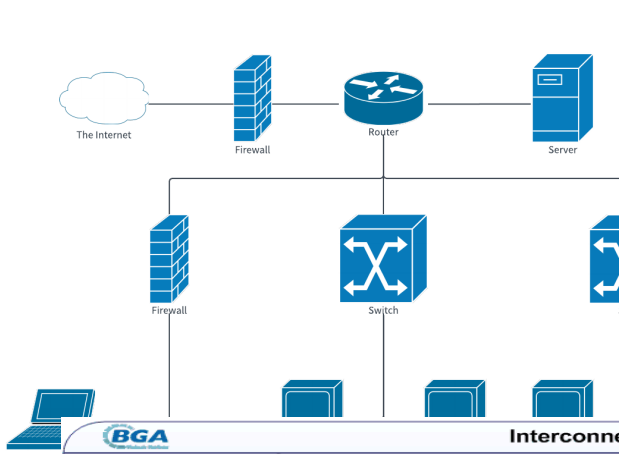
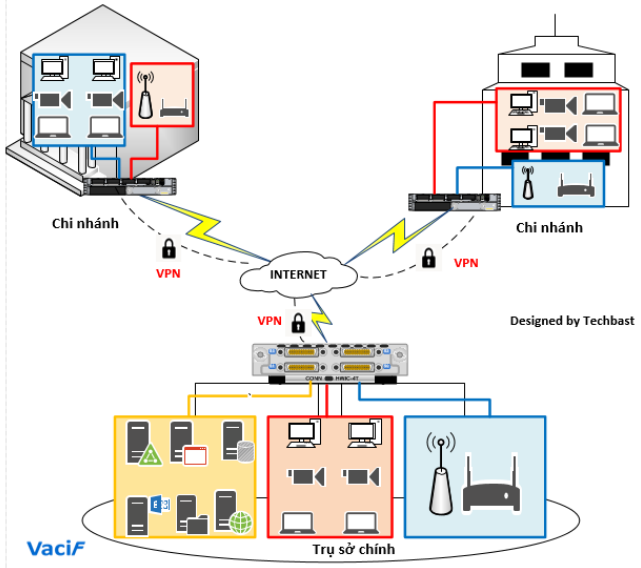
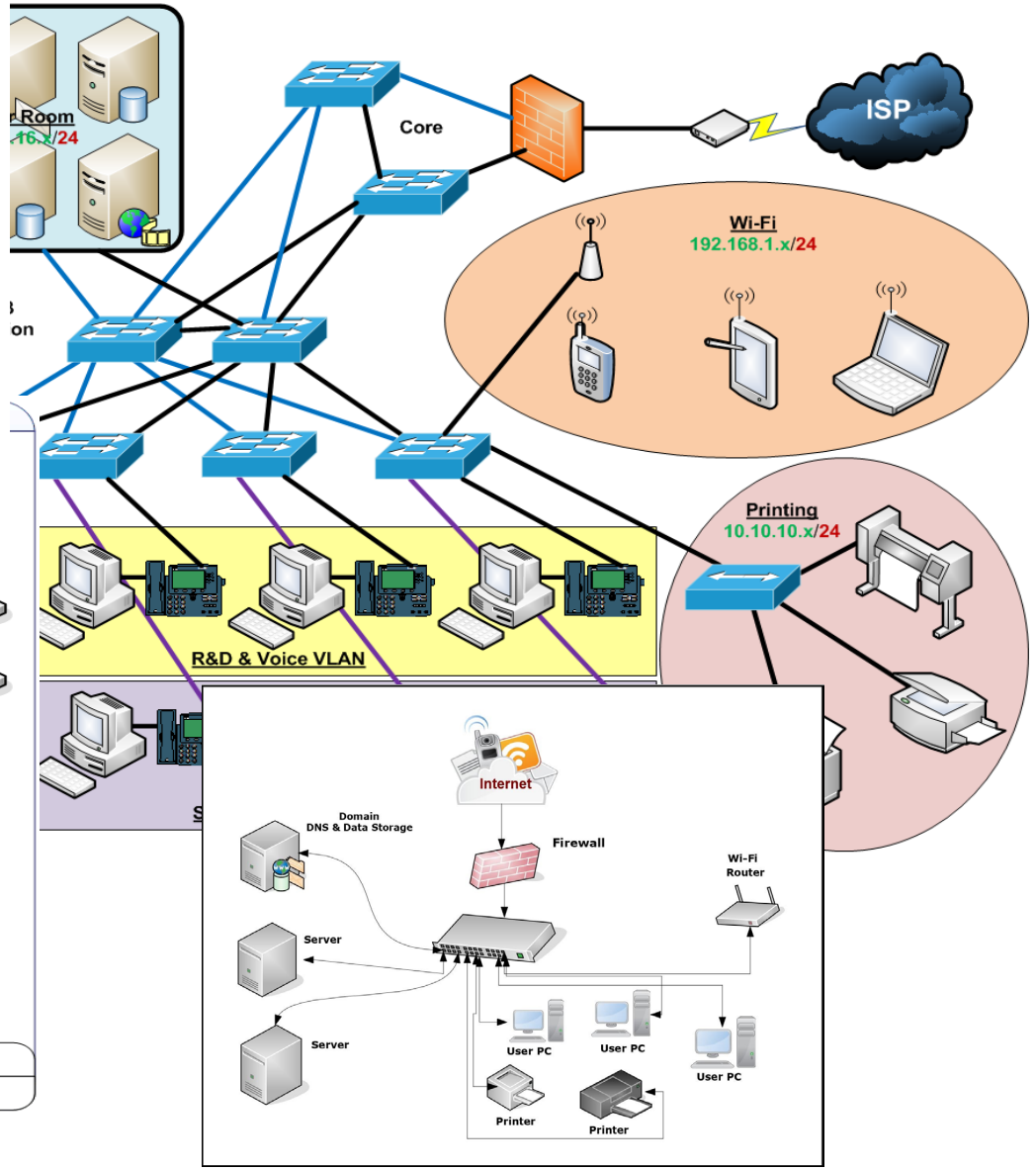
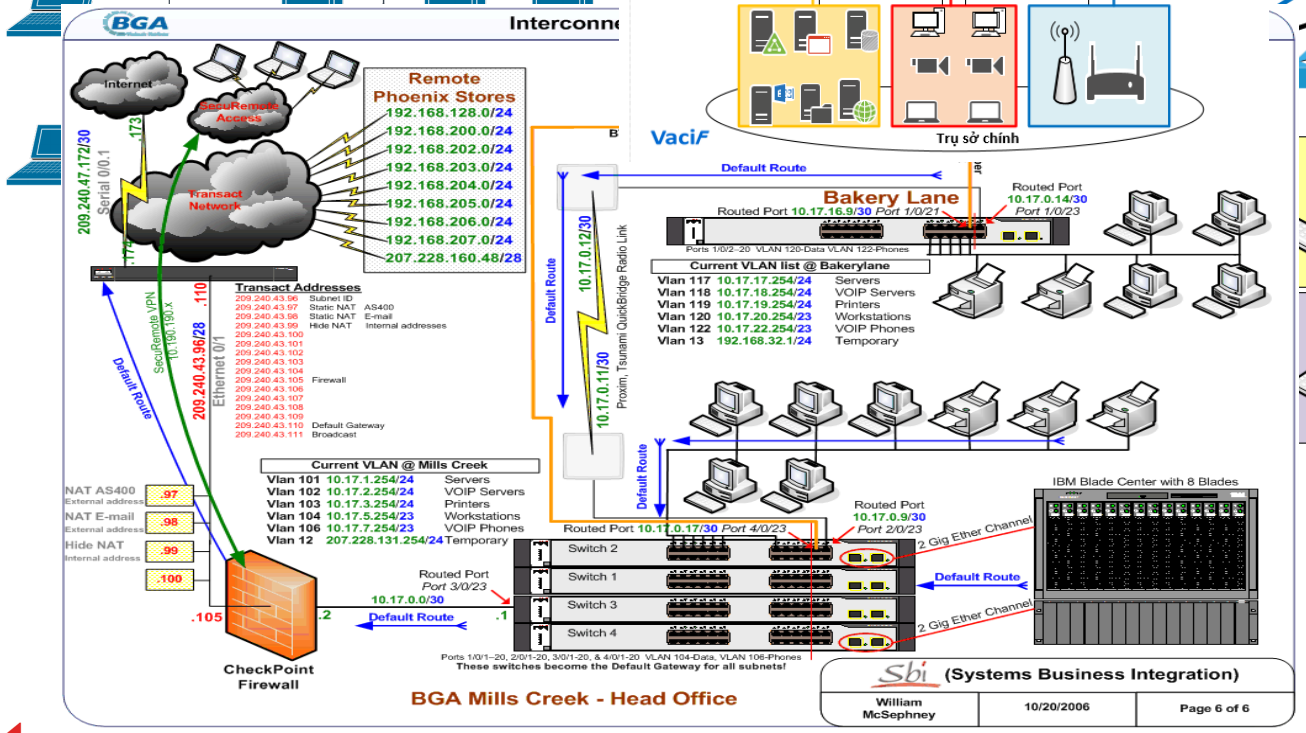
NAT


The Internet
Firewall
Router
Server
Firewall
Switch


Chi nhánh
Chi nhánh
VPN
INTERNET
VPN
VPN
Designed by Techbast
Trụ sở chính
VaciF


Room
Core
ISP
Wi-Fi
192.168.1.x/24
Printing
10.10.10.x/24
R&D & Voice VLAN
Internet
Domain
DNS & Data Storage
Firewall
Wi-Fi
Router
Server
Server
User PC
User PC
User PC
Printer
Printer


BGA
Interconne
Internet
SecuRemote Access
Transact Network
209.240.47.172/30
Serial 0/0/1
Remote Phoenix Stores
192.168.128.0/24
192.168.200.0/24
192.168.202.0/24
192.168.203.0/24
192.168.204.0/24
192.168.205.0/24
192.168.206.0/24
192.168.207.0/24
207.228.160.48/28
Transact Addresses
209.240.43.96/28
Ethernet 0/1
SecuRemote VPN
10.190.190.x
Default Route
Default Route
Bakery Lane
Routed Port 10.17.16.9/30 Port 1/0/21
Routed Port 10.17.0.14/30 Port 1/0/23
Current VLAN list @ Bakerylane
Vlan 117 10.17.17.254/24 Servers
Vlan 118 10.17.18.254/24 VOIP Servers
Vlan 119 10.17.19.254/24 Printers
Vlan 120 10.17.20.254/23 Workstations
Vlan 122 10.17.22.254/23 VOIP Phones
Vlan 13 192.168.32.1/24 Temporary
10.17.0.12/30
10.17.0.11/30
Proxim, Tsunami QuickBridge Radio Link
Current VLAN @ Mills Creek
Vlan 101 10.17.1.254/24 Servers
Vlan 102 10.17.2.254/24 VOIP Servers
Vlan 103 10.17.3.254/24 Printers
Vlan 104 10.17.5.254/23 Workstations
Vlan 106 10.17.7.254/23 VOIP Phones
Vlan 12 207.228.131.254/24 Temporary
NAT AS400
NAT E-mail
Hide NAT
Routed Port 10.17.0.17/30 Port 4/0/23
Routed Port 10.17.0.9/30 Port 2/0/23
IBM Blade Center with 8 Blades
Switch 2
Switch 1
Switch 3
Switch 4
2 Gig Ether Channel
2 Gig Ether Channel
Routed Port Port 3/0/23
10.17.0.0/30
Default Route
Default Route
CheckPoint Firewall
BGA Mills Creek - Head Office
Sbi (Systems Business Integration)
William McSephney
10/20/2006
Page 6 of 6

INFO-6047 Switching and Routing

ISM1 - Information Security Management (ISM1-ITY-20189) Detailed Weekly Content

Week	Date of Lecture or Tests, 7:00 – 9:00 PM EST	Lecture/Test	Reading	Lab Time INFO-6047-01 Wednesday 5:00 – 8:00 PM EST INFO-6047-02 Tuesday 5:00 – 8:00 PM EST	Grade
Week 01	Monday, January 02, 2023	College-Wide Orientation			
Week 02	Monday, January 09, 2023	Introduction	N/A	Lab 01 - Basics of PT	3.0%
Week 03	Monday, January 16, 2023	Basics of Routing	Chapter 01 & 02 *(Introduction to Networking, Network Media Copper)*	Lab 02 - Intro to Routing	3.0%
Week 04	Monday, January 23, 2023	Basics of Switching	Chapter 03 & 04 *(Network Media Fiber Network Media Wireless)*	Lab 03 - Intro to Switching	3.0%
Week 05	Monday, January 30, 2023	VLANs	Chapter 05 *(Data Encoding & Transmission)*	Lab 04 - VLANs	3.0%
Week 06	Monday, February 06, 2023	Routing	Chapter 06 *(Network OS & Communications)*	Lab 05 - Routing	3.0%
Week 07	Monday, February 13, 2023	Mid-Term Test		Mid-Term (Test 1)	32.0%
Study Break	Monday, February 20, 2023	Study Break - No Class This Week			
Week 08	Monday, February 27, 2023	Inter-VLAN Routing	Chapter 10 *(TCP/IP Fundamentals)*	Lab 06 - Inter VLAN Routing	3.0%
Week 09	Monday, March 06, 2023	Static Routing	Chapter 11 *(Subnetting)*	Lab 07 - Static & Default Routs	3.0%
Week 10	Monday, March 13, 2023	Dynamic Routing - RIP	Chapter 12 *(Additional Transmission Modalities)*	Lab 08 - RIP Protocol	3.0%
Week 11	Monday, March 20, 2023	Dynamic Routing - OSPF	Chapter 14 *(RA & LD Communications)*	Lab 09 - OSPF Protocol	3.0%
Week 12	Monday, March 27, 2023	Access Control Lists	Chapter 15 *(Network Security)*	Lab 10 - ACLs	3.0%
Week 13	Monday, April 03, 2023	DHCP	Chapter 16 *Maintaining the Network)*	Lab 11 - DHCP	3.0%
Week 14	Monday, April 10, 2023	NAT	Chapter 17 *(Troubleshooting Fundamentals of a Network)*	Lab 12 - NAT	3.0%
Week 15	Monday, April 17, 2023	Final Test		Final Test (Test 2)	32%

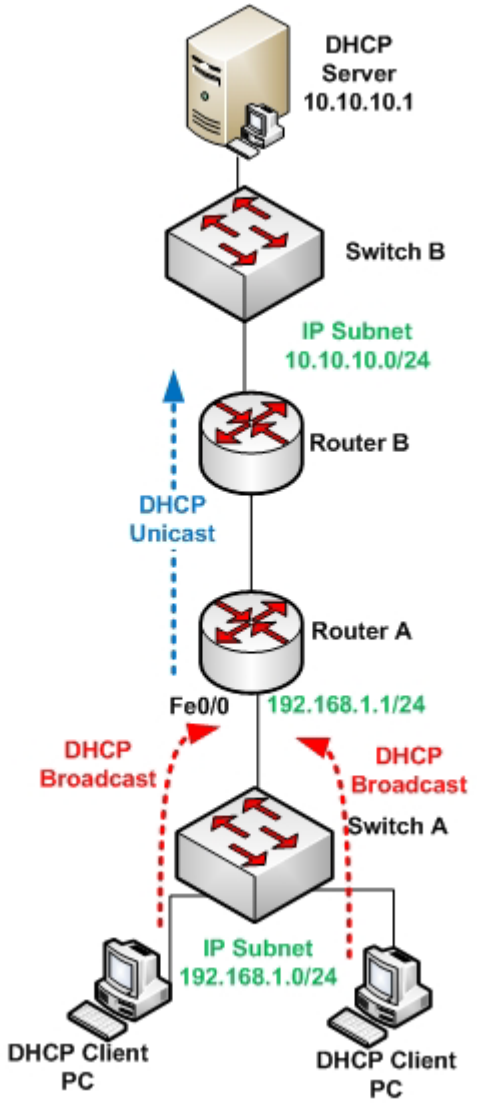
Final Exam

- Section 1 and 2
- When: Monday April 17th at 7:00 PM
- Where: B1071
- How: Open book (120 minutes for 120 points)
  - Allowed resources: Lecture slides, labs, and textbook
  - Not allowed: Phones, Google, and instant messaging.
- Note: Bring your laptop charger as you will be asked to keep your screen brightness up and to avoid having your laptop battery dying.

- Online and part-time
- When: Tuesday April 18th 12:00 AM to 11:59 PM (24 hours to begin exam)
- Where: Online (120 minutes for 120 points)
- How: Open book
  - Allowed resources: Lecture slides, labs, and textbook
  - Not allowed: Phones, Google, and instant messaging.

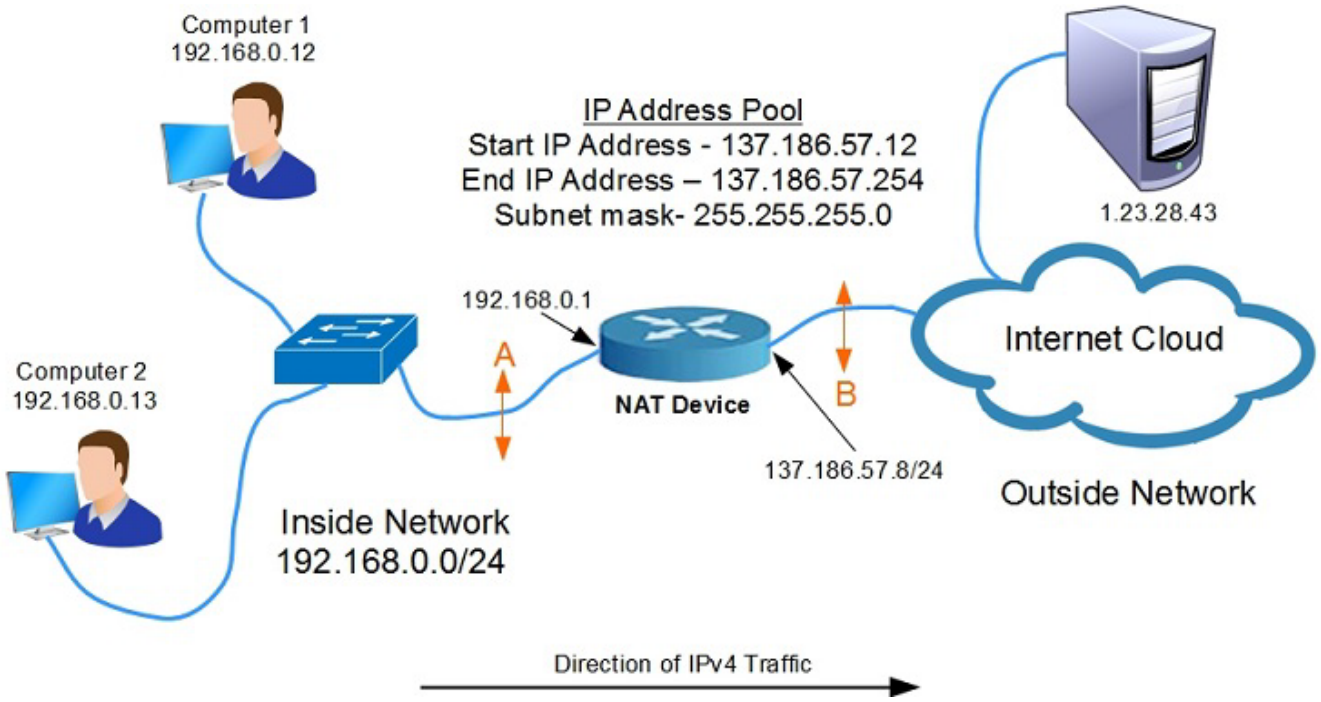
Review - Lecture 11 – DHCP

- DHCPv4 Operation
- Configuring a DHCPv4 Client
- SLAAC and DHCPv6
- Lab



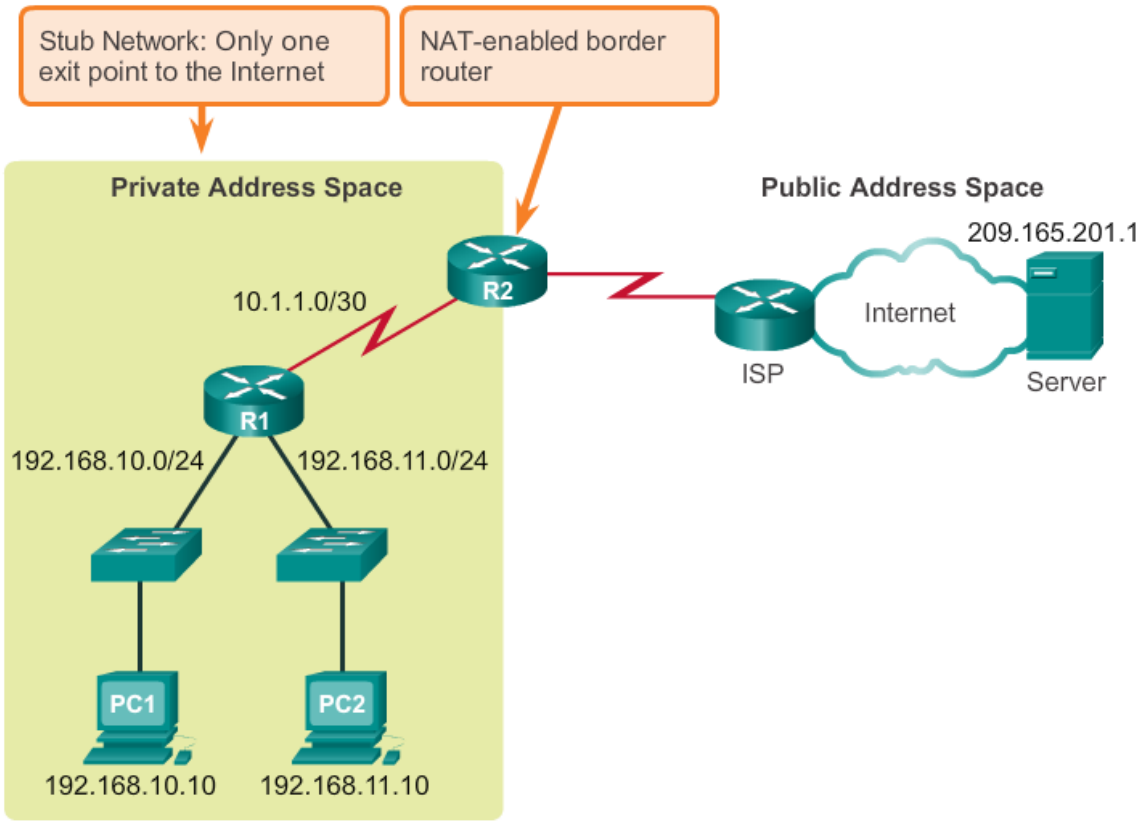
Summary - NAT

- NAT Video
- NAT Characteristics
- Types of NAT
- Benefits / Disadvantages of NAT
- Configuring NAT
- Port Forwarding
- Configuring NAT and IPv6
- Lab



NAT Characteristics

- What is NAT?
  - NAT is a process used to translate network addresses.
  - NAT's primary use is to conserve public IPv4 addresses.
  - NAT is usually implemented at border network devices, such as firewalls or routers.
  - NAT allows the networks to use private addresses internally, only translating to public addresses when needed.
  - Devices within the organization can be assigned private addresses and operate with locally unique addresses.
  - When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address.

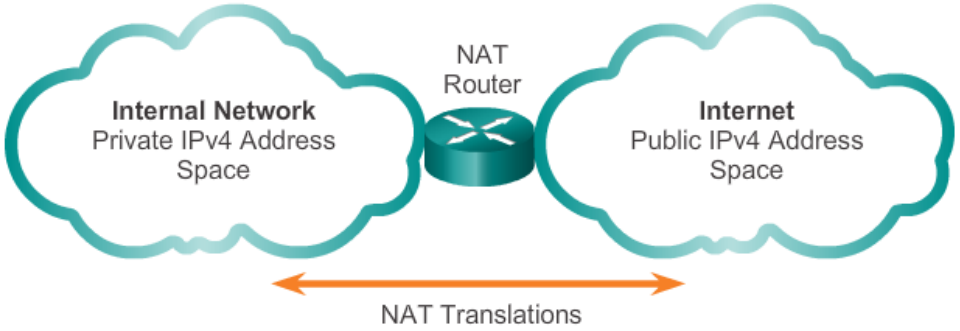


NAT Characteristics (continued)

- IPv4 Private Address Space
  - IPv4 address space is not big enough to uniquely address all the devices that must be connected to the Internet.
  - Network private addresses are described in RFC 1918 and are to designed to be used within an organization or site only.
  - Private addresses are not routed by Internet routers while public addresses are.
  - Private addresses can alleviate IPv4 scarcity, but because they aren't routed by Internet devices, they first need to be translated.
  - NAT is process used to perform such translation.

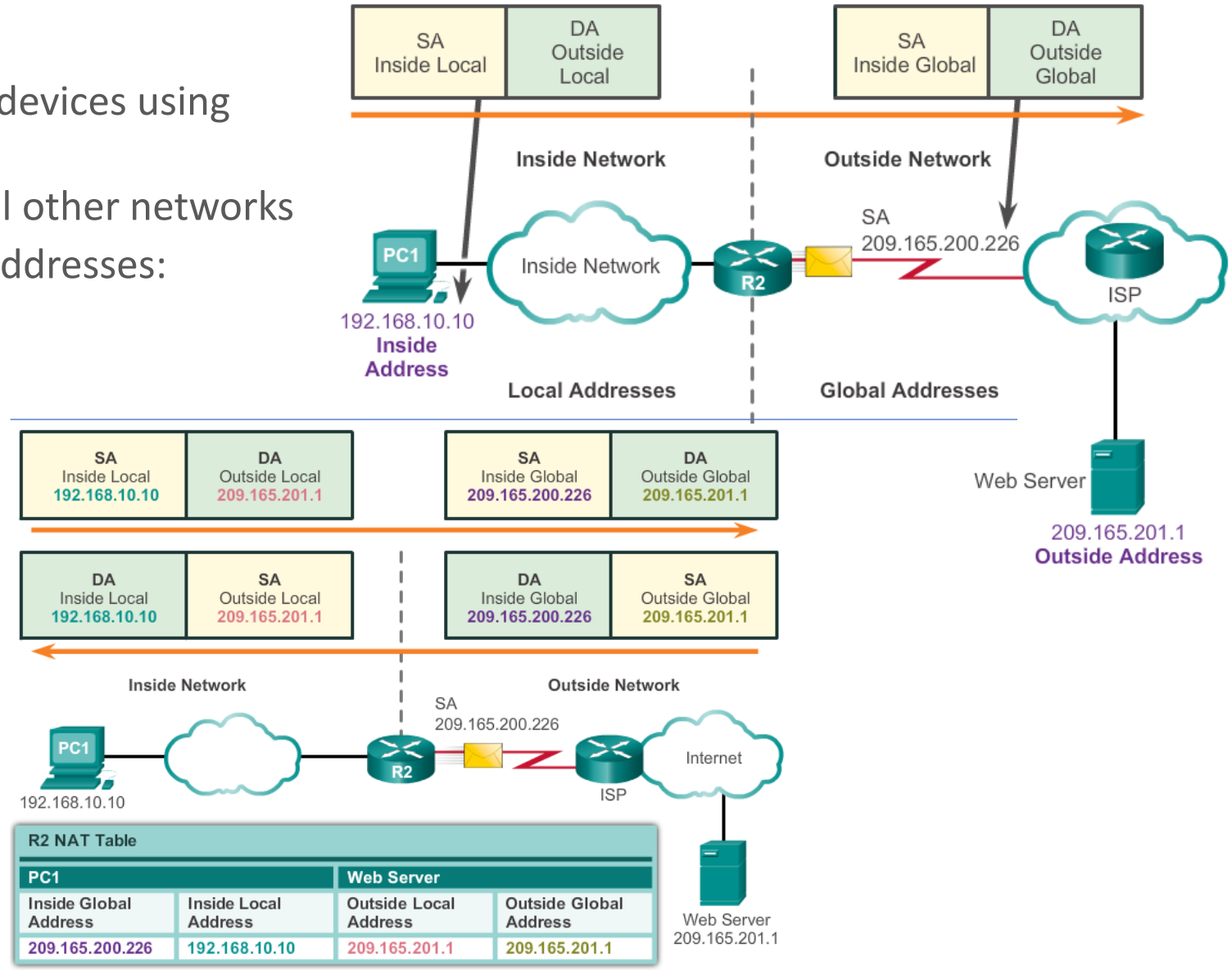
Private Internet addresses are defined in RFC 1918:

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



NAT Characteristics (continued)

- NAT Terminology
  - Inside network is the set of devices using private addresses
  - Outside network refers to all other networks
  - NAT includes four types of addresses:
    - Inside local address
    - Inside global address
    - Outside local address
    - Outside global address

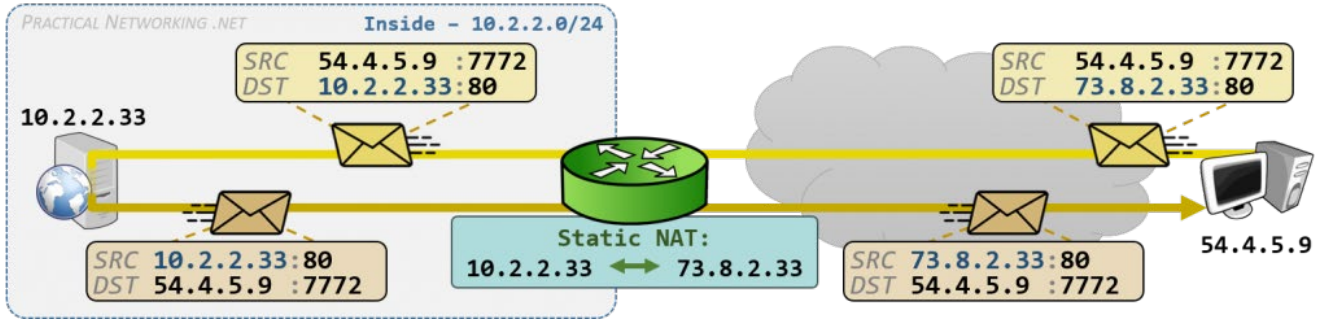


Types of NAT

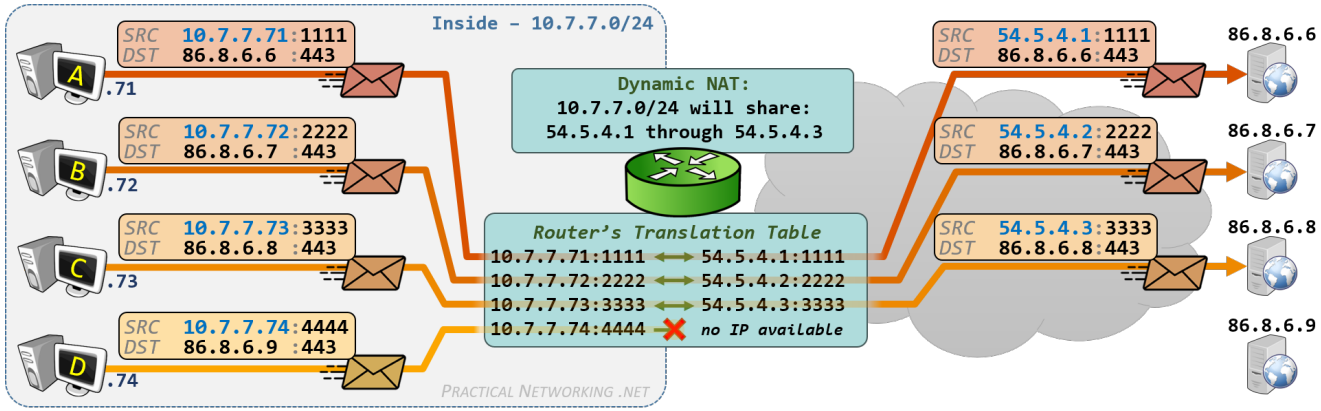
- Static NAT
  - Static NAT uses a one-to-one mapping of local and global addresses.
  - These mappings are configured by the network administrator and remain constant.
  - Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network.
  - A network administrator can SSH to a server in the inside network by pointing the SSH client to the proper inside global address.
- 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.
  - Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.
- Port Address Translation
  - Port Address Translation (PAT) maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
  - PAT uses the pair source port and source IP address to keep track of what traffic belongs to what internal client.
  - PAT is also known as NAT overload.
  - By also using the port number, PAT forwards the response packets to the correct internal device.
  - The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session.

Types of NAT (continued)

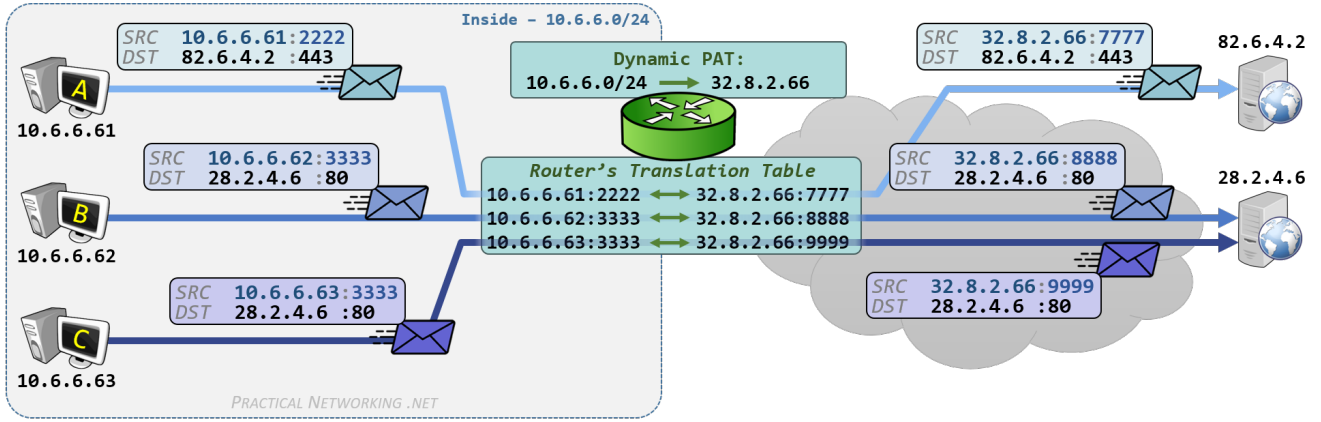
- NAT – Static
  - One to one address inside to outside



- NAT – Dynamic
  - One to one address, inside to outside pool (the pool is a limited number of addresses in the pool) of address



- NAT – PAT
  - May to one outside address, **BUT** the port numbers change



Types of NAT (continued)

- Comparing NAT and PAT
  - NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses.
  - PAT modifies both the address and the port number.
  - NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address provided by the host on the public network.
  - With PAT, there is generally only one or a very few publicly exposed IPv4 addresses.
  - PAT is able to translate protocols that do not use port numbers, such as ICMP; each one of these protocols is supported differently by PAT.

Benefits / Disadvantages of NAT

- Benefits of NAT
  - 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

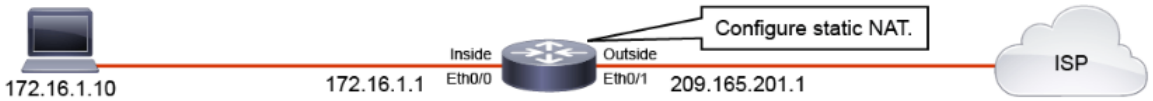
- Disadvantages of NAT
  - Performance is degraded
  - End-to-end functionality is degraded
  - End-to-end IP traceability is lost
  - Tunneling is more complicated
  - Initiating TCP connections can be disrupted

Configuring NAT

- Configuring Static NAT
  - There are two basic tasks to perform when configuring static NAT translations:
    - Create the mapping between the inside local and outside local addresses.
    - Define which interfaces belong to the inside network and which belong to the outside network.

Static NAT Configuration Steps	
Step 1	Connects the interface to the inside network, which is subject to NAT. **interface** *type number* **ip nat inside**
Step 2	Connects the interface to the outside network. **interface** *type number* **ip nat outside**
Step 3	Make the connection from the inside address to the outside address **ip nat inside source static** *inside-ipaddress outside-ipaddress*

```
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static 172.16.1.10 209.165.201.5
```



Configuring NAT (continued)

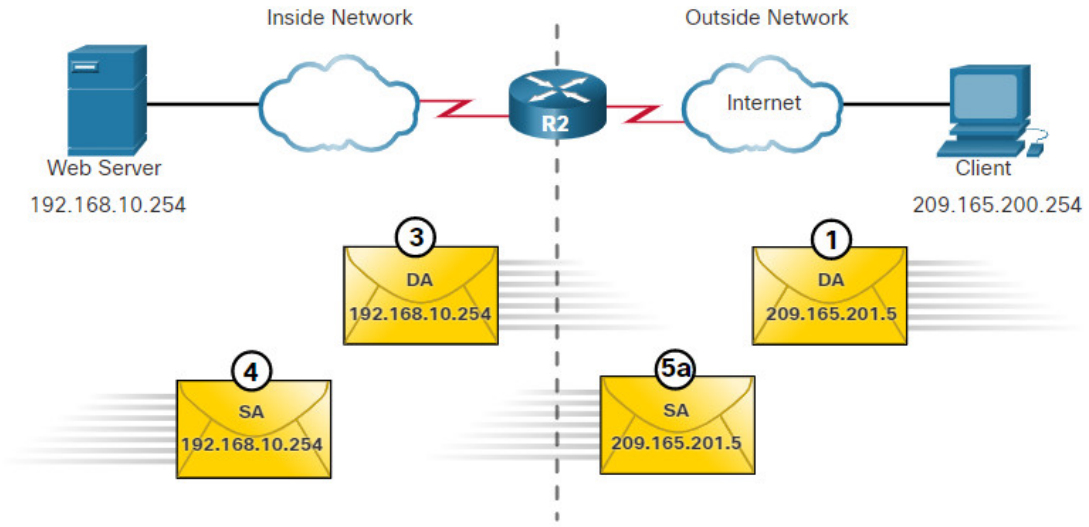
- Analyzing Static NAT
  - There are two basic tasks to perform when configuring static NAT translations:
    - Create the mapping between the inside local and outside local addresses.
    - Define which interfaces belong to the inside network and which belong to the outside network.

- Verifying Static NAT
  - The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

  - The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```



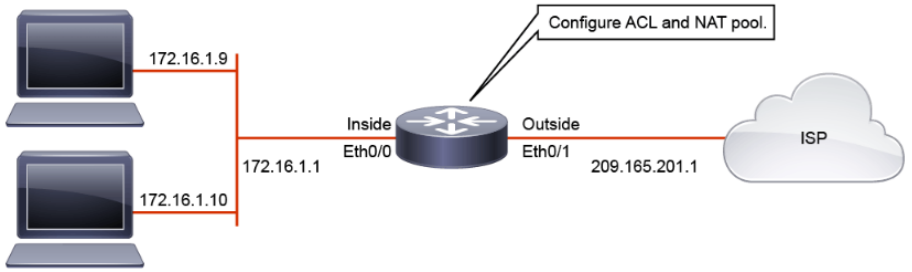
	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

Configuring NAT (continued)

- Configuring Dynamic NAT
  - The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come, first-served basis.
  - With dynamic NAT, a single inside address is translated to a single outside address.
  - The pool must be large enough to accommodate all inside devices.
  - A device is unable to communicate to any external networks if no addresses are available in the pool.

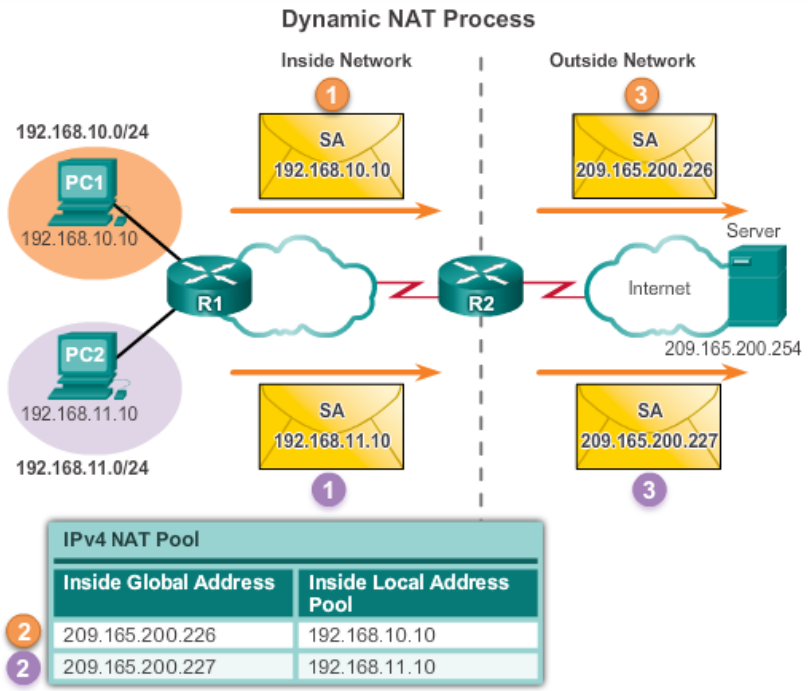
Dynamic NAT Configuration Steps	
Step 1	Defines a pool of global addresses to be allocated as needed. **ip nat pool** *name start-ip end-ip* {**netmask** netmask | **prefix-length** prefix-length }
Step 2	Defines a standard access list permitting those addresses that are to be translated. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 3	Establishes dynamic source translation, specifying the access list defined in prior Step. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Connects the interface to the inside network, which is subject to NAT. **interface** *type number* **ip nat inside**
Step 5	Connects the interface to the outside network. **interface** *type number* **ip nat outside**

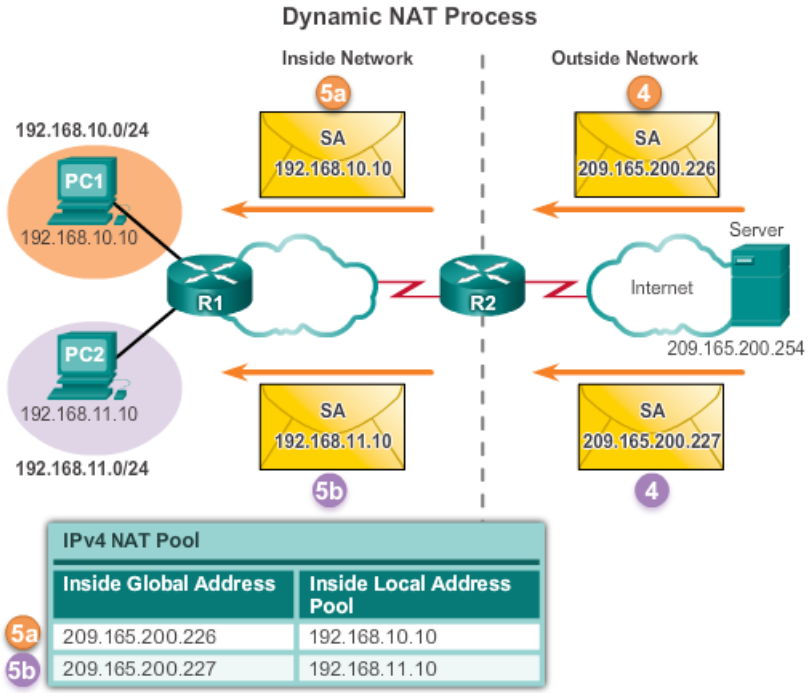
```
Router(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router(config)# ip nat pool NAT-POOL 209.165.201.5 209.165.201.10 netmask 255.255.255.240
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source list 1 pool NAT-POOL
```



Configuring NAT (continued)

- Analyzing Dynamic NAT
  1. PC1 and PC2 open a web browser for a connection to a web server
  2. R2 receives the packets on the inside interface and check if translation should be preformed (via an ACL). R2 assigns a global address from the NAT pool and creates a NAT table entry for both packets.
  3. R2 replaces the inside local source address on each packet with the translated inside global address from the pool.
  4. The server responds to PC1 using the destination address of 209.165.200.226 (the NAT- assigned address) and to PC2 using the destination address of 209.165.200.227
  5. (a and b) R2 looks up each received packets and forwards based on the private address found in the NAT table for each od the destination addresses





Configuring NAT (continued)

- Verifying Dynamic NAT

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

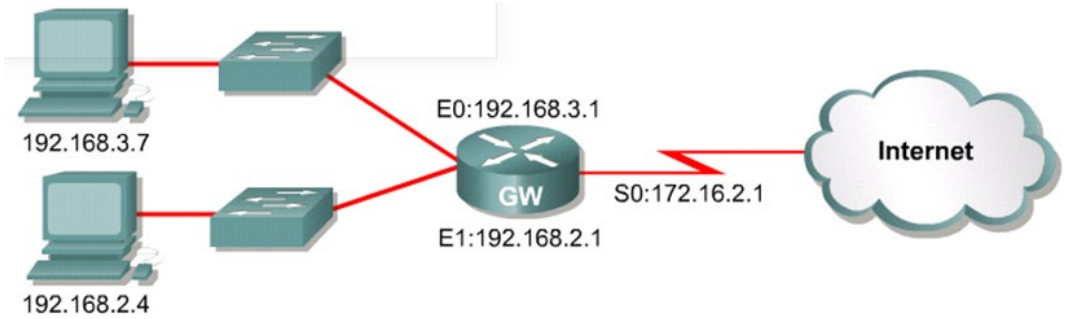
```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

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

Configuring NAT (continued)

- PAT Configuring, PAT: Single Outside Address
  (multiple outside addresses can be use if you create a NAT address pool)

Configuring PAT	
Step 1	Defines a pool of global addresses to be allocated as needed. **ip nat pool** *name start-ip end-ip* {**netmask** netmask | **prefix-length** prefix-length }
Step 2	Defines a standard access list permitting those addresses that are to be translated. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 3	Establishes dynamic source translation with overloading, specifying the access list defined in prior Step. **ip nat inside source list** *access-list-number* **pool** *name* **overload**
Step 4	Connects the interface to the inside network, which is subject to NAT. **interface** *type number* **ip nat inside**
Step 5	Connects the interface to the outside network. **interface** *type number* **ip nat outside**

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



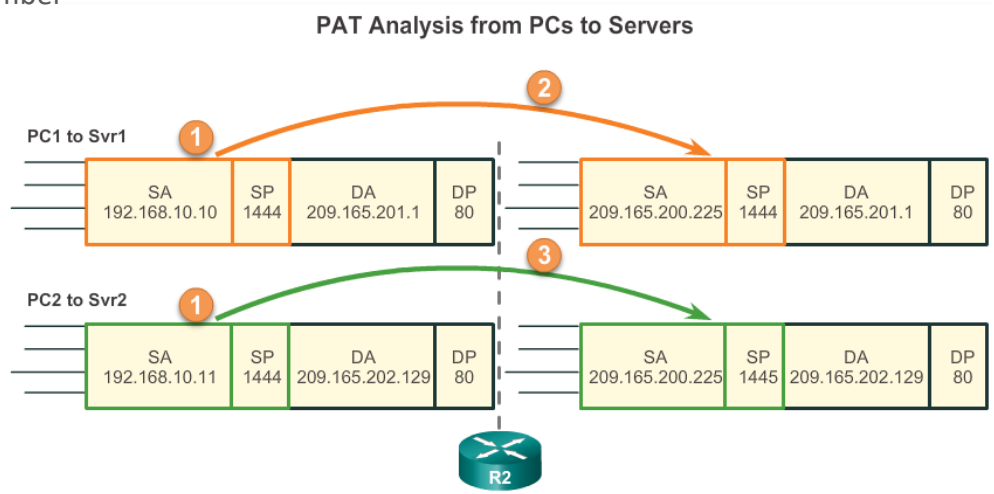

```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Interface is used in place of a NAT pool.

Configuring NAT (continued)

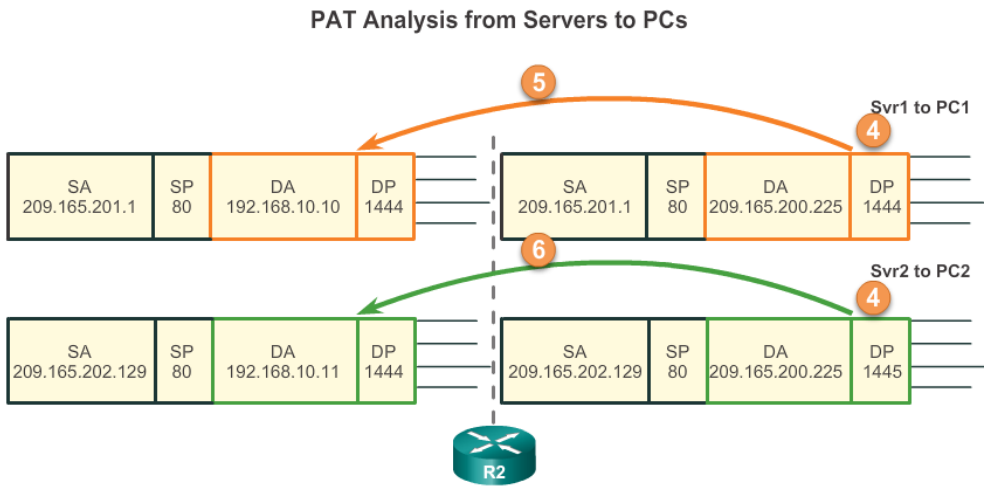
- ## Analyzing PAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if the translation should be preformed (via and ACL). R2 assigns the IP address of the outside interface, adds a port number and creates a NAT table entry for both packets
3. R2 replaces the inside source address on each packet with the translated inside global address
4. Each server responds to PC1 and PC2 using the destination address of the public address assigned to the external interface on the border router.
5. R2 looks up the received packet and forwards to PC1 because that is the private IP address found in the NAT table for the destination address and port number.
6. R2 looks up the received packet an forwards to PC2 because that is the private IP address found in the NAT table for the destination address and port number



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

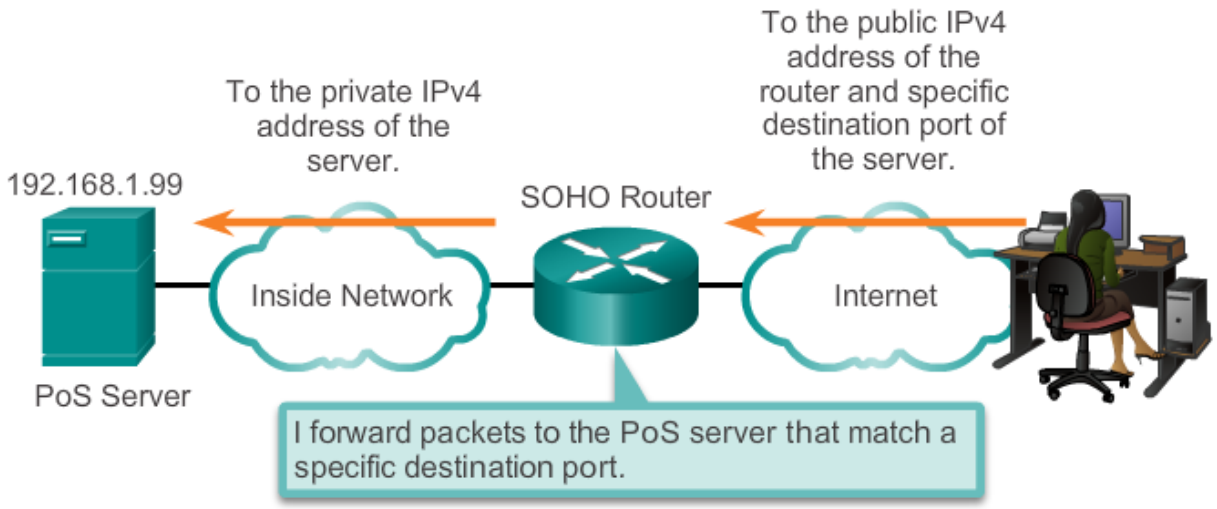
Configuring NAT (continued)

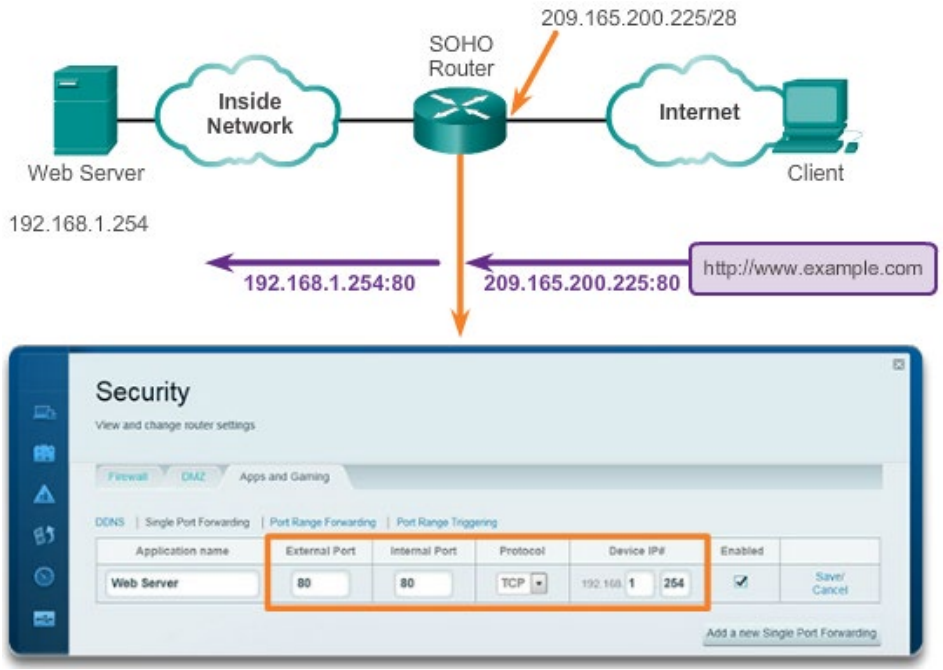
- Verifying PAT Translations

```
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#
```

Port Forwarding

- Port Forwarding
  - Port forwarding in technically **not** NAT,
    although it uses a NAT entry on the Cisco router to make it work
  - Port forwarding is the act of forwarding a network port from one network node to another.
  - 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.



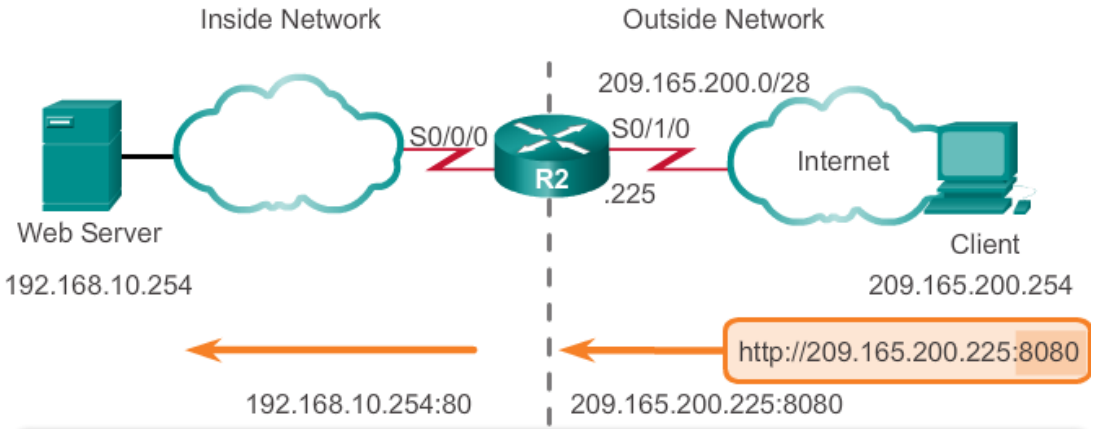


Port Forwarding (continued)

- Configuring Port Forwarding with IOS

Configuring Port Forwarding (IOS)

Step 1	Setup NAT for port forwarding **ip nat inside** {**static** {*tcp* |*udp*} *local-ip local-port global-ip global-port*} [**extendable**]		
		tcp or udp	Indicates if this is a TCP or UDP port number
		local-ip	This is the IPv4 address assigned to the host on the inside network
		local-port	Sets the local TCP/UDP port number in the range from 1-65535, (the service is listening on this port)
		global-ip	This is the IPv4 globally unique IP address of the inside host. This is the IP address the outside clients will use to reach the internal server.
		global-port	Sets the global TCP/UDP port number in the range from 1-65535, This is the port number the outside clients will use to reach the internal server.
		extendable	The extendable option is applied automatically, the extendable key word allows the user to configure serval ambiguous static translations, where ambiguous translations are translations with the same local or global address. It allows the router to extend the translation to more than one port if necessary.
Step 2	Connects the interface to the inside network, which is subject to NAT. **interface** *type number* **ip nat inside**		
Step 3	Connects the interface to the outside network. **interface** *type number* **ip nat outside**		



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.

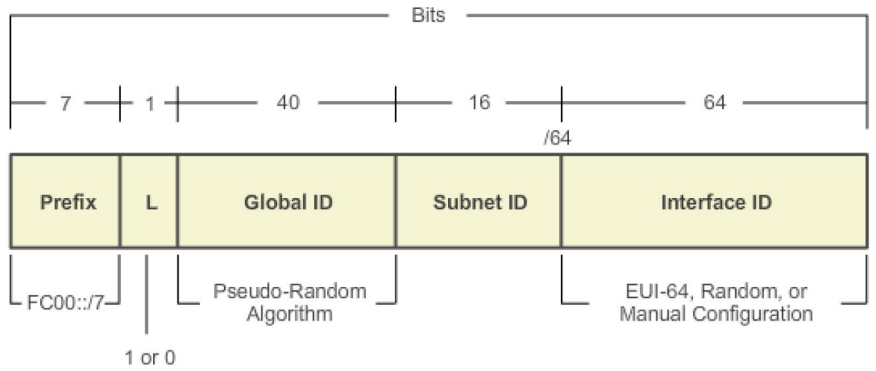
```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

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

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

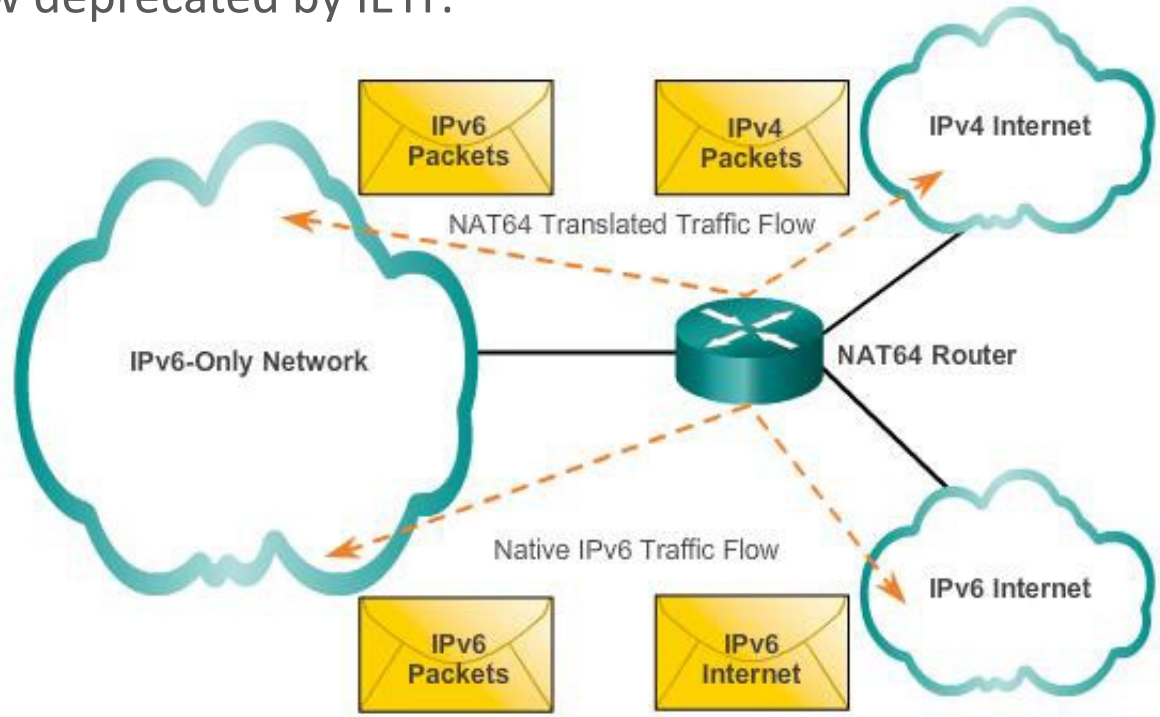
Configuring NAT and IPv6

- NAT for IPv6?
  - NAT is a workaround for IPv4 address scarcity.
    - IPv6 with a 128-bit address provides 340 undecillion addresses.
    - Address space is not an issue for IPv6.
    - IPv6 makes IPv4 public-private NAT unnecessary by design; however, IPv6 does implement a form of private addresses, and it is implemented differently than they are for IPv4.
    - IPv6 also uses NAT, but in a much different context
    - In IPv6, NAT is used to provide transparent communication between IPv6 and IPv4
    - IETF has developed several transition techniques to accommodate a variety of IPv4-to-IPv6 scenarios, including dual-stack, tunneling, and translation
    - Network Address Translation-Protocol Translation (NAT-PT) was another NAT-based transition mechanism for IPv6, but is now deprecated by IETF
    - NAT64 is not intended to be a permanent solution; it is meant to be a transition mechanism to assist migration
    - NAT64 is now recommended
  - IPv6 **U**nique **L**ocal **A**ddresses (ULAs)
    - ULAs are designed to allow IPv6 communications within a local site.
    - ULAs are not meant to provide additional IPv6 address space.
    - ULAs have the prefix FC00::/7, which results in a first hextet range of FC00 to FDFF.
      - ULAs are also known as local IPv6 addresses (not to be confused with IPv6 link-local addresses).
      - First 64 bits of a ULA
        - Prefix of FC))::/7 (FC00 to FDFF)
        - Next bit is a 1 if the prefix is locally assigned
        - Next 40 bits define a global ID
        - Next 16 bits is a subnet ID
      - Last 64 bits of a ULA is the host portion of the address
    - Allows sites to communicate with out address conflicts
    - Allows internal connectivity
    - Not routable on the internet



Configuring NAT and IPv6 (continued)

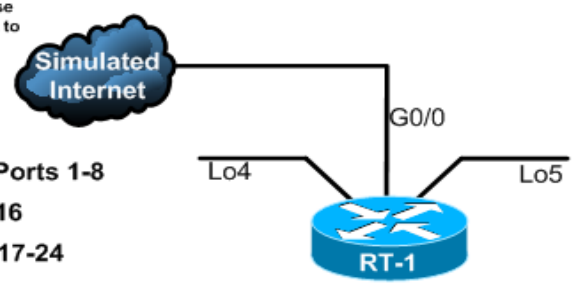
- NAT for IPv6 (continued)
  - IPv6 also uses NAT, but in a much different context.
  - In IPv6, NAT is used to provide transparent communication between IPv6 and IPv4.
  - NAT64 is not intended to be a permanent solution; it is meant to be a transition mechanism.
  - Network Address Translation-Protocol Translation (NAT-PT) was another NAT-based transition mechanism for IPv6, but is now deprecated by IETF.
  - NAT64 is now recommended.



LAB

For the on-line user, in Packet Tracer use the Wireless Router WRT300N (connect to 1 of the Ethernet Ports)

For the in-house users we will plug into the Fanshawe network.



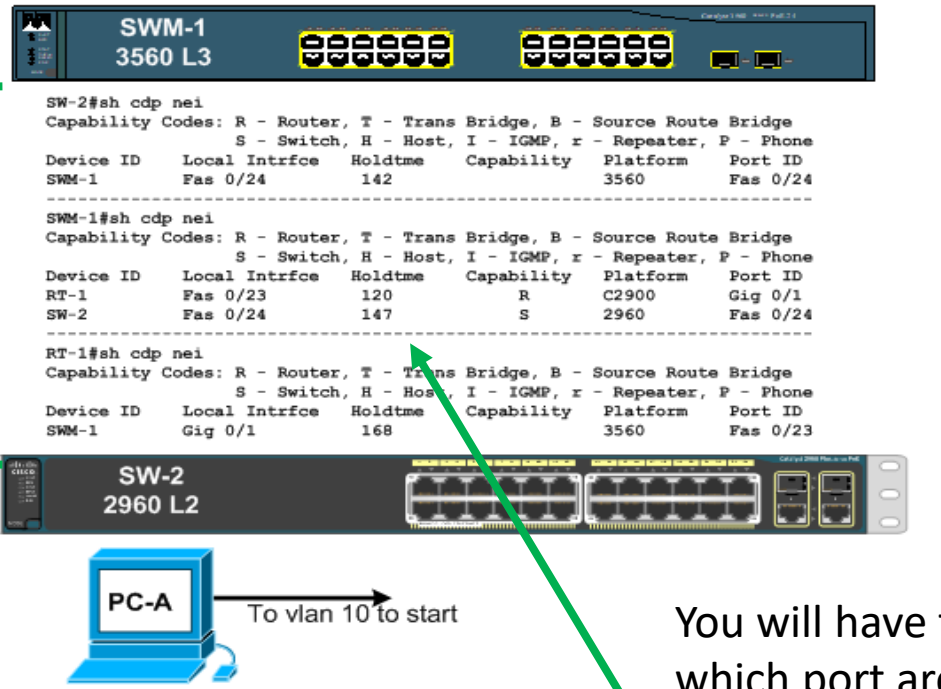
Vlan 10 - Workstations – Ports 1-8

Vlan 20 - Voice – Ports 9-16

Vlan 30 - Servers – Ports 17-24

Vlan 99 - Mgmt

CDP Information

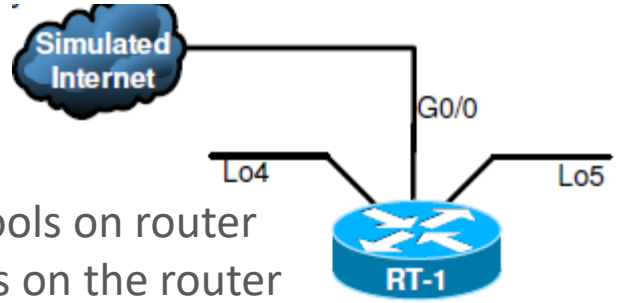


Device	Interface	IP Adress	Subnet Mask	Vlan Names
RT-1	G0/0	**DHCP**		
		172.17.1.26	/30	
	Lo4	172.16.40.1	/24	
	Lo5	172.16.50.1	/24	
SW-1	Vlan 10	172.16.10.254	/24	Workstations
	Vlan 20	172.16.20.254	/24	Voice
	Vlan 30	172.16.30.254	/24	Server
	Vlan 99	172.16.99.254	/24	Mgmt
		172.17.1.25	/30	
		Trunk		
SW-2		**Trunk**		
	Vlan 10			Workstations
	Vlan 20			Voice
	Vlan 30			Server
	Vlan 99	172.16.99.253	/24	Mgmt
PC-A		DHCP		

You will have to figure out which port are here

By reading the CDP information in the lab

LAB (continued)



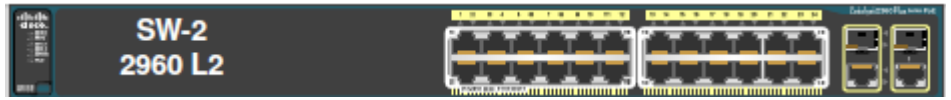
DHCP Scopes/Pools on router
OSPF 3 networks on the router
OSPF G0/0 Marked Passive
OSPF redistributes a static address

Not a trunk no sub interfaces on the router
(Not router on a stick!)
IP addresses on both end of this link

DHCP help needed on each Vlan
OSPF 5 networks on SWM-1

Trunk between switches,
leave the L3 switch in auto mode,
set the L2 switch to mode trunk

L2 Switch Vlans are an extension of the Vlans on the L3 switch through the Trunk



QUESTIONS