BRAC UNIVERSITY

Inspiring Excellence

DHCPv4 & NAT

Lecture 09 | CSE421 – Computer Networks

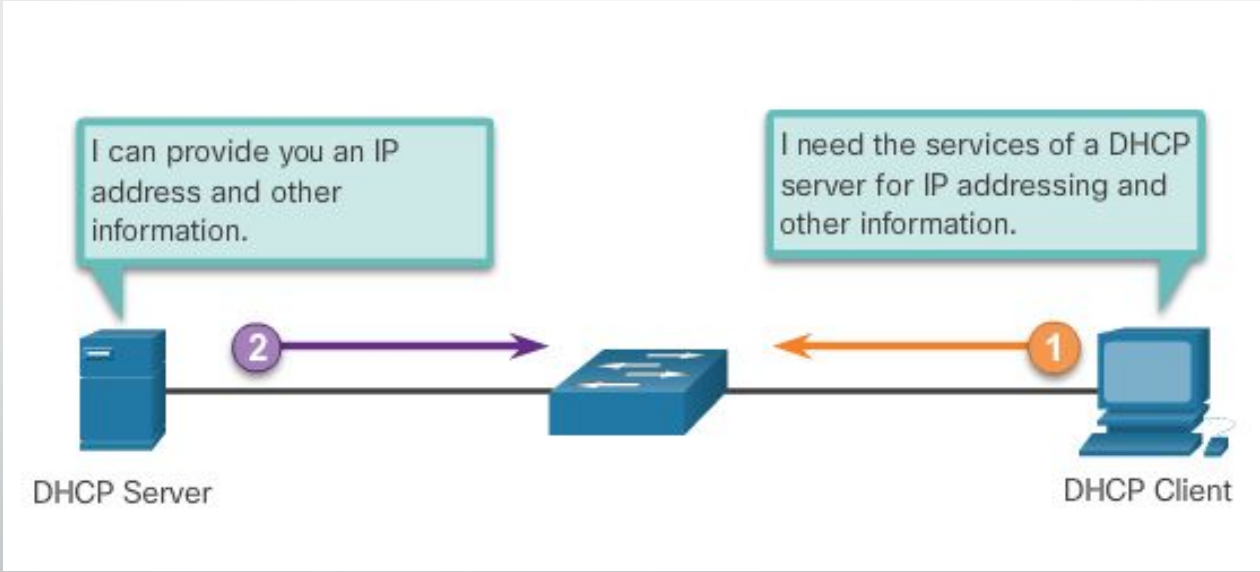
Department of Computer Science and Engineering
School of Data & Science

Objectives

- DHCPv4
- Configure a Cisco IOS DHCPv4 Server
- Configure a DHCPv4 Client
- NAT Concepts
  - Introduction to NAT
  - PAT (NAT Overloading)
  - Port Forwarding

BRAC UNIVERSITY
Inspiring Excellence

DHCPv4 Concepts



Why DHCP?

- Every device that connects to a network needs an IP address.
  - Network administrators assign static IP addresses to routers, servers, and other network devices whose locations (physical and logical) are not likely to change.
  - User computers in an organization often change locations, physically and logically.
    - Mobile/Moving clients do not require a static address.
    - A workstation can use any address within a range of addresses.
    - This range is typically within an IP subnet.

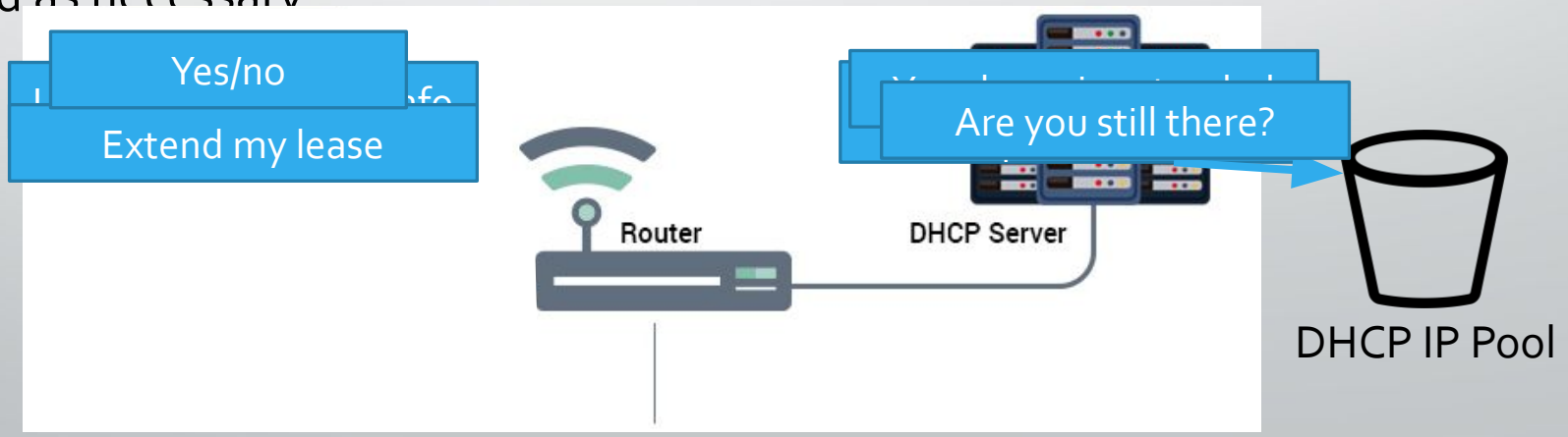
DHCP Operations

- Dynamic Host Configuration Protocol v4 (DHCPv4) **assigns IPv4 addresses** and **other network configuration** information **dynamically**.
- A dedicated DHCPv4 server is **scalable and relatively easy to manage**. However, in a small branch or SOHO location, a **Cisco router can be configured to provide DHCPv4 services** without the need for a dedicated server.
- The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a **pool of addresses** for a **limited period of time** chosen by the server, or until the client no longer needs the address.
- Clients **lease** the information from the server for an **administratively defined period**. The lease is typically anywhere from few hours to a week or more. When the **lease expires**, the client must ask for an extension of the lease.

DHCP Operations (Continued)

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client.

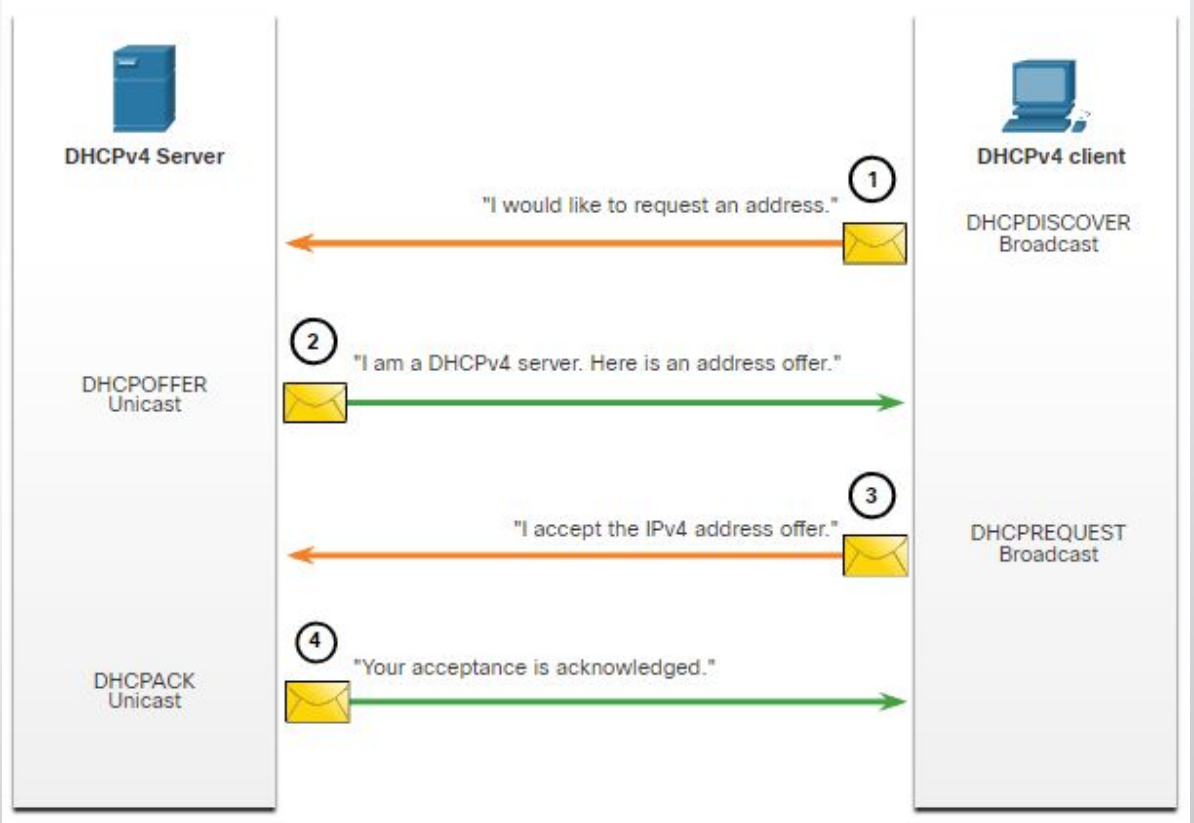
- The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease.
- This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need.
- When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary



Steps to Obtain a Lease (DORA)

When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease:

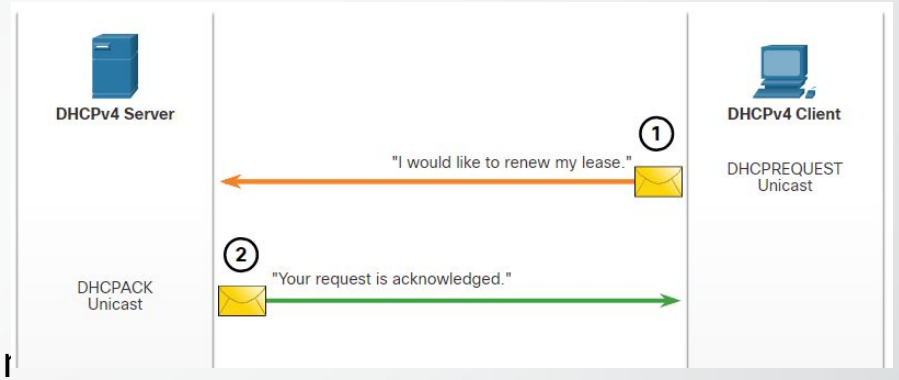
- **DHCP Discover (Broadcast)**
  - Finds the DHCP server(s) on the network.
- **DHCP Offer (Unicast)**
  - Contains an available IP address to lease
- **DHCP Request (Broadcast)**
  - It serves as an acceptance notice to the selected server and an implicit decline to any other servers
  - Also used for lease renewal and verification
- **DHCP Acknowledgment (Unicast)**




```
IP address: 192.168.10.15
Subnet mask: 255.255.255.0
Default gateway: 192.168.10.1
DNS servers:
Lease Time: 3 days
```

Steps to Renew a Lease

Prior to lease expiration, the client begins a two-step process to renew the lease with the DHCPv4 server, as shown in the figure:

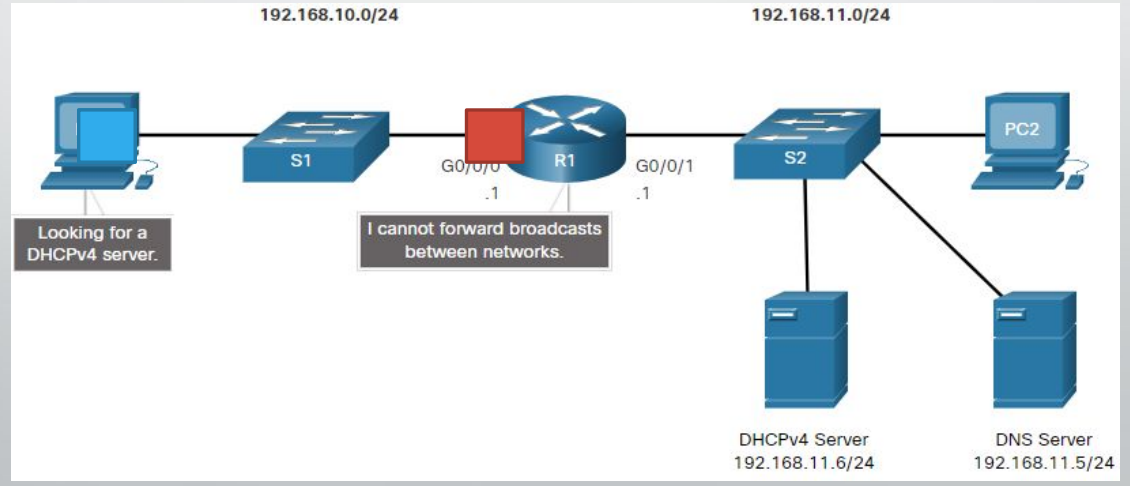


- **DHCP Request (DHCPREQUEST)**
  - Before the lease expires, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.
- **DHCP Acknowledgment (DHCPACK)**
  - On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK.

Note: These messages (primarily the DHCPOFFER and DHCPACK) can be sent as unicast or broadcast according to IETF RFC 2131.

DHCP Relay

- In a complex hierarchical network, enterprise servers are usually located centrally. These servers may provide DHCP, DNS, TFTP, and FTP services for the network. Network clients are not typically on the same subnet as those servers. In order to locate the servers and receive services, clients often use broadcast messages.
- In the figure, PC1 is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. In this scenario, R1 is not configured as a DHCPv4 server and does not forward the broadcast. Because the DHCPv4 server is located on a different network, PC1 cannot receive an IP address using DHCP. R1 must be configured to relay DHCPv4 messages to the DHCPv4 server.



Other Service Broadcast Relayed

DHCPv4 is not the only service that the router can be configured to relay. By default, the ip helper-address command forwards the following eight UDP services:

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP server
- Port 68: DHCP/BOOTP client
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

Configuring DHCP Relay

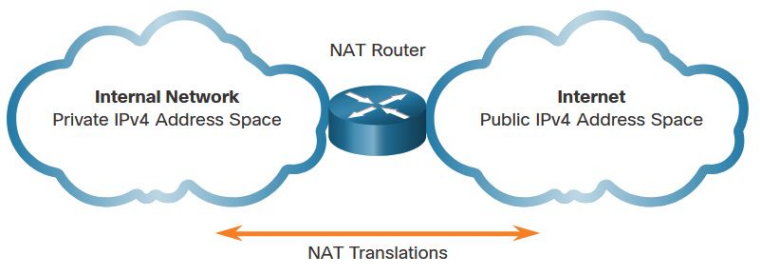
- Configure R1 with the **ip helper-address [address]** interface configuration command. This will cause R1 to relay DHCPv4 broadcasts to the DHCPv4 server. As shown in the example, the interface on R1 receiving the broadcast from PC1 is configured to relay DHCPv4 address to the DHCPv4 server at 192.168.11.6.
- When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6. The network administrator can use the show ip interface command to verify the configuration.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
(output omitted)
```

BRAC UNIVERSITY
Inspiring Excellence

NAT



Scaling Networks with NAT

- Reuse IP addresses by using NAT by creating two types of addresses: Private and Public Addressing.
  - All public Internet addresses must be registered with a Regional Internet Registry (RIR).
- Organizations can lease public addresses from an ISP.
  - Then, they can use the private addresses in their internal networks
- 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

Category of Addresses

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

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

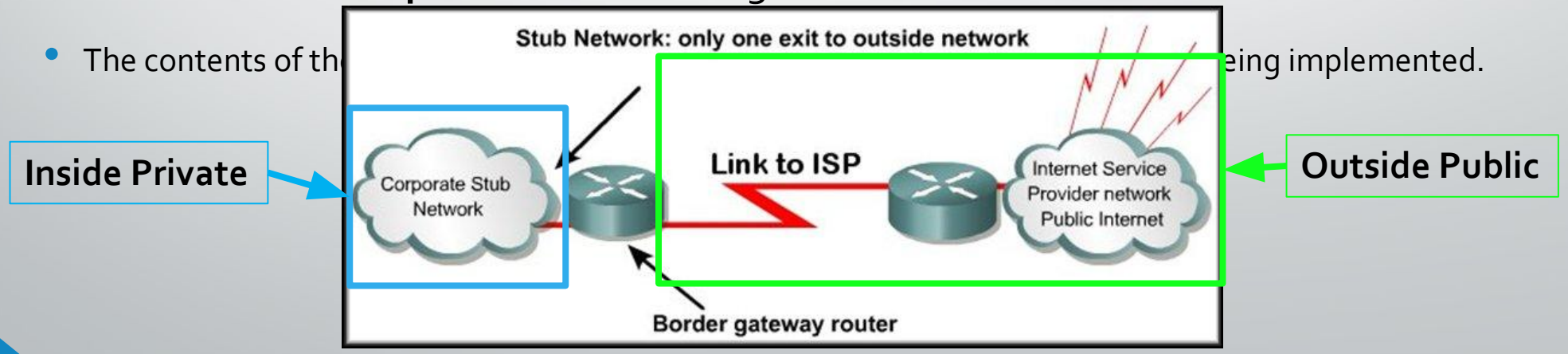
- Public Internet Addresses
  - These are for public routing
  - Can be advertised globally.

What is NAT?

- Networks need a mechanism to **translate private addresses to public addresses** at the edge of their network that works in both directions.
- **NAT-enabled routers** retain one or many valid Internet IP addresses outside of the network and uses DHCP to provide private IPs to the users 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.

How NAT Works

- A NAT enabled device typically operates **at the border** of a stub network.
- When a host on the **inside (private) network** wants to access a host on the **outside (public) network**, the packet is sent to the border gateway router.
  - **Inside Network:** Usually an organization's LAN
  - **Outside Network:** usually the Internet but it can be any network
- The border gateway router performs the NAT process, **translating the inside private address to an outside public address** using an internal translation table.
  - The contents of th eing implemented.



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.
  - **Local address -** A local address appears on the inside portion of the network.
  - **Global address -** A global address appears on the outside portion of the network.

Types of Addresses

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

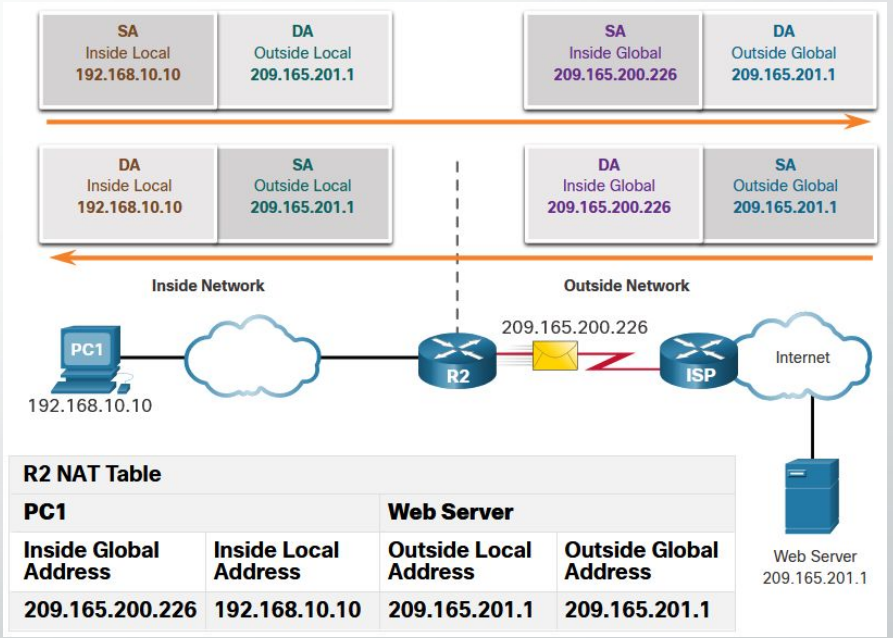
- The address of source as seen from the outside network. The inside global address of PC1 is 209.165.200.226

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

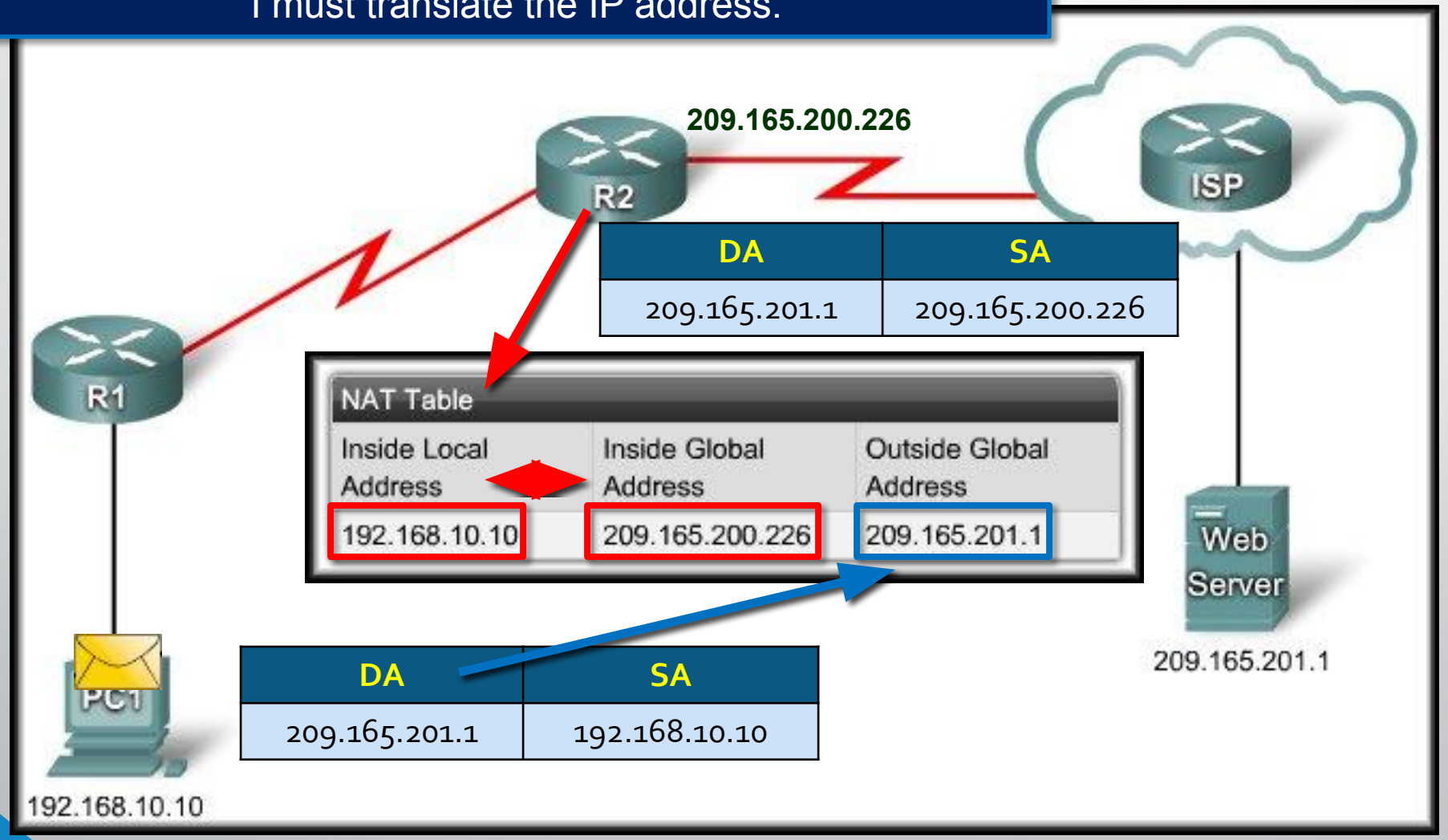
- The address of the destination as seen from the inside network. PC1 sends traffic to the web server at the IPv4 address 209.165.201.1. While uncommon, this address could be different than the globally routable address of the destination.



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

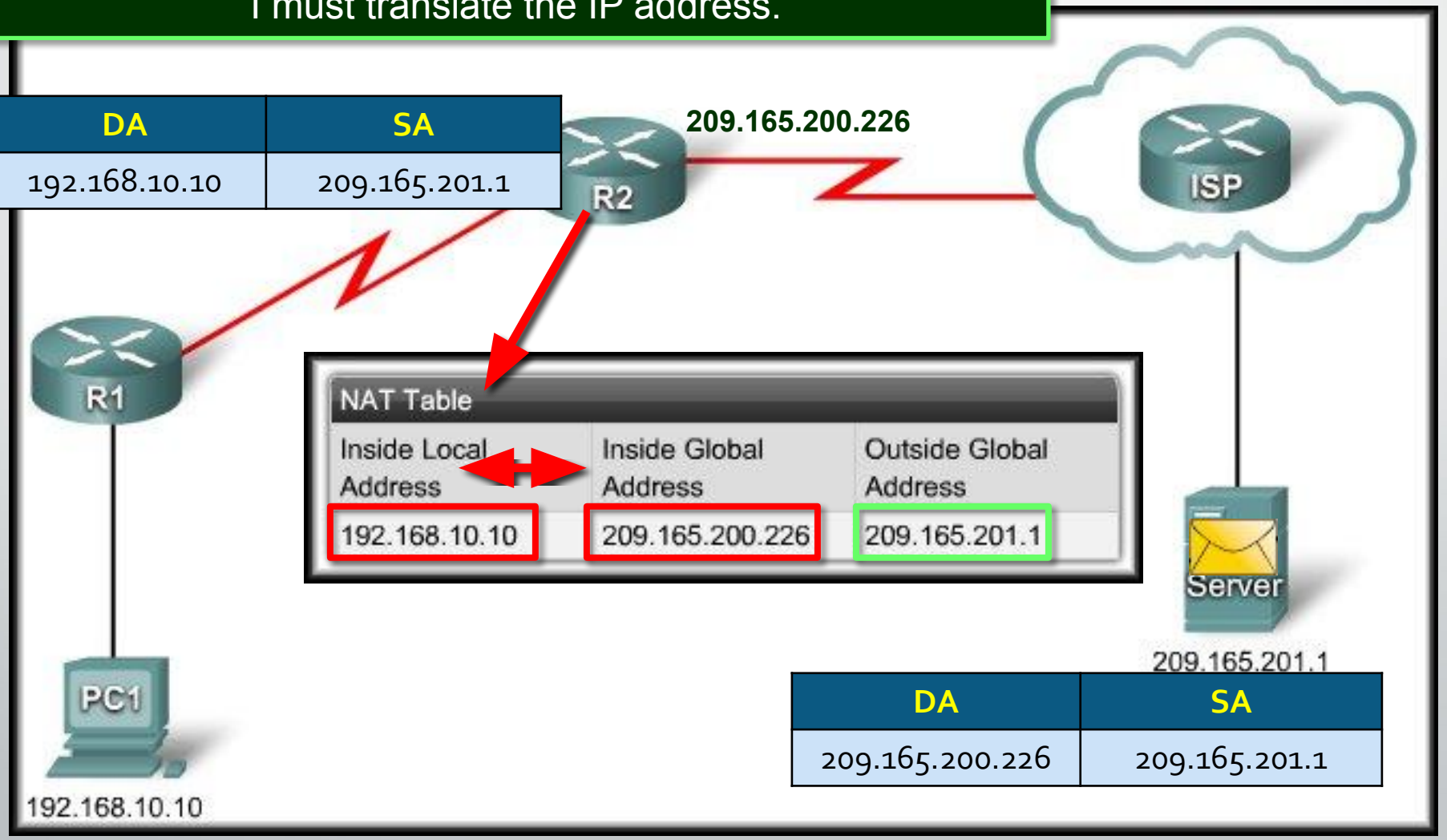
Example: NAT; Sending

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



Example: NAT; Receiving

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



Advantages of NAT

BRAC UNIVERSITY
Inspiring Excellence

- 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**.

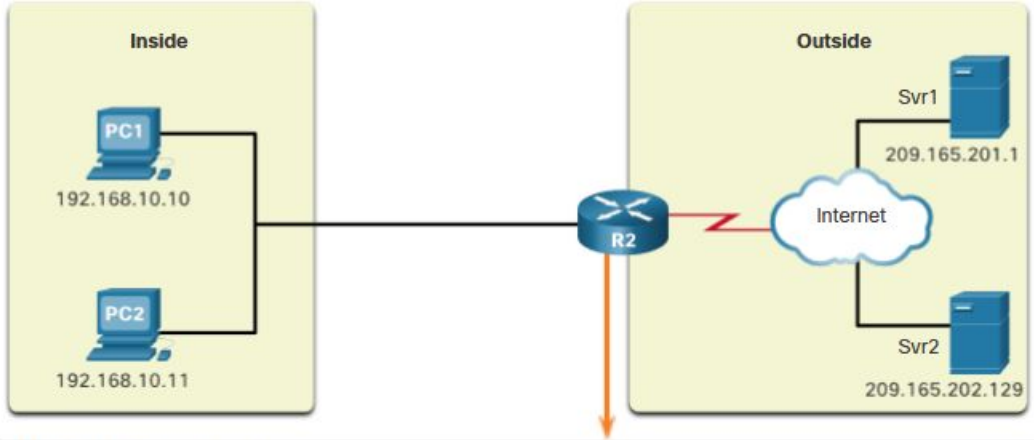
BRAC UNIVERSITY
Inspiring Excellence

PAT (NAT Overload)

PAT

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.



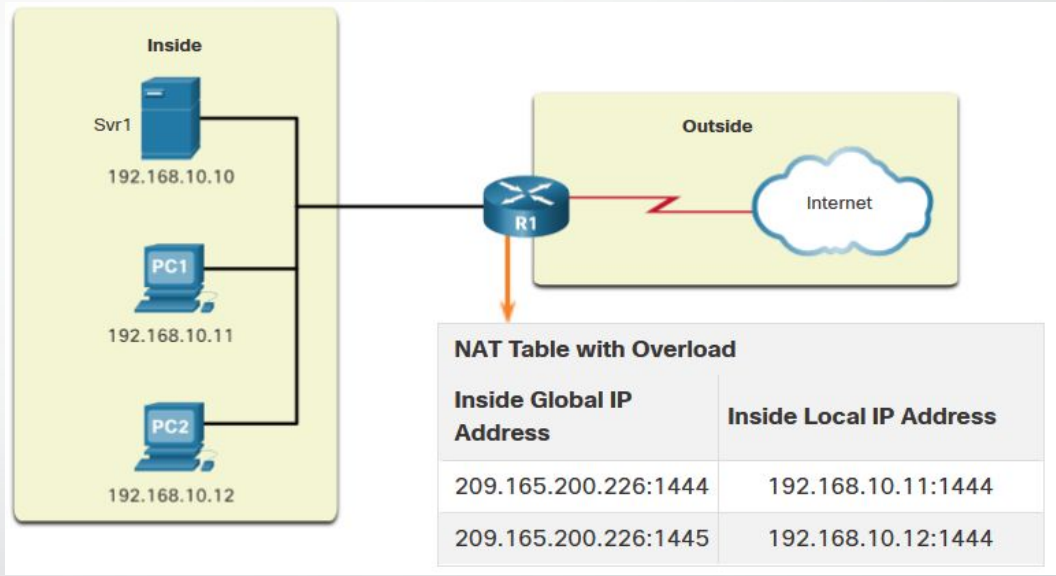
NAT Table with Overload

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 Table with Overload

Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

Packets without Layer 4 Segments

Some packets do not contain a Layer 4 port number, such as ICMPv4 messages. Each of these types of protocols is handled differently by PAT.

For example, ICMPv4 query messages, echo requests, and echo replies include a Query ID. ICMPv4 uses the Query ID to identify an echo request with its corresponding echo reply.

Note: Other ICMPv4 messages do not use the Query ID. These messages and other protocols that do not use TCP or UDP port numbers vary and are beyond the scope of this curriculum.

NAT vs PAT

- NAT - Only modifies the IPv4 addresses

Inside Global Address	Inside Local Address
209.165.200.226	192.168.10.10

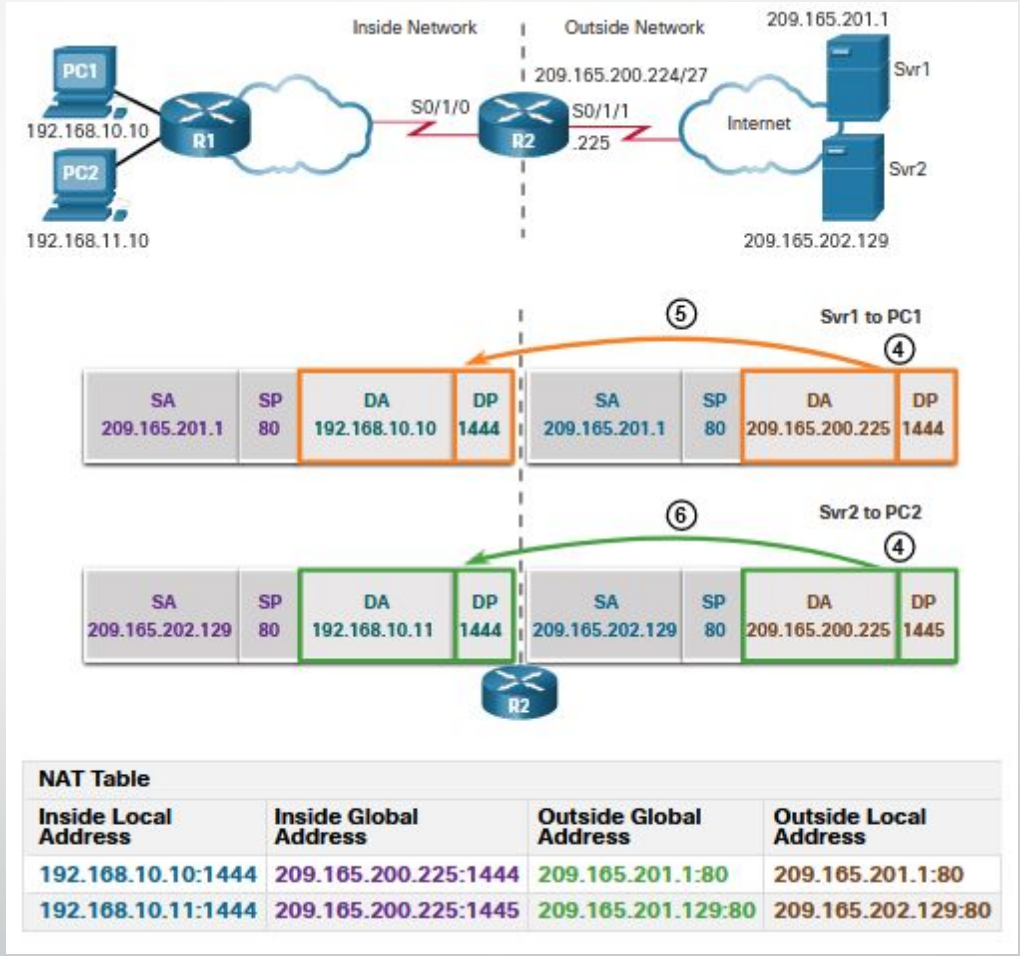
- PAT - PAT modifies both the IPv4 address and the port number.

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.

Example: 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.

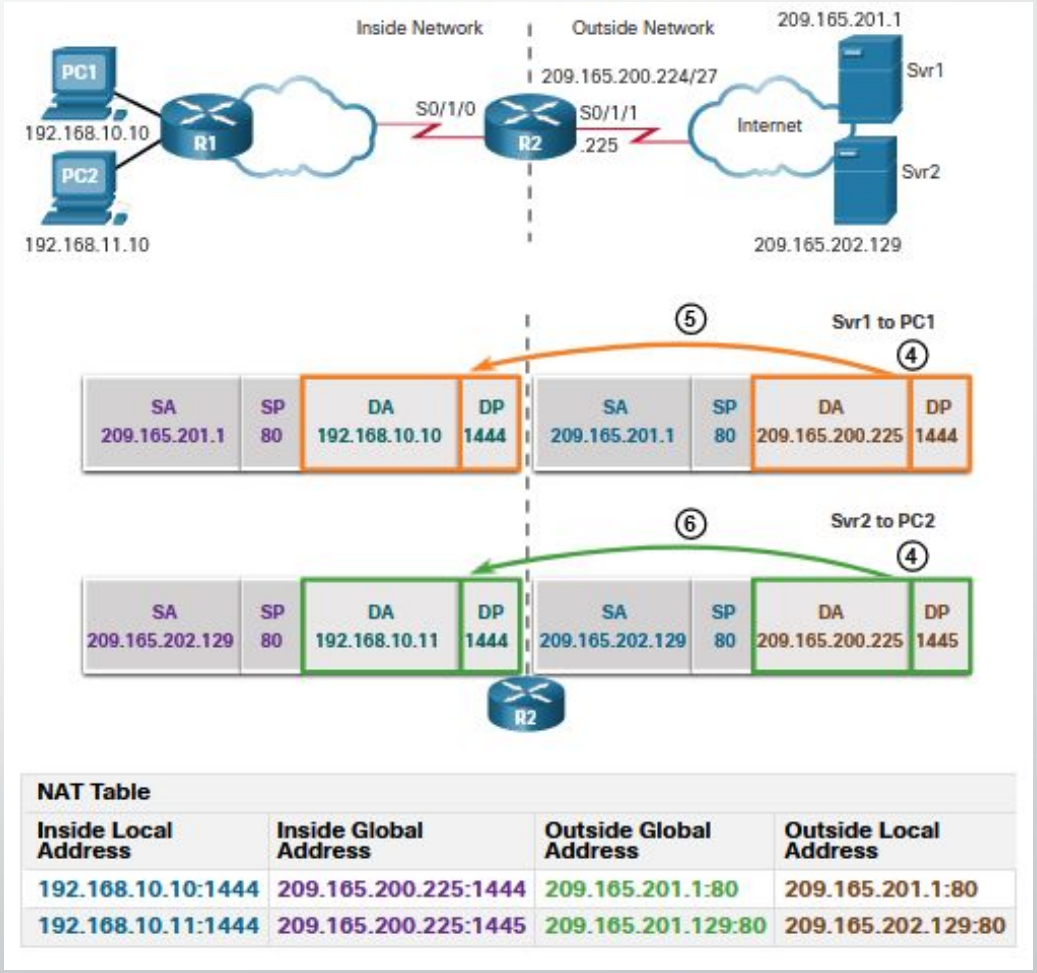


NAT Table

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

Example: 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.

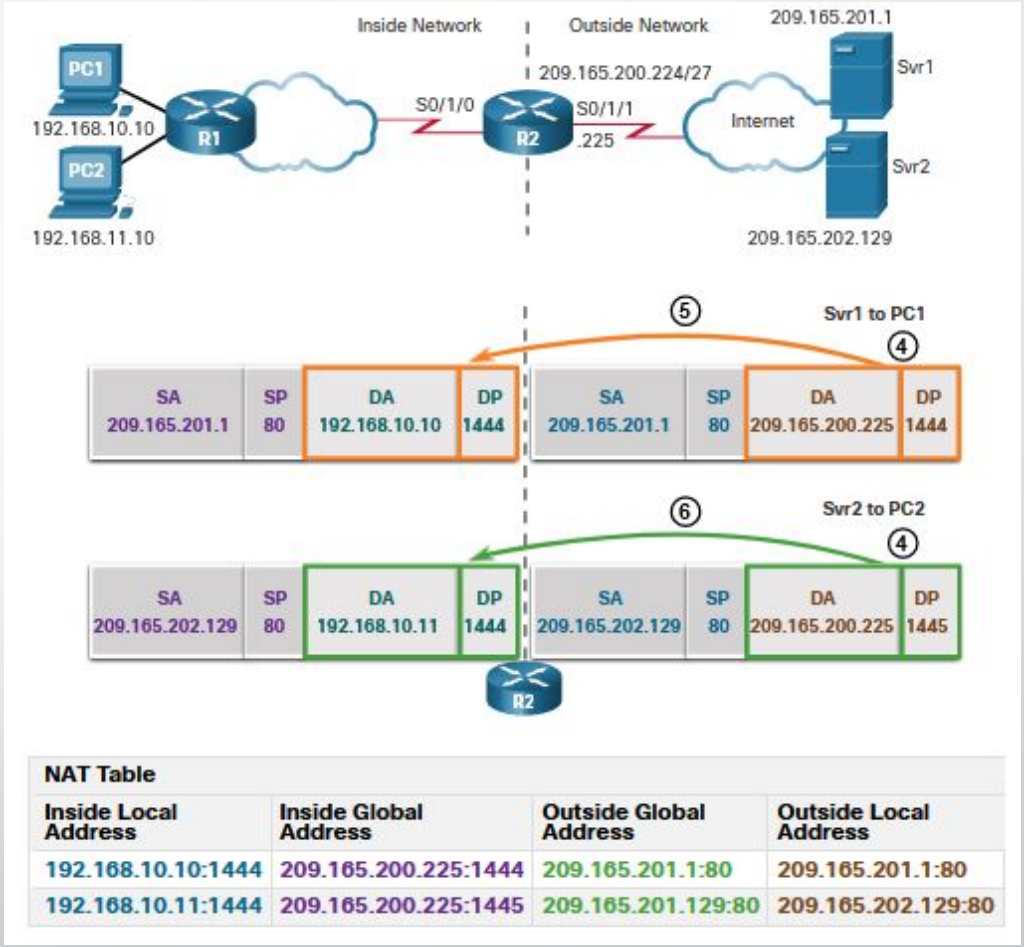


NAT Table

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

Example: 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

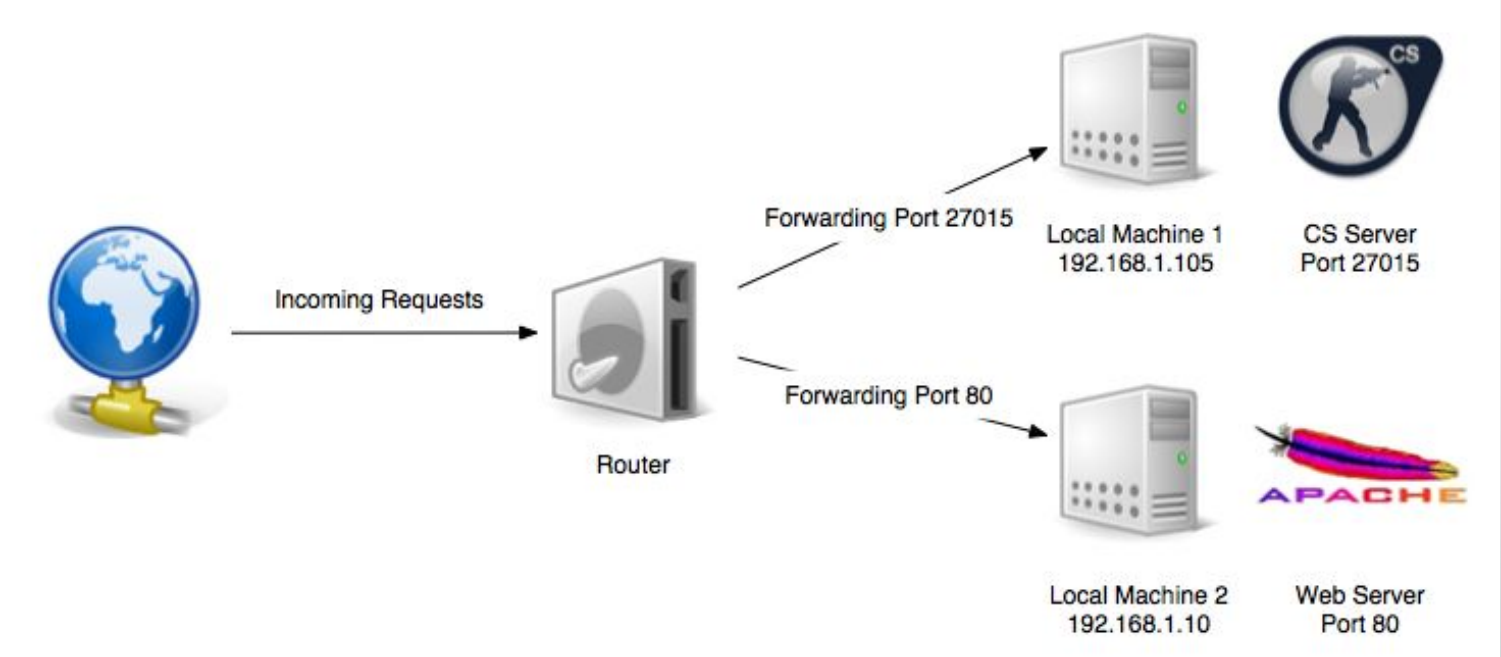
BRAC UNIVERSITY
Inspiring Excellence

Port Forwarding

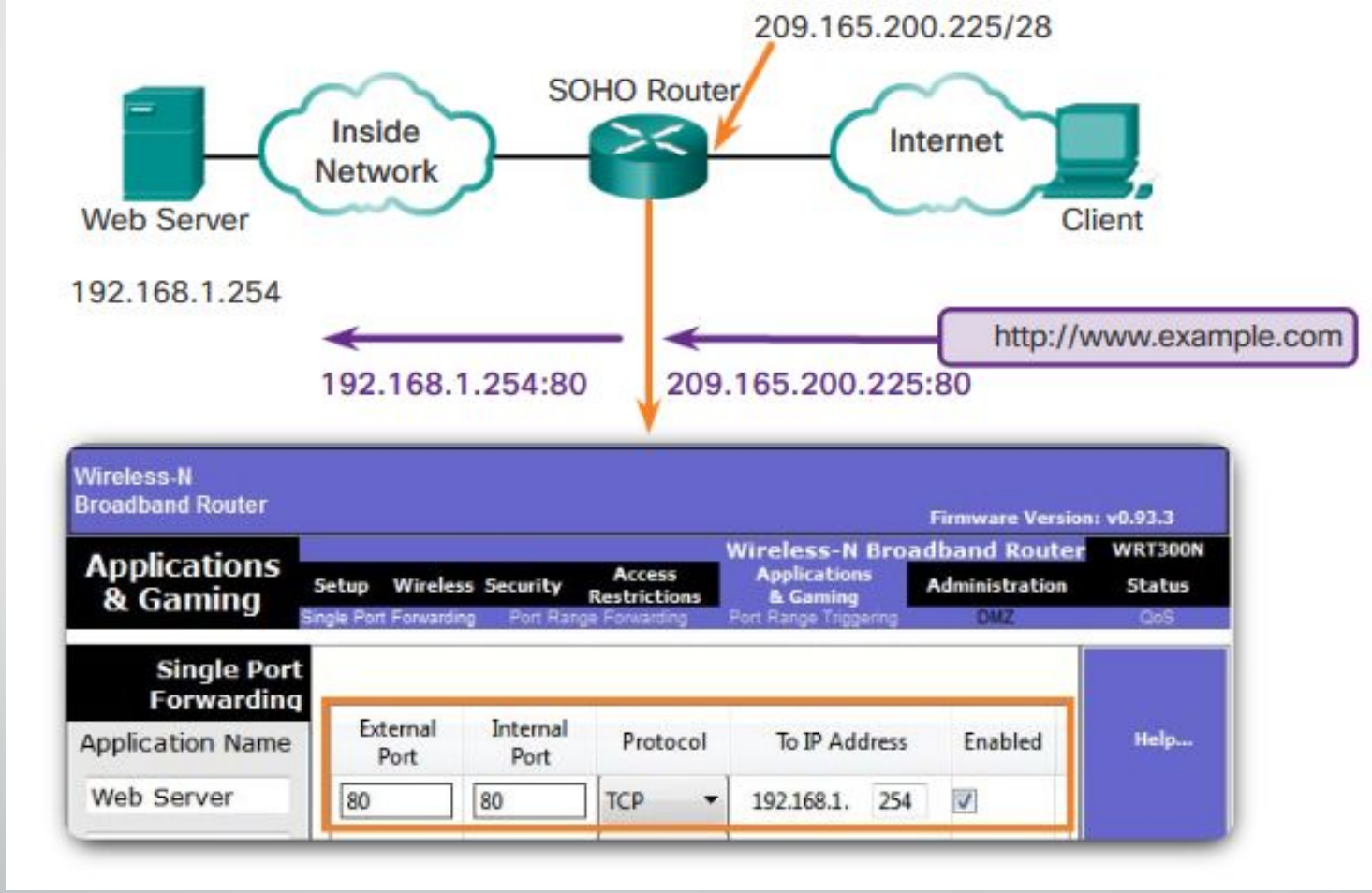
Port Forwarding

- 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.

Example: Port Forwarding

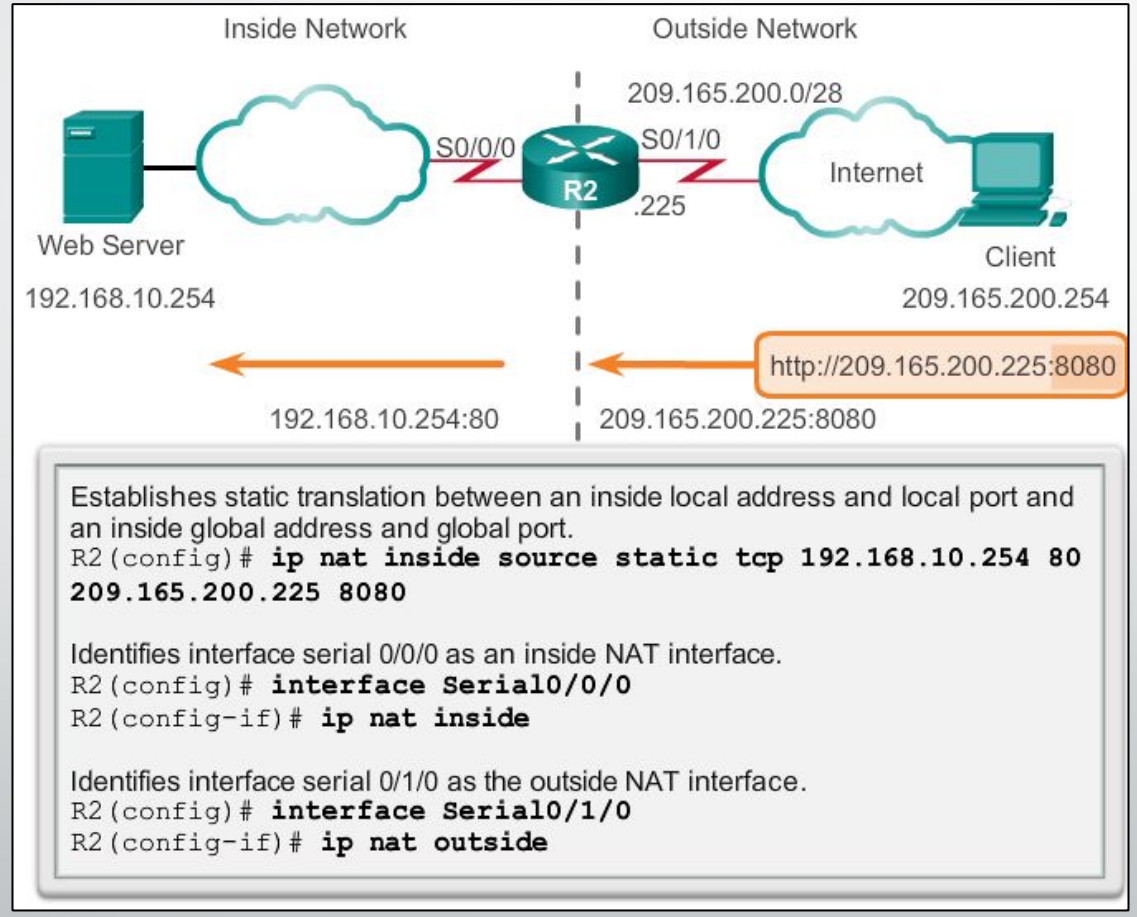


Example: Port Forwarding; SOHO



Configuring Port Forwarding

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



BRAC UNIVERSITY
Inspiring Excellence

The End