

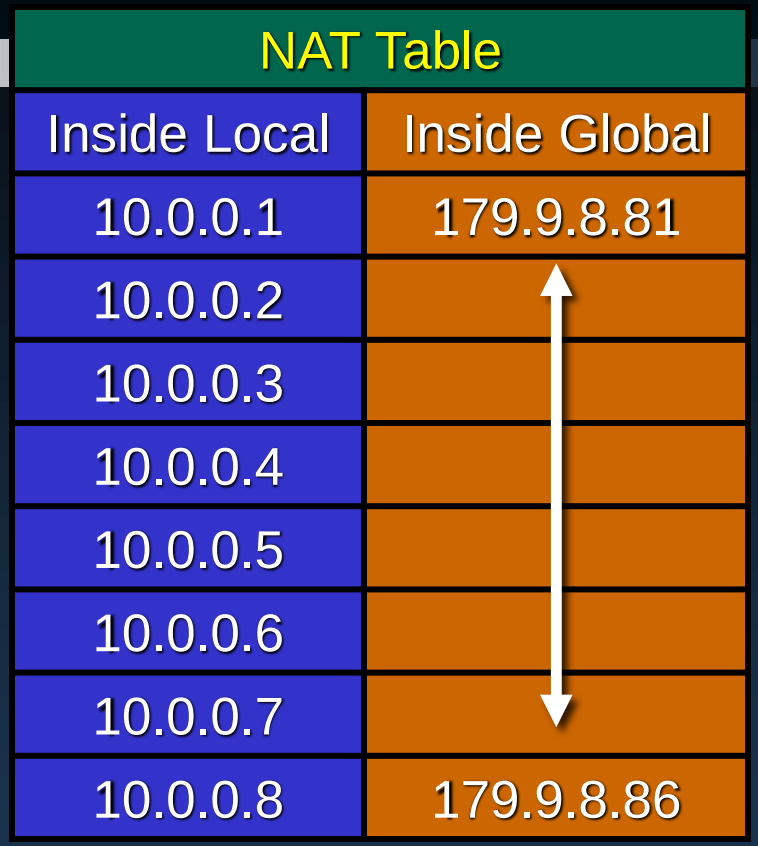
DA	SA
192.168.10.10	209.165.201.1



DA	SA
209.165.200.226	209.165.201.1

Dynamic Mapping and Static Mapping

- Dynamic Mapping:
  - Mapping of local addresses dynamically to a pool of global addresses.
  - The hosts able to use NAT is limited by the number of addresses in the range.
  - If you have allocated 6 public addresses for NAT, any 6 users can use NAT simultaneously.
    - The NAT device dynamically assigns an address when a request is received. When a session ends, the address is returned to the pool for another user.



Dynamic Mapping and Static Mapping

- Static Mapping:
  - One to one mapping of local and global addresses.
  - The hosts able to use NAT is limited by the static assignment in the table.

NAT Table	
Inside Local	Inside Global
10.0.0.1	179.9.8.81
10.0.0.2	179.9.8.82
10.0.0.3	179.9.8.83
10.0.0.4	179.9.8.84
10.0.0.5	179.9.8.85
10.0.0.6	179.9.8.86

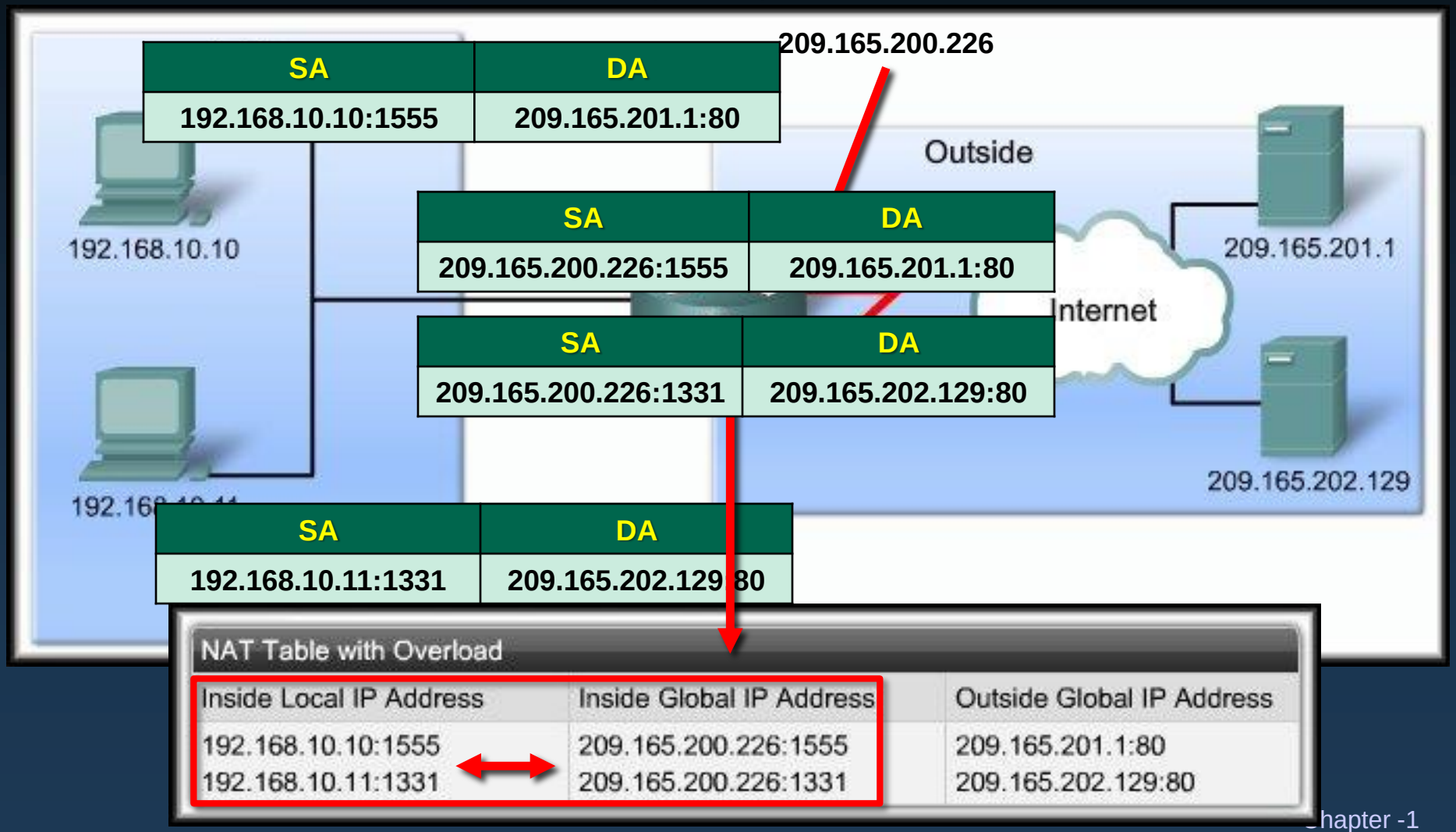
  - If you have allocated 6 public addresses for NAT, only these 6 users can use NAT.
    - No other network users will have access unless you allocate another global address and add it to the table.

NAT Overload

- Port Address Translation (PAT):
  - Allows you to use a single Public IP address and assign it up to 65,536 inside hosts (4,000 is more realistic).
  - Modifies the TCP/UDP source port to track inside host addresses.
  - Tracks and translates:
    - Source IP Address.
    - Destination IP Address.
    - TCP/UDP Source Port Number.
  - These uniquely identify each connection for each stream of traffic.

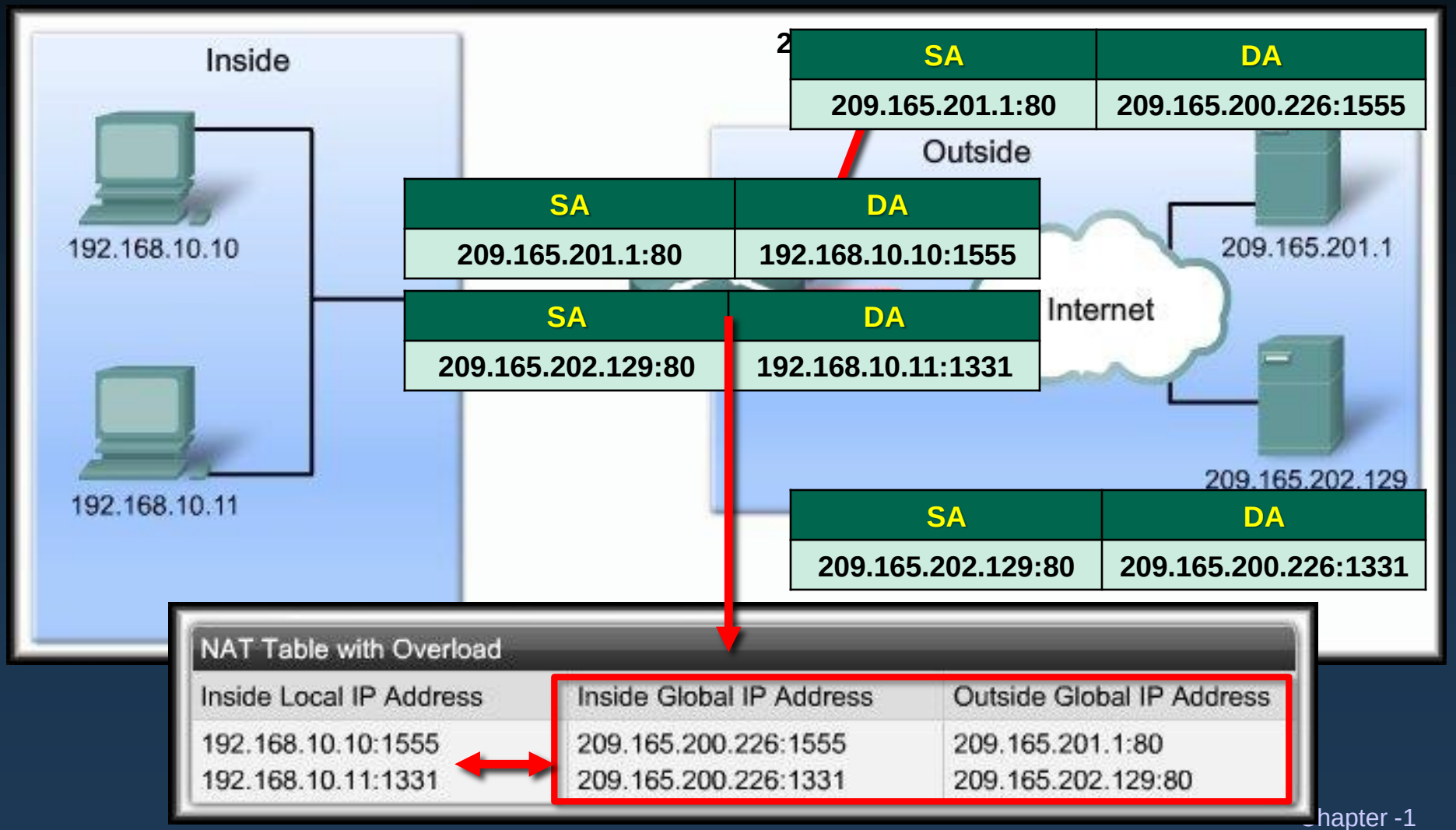
NAT Overload

- Port Address Translation (PAT):



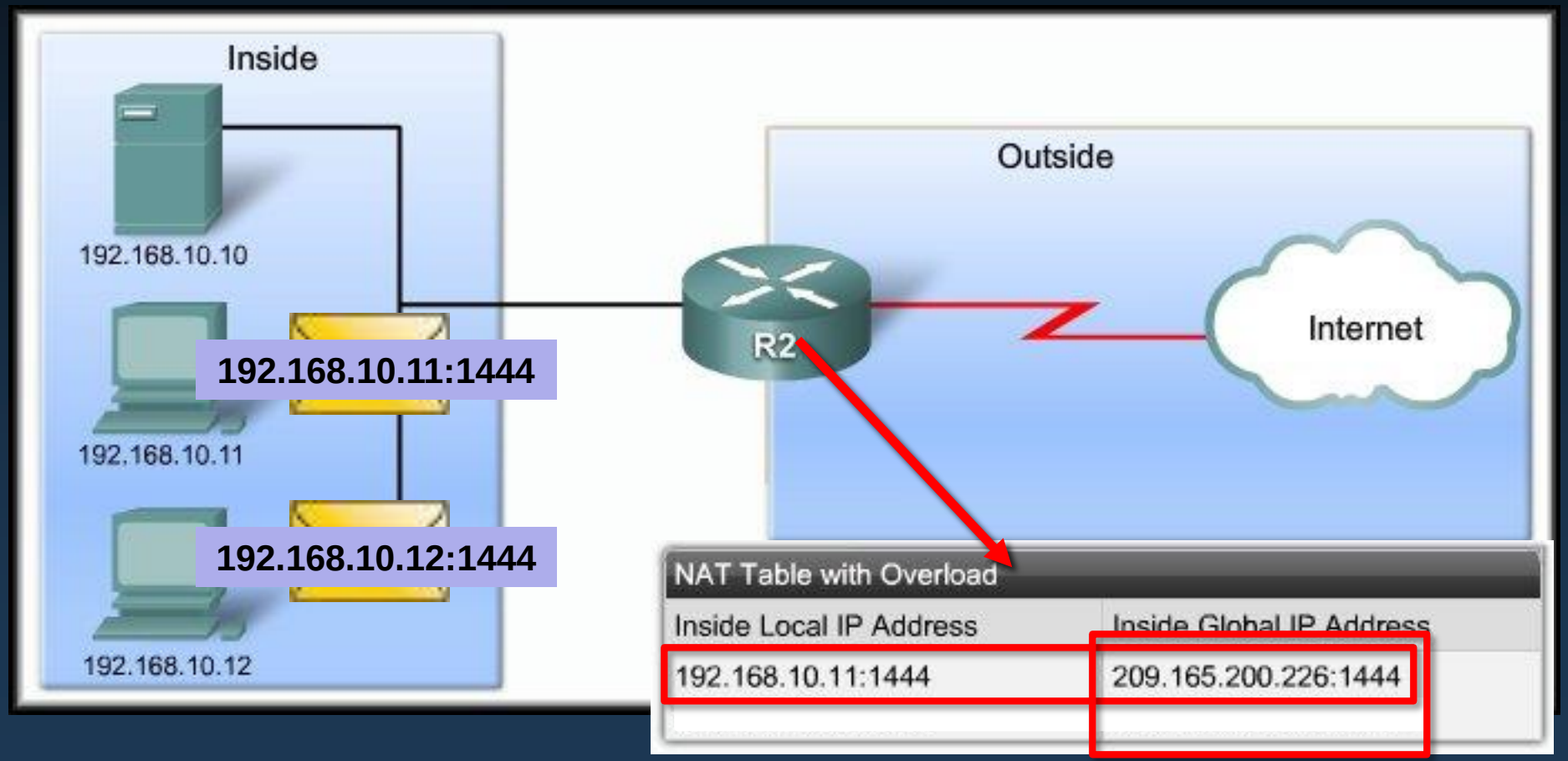
NAT Overload

- Port Address Translation (PAT):



NAT Overload

- Port Address Translation (PAT): *NEXT AVAILABLE PORT*



Benefits and Drawbacks

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

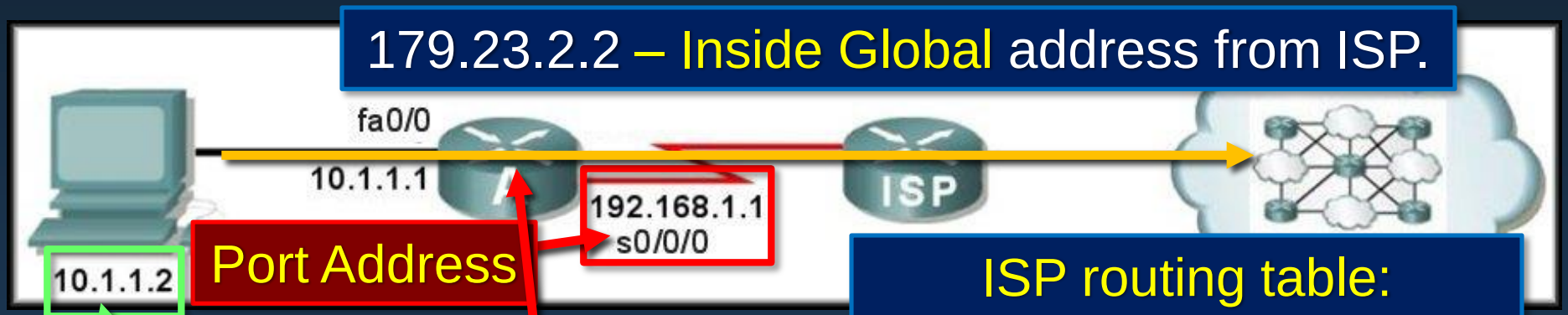
Benefits and Drawbacks

- NAT Drawbacks:
  - Performance is degraded.
  - End-to-end functionality is degraded.
  - End-to-end trace is lost.

Configuring Static NAT

- Step 1:
  - Specify static translation between an inside local and inside global address.

```
ip nat inside source static
                local-ip global-ip
```



Configuring Static NAT

- Step 2:
  - Mark the router interfaces as an inside interface or an outside interface.

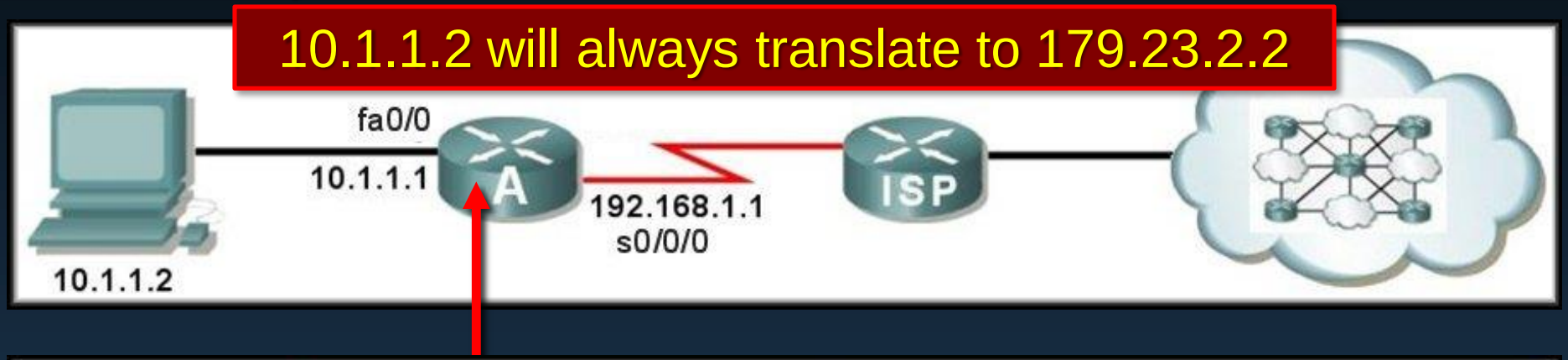
```
RA(config)#interface fa0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.0
RA(config-if)#ip nat inside
```

ISP routing table:
179.23.2.0 via 192.168.1.1

```
RA(config)#interface s0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#ip nat outside
```

Configuring Static NAT

- Summary:




```
RA(config)#ip nat inside source static 10.1.1.2 179.23.2.2

RA(config)#interface fa0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.0
RA(config-if)#ip nat inside

RA(config)#interface s0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#ip nat outside
```

Configuring Dynamic NAT

1. Define a *named address pool* of outside addresses to be used for translation.

2. Define an *access list* to specify those inside addresses that are eligible for translation.

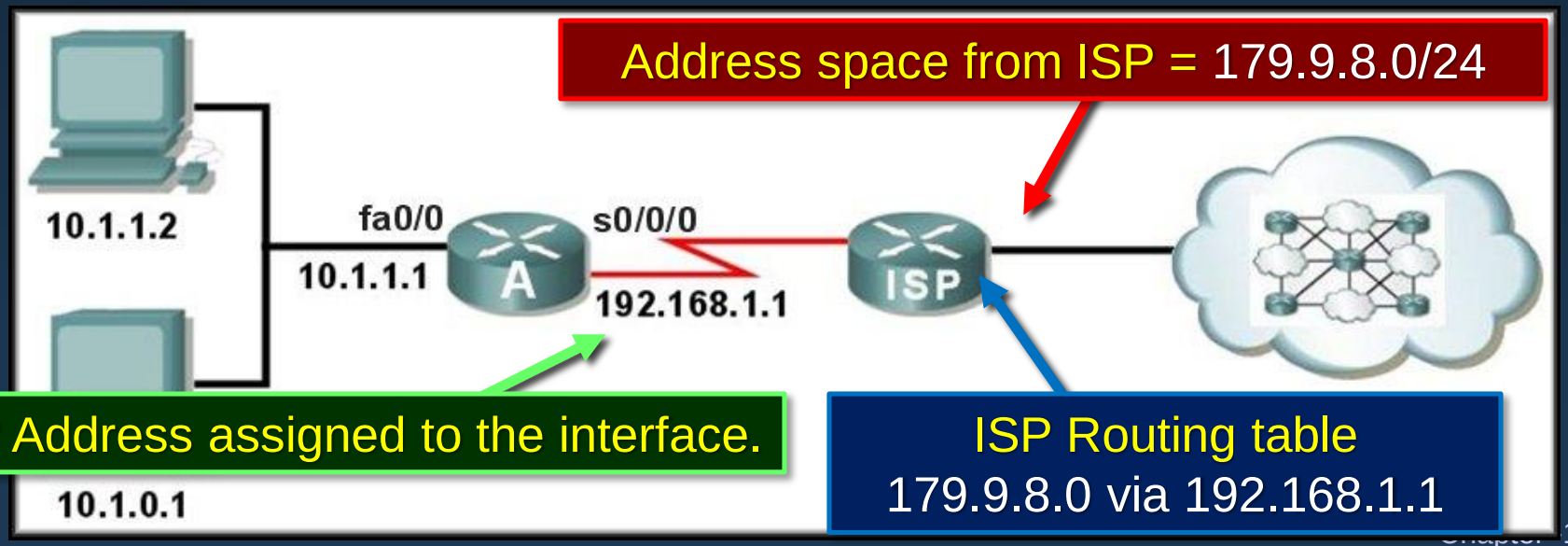
3. *Specify dynamic translation* between the inside addresses allowed by the access list and the pool of outside addresses.

4. *Mark the interfaces* as inside or outside.

Configuring Dynamic NAT

- Step 1:
  - Define a *named address pool* of outside addresses to be used for translation.

```
ip nat pool name start-ip end-ip
        (netmask netmask |
              prefix-length prefix-length)
```



Configuring Dynamic NAT

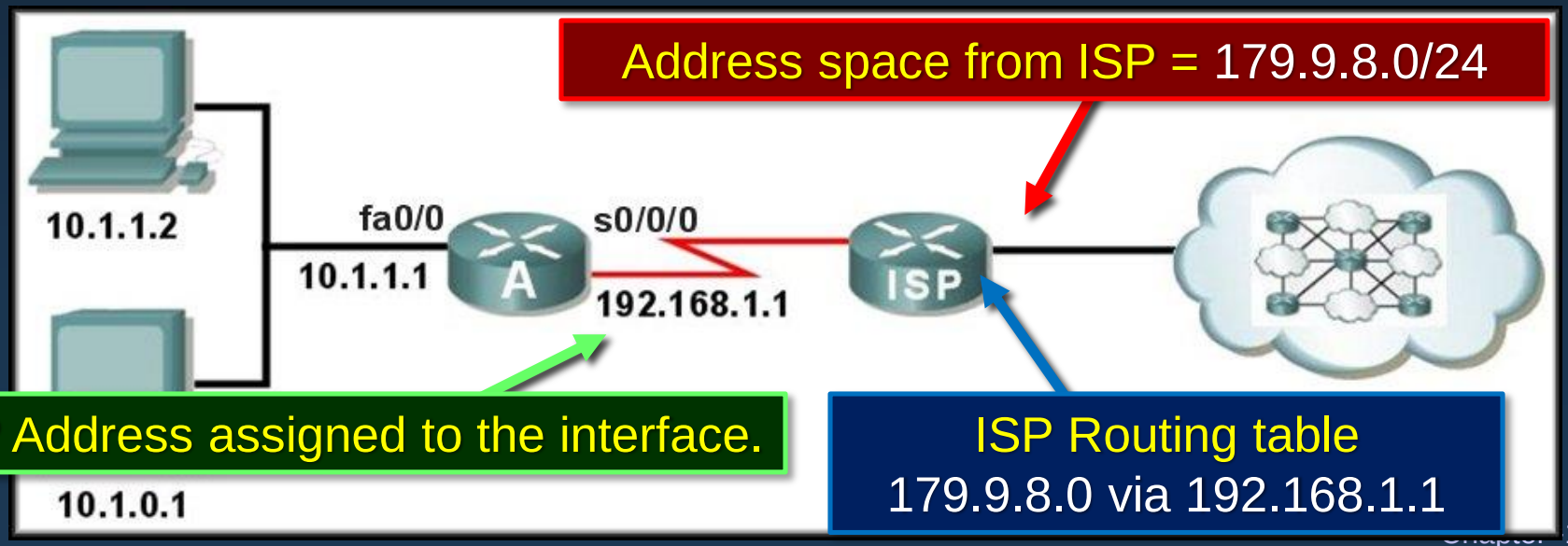
- Step 1:
  - Define a *named address pool* of outside addresses to be used for translation.

```
ip nat pool NAT-POOL1 179.9.8.80 179.9.8.85
netmask 255.255.255.0
```

Range

Name

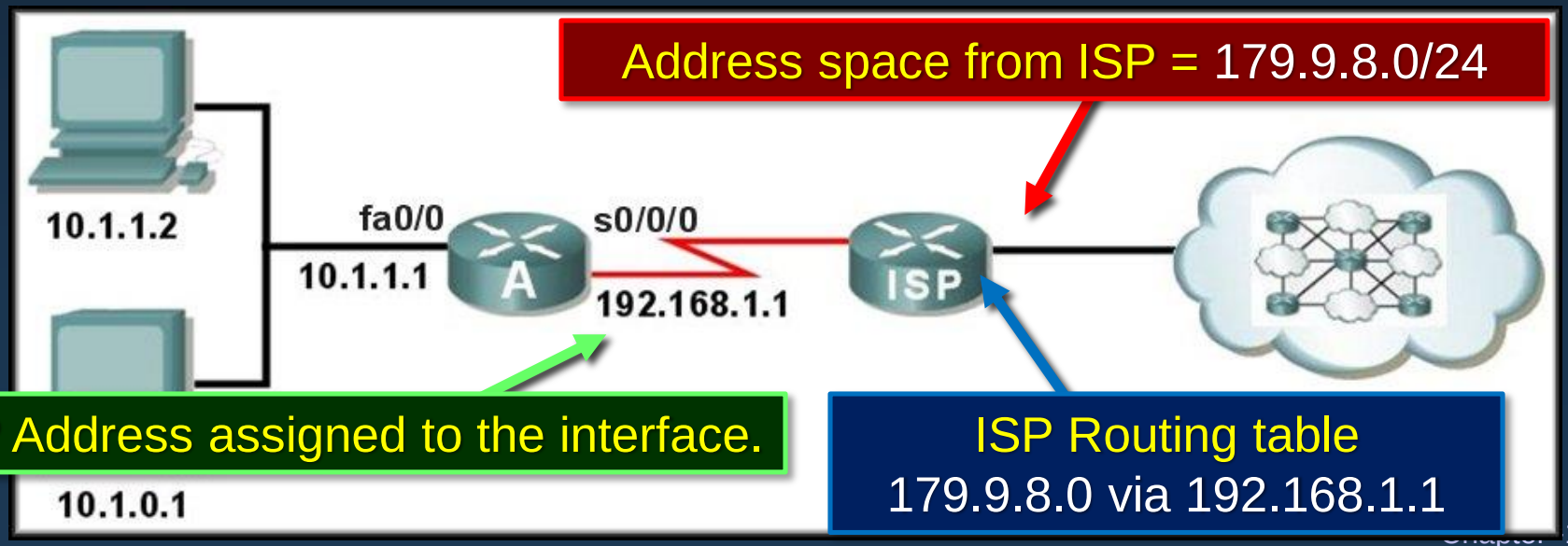
Mask



Configuring Dynamic NAT

- Step 2:
  - Define an *access list* to specify those inside addresses that are eligible for translation.

```
ip access-list standard access-list-name
                    permit source [source wildcard]
```

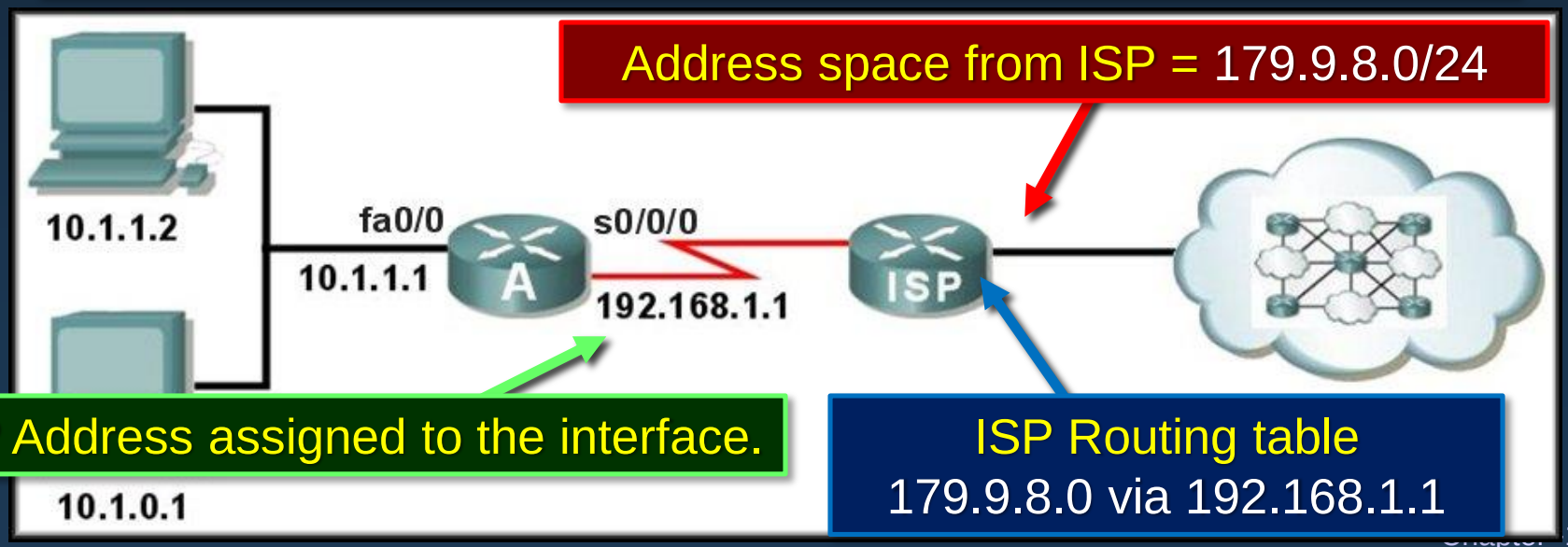


Configuring Dynamic NAT

- Step 2:
  - Define an *access list* to specify those inside addresses that are eligible for translation.

```
ip access-list standard NAME
permit 10.1.0.0 0.0.255.255
```

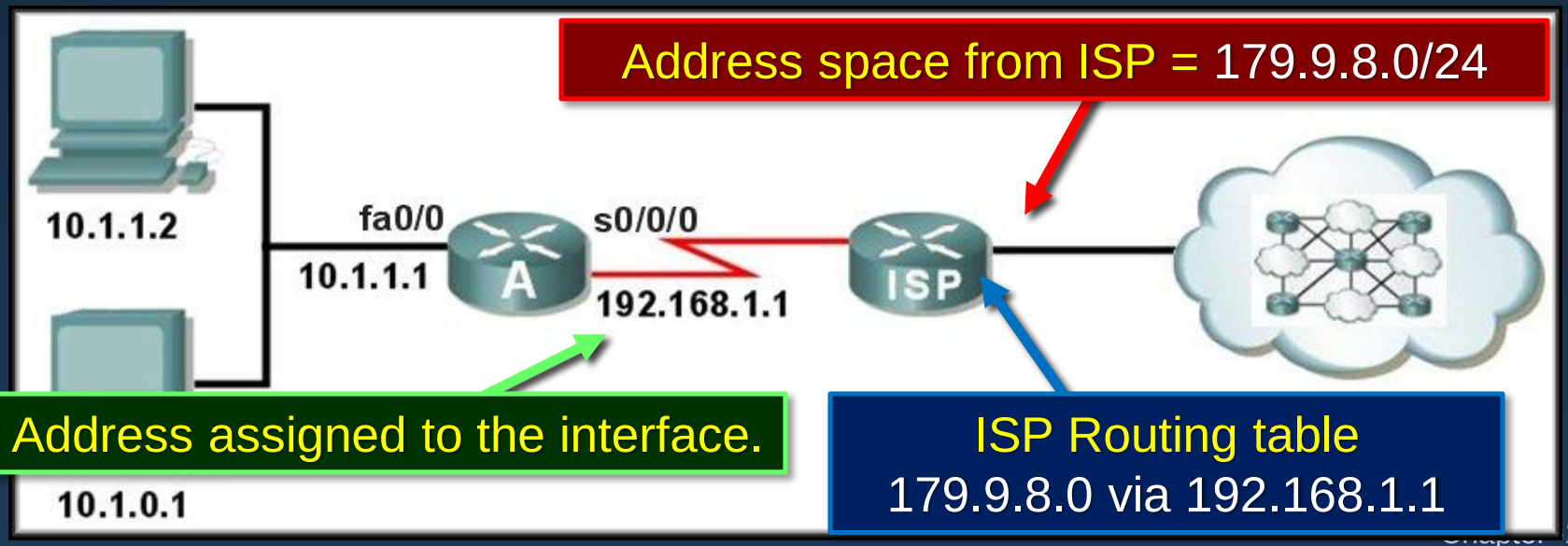
Allows ALL inside network addresses to be translated.



Configuring Dynamic NAT

- Step 2:
  - *Specify dynamic translation* between the inside addresses allowed by the access list and the pool of outside addresses.

```
ip nat inside source list access-list-name
                     pool pool-name
```



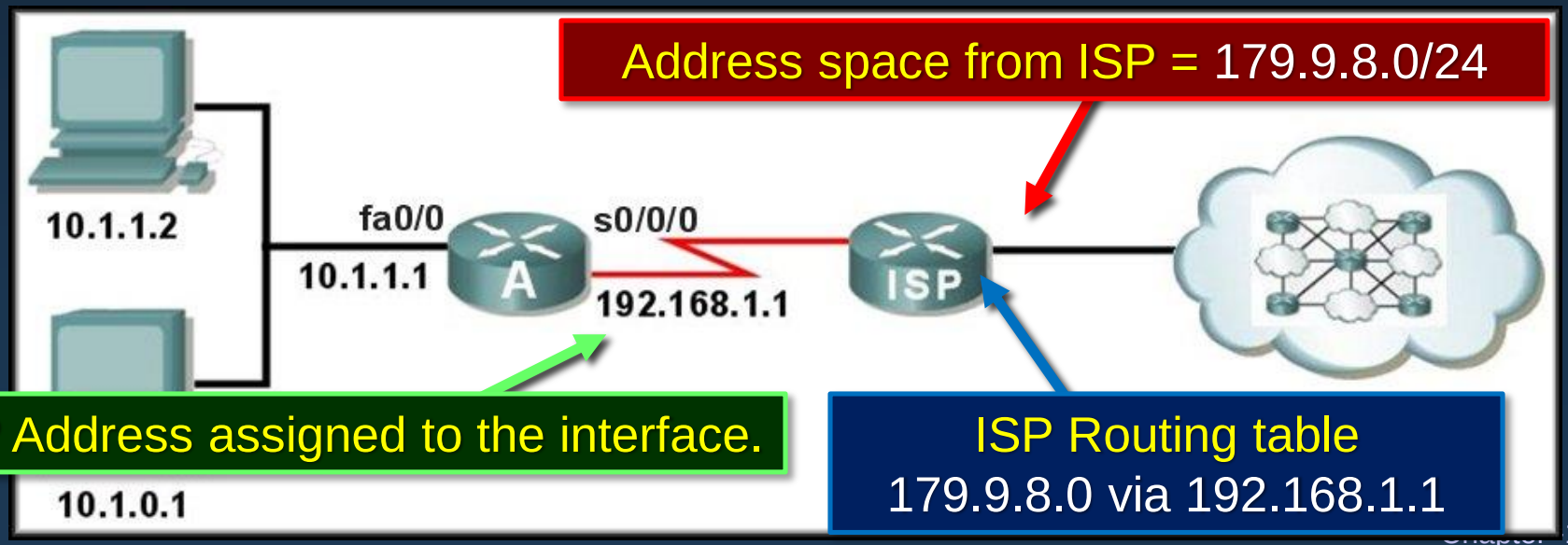
Configuring Dynamic NAT

- Step 3:
  - *Specify dynamic translation* between the inside addresses allowed by the access list and the pool of outside addresses.

From Step 1

```
ip nat inside source list NAME pool NAT-POOL1
```

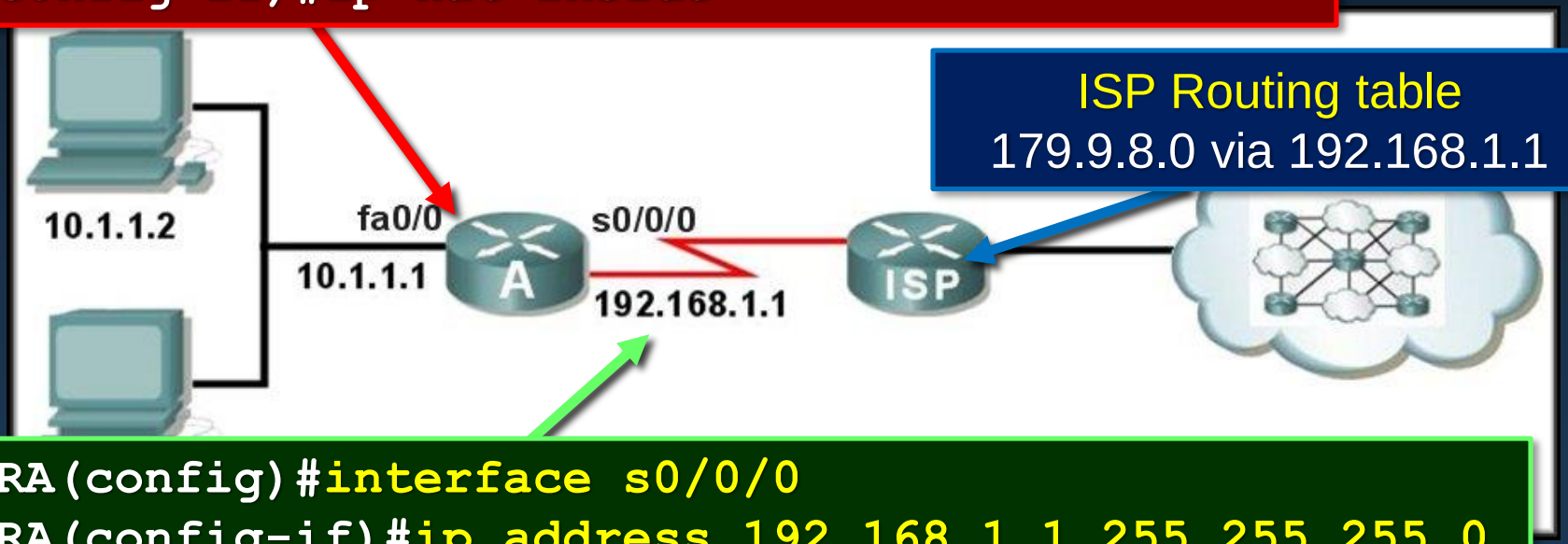
From Step 2



Configuring Dynamic NAT

- Step 4:
  - *Mark the interfaces* as inside or outside.

```
RA(config)#interface fa0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.0
RA(config-if)#ip nat inside
```

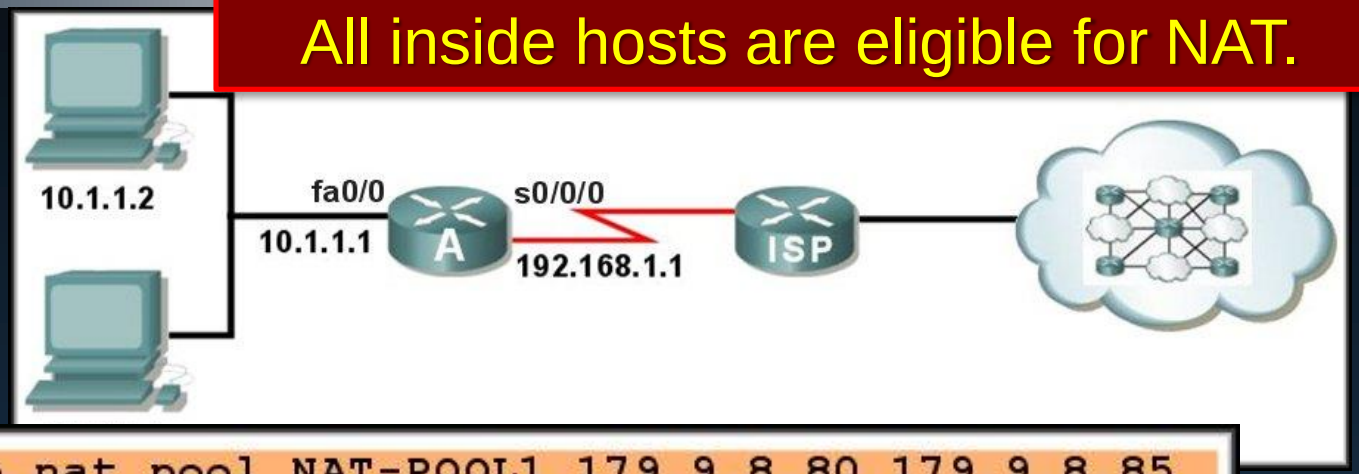



```
RA(config)#interface s0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#ip nat outside
```

Configuring Dynamic NAT

- Summary:

All inside hosts are eligible for NAT.




```
RA(config)#ip nat pool NAT-POOL1 179.9.8.80 179.9.8.85
                                 netmask 255.255.255.0
```

```
RA(config)#ip access-list standard NAT-LIST1
RA(config-nacl)#permit 10.1.0.0 0.0.0.255
```

```
RA(config)#ip nat inside source list NAT-LIST1 pool NAT-POOL1
```

```
RA(config)#interface fa0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.0
RA(config-if)#ip nat inside

RA(config)#interface s0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#ip nat outside
```

Configuring NAT Overload (PAT)

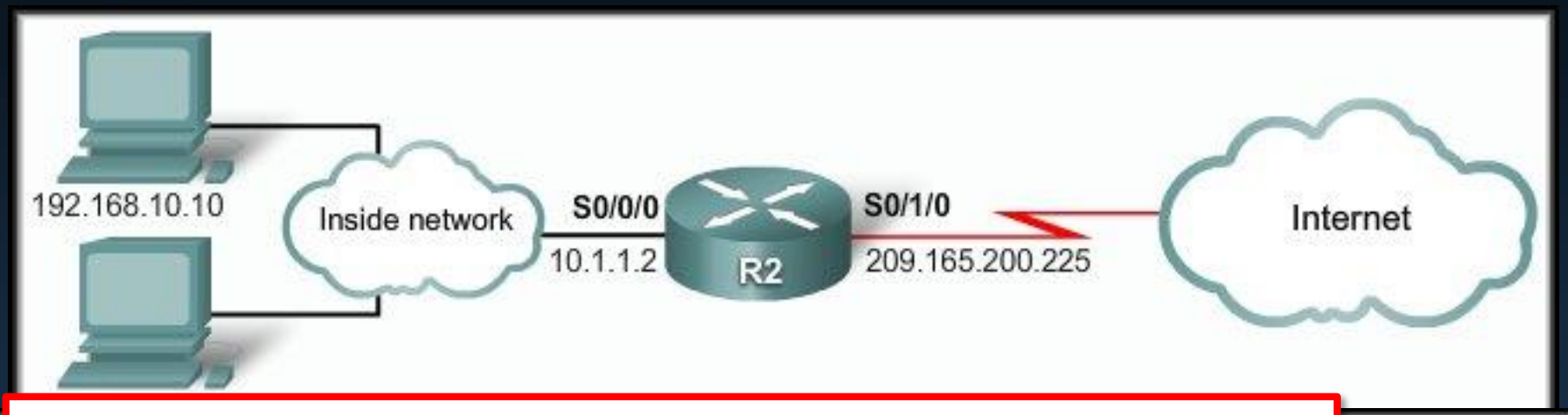
- There are two possible ways to configure overloading.
  - It depends on how the ISP allocates public IP addresses.
    - The ISP allocates one public IP address to the organization.
    - The ISP allocates more than one public IP address.
    - In either case, the configuration will include the **`overload`** keyword.
      - This keyword specifies to the router that Port Address Translation (PAT) is to be used.

Configuring NAT Overload (PAT)

- The ISP allocates one public IP address to the organization.
  1. Assign the IP address received from the ISP as the IP address of the outside interface.
  2. Define a standard access list permitting those addresses to be translated.
  3. Establish dynamic translation specifying the access list and the actual interface instead of a pool of addresses and include the **`overload`** keyword.
  4. Identify the inside and outside interfaces.

Configuring NAT Overload (PAT)

- The ISP allocates one public IP address to the organization.

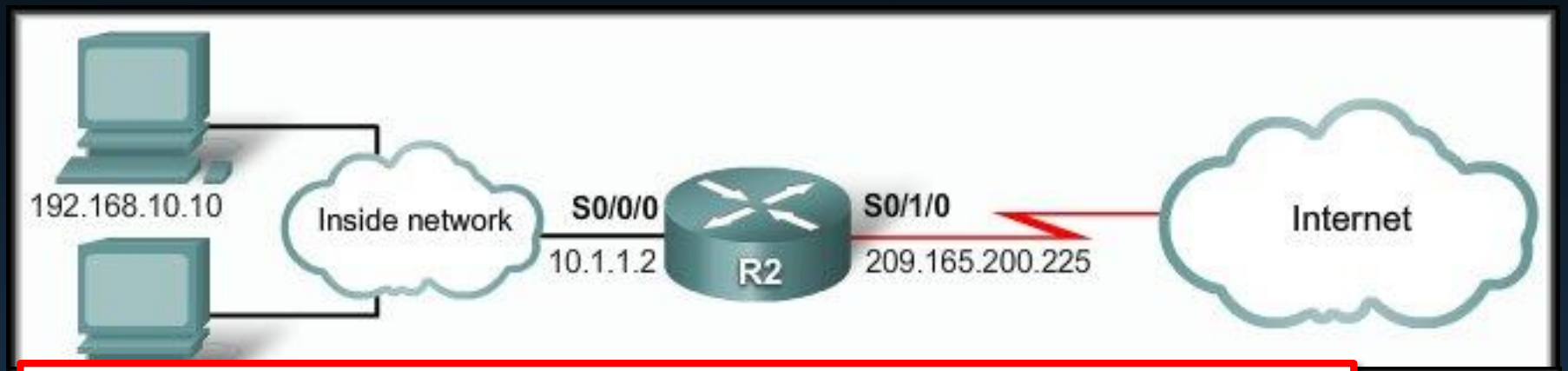



```
R2(config)#ip access-list standard NAT-LIST1
R2(config-nacl)#permit 192.168.0.0 0.0.255.255
R2(config)#ip nat inside source list NAT-LIST1 interface s0/1/0 overload

R2(config)#interface s0/0/0
R2(config-if)ip address 10.1.1.2 255.255.255.252
R2(config-if)ip nat inside

R2(config)#interface s0/1/0
R2(config-if)#ip address 209.165.200.225 255.255.255.252
R2(config-if)#ip nat outside
```

Assigned by ISP

Configuring NAT Overload (PAT)

- The ISP allocates more than one public IP address.



R2(config)#ip access-list standard NAT-LIST2
R2(config-nacl)#permit 192.168.0.0 0.0.255.255

```
R2(config)#ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
```

R2(config)#ip nat inside source list NAT-LIST2 pool NAT-POOL2 overload

```
R2(config)#interface s0/0/0
R2(config-if)ip address 10.1.1.2 255.255.255.252
R2(config-if)ip nat inside

R2(config)#interface s0/1/0
R2(config-if)#ip address 209.165.200.225 255.255.255.252
R2(config-if)#ip nat outside
```

Verifying NAT and NAT Overload

- **show ip nat translations**

```
R2#show ip nat translations
Pro Inside global          Inside local       Outside local      Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642  209.165.200.254:80  209.165.200.254:80
tcp 209.165.200.225:62452  192.168.11.10:62452  209.165.200.254:80  209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global          Inside local       Outside local      Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642  209.165.200.254:80  209.165.200.254:80
    create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452  192.168.11.10:62452  209.165.200.254:80  209.165.200.254:80
    create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

Verifying NAT and NAT Overload

- **show ip nat statistics**

```
R2#show ip nat translations
Pro Inside global          Inside local       Outside local      Outside global
icmp 209.165.200.225:3     192.168.10.10:3    209.165.200.254:3  209.165.200.254:3
tcp  209.165.200.225:11679 192.168.10.10:11679 209.165.200.254:80 209.165.200.254:80
icmp 209.165.200.225:0     192.168.11.10:0    209.165.200.254:0  209.165.200.254:0
tcp  209.165.200.225:14462 192.168.11.10:14462 209.165.200.254:80 209.165.200.254:80
```

```
R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

Verifying NAT and NAT Overload

- **clear 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

Troubleshooting NAT and NAT Overload

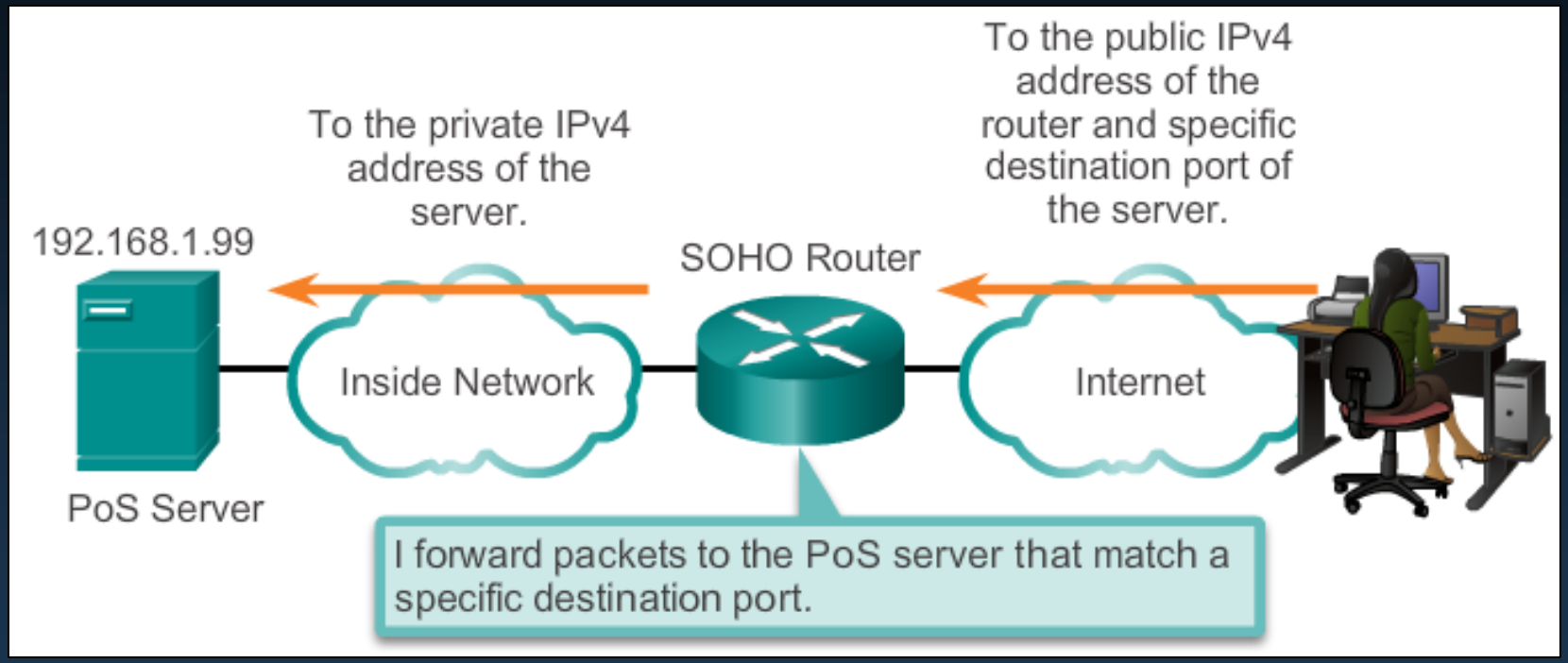
- **show ip nat translations**
- **clear ip nat translation**
- **debug ip nat**

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Oct  6 19:55:31.579: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14434]
*Oct  6 19:55:31.595: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6334]
*Oct  6 19:55:31.611: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14435]
*Oct  6 19:55:31.619: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14436]
*Oct  6 19:55:31.627: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14437]
*Oct  6 19:55:31.631: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6335]
*Oct  6 19:55:31.643: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6336]
*Oct  6 19:55:31.647: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14438]
*Oct  6 19:55:31.651: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6337]
*Oct  6 19:55:31.655: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14439]
*Oct  6 19:55:31.659: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6338]

<Output omitted>
```

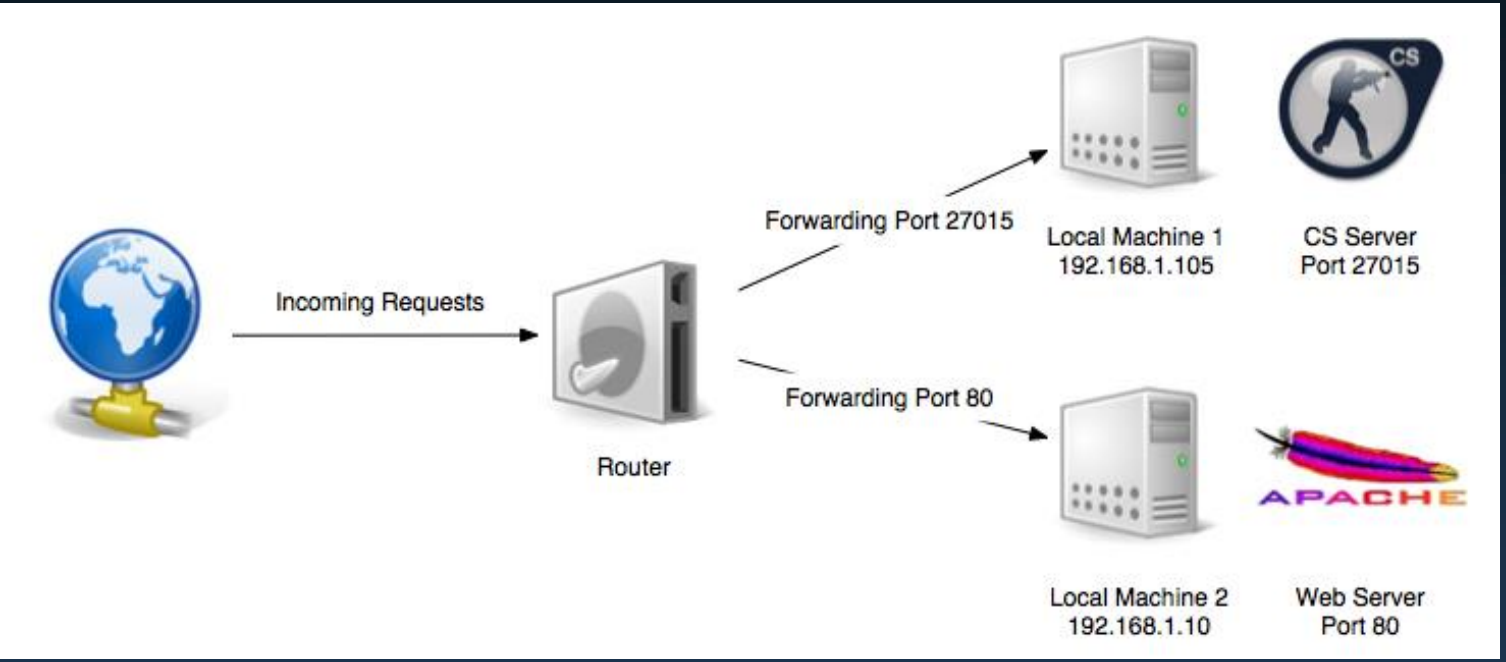
Port Forwarding

- Port forwarding on your router allows you to enter a port number (or possibly a range or combination of numbers, depending on the router), and an IP address.
- All incoming connections with a matching port number will be forwarded to the internal computer with that address.
- A packet sent to the public IP address and port of a router can be forwarded to a private IP address and port in inside network.
- Port forwarding is helpful in situations where servers have private addresses, not reachable from the outside networks.

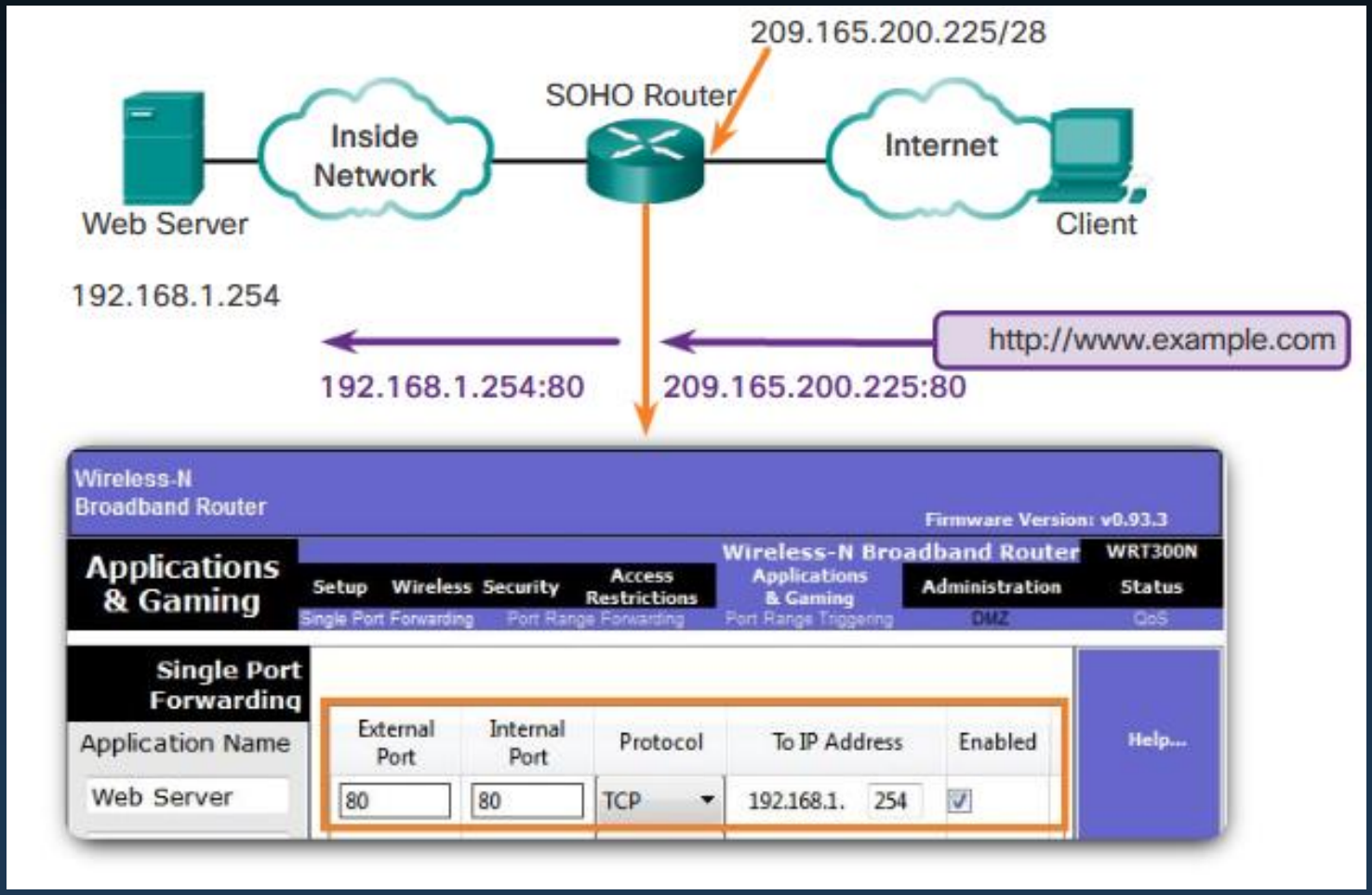
Port Forwarding



Port Forwarding

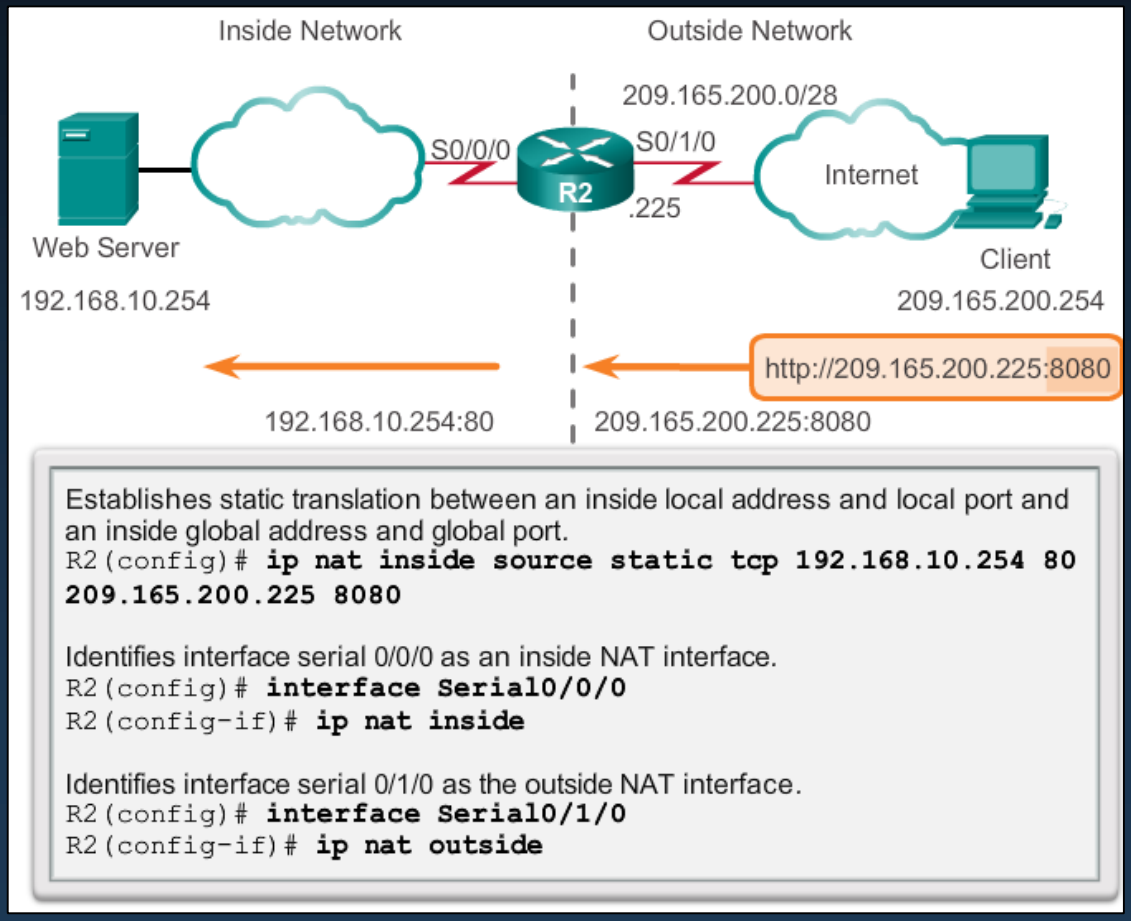


SOHO Example



Configuring Port Forwarding with IOS

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



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

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

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

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

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

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