Basic Switch
Address Resolution Protocol

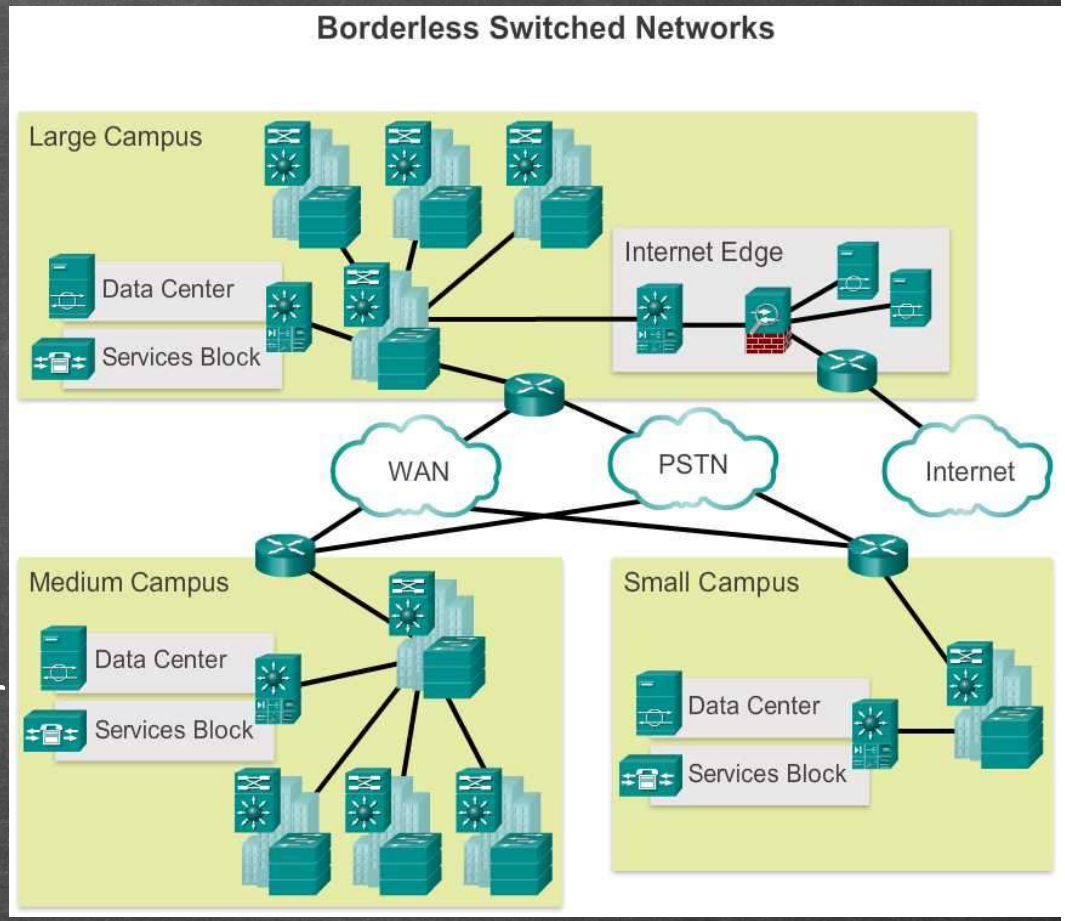
Jirasak Sittigorn
Internetworking Standards & Technologies
Department of Computer Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang

Cisco | Networking Academy®
Mind Wide Open™

- Introduction to Switch Network
  - LAN Design
  - The Switched Environment
    - Switching Domains

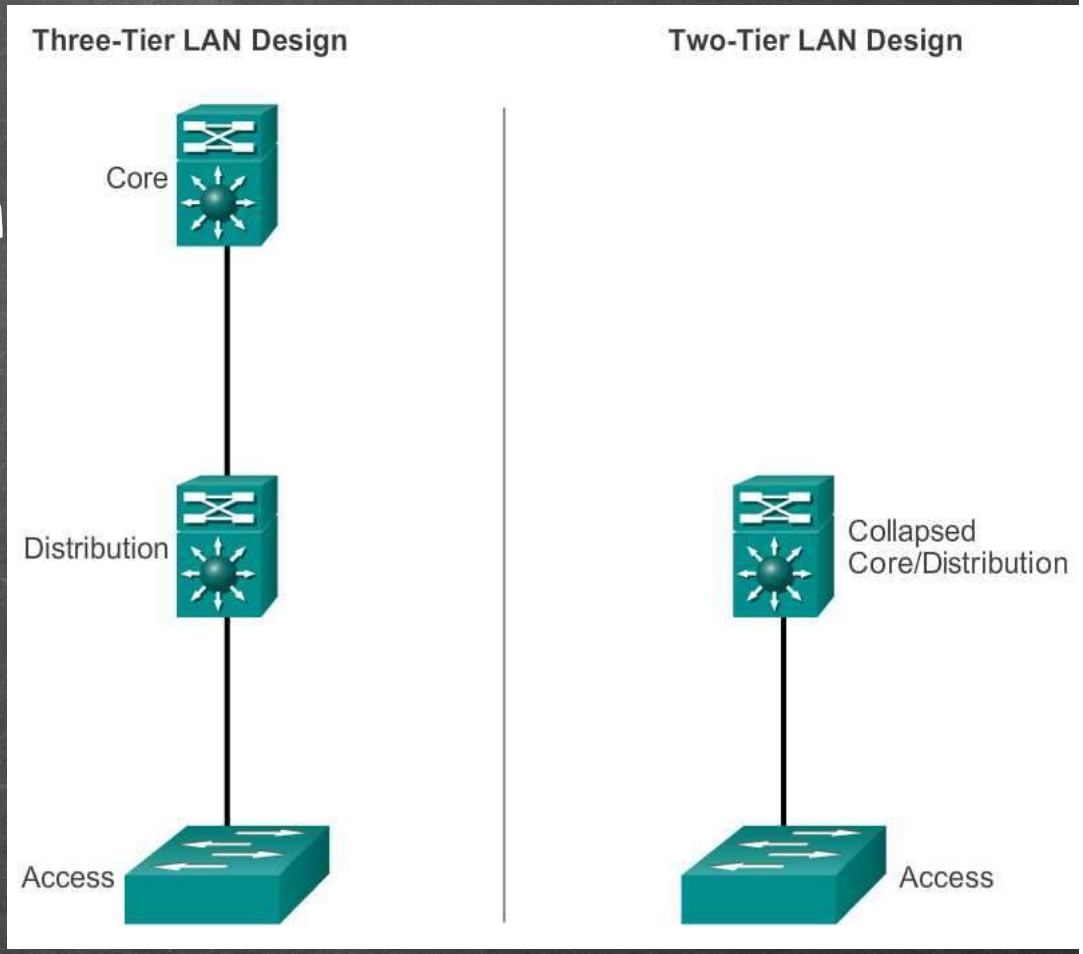
LAN Design

- Borderless Switched Networks
  - Cisco Borderless Network is a network architecture that allow organizations to connect anyone, anywhere, anytime, and on any device securely, reliably, and seamlessly
  - It is designed to address IT and business challenges, such as supporting the converged network and changing work patterns



LAN Design

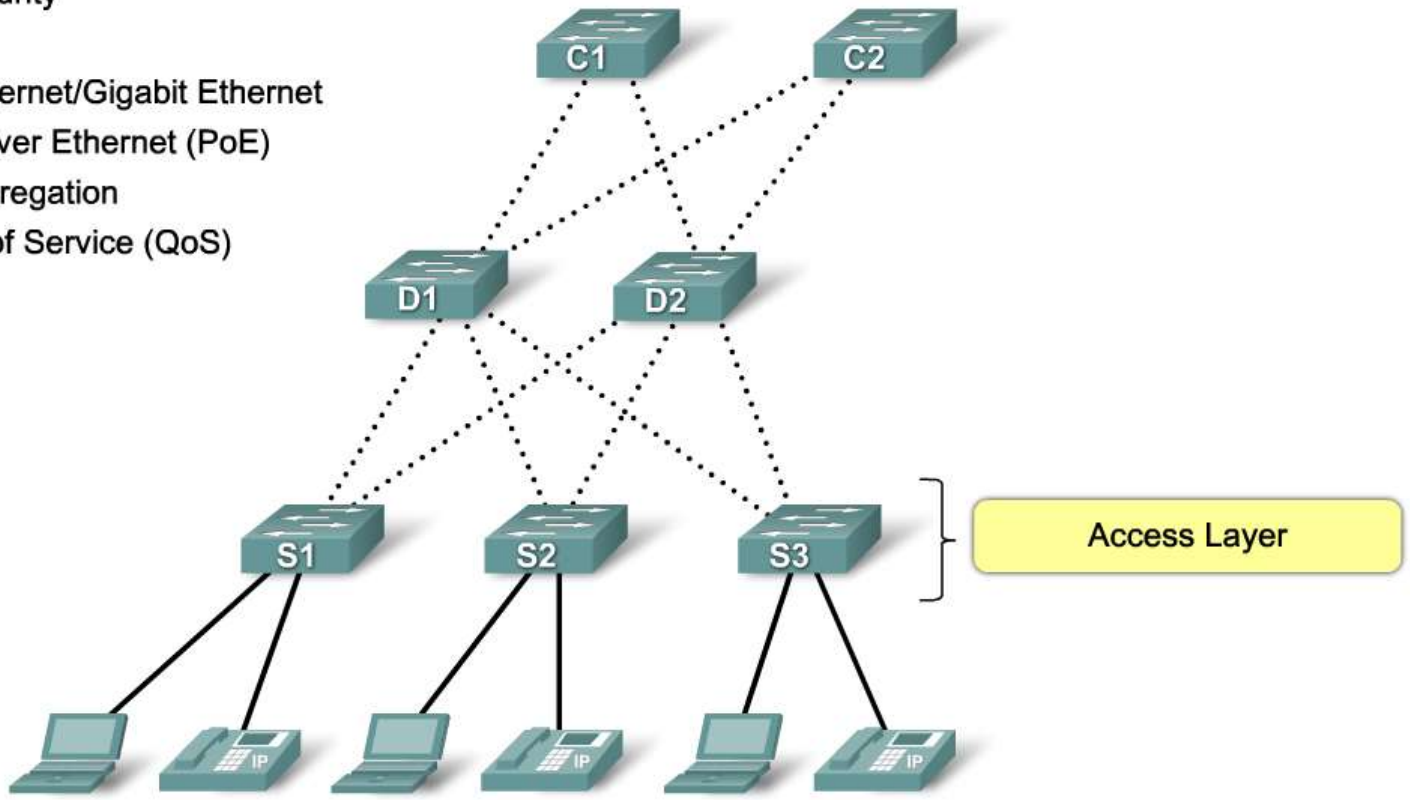
- Borderless switched network design guidelines are built upon the following principles:
  - Hierarchical
  - Modularity
  - Resiliency
  - Flexibility



LAN Design

Access Layer Switch Features

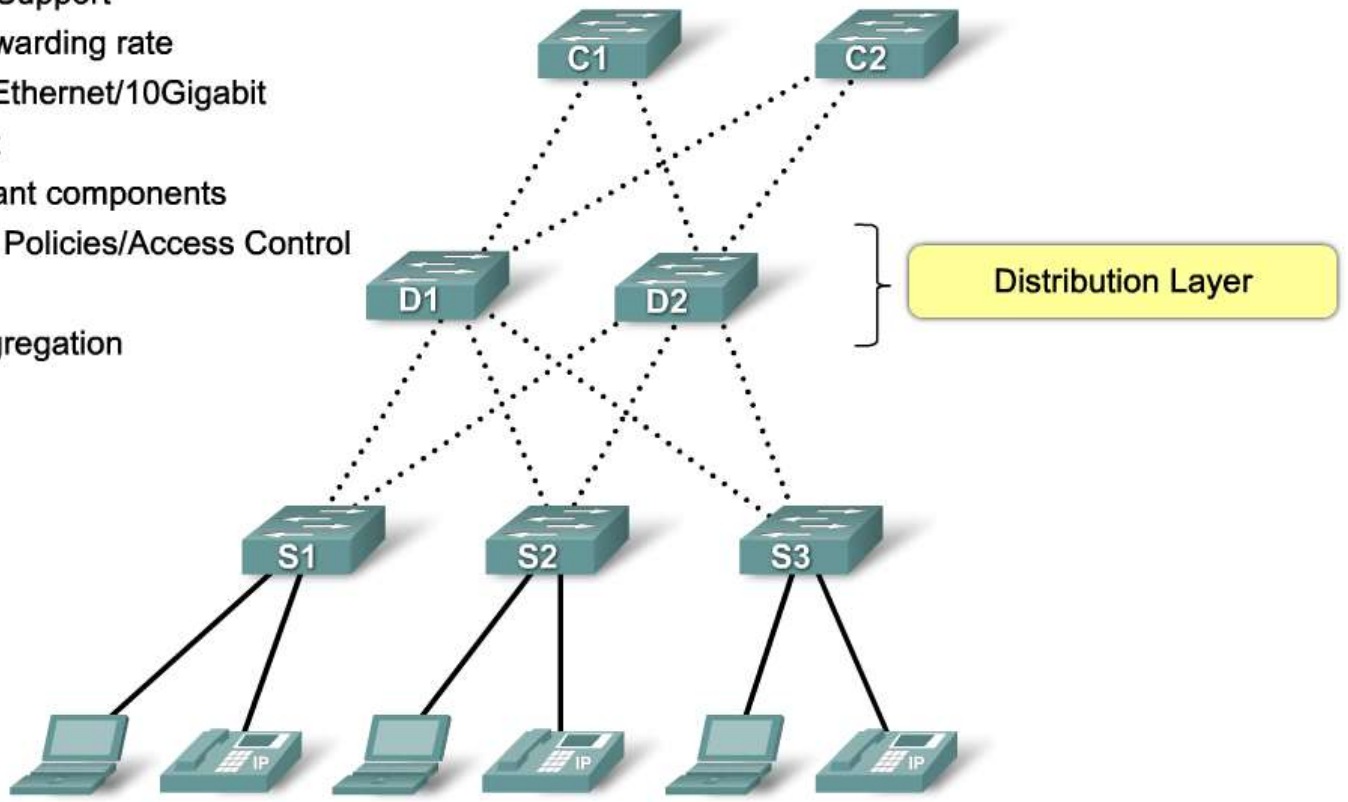
- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation
- Quality of Service (QoS)



LAN Design

Distribution Layer Switch Features

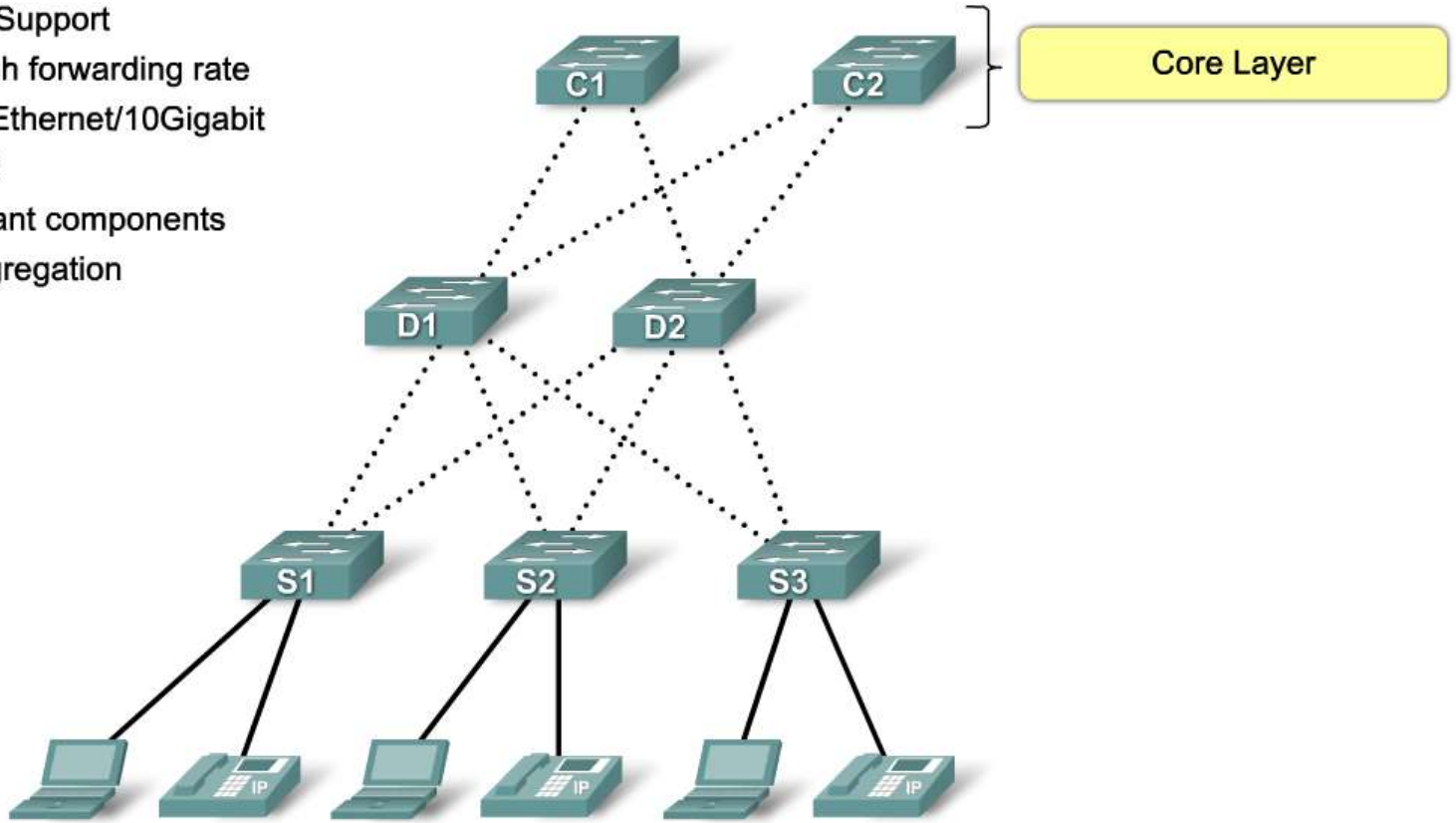
- Layer 3 Support
- High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Security Policies/Access Control Lists
- Link Aggregation
- QOS



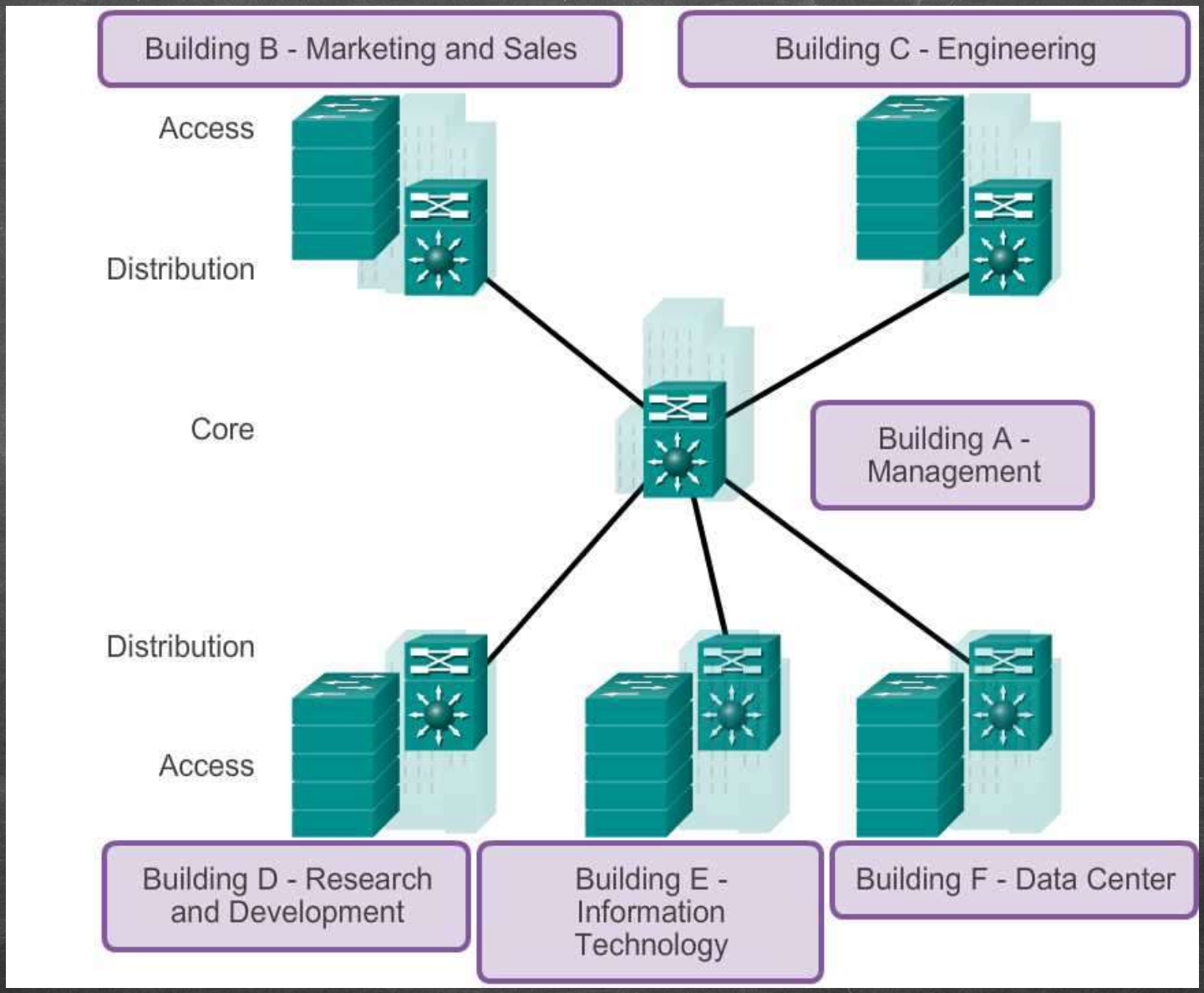
LAN Design

Core Layer Switch Features

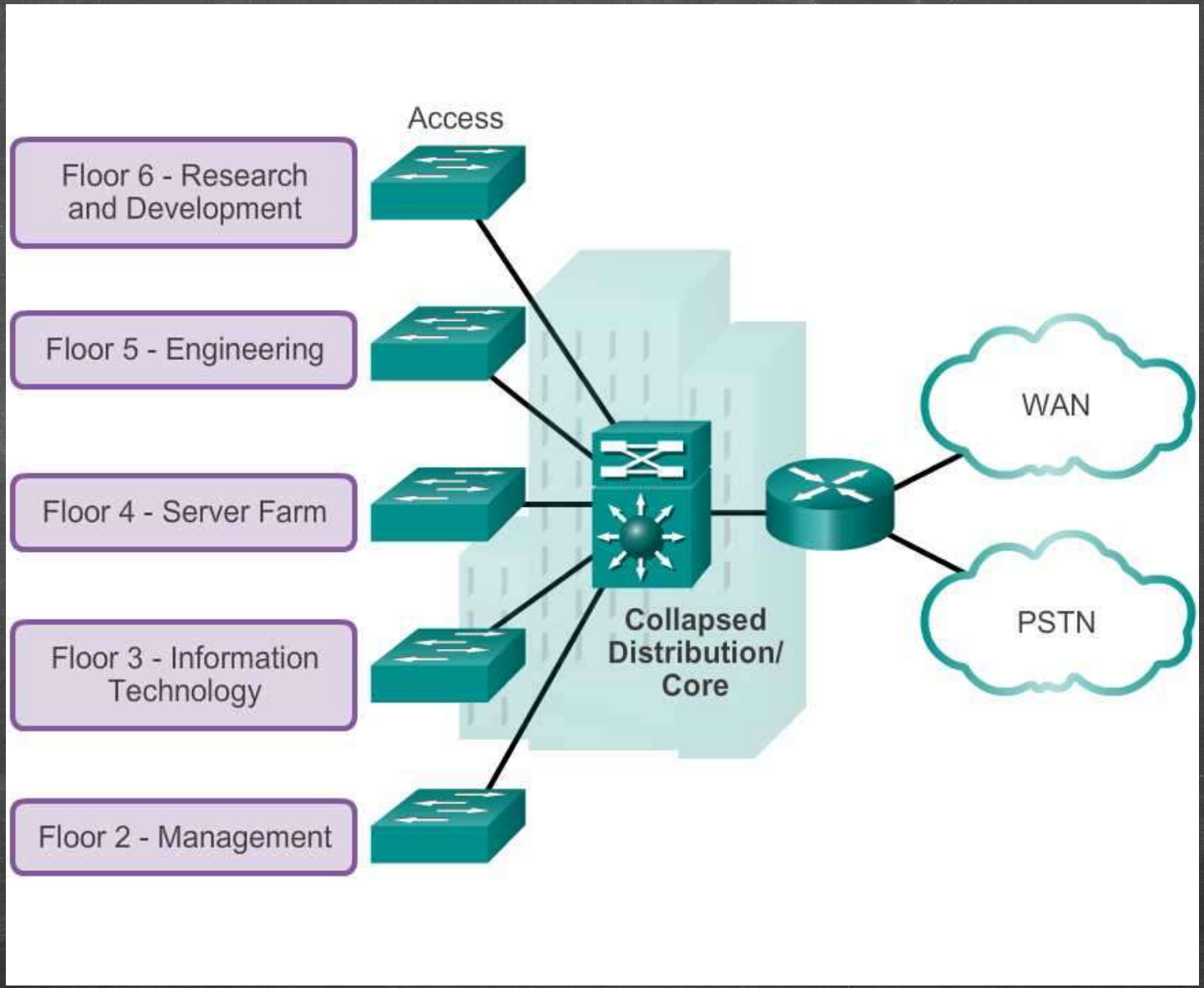
- Layer 3 Support
- Very High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Link Aggregation
- QoS



LAN Design


Building B - Marketing and Sales
Building C - Engineering
Access
Distribution
Core
Building A - Management
Distribution
Access
Building D - Research and Development
Building E - Information Technology
Building F - Data Center

LAN Design


Access
Floor 6 - Research and Development
Floor 5 - Engineering
Floor 4 - Server Farm
Floor 3 - Information Technology
Floor 2 - Management
Collapsed Distribution/ Core
WAN
PSTN

LAN Design

Common Business Considerations When Selecting Switch Equipment:

- **Cost** - The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density** - Network switches must support the appropriate number of devices on the network.
- **Power** - It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
- **Reliability** - The switch should provide continuous access to the network.
- **Port Speed** - The speed of the network connection is of primary concern to end users.
- **Frame Buffers** - The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
- **Scalability** - The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

Fixed Configuration Switches

Modular Configuration Switches

Stackable Configuration Switches

LAN Design

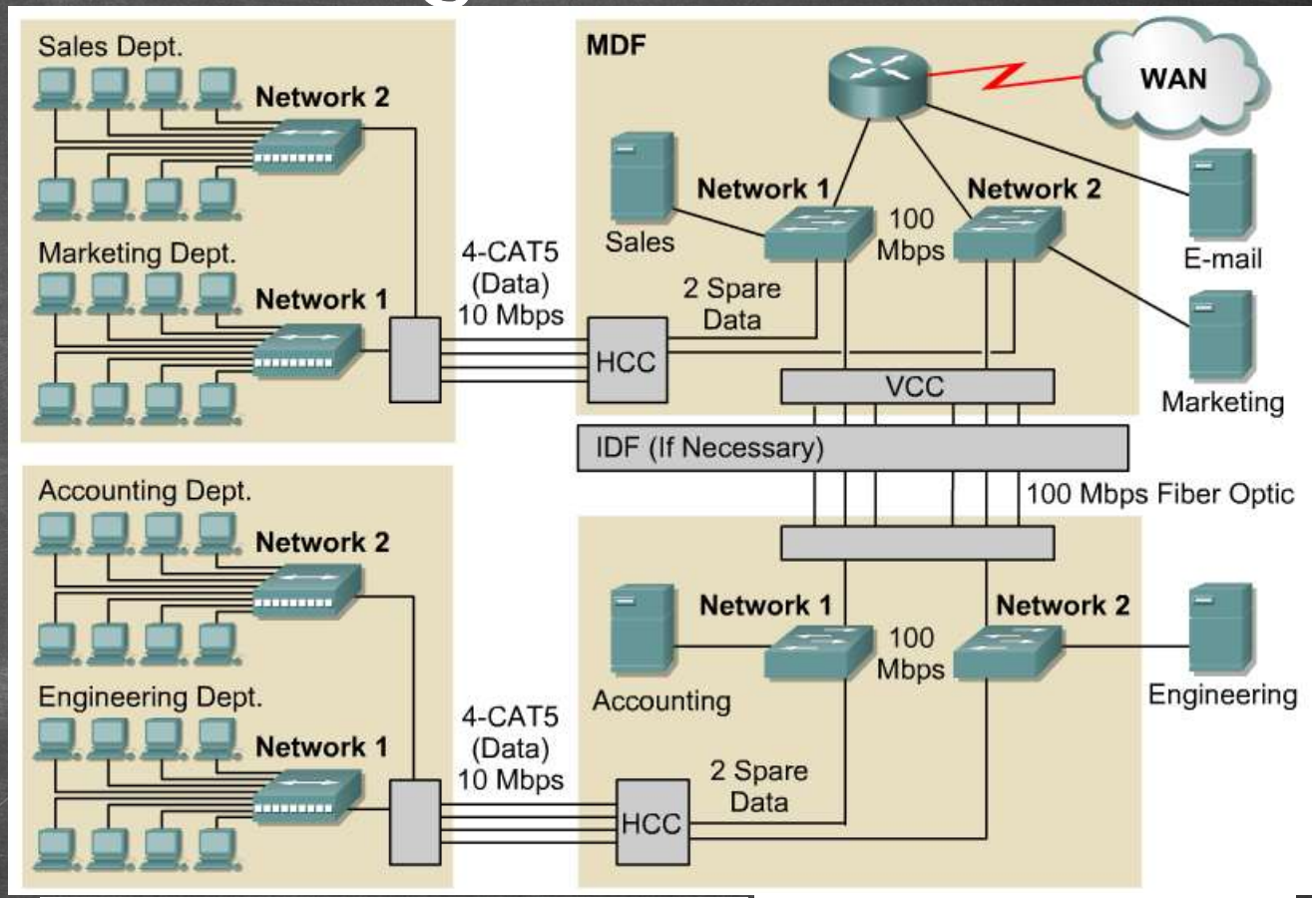
- To maximize available LAN bandwidth and performance:
  - The function and placement of servers
    - Enterprise servers
    - Workgroup servers
  - Collision detection issues
  - Segmentation issues
  - Broadcast domain issues

MDF : Main Distribution Facility

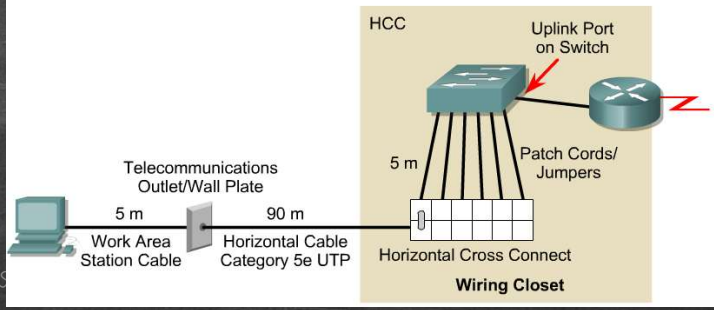
IDF : Intermediate Distribution Facility

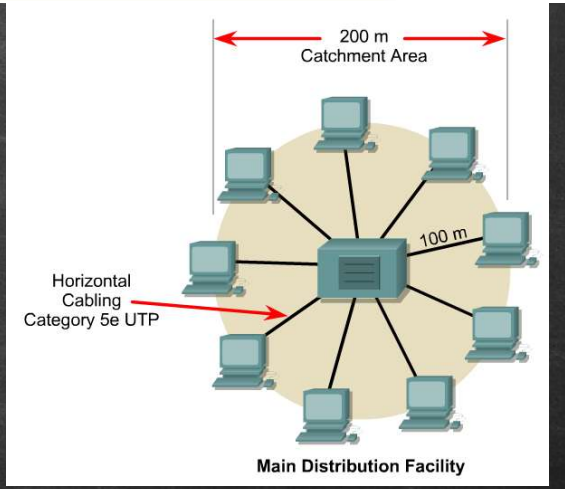
VCC : Vertical cross-connect

HCC : Horizontal cross-connect



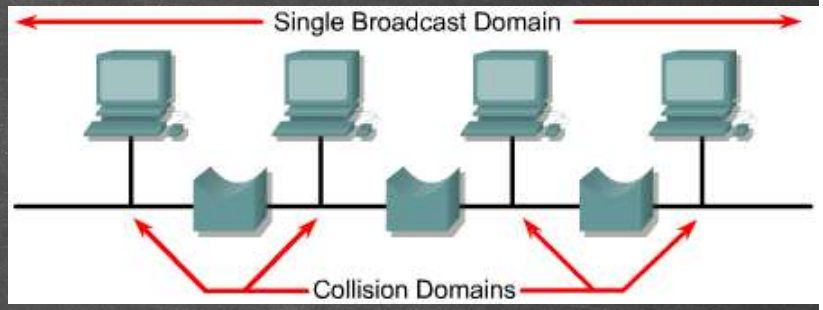
Characteristic	10BASE-T	10BASE-FL	100BASE-TX	100BASE-FX
Data rate	10 Mbps	10 Mbps	100Mbps	100 Mbps
Signaling method	Baseband	Baseband	Baseband	Baseband
Medium type	Category 5e UTP	Fiber-optic	Category 5e UTP	Multi-mode fiber (two strands)
Maximum length	100 meters	2000 meters	100 meters	2000 meters

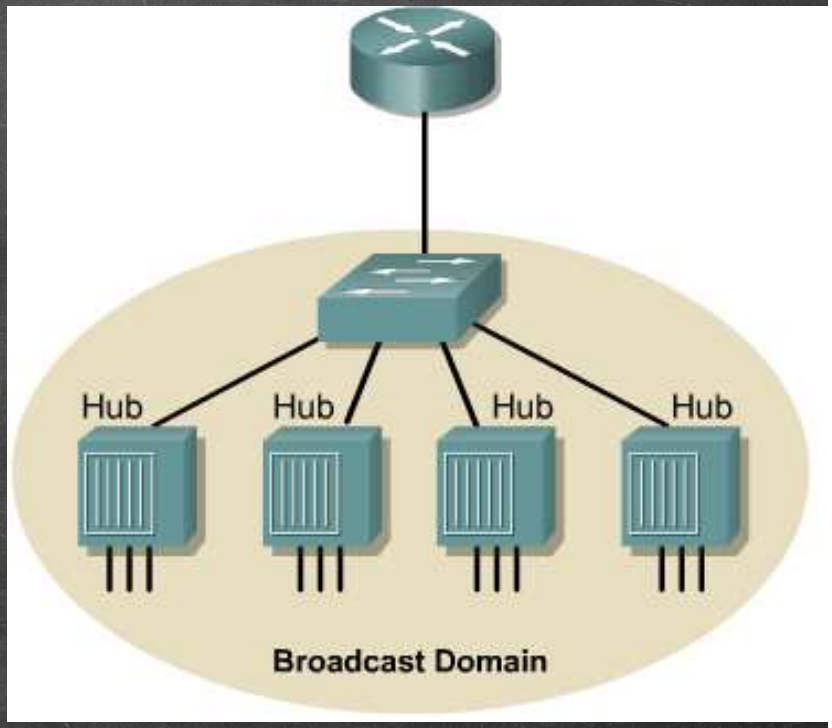




LAN Design

- Segmentation is the process of splitting a single collision domain into smaller collision domains.
  - Creating smaller collision domains reduces the number of collisions on a LAN segment, and allows for greater utilization of bandwidth.
  - Layer 2 devices such as bridges and switches can be used to segment a LAN into smaller collision domains.
- A broadcast domain refers to the set of devices that receive a broadcast data frame originating from any device within that set.
  - Processing the broadcast data will consume the resources and available bandwidth of the host.
  - Layer 2 devices such as bridges and switches reduce the size of a collision domain but do not reduce the size of the broadcast domain.
  - Routers reduce the size of the collision domain and the size of the broadcast domain at Layer 3.



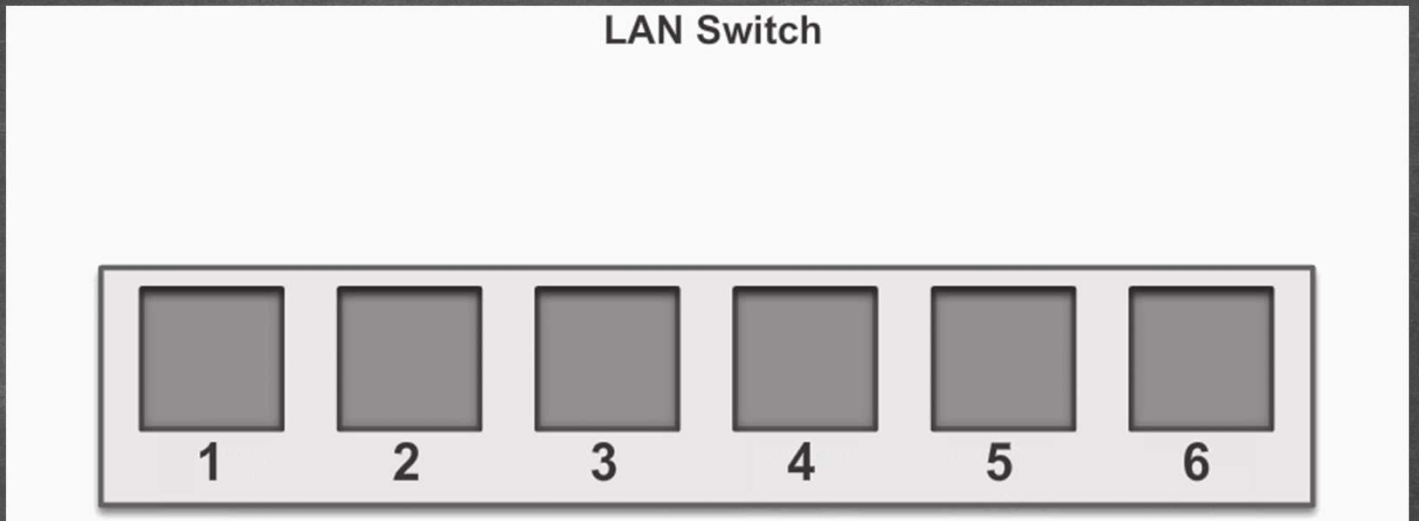


The Switched Environment

- Switch Operation
  - Learning
  - Aging
  - Flooding
  - Forwarding
  - Filtering

The Switched Environment

- Switching

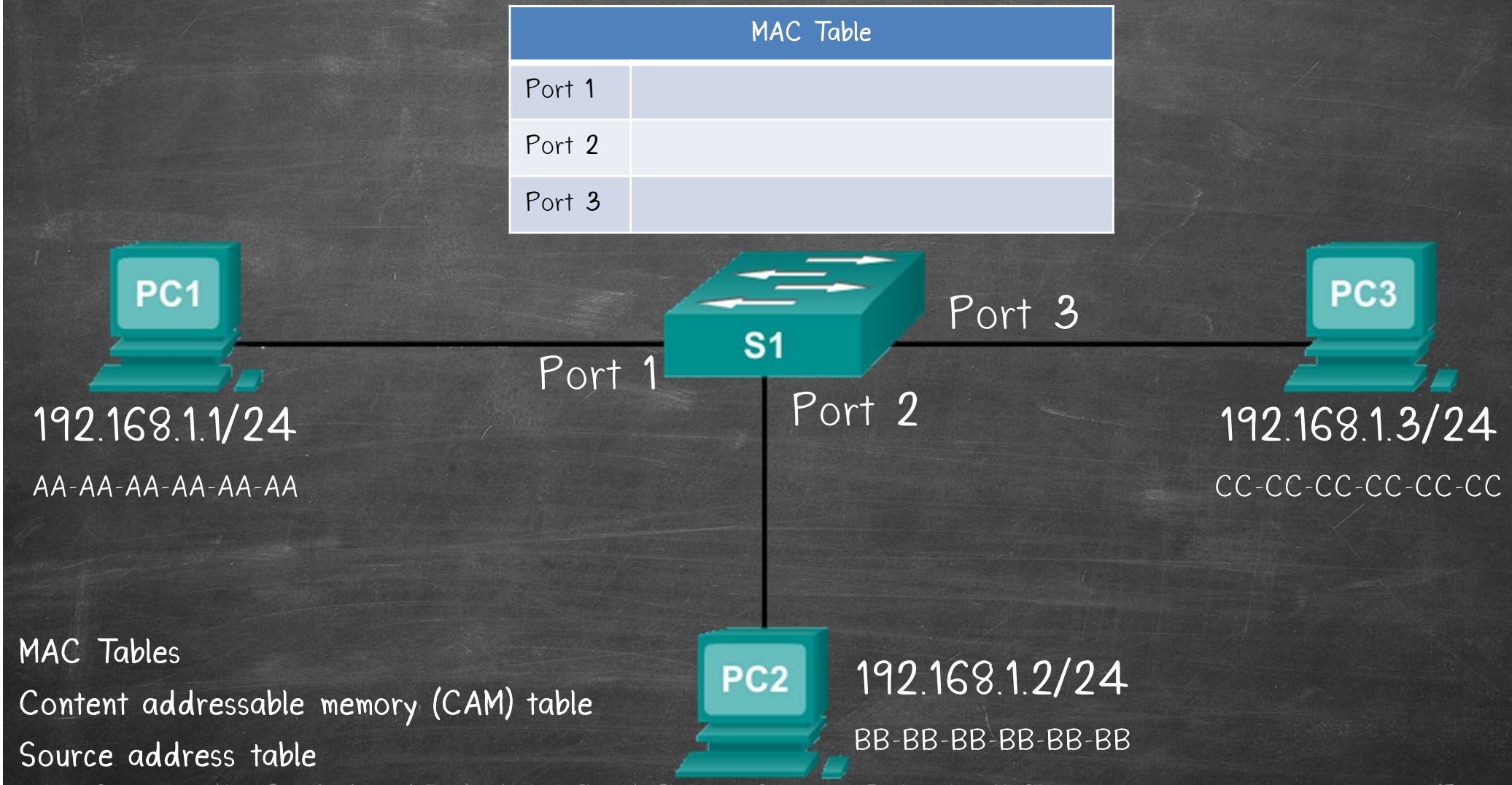


Port Table

Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

The Switched Environment

- MAC Addressing & Switch MAC Tables



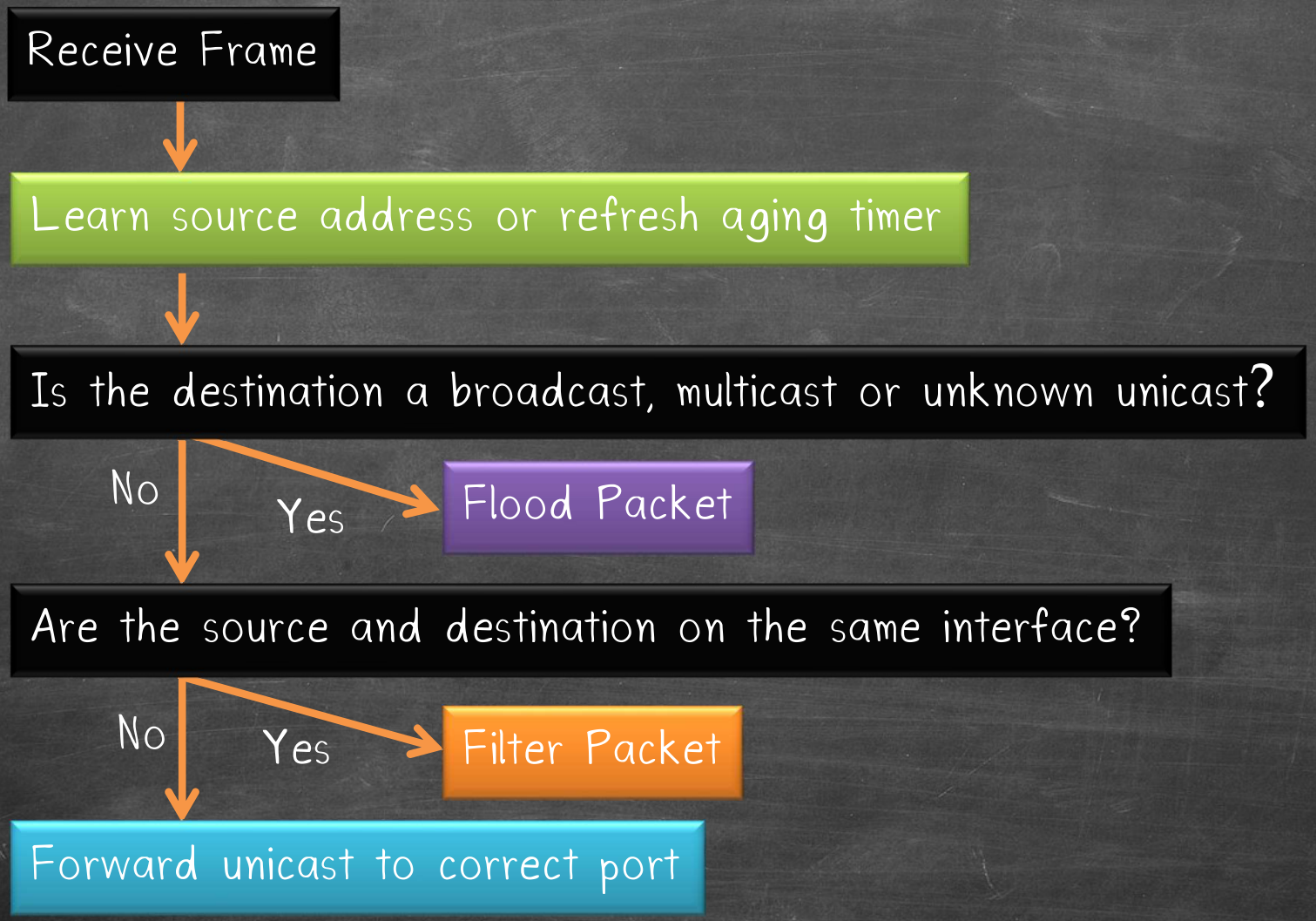
MAC Tables

Content addressable memory (CAM) table

Source address table

The Switched Environment

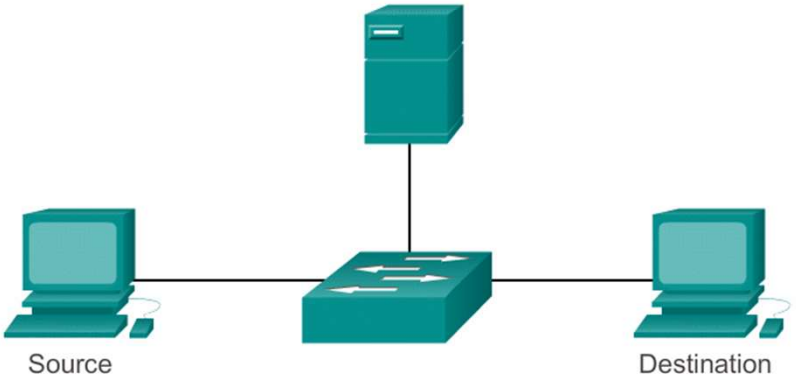
- Transparent Bridge Process - Jeff Doyle



The Switched Environment

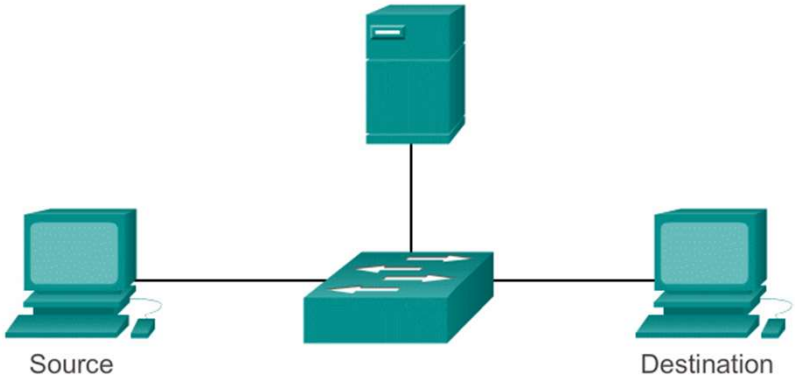
- Switch Forwarding Methods

Store-and-Forward Switching



A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-Through Switching



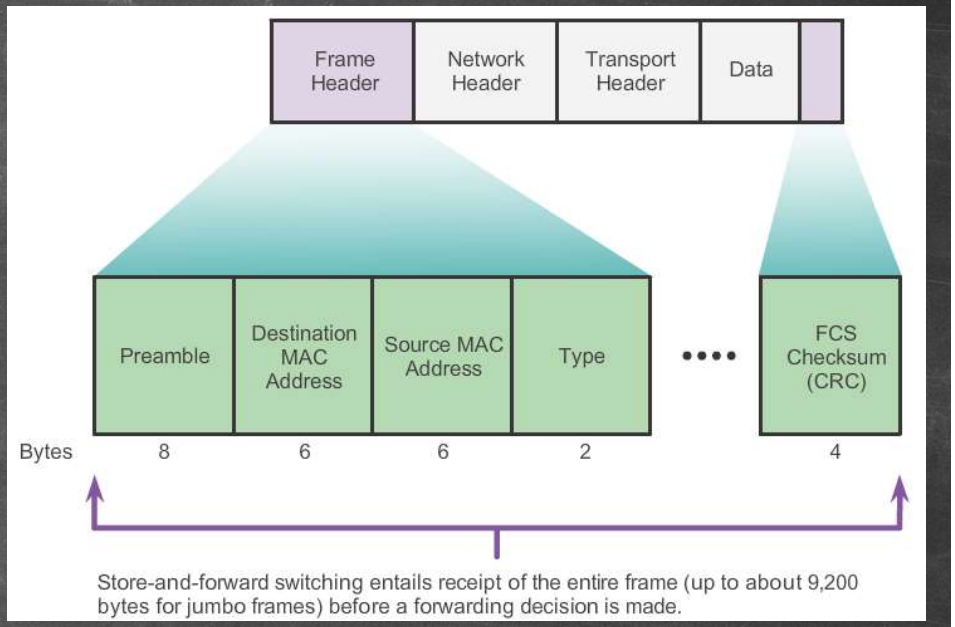
A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

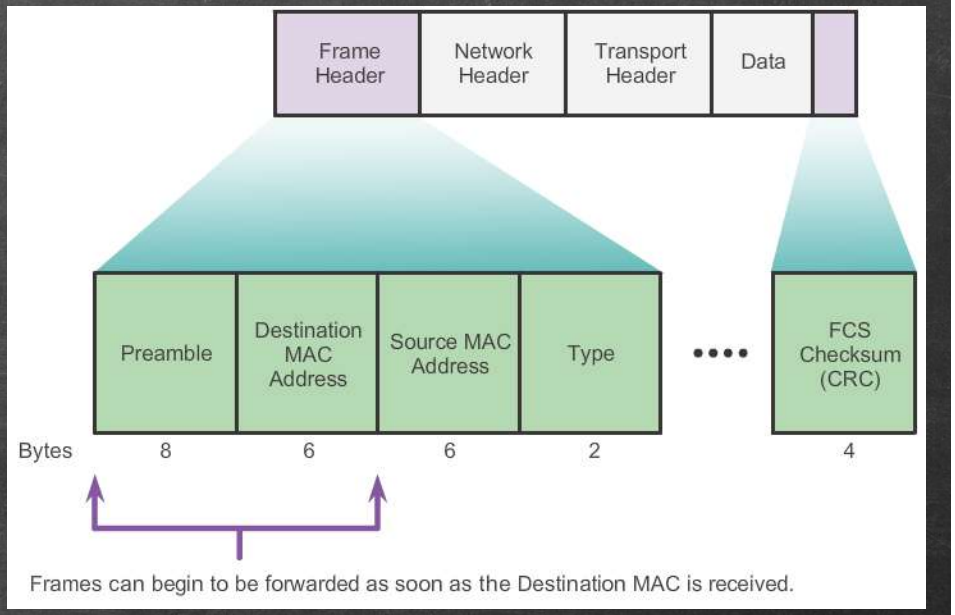
The Switched Environment

- Frame Forwarding
  - Store-and-Forward Switching
    - Store-and-Forwarding allows the switch to:
      - Check for errors (via FCS check)
      - Perform Automatic Buffering
    - Slower forwarding
  - Cut-Through Switching
    - Cut-Through allows the switch to start forwarding in about 10 microseconds
    - No FCS check
    - No Automatic Buffering

    Fast-forward ~ 12 bytes

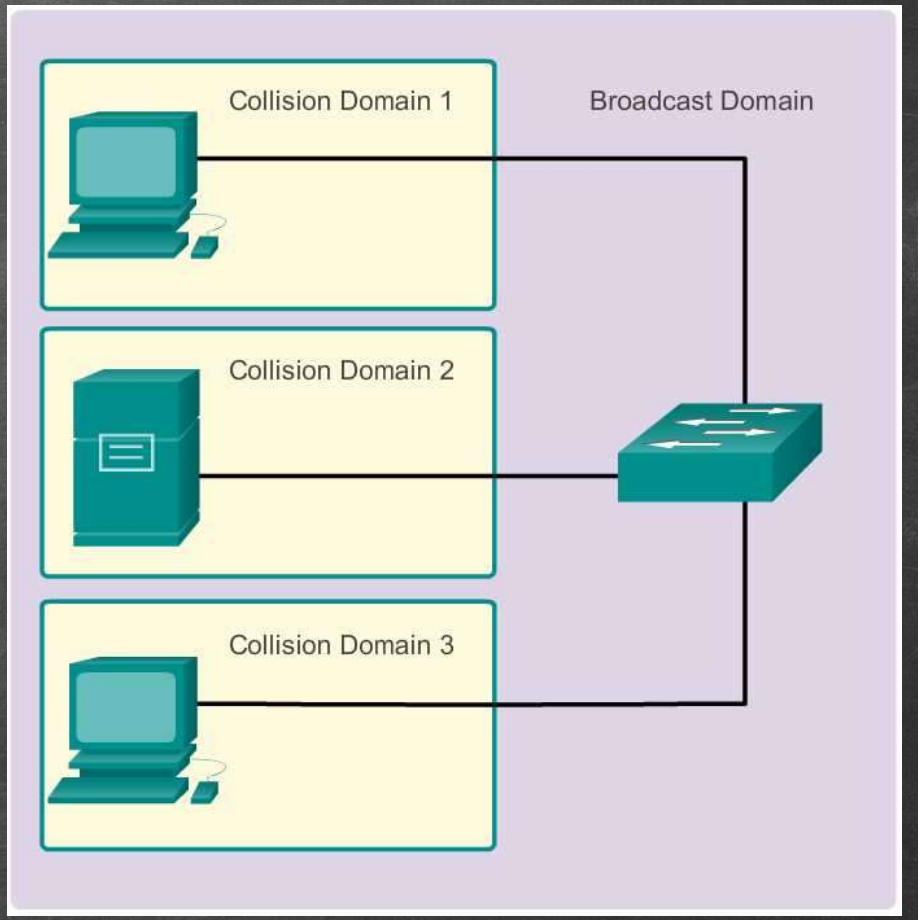
    Fragment-free ~ 64 bytes





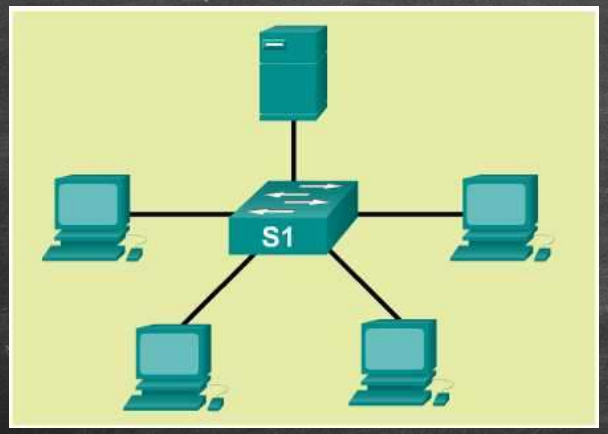
Switching Domains

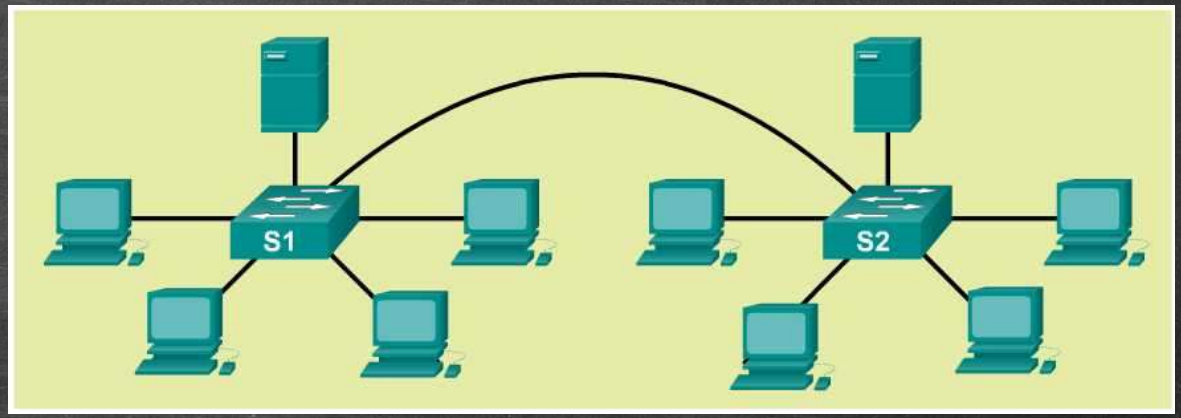
- Collision Domains
  - Collision domain is the segment where devices must compete to communicate
  - All ports of a hub belong to the same collision domain
  - Every port of a switch is a collision domain on its own
  - A switch break the segment into smaller collision domains, easing device competition.



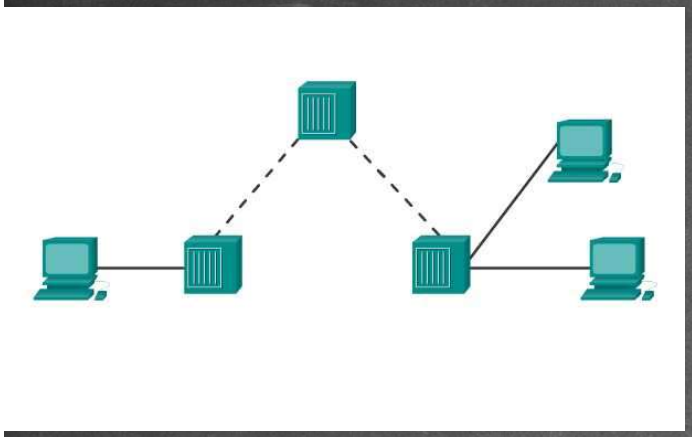
Switching Domains

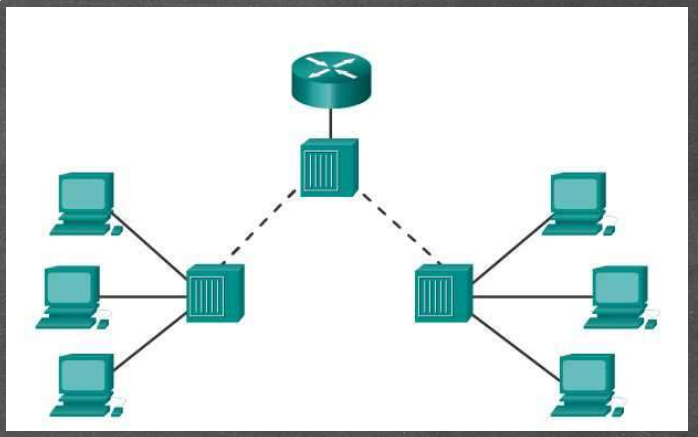
- Broadcast Domains
  - Broadcast domain is the extend of the network where a broadcast frame can be heard.
  - Switches forward broadcast frames to all ports. Therefore switches don't break broadcast domains.
  - All ports of a switch (with its default configuration) belong to the same broadcast domain
  - If two or more switches are connected, broadcasts will be forward to all ports of all switches (except for the port that originally received the broadcast)

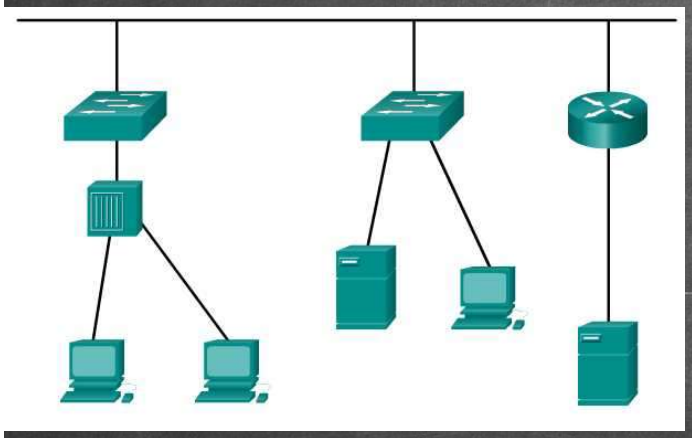


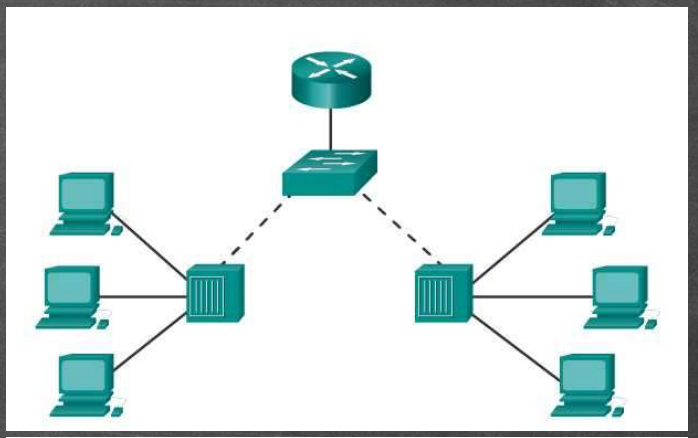


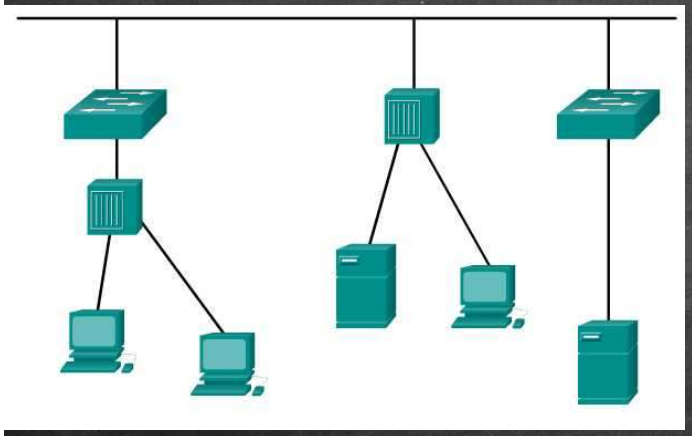
Switching Domains

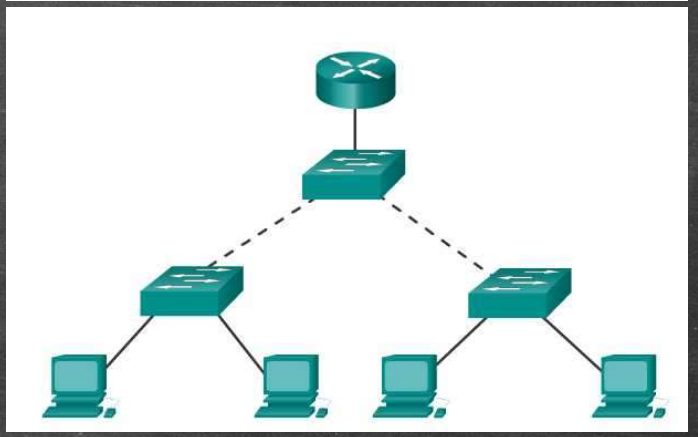












- Basic Switch Concept & Configuration
  - Basic Switch Configuration
    - Switch Boot Sequent
    - Preparing for Basic Switch Management
    - Configure Switch Ports
  - Switch Security : Security Remote Access
  - Switch Port Security

Switch Boot Sequence

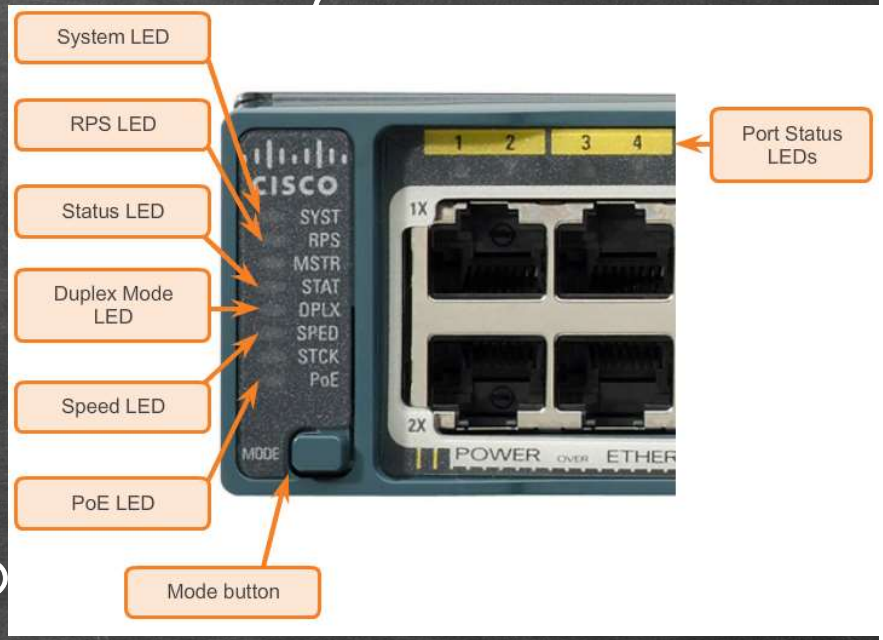
- POST
- Run boot loader software
- Boot loader does low-level CPU initialization
- Boot loader initializes the flash filesystem
- Boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

Switch Boot Sequence

- In order to find a suitable IOS image, the switch goes through the following steps:
  - It attempts to automatically boot by using information in the BOOT environment variable
  - If this variable is not set, the switch performs a top-to-bottom search through the flash file system. It will load and execute the first executable file, if it can.
  - The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the configuration file, startup configuration, which is stored in NVRAM.
- Note: the command boot system can be used to set the BOOT environment variable.

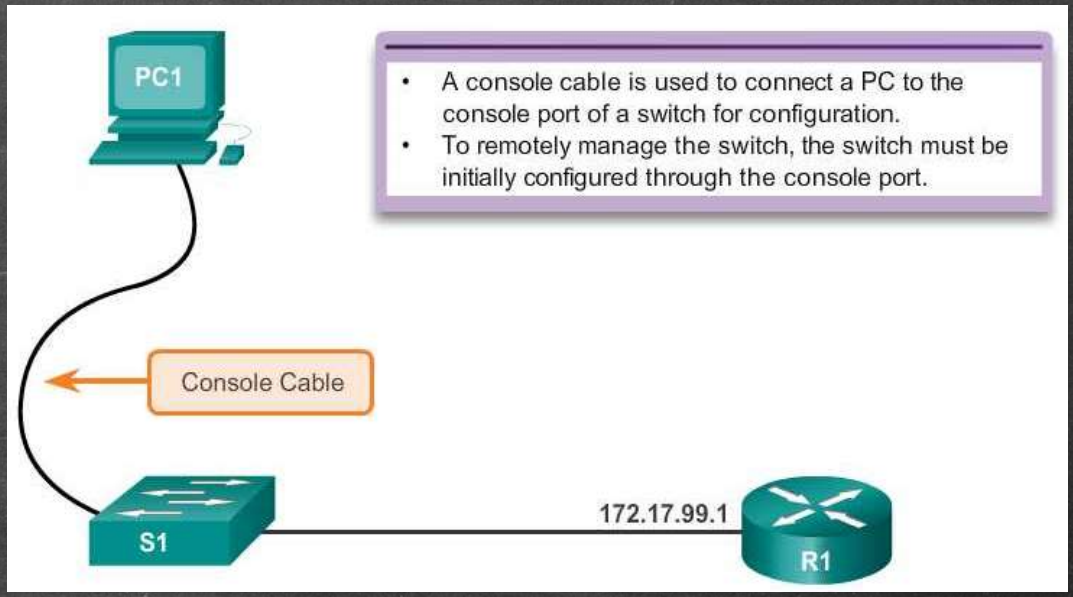
Switch LED Indicators

- Each port on Cisco Catalyst switches have status LED indicator lights.
- By default these LED lights reflect port activity but they can also provide other information about the switch through the Mode button
- The following modes are available on Cisco Catalyst 2960 switches:
  - System LED
  - Redundant Power System (RPS) LED
  - Port Status LED
  - Port Duplex LED
  - Port Speed LED
  - Power over Ethernet (PoE) Mode LED



Preparing for Basic Switch Management

- In order to remotely manage a Cisco switch, it needs to be configured to access the network
- An IP address and a subnet mask must be configured
- If managing the switch from a remote network, a default gateway must also be configured
- The IP information (address, subnet mask, gateway) is to be assigned to a switch SVI (switch virtual interface)
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.



Preparing for Basic Switch Management

Configure Switch Management Interface

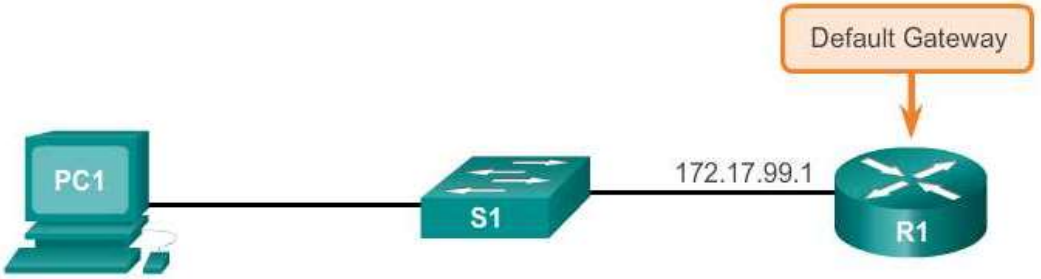
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan 99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11 255.255.0.0**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configure Switch Default Gateway

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.1**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

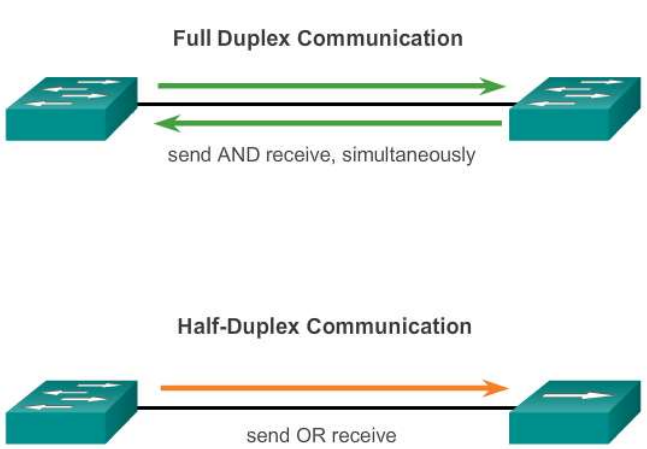
Verify Switch Management Interface Configuration

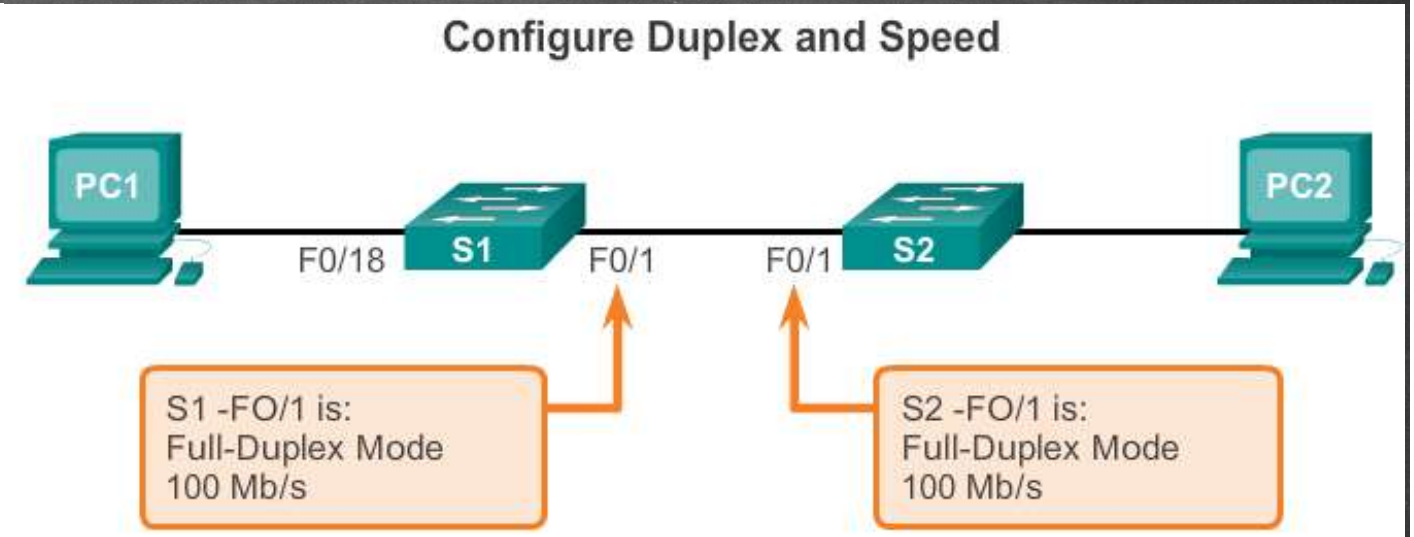
```
S1# show running-config
...
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
...
 <output omitted>

S1# show ip interface brief

Interface          IP-Address     OK?  Method Status  Protocol
Vlan99             172.17.99.11   YES  manual up      up
FastEthernet0/18   unassigned     YES  unset  up      up
```



Configure Switch Ports

- Duplex Communication





Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configure Switch Ports

- Auto-MDIX

Enable auto-MDIX

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface to autonegotiate duplex with the connected device.	S1(config-if)# **duplex auto**
Configure the interface to autonegotiate speed with the connected device	S1(config-if)# **speed auto**
Enable auto-MDIX on the interface.	S1(config-if)#**mdix auto**
Return to the privileged EXEC mode.	S1(config-if)#**end**
Save the running config to the startup config.	S1#**copy running-config startup-config**

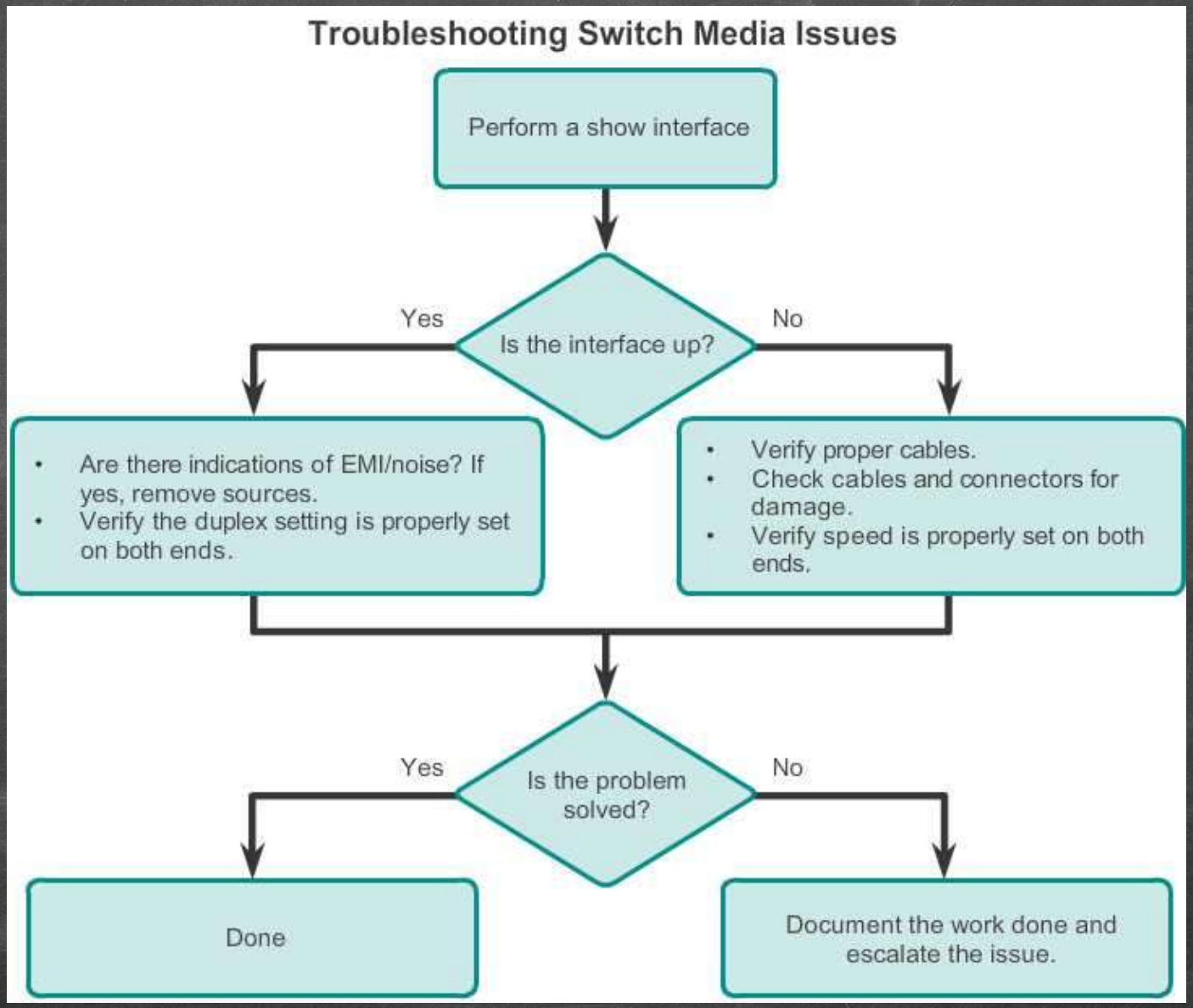
Configure Switch Ports

- Verifying Switch Port Configuration

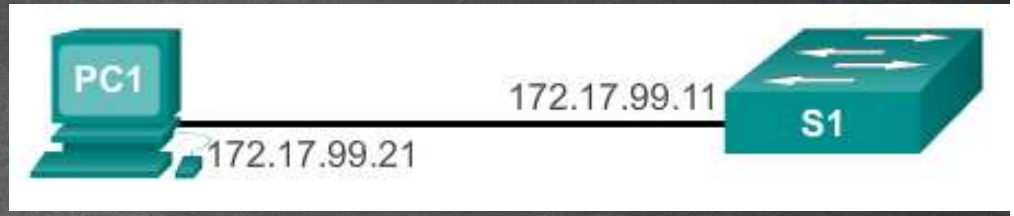
Verification Commands

Cisco Switch IOS Commands	
Display interface status and configuration.	S1# **show interfaces [interface-id]**
Display current startup configuration.	S1# **show startup-config**
Display current operating config.	S1# **show running-config**
Displays info about flash filesystem.	S1# **show flash**
Displays system hardware & software status.	S1# **show version**
Display history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip [interface-id]**
Display the MAC address table.	S1# **show mac-address-table**

Configure Switch Ports



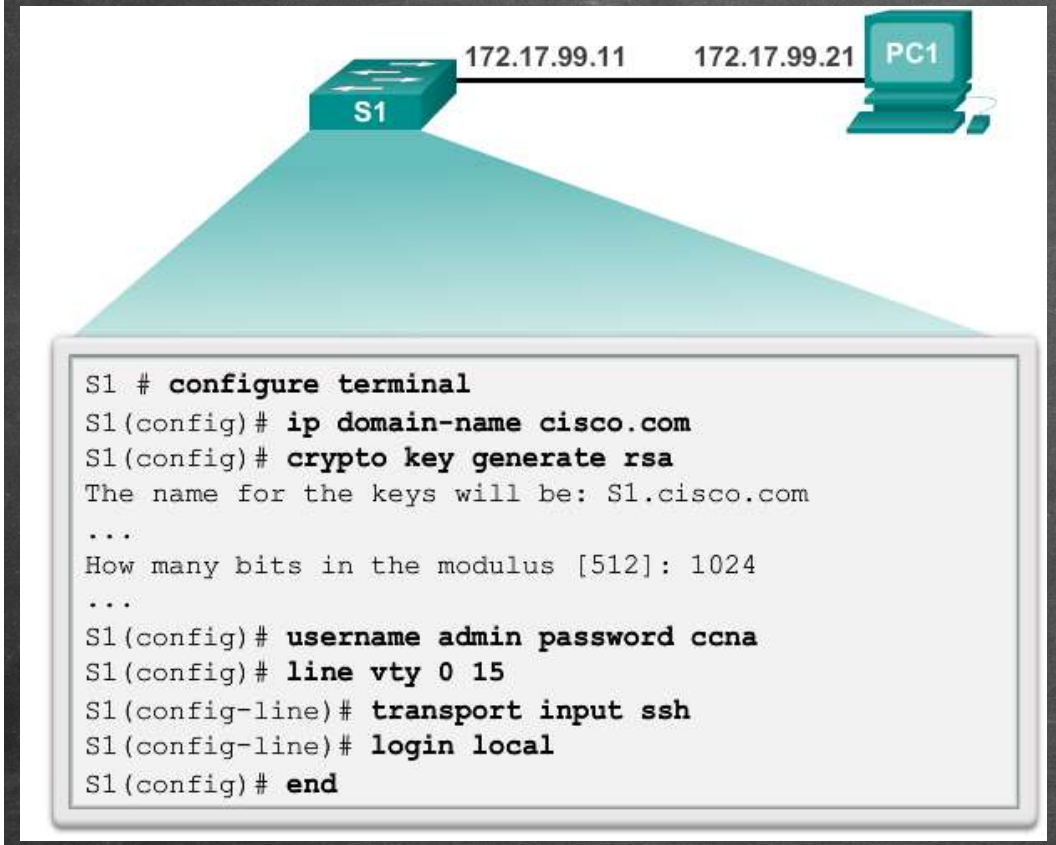
Security Remote Access



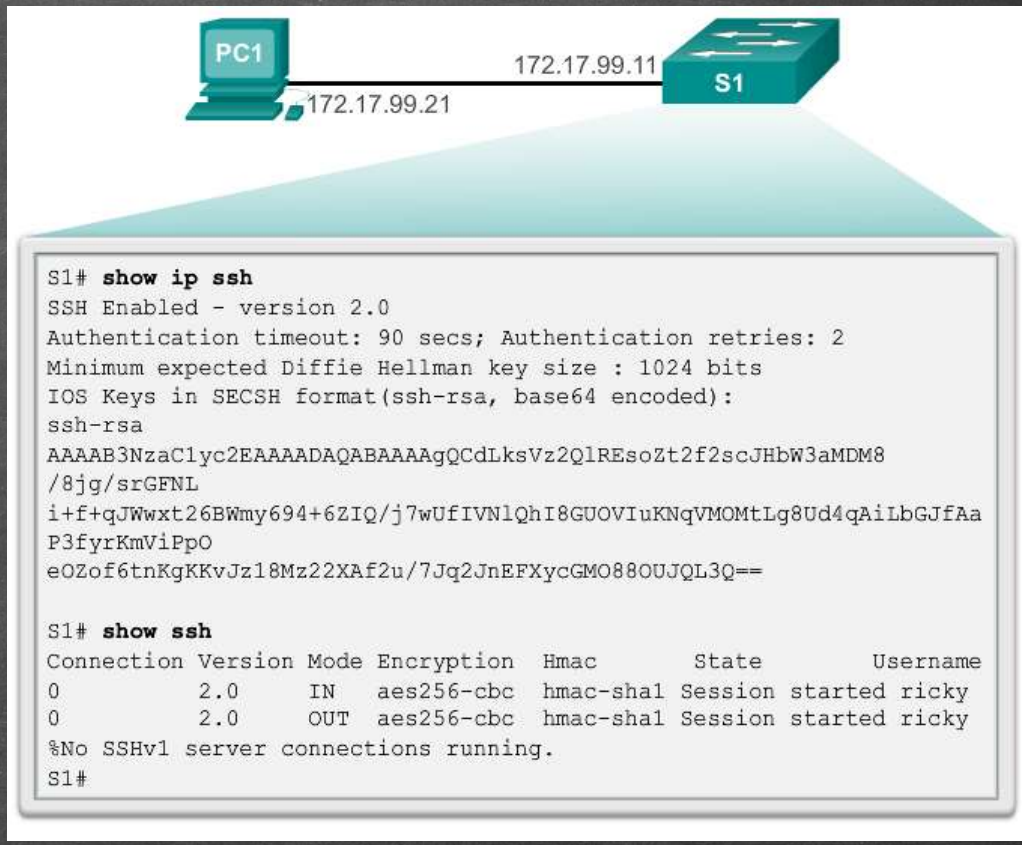
- SSH Operation
  - Secure Shell (SSH) is a protocol that provides a secure (encrypted) command-line based connection to a remote device
  - SSH is commonly used in UNIX-based systems
  - Cisco IOS also supports SSH
  - A version of the IOS software including cryptographic (encrypted) features and capabilities is required in order to enable SSH on Catalyst 2960 switches
  - Because its strong encryption features, SSH should replace Telnet for management connections
  - SSH uses TCP port 22 by default. Telnet uses TCP port 23

Security Remote Access

- Configuring SSH
- Verifying SSH




```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started ricky
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started ricky
%No SSHv1 server connections running.
S1#
```

Switch Port Security

- Operation : Secure MAC Address Types
  - Static secure MAC addresses
    - MAC addresses that are manually configured on a port by using the **switchport port-security mac-address *mac-address*** interface configuration mode command.
  - Dynamic secure MAC addresses
    - MAC addresses that are dynamically learned and stored only in the address table by using **switchport port-security mac-address sticky** interface configuration mode command.
  - Sticky secure MAC addresses
    - MAC addresses that can be dynamically learned or manually confiugred, then stored in the address table and added to the running configuration.

Switch Port Security

- Violation mode : IOS considers a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses for that interface have been added to the CAM, and a station whose MAC address is not in the address table attempts to access the interface.
  - An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
- There are three possible action to be taken when a violation is detected:

Security violation modes include: Protect, Restrict, and Shutdown.

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Switch Port Security

Port Security Defaults

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Switch Port Security

- Static secure MAC addresses

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address MAC-ADD
```

- Dynamic secure MAC addresses

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
```

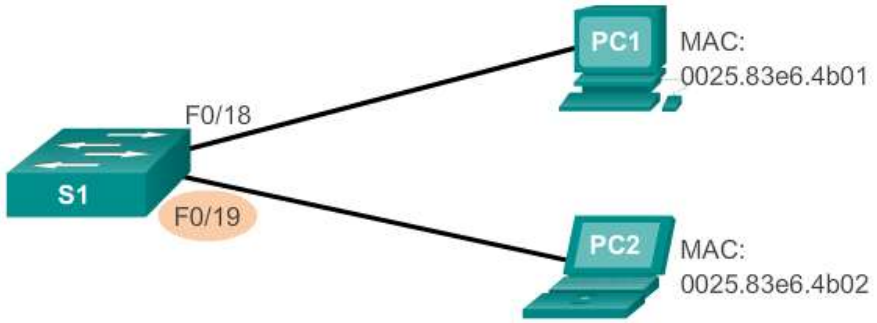
- Maximum MAC addresses

```
Switch(config-if)#switchport port-security maximum MAX
```

- Violation mode

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

Switch Port Security



Cisco IOS CLI Commands

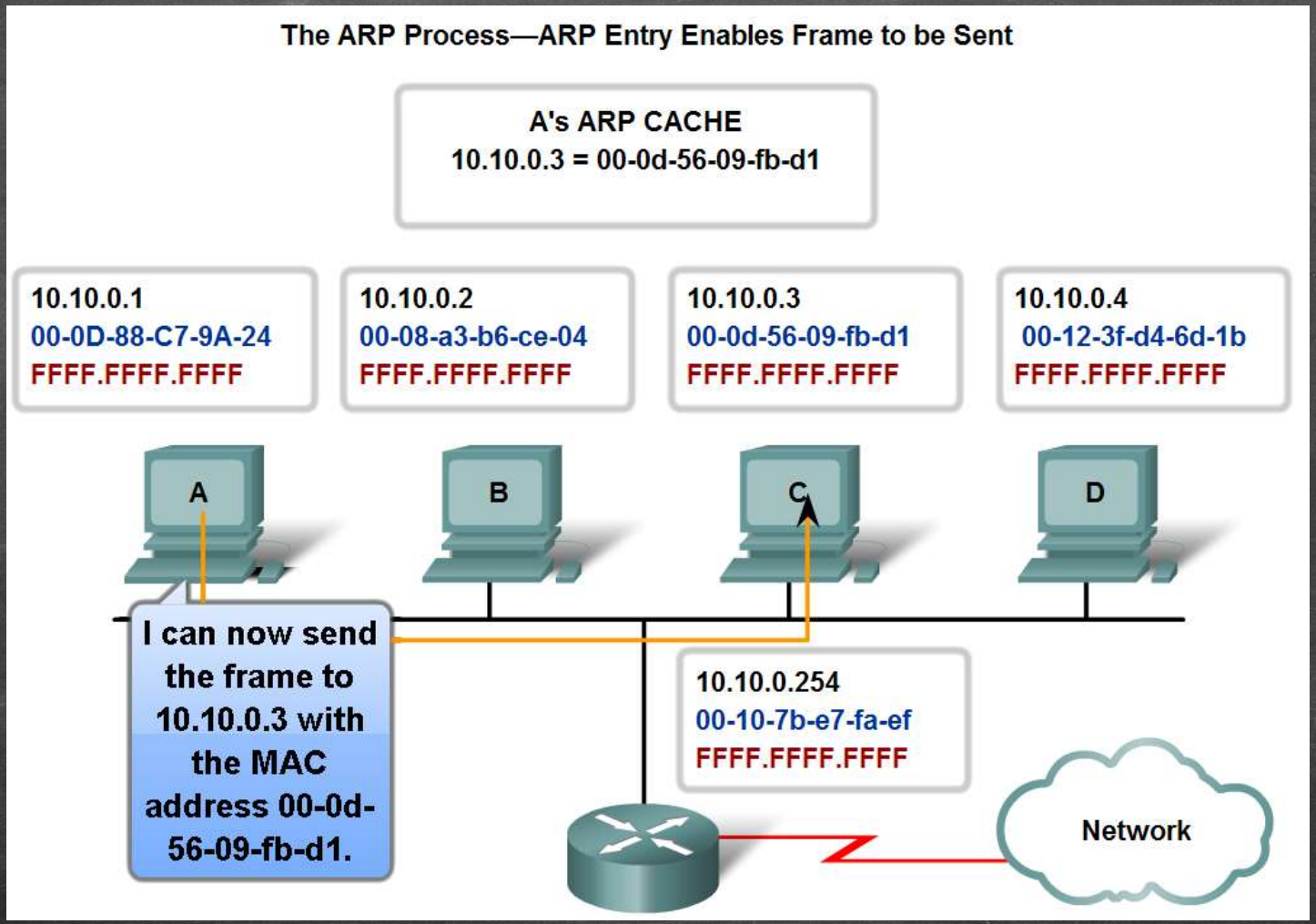
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.
S1(config-if)#**switchport port-security maximum 50**	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#**switchport port-security mac-address sticky**	Enable sticky learning.

```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18       -
1       0025.83e6.4b02    SecureSticky      Fa0/19       -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

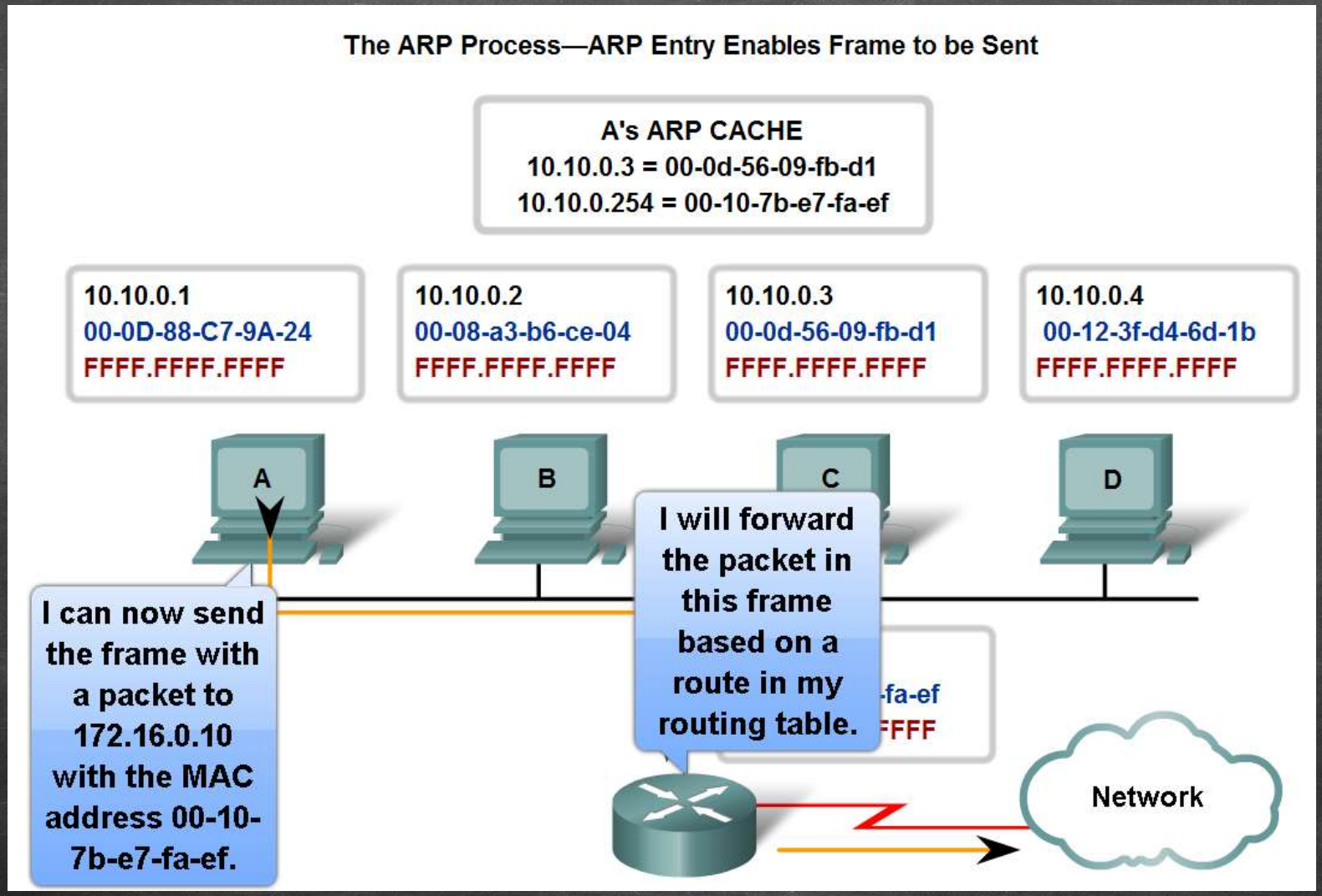
Address Resolution Protocol

- Mapping IP to MAC Addresses



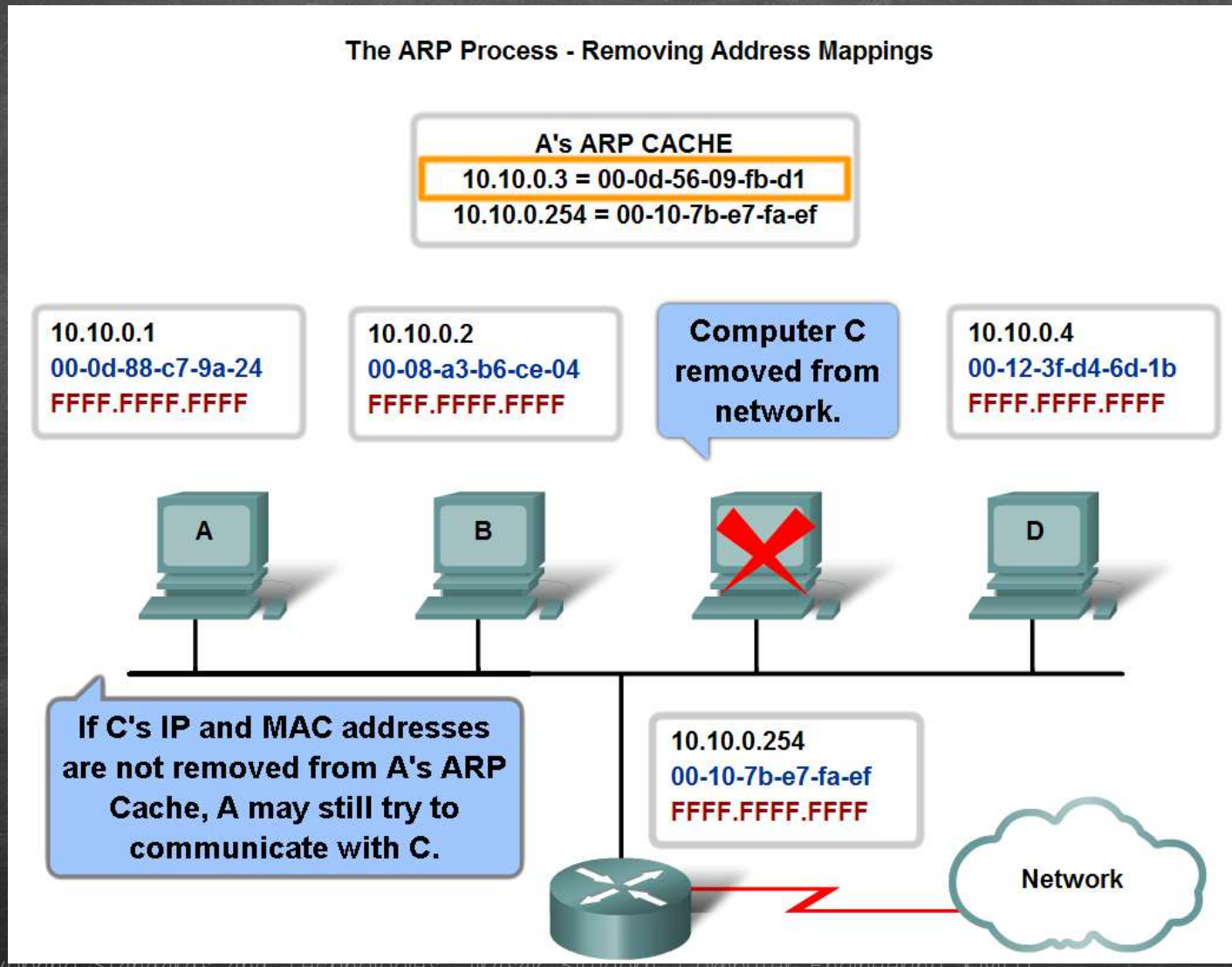
Address Resolution Protocol

- ARP - Destinations Outside the Local Network

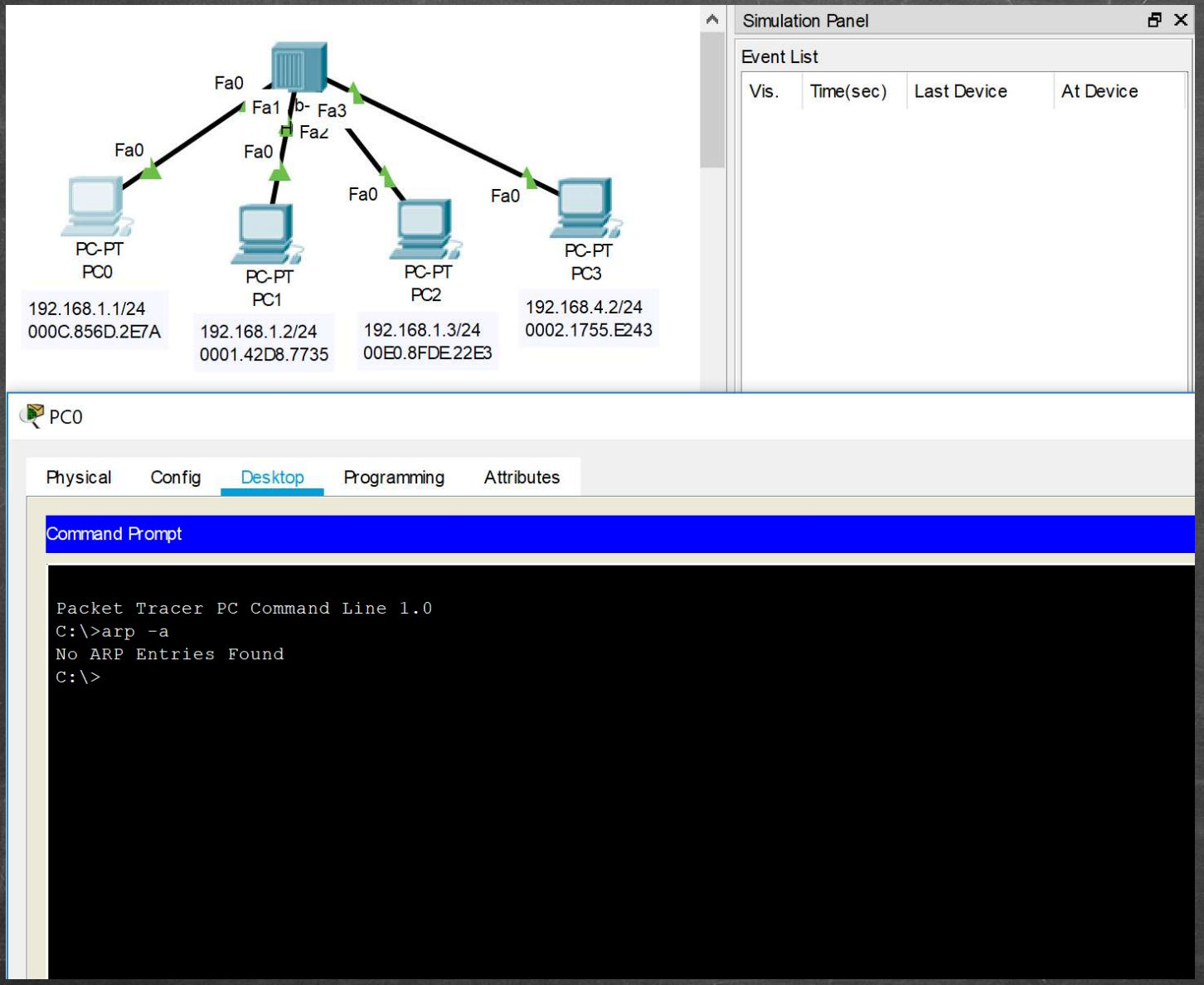


Address Resolution Protocol

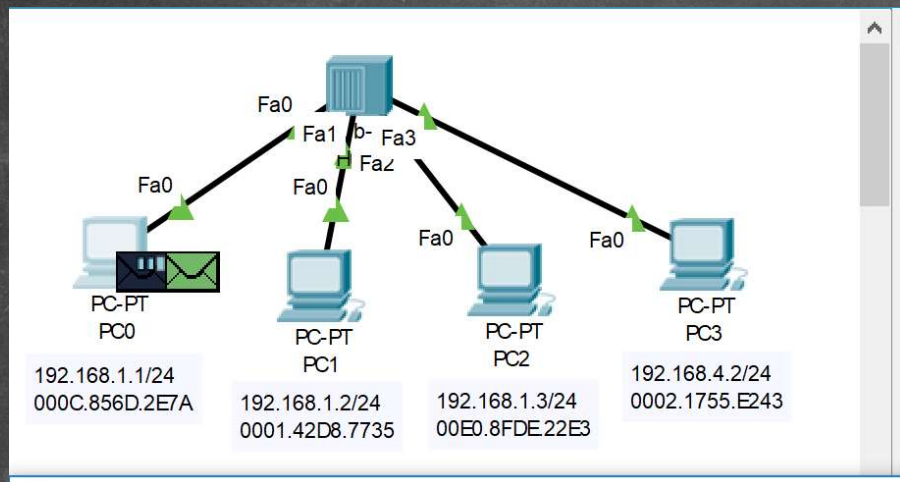
- ARP - Removing Address Mappings

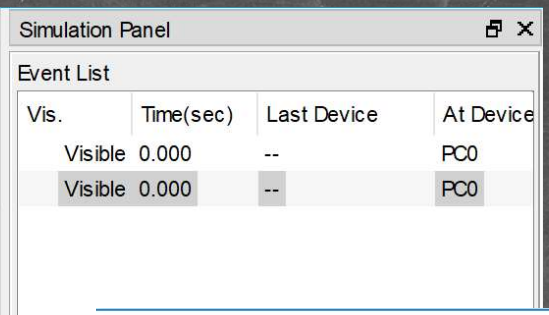


Address Resolution Protocol

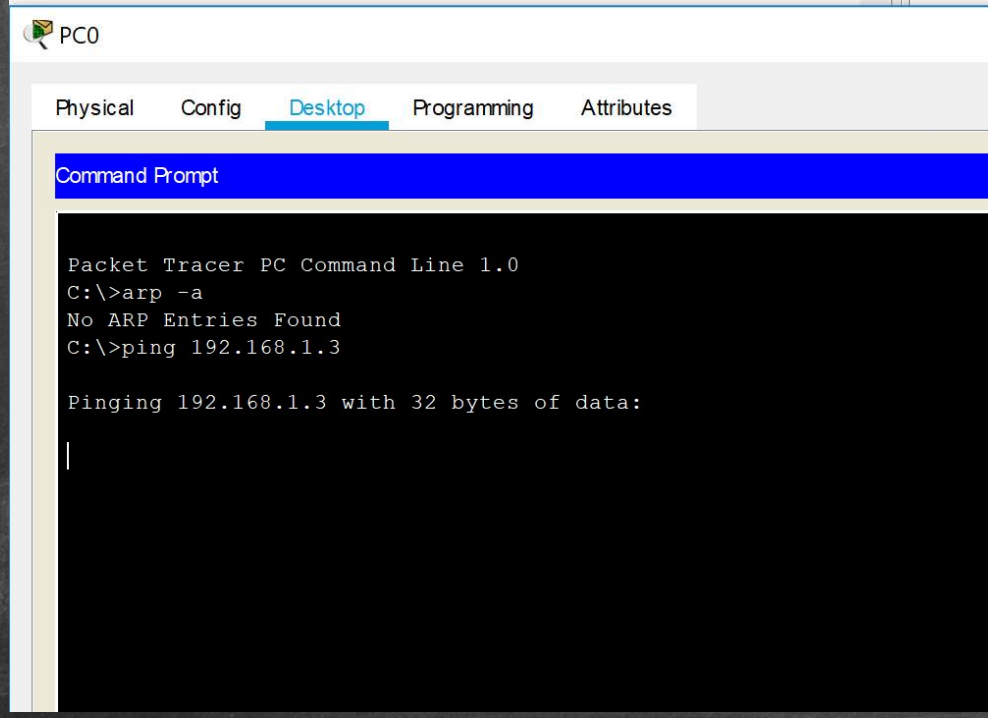


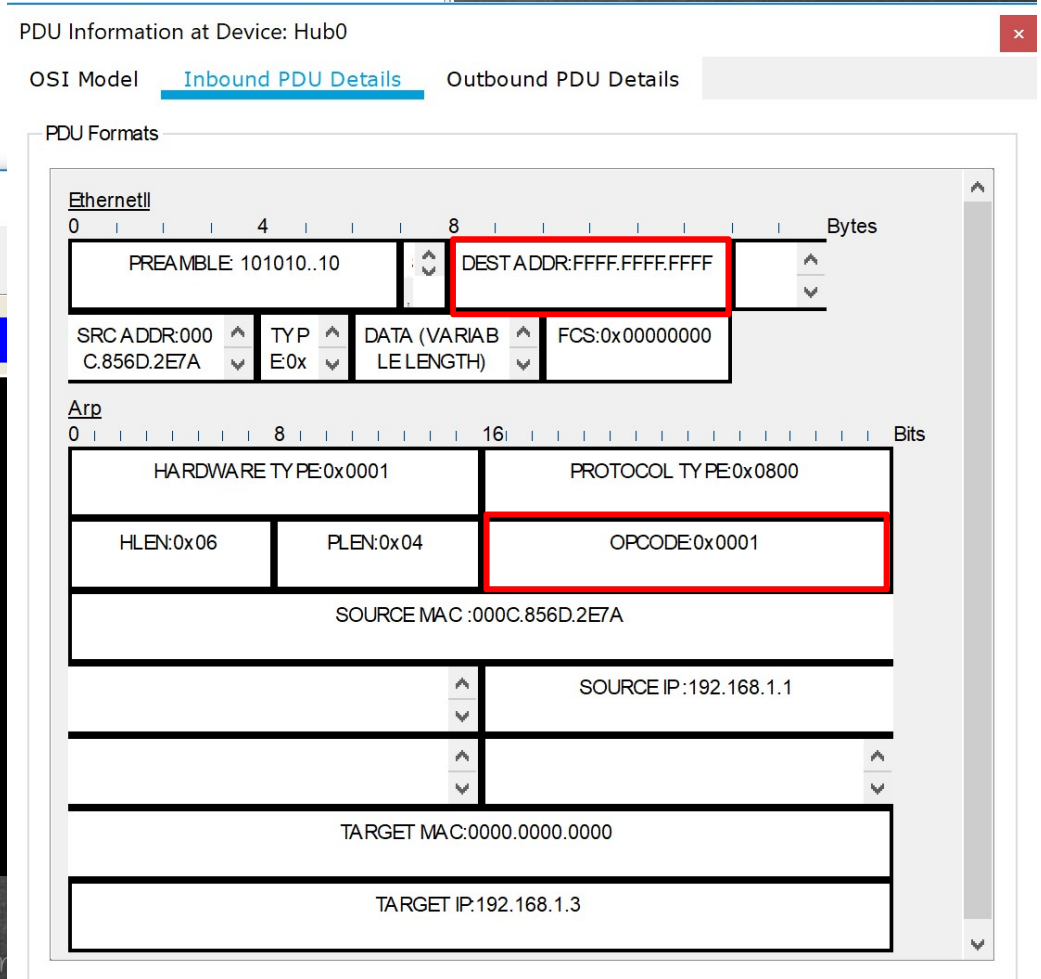
Address Resolution Protocol



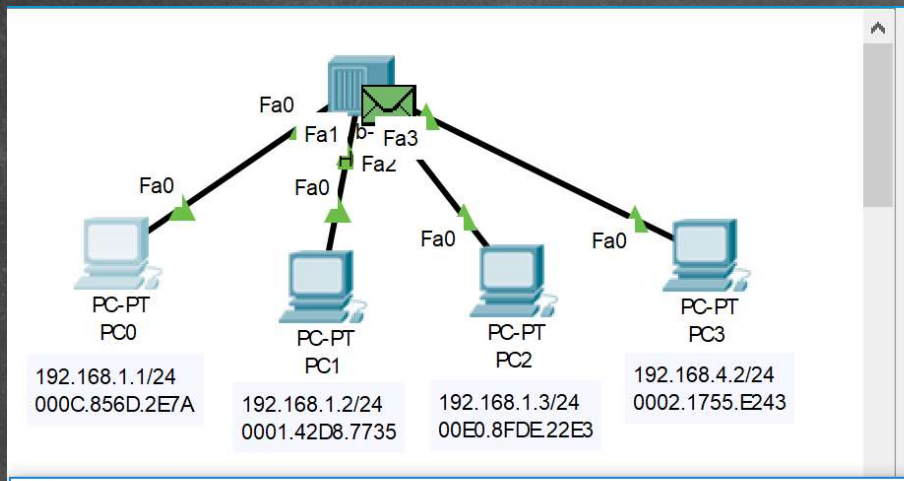


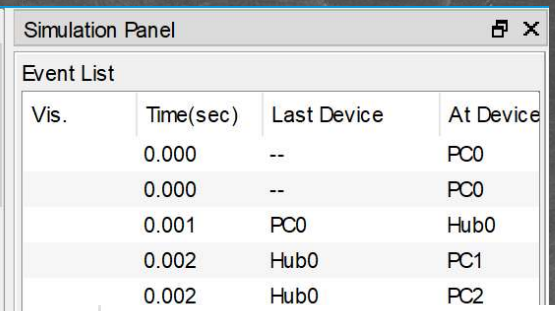
ARP request



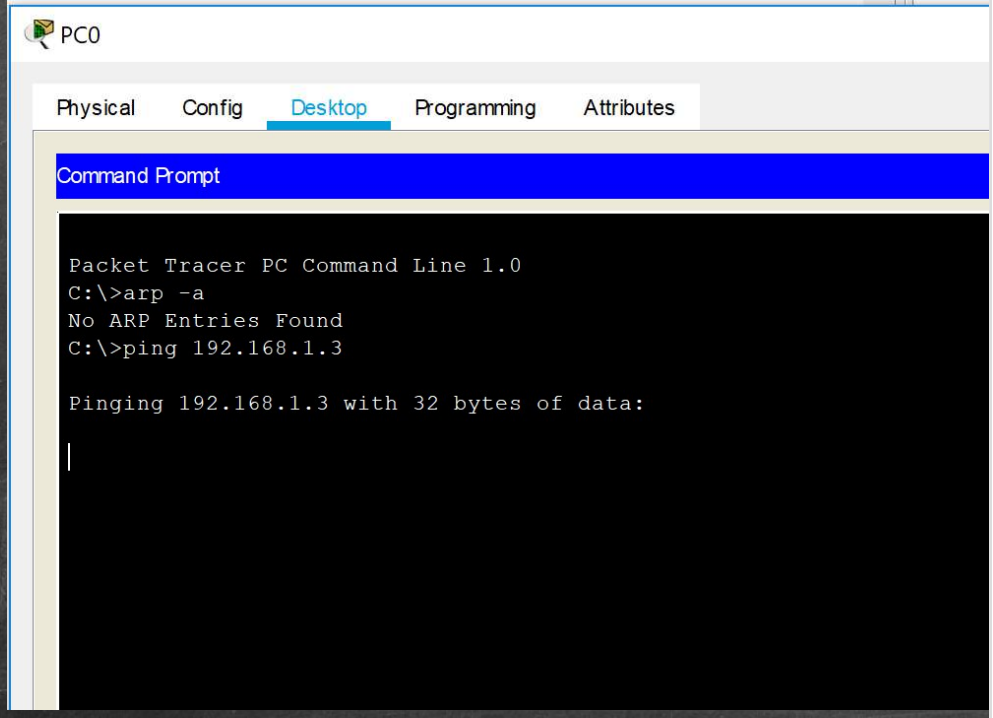


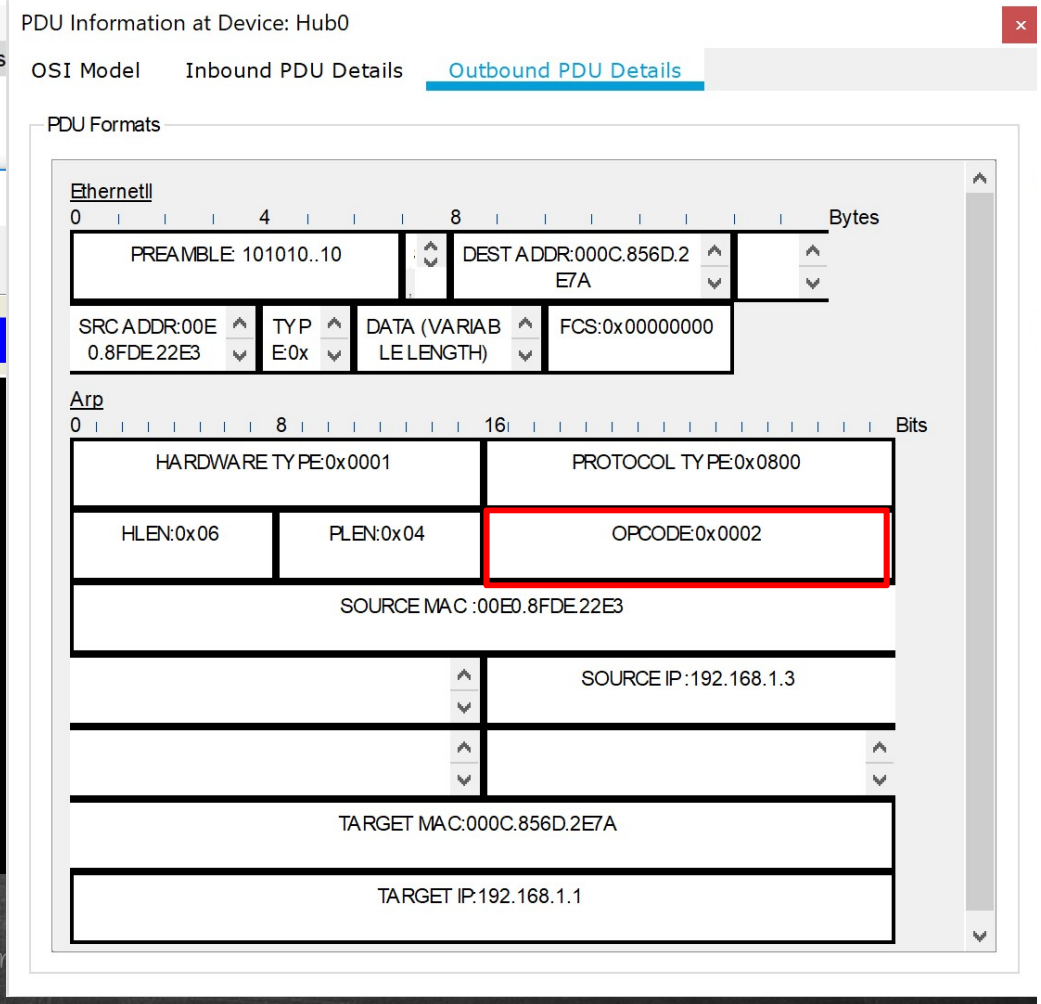
Address Resolution Protocol



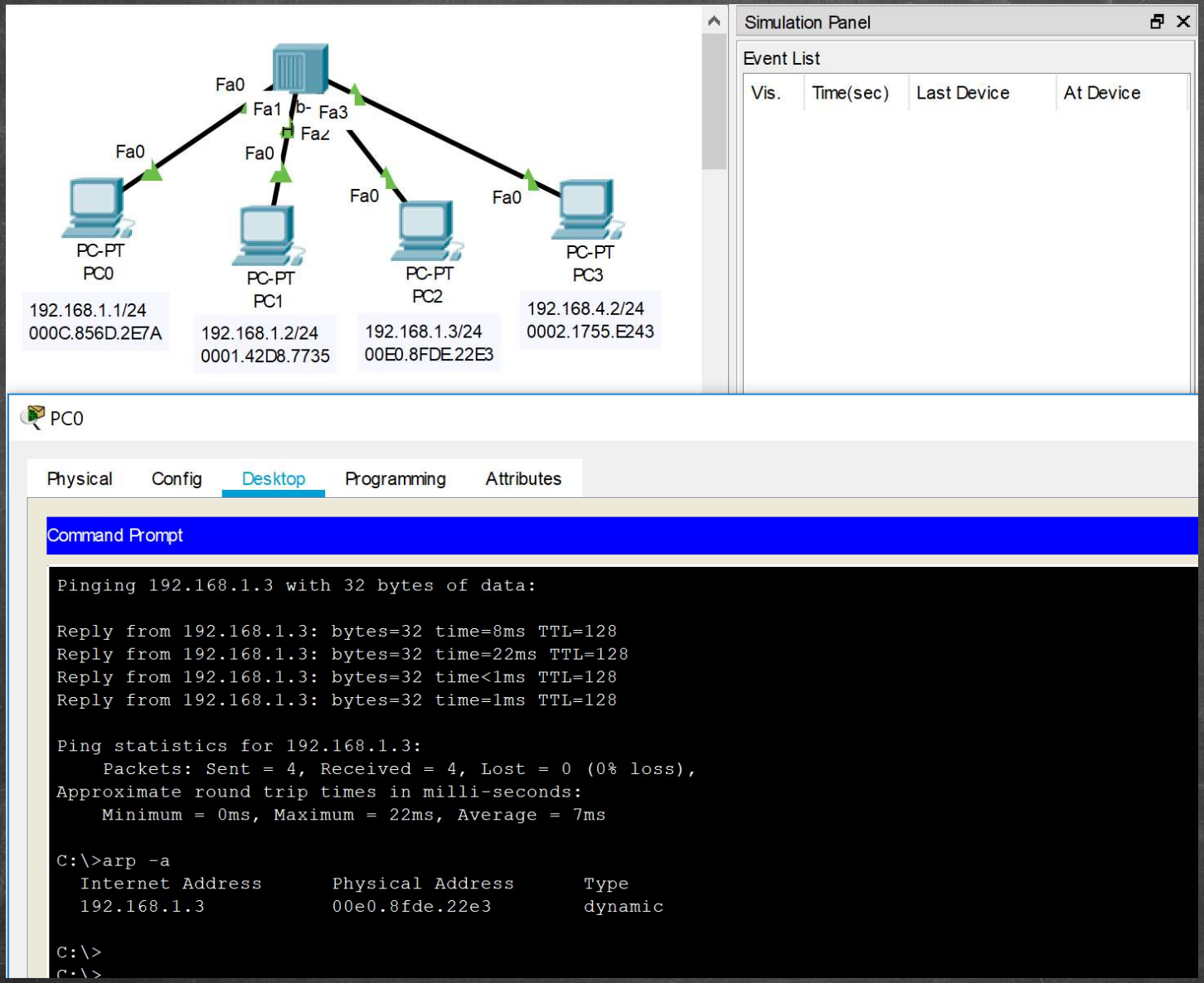


- ARP reply



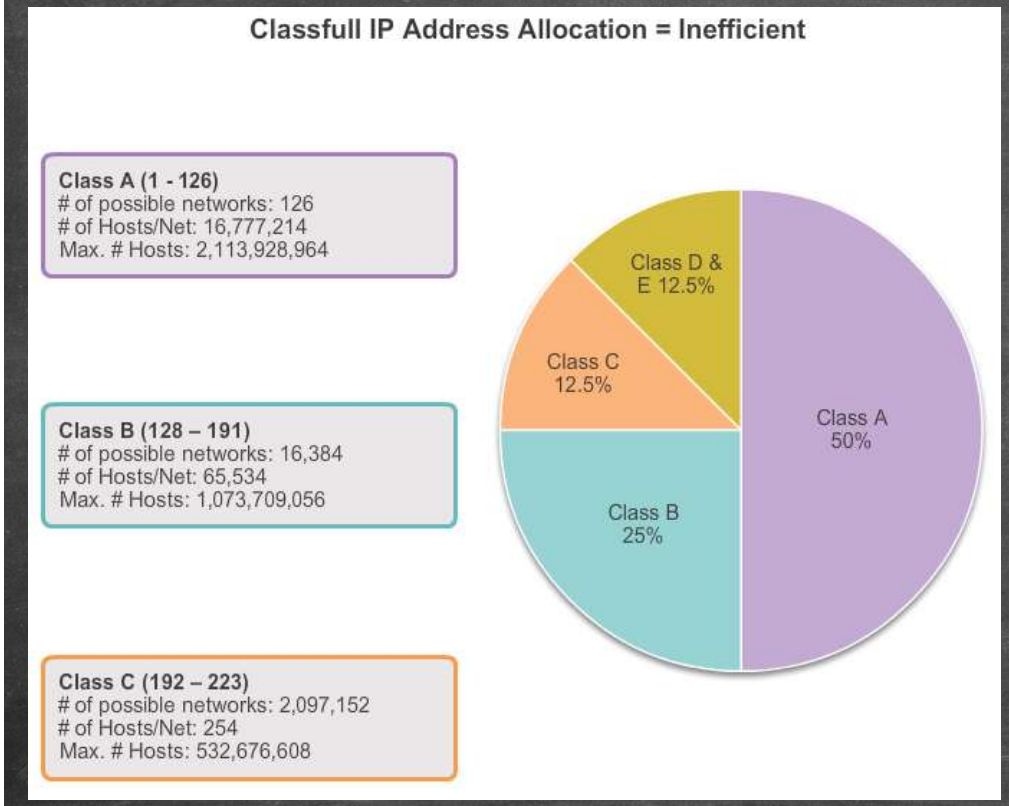


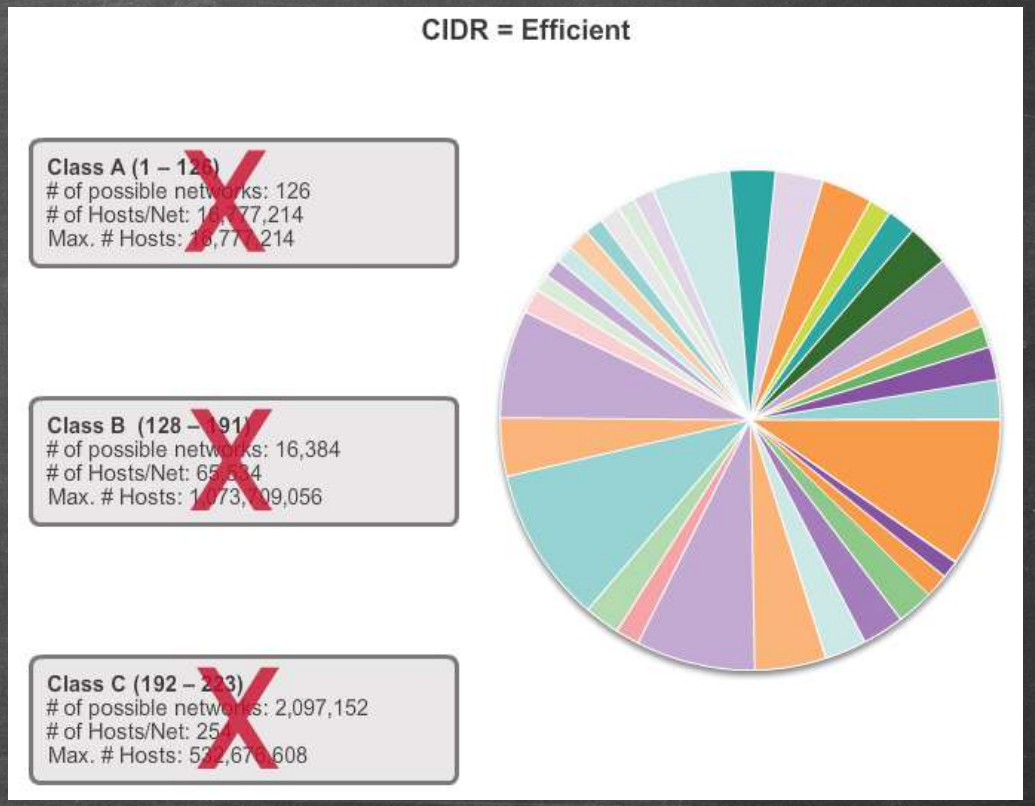
Address Resolution Protocol



IPv4

- Classful Addressing Waste
- Classless Inter-Domain Routing



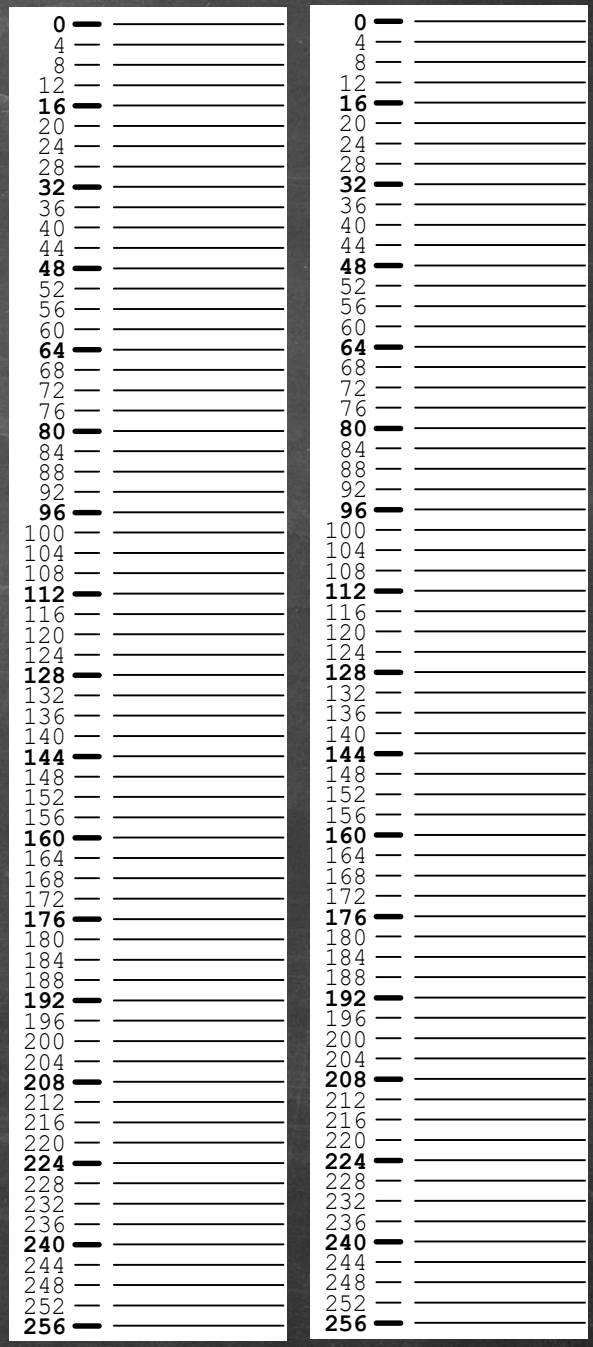


IPv4

- Classless Inter-Domain Routing
  - Fixed Length Subnet Masking
  - Variable Length Subnet Masking

Subnet Mask	CIDR Value
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19

Subnet Mask	CIDR Value
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31 Not valid

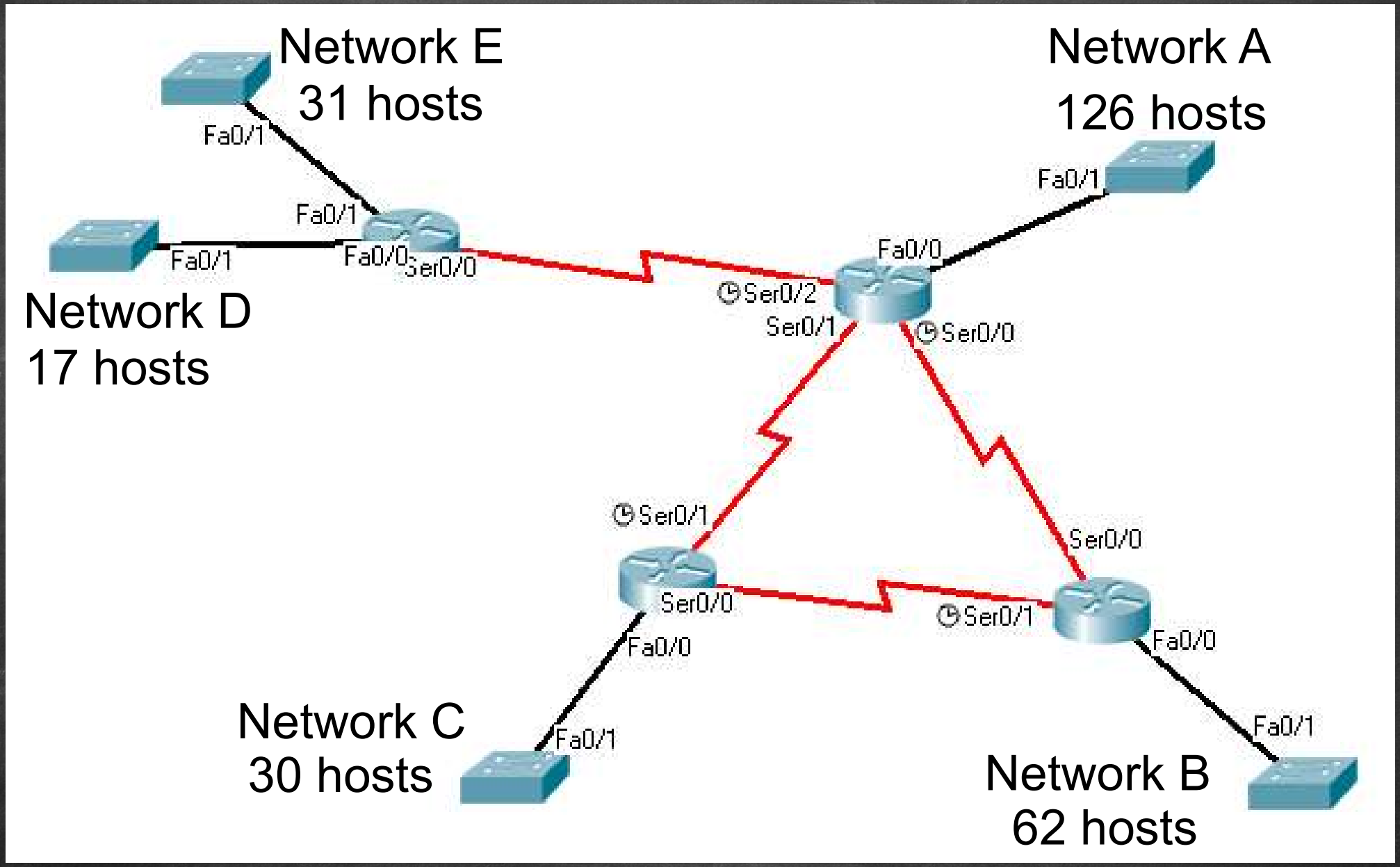


Subnet Planning

- Network 161.246.6.0/23
  - IP Address 161.246.6.0
  - IP Address 161.246.6.1
  - ...
  - IP Address 161.246.6.255
  - IP Address 161.246.7.1
  - IP Address 161.246.7.2
  - ...
  - IP Address 161.246.7.255

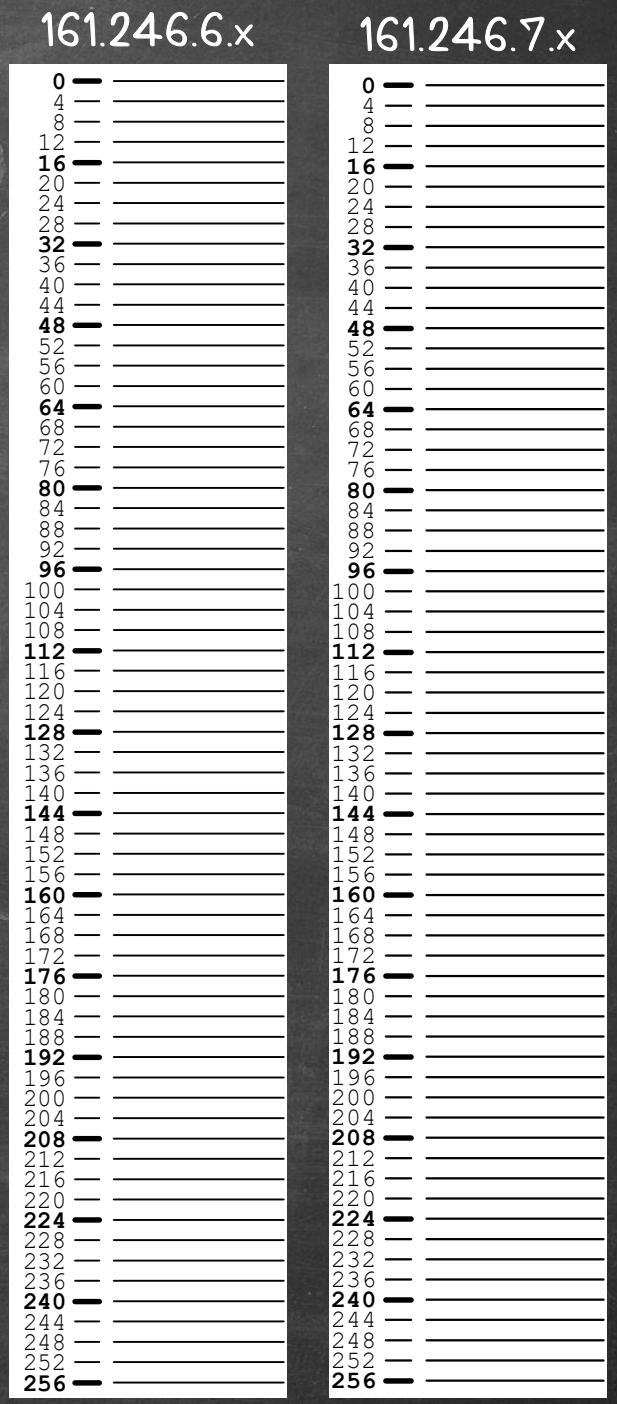
512 IP Address

Subnet Planning

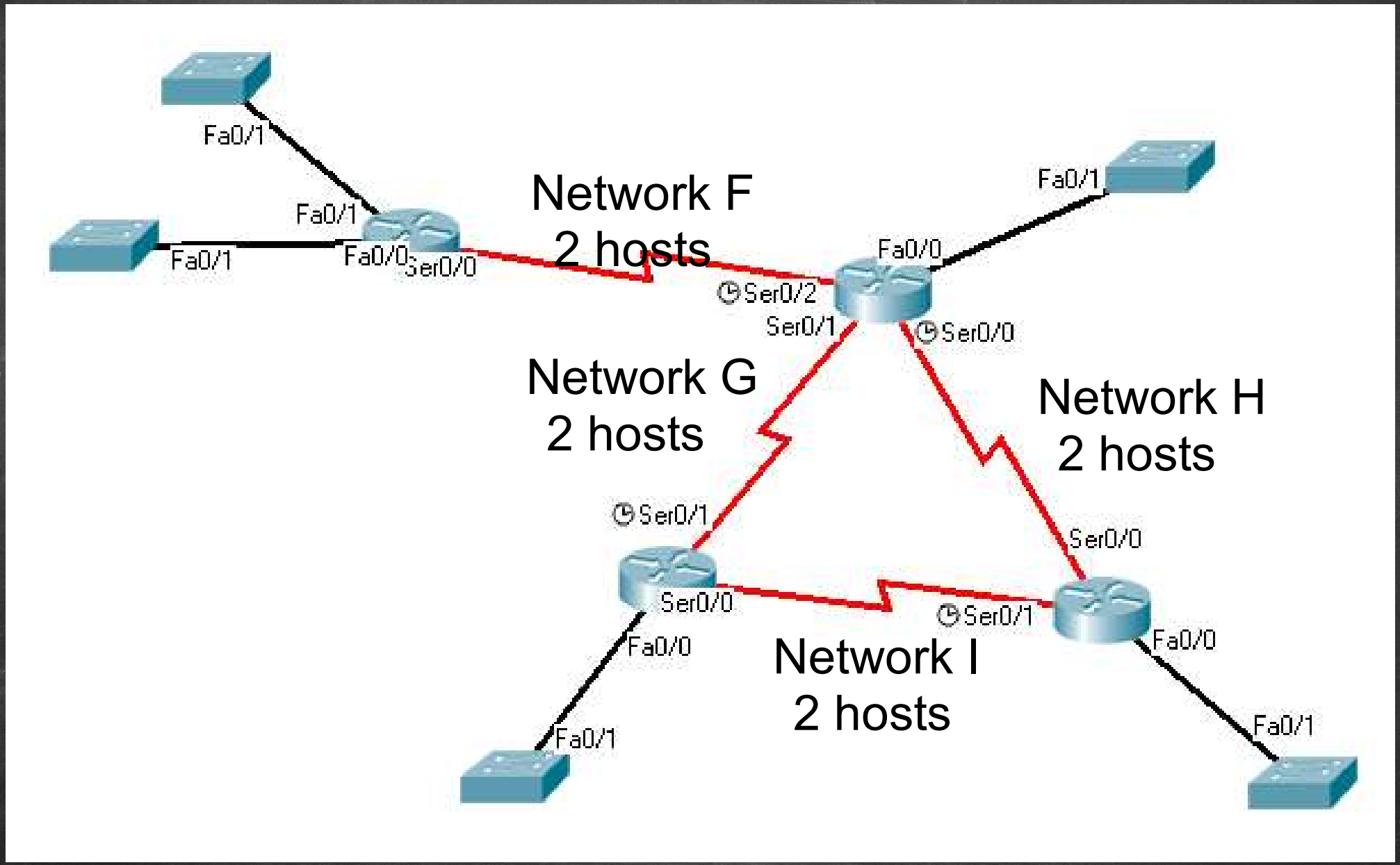


Subnet Planning

Network	Req. Host	Max. Host	Subnetwork	Subnet mask
A	126			
B	62			
C	30			
D	17			
E	31			

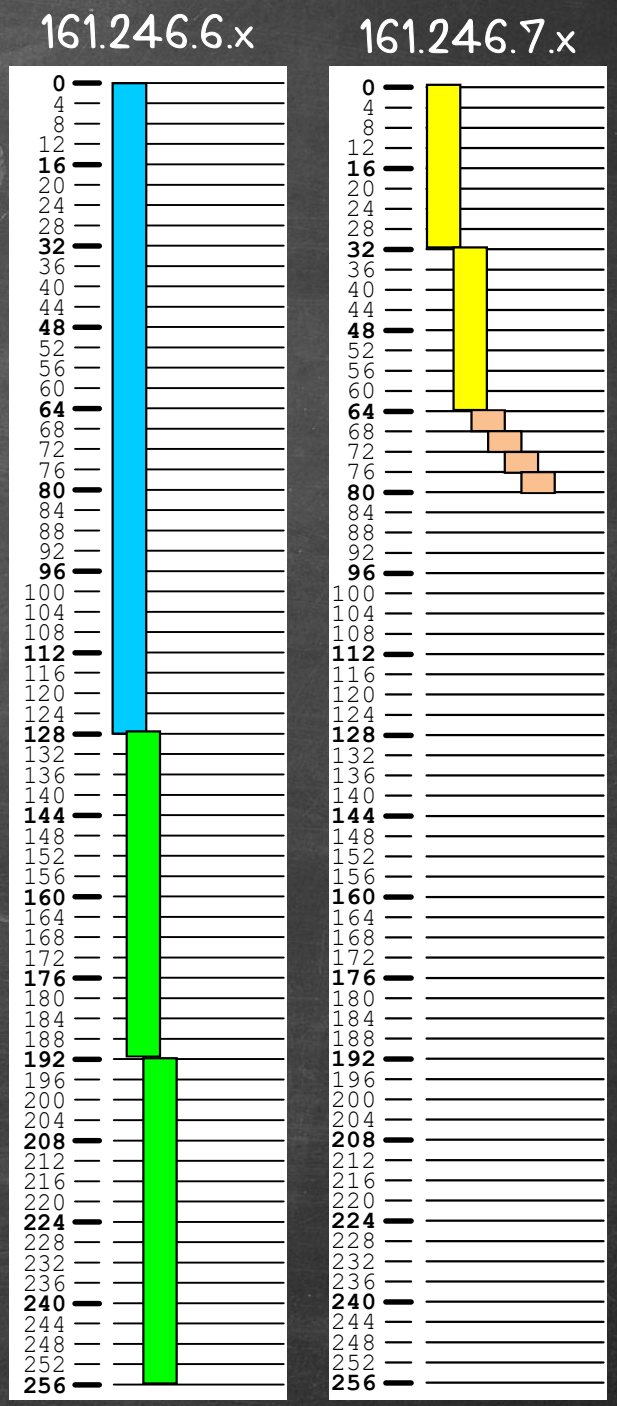


Subnet Planning



Subnet Planning

Network	Req. Host	Max. Host	Subnetwork	Subnet mask
A	126			
B	62			
C	30			
D	17			
E	31			
F				
G				
H				
I				



Questions and Answers