Chapter 2

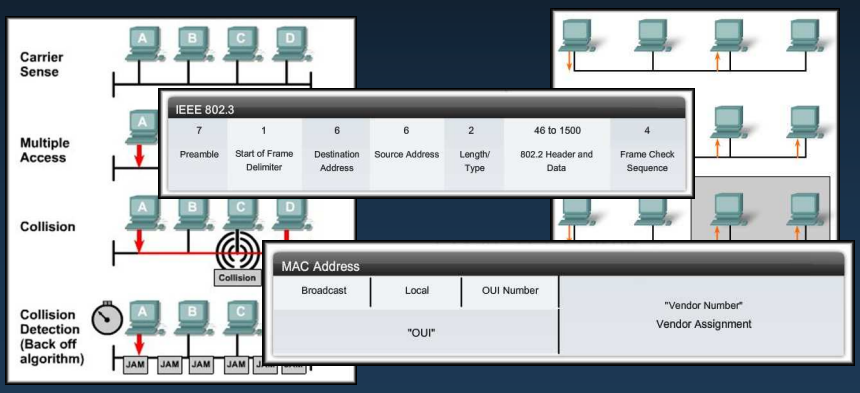
Switch Concepts and Configuration

Part I

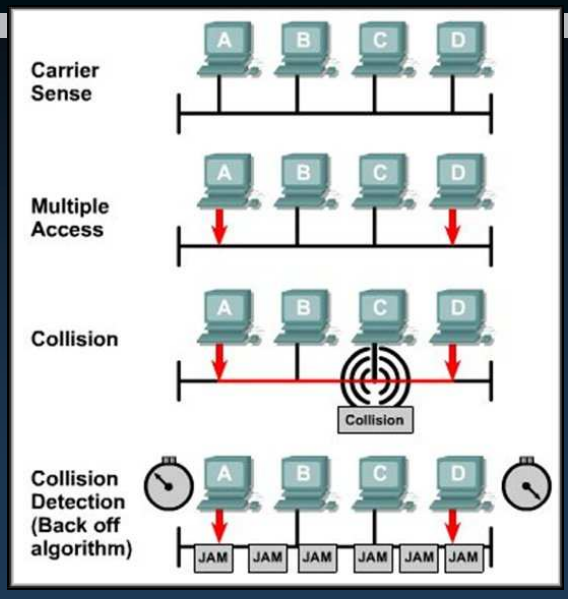
Note for Instructors

- These presentations are the result of a collaboration among the instructors at St. Clair College in Windsor, Ontario.
- Thanks must go out to Rick Graziani of Cabrillo College. His material and additional information was used as a reference in their creation.
- If anyone finds any errors or omissions, please let me know at:
  - tdame@stclaircollege.ca.

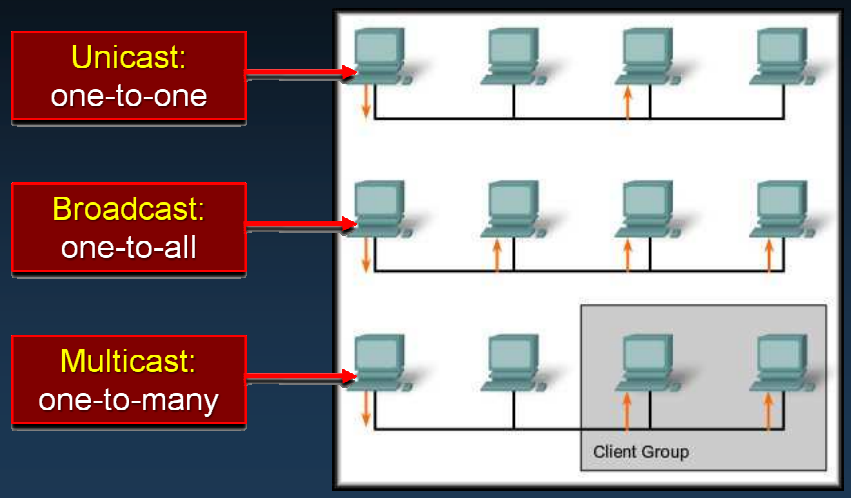
Key Elements of Ethernet/802.3 LANs



CSMA/CD



Ethernet Communications



Ethernet Communications

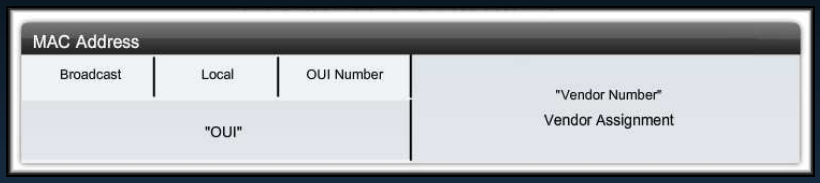
- **Ethernet Frame:** Minimum 64 bytes, Maximum 1518 bytes

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence

- **Preamble/SOFD:** Synchronize to medium.
- **Destination Address:** MAC Address of destination device.
- **Source Address:** MAC address of source device.
- **Length/Type:** Length of frame or protocol type code.
- **Data:** Encapsulated data from OSI Layers 7 to 3.
- **FCS:** Frame Check Sequence.

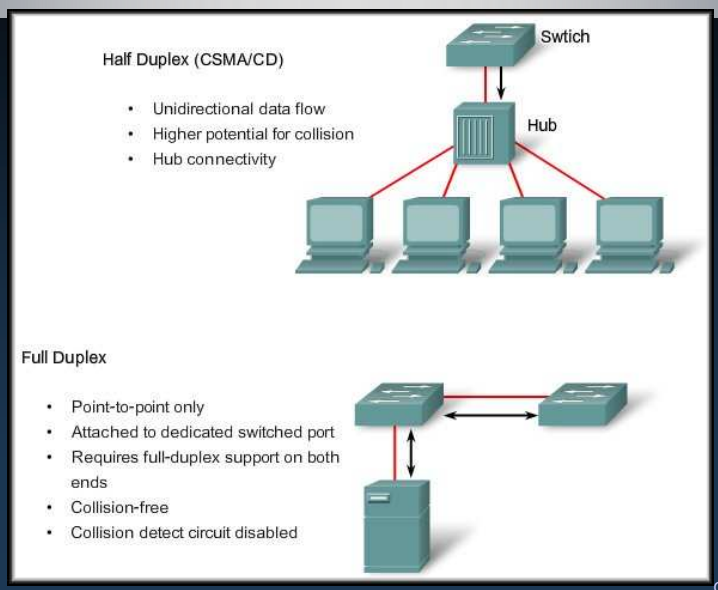
Ethernet Communications

- **MAC Address:** 12 hexadecimal digits



- **Broadcast:** Indicates a broadcast or multicast frame.
- **Local:** indicates whether the address can be modified locally.
- **OUI Number:** Manufacturer of the NIC.
- **Vendor Number:** Unique, vendor assigned number.

Ethernet Communications



Ethernet Communications

- Switch Port Settings:
  - AUTO:
    - Auto-negotiation of duplex mode. The two ports communicate to determine the best mode.
      - Default for FastEthernet and 10/100/1000 ports.
  - FULL:
    - Full-duplex mode.
      - Default for 100BASE-FX ports.
  - HALF:
    - Half-duplex mode.

Configuration commands later in the chapter.

Ethernet Communications

- Switch Port Settings:
  - AUTO:
    - Auto-negotiation of duplex mode. The two ports communicate to determine the best mode.
  - *Auto-negotiation can produce unpredictable results.*
    - If auto-negotiation fails because the attached device does not support it, the Catalyst switch defaults the switch port to half-duplex mode.
    - Half-duplex on one end and full-duplex on the other causes late collision errors at the half-duplex end.
    - To avoid this, manually set the duplex parameters of the switch to match the attached device.

Ethernet Communications

- Switch Port Settings:
  - Auto-MDIX feature:
    - In the past, either a cross-over or a straight-through cable was required depending on the type of device that was being connected to the switch.
    - Instead, the mdix auto interface configuration command enables the **automatic medium-dependent interface crossover (auto-MDIX)** feature.
    - With this feature enabled, the switch detects the interface required for copper media and configures the interface accordingly.

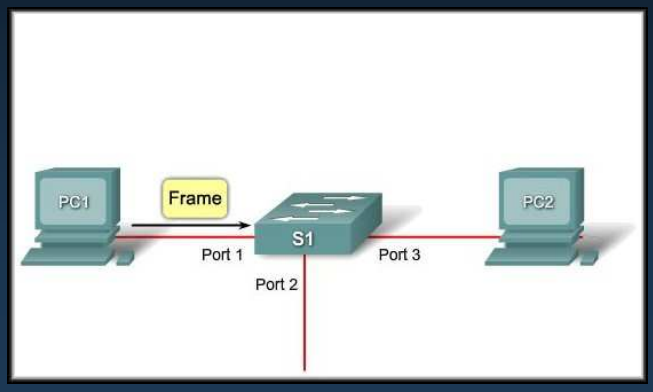
Configuration commands later in the chapter.

Switch MAC Address Table

- *Switches use MAC addresses to direct network traffic to the appropriate port.*
  - A switch builds a MAC address table by learning the MAC addresses of each device connected to each of its ports.
  - Once the MAC address has been added to the table, the switch uses the table entry to forward traffic to that node.
  - **If a destination address is not in the table, the switch forwards the frame out all ports except the receiving port.**
  - When the destination responds, the MAC address is added to the table.
  - If the port is connected to another switch or a hub, multiple MAC addresses will be recorded in the table.

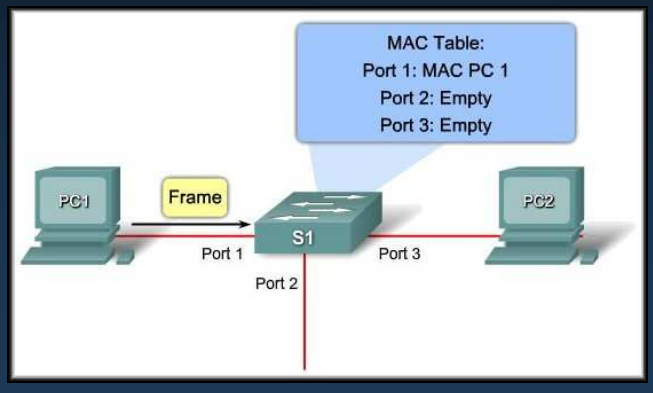
Switch MAC Address Table

- Example Step 1:
  - The switch receives a broadcast frame from PC 1 on Port 1.



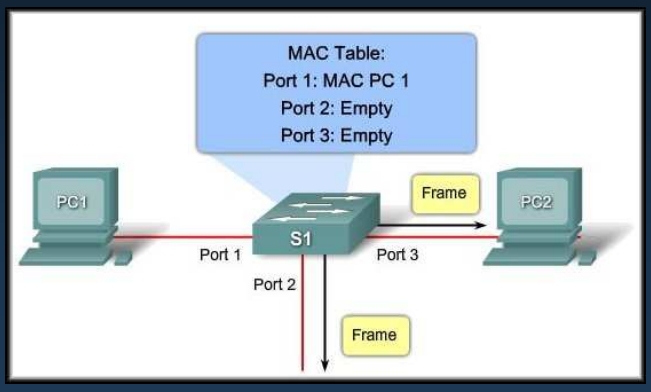
Switch MAC Address Table

- Example Step 2:
  - The switch enters the source MAC address and the switch port that received the frame into the address table.



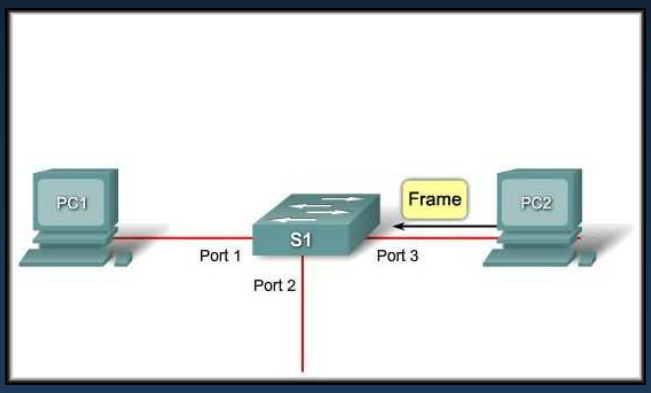
Switch MAC Address Table

- Example Step 3:
  - Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.



Switch MAC Address Table

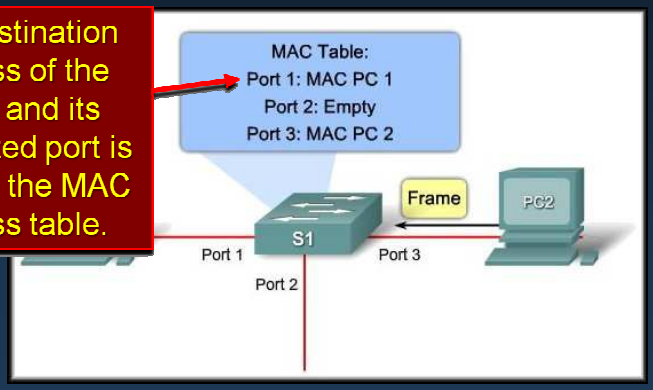
- Example Step 4:
  - The destination device replies to the broadcast with a unicast frame addressed to PC 1.



Switch MAC Address Table

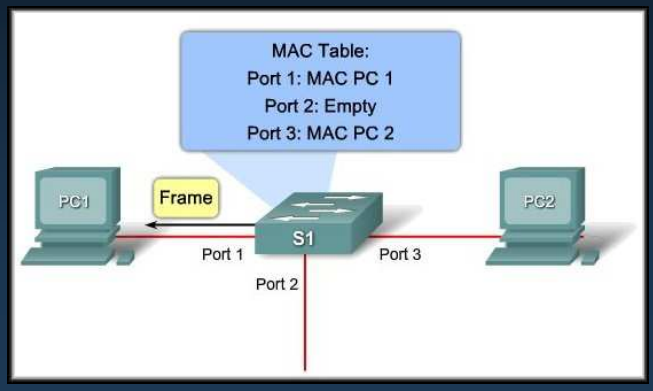
- **Example Step 5:**
  - The switch enters the source MAC address of PC 2 and the port number of the switch port that received the frame into the address table.

The destination address of the frame and its associated port is found in the MAC address table.



Switch MAC Address Table

- **Example Step 6:**
  - The switch can now forward frames between source and destination devices because it has entries in the address table that identify the associated ports.



Design Considerations – Ethernet/802.3

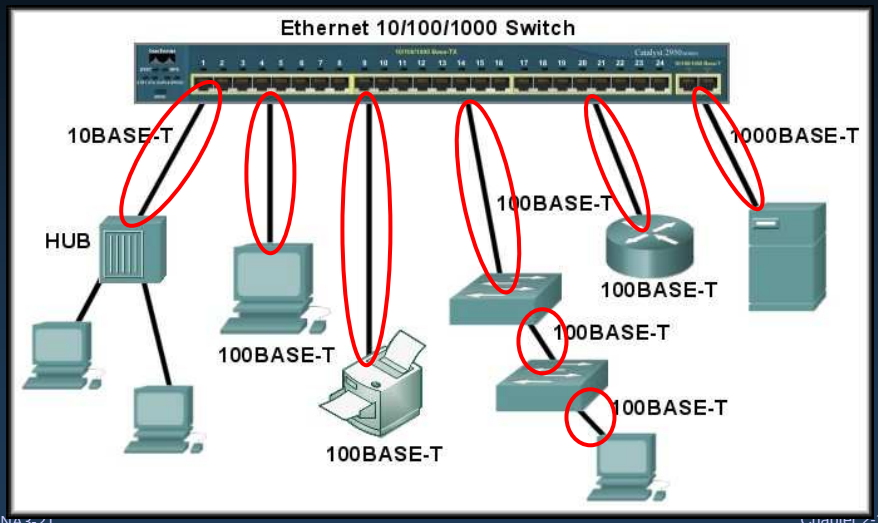
- **Bandwidth and Throughput:**
  - A **major disadvantage** of Ethernet is collisions.
    - When two hosts transmit frames simultaneously, the collision results in the transmitted frames being corrupted or destroyed.
    - The sending hosts stop sending based on the Ethernet 802.3 rules of CSMA/CD.
  - ***It is important to understand that when stating the bandwidth of the Ethernet network is 10 Mb/s, full bandwidth for transmission is available only after any collisions have been resolved.***

Design Considerations – Ethernet/802.3

- **Bandwidth and Throughput:**
  - A **major disadvantage** of Ethernet is collisions.
    - **A hub offers no mechanisms** to either eliminate or reduce collisions and the available bandwidth that any one node has to transmit is correspondingly reduced.
    - As a result, the **number of nodes** sharing the Ethernet network will have **effect on the throughput**.

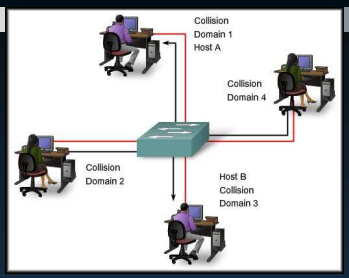
Design Considerations – Ethernet/802.3

- Collision Domains:



Design Considerations – Ethernet/802.3

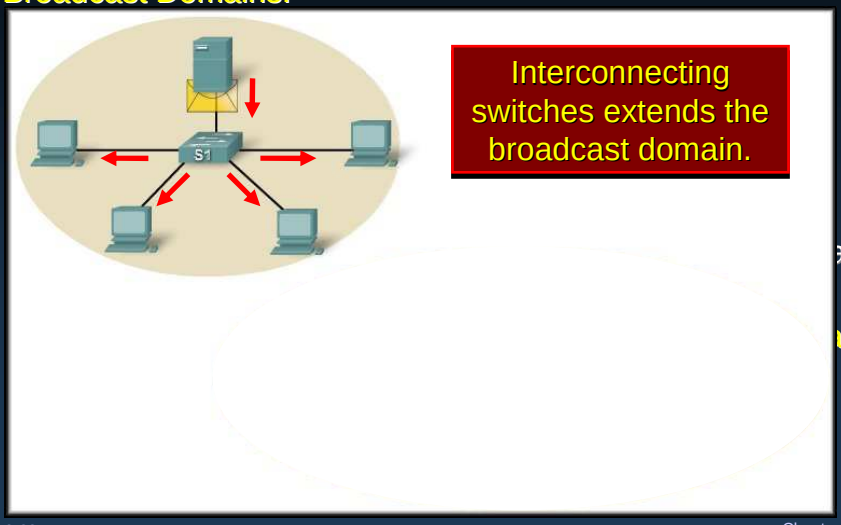
- Microsegment:
  - When two connected hosts want to communicate with each other, the switch uses the switching table to establish a connection between the ports.



  - The circuit is maintained until the session is terminated.
  - The microsegment behaves as if the network has only two hosts, providing maximum available bandwidth to both hosts.
  - *Switches reduce collisions and improve bandwidth use on network segments because they provide dedicated bandwidth to each network segment.*

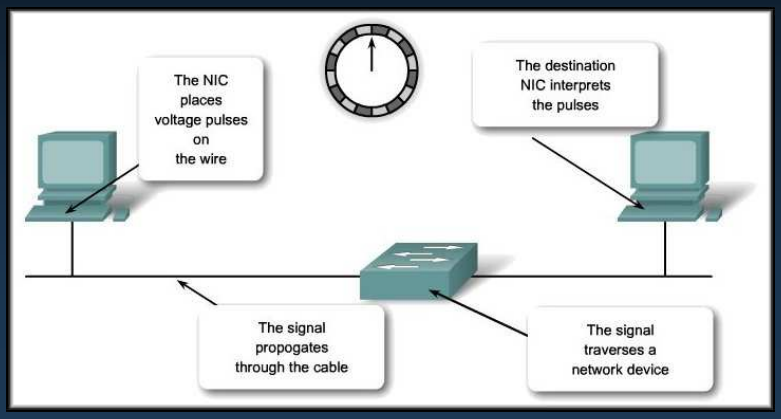
Design Considerations – Ethernet/802.3

- **Broadcast Domains:**



Design Considerations – Ethernet/802.3

- **Network Latency:**
  - Latency is the time a frame or a packet takes to travel from the source to the final destination.

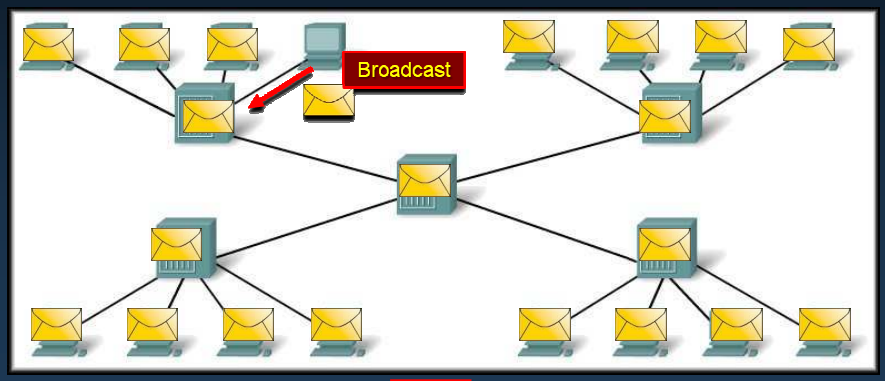


Design Considerations – Ethernet/802.3

- Network Congestion:
  - The primary reason for segmenting a LAN into smaller parts is to isolate traffic and to achieve better use of bandwidth per user.
  - Without segmentation, a LAN quickly becomes clogged with traffic and collisions.
  - Most common causes:
    - Increasingly powerful computer and network technologies.
    - Increasing volume of network traffic.
    - High-bandwidth applications.

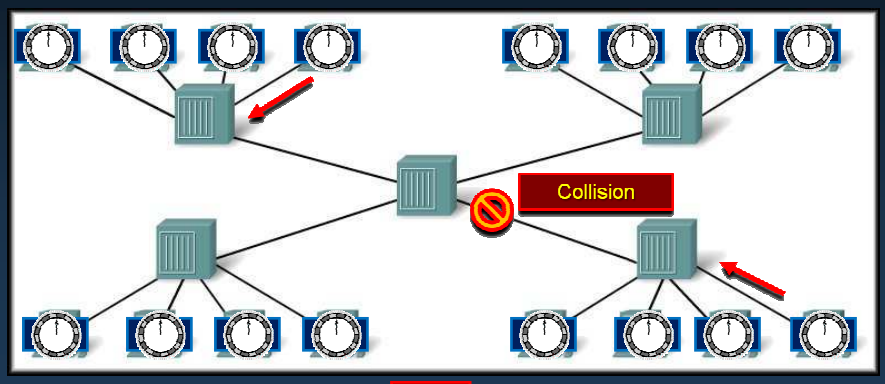
Design Considerations – Ethernet/802.3

- LAN Segmentation:
  - LANs are segmented into a number of smaller collision and broadcast domains using routers and switches.



Design Considerations – Ethernet/802.3

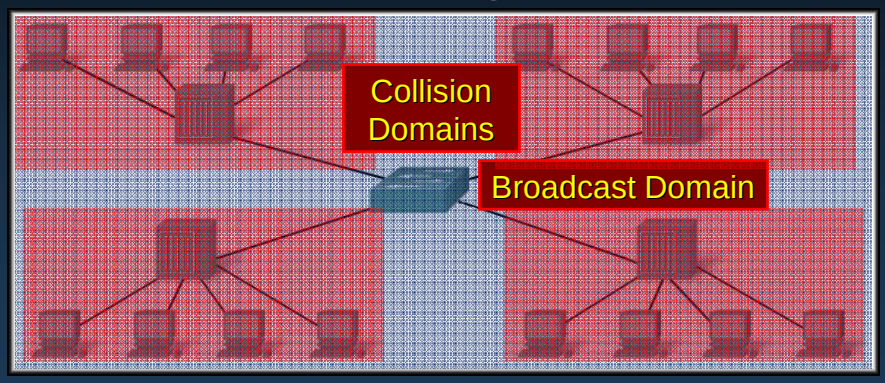
- LAN Segmentation:
  - LANs are segmented into a number of smaller collision and broadcast domains using routers and switches.



Hub

Design Considerations – Ethernet/802.3

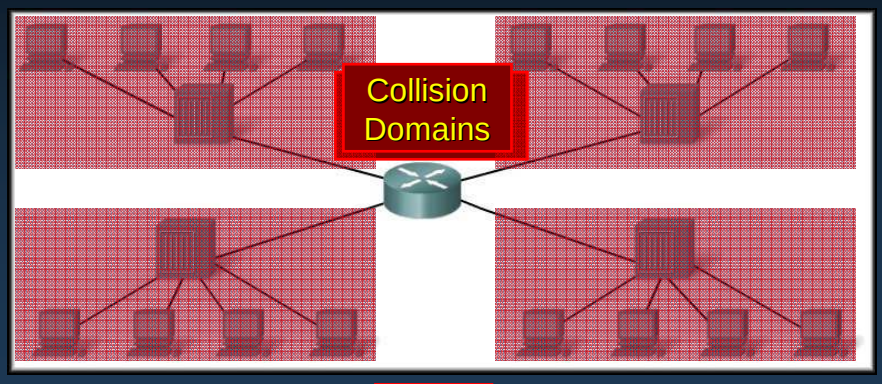
- LAN Segmentation:
  - LANs are segmented into a number of smaller collision and broadcast domains using routers and switches.



Switch

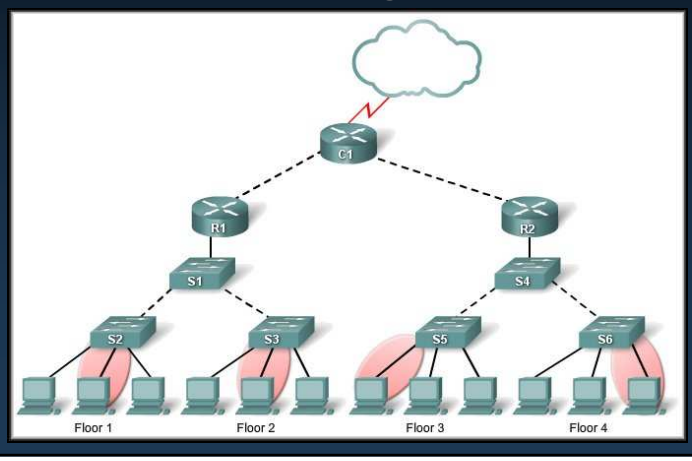
Design Considerations – Ethernet/802.3

- LAN Segmentation:
  - LANs are segmented into a number of smaller collision and broadcast domains using routers and switches.



Design Considerations – Ethernet/802.3

- LAN Segmentation:
  - LANs are segmented into a number of smaller collision and broadcast domains using routers and switches.



LAN Design Considerations

- There are two primary considerations when designing a LAN:
  - Controlling network latency
  - Removing bottlenecks

LAN Design Considerations

- Controlling Network Latency:
  - Consider the latency caused by each device on the network.

    - Switches at Layer 2 can introduce latency on a network when oversubscribed on a busy network.
      - If a core level switch has to support 48 ports, each one capable of running at 1000 Mb/s full duplex, the switch should support around 96 Gb/s internal throughput if it is to maintain full wire speed across all ports simultaneously.

LAN Design Considerations

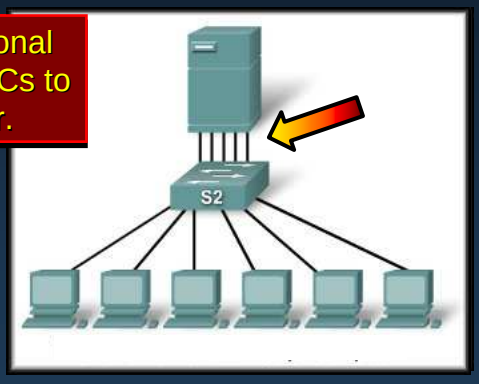
- **Controlling Network Latency:**
  - Consider the latency caused by each device on the network.

  - The use of higher layer devices can also increase latency on a network.
    - When a Layer 3 device, such as a router, needs to examine the Layer 3 addressing information contained within the frame, it must read further into the frame than a Layer 2 device, which creates a longer processing time.

LAN Design Considerations

- **Removing Network Bottlenecks:**
  - Each workstation and the server are connected at 1000Mbps.

Add 4 additional 1000Mbps NICs to the server.



Forwarding Frames Using a Switch

Store-and-forward

Cut-through

Fast-forward

Fragment-free

Layer 2 and Layer 3 Switching

Symmetric

Asymmetric

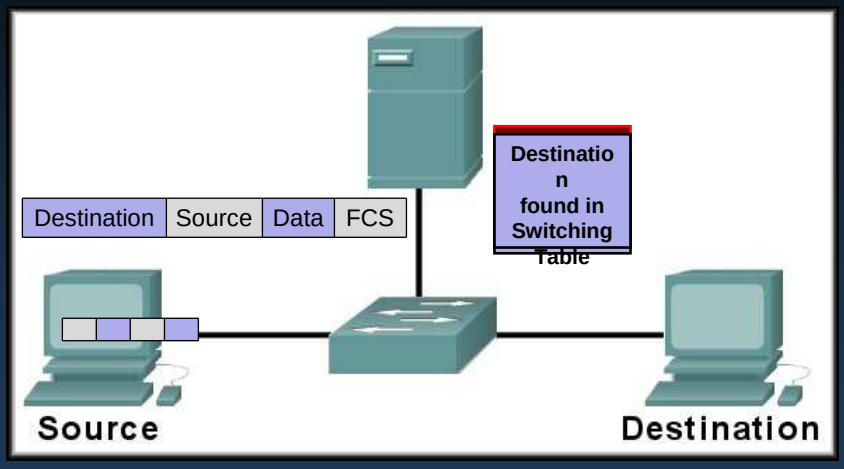
Memory Buffering

Switch Forwarding Methods

- Methods switches use to forward Ethernet frames.
  - Store-and-forward.
  - Cut-through:
    - Fast-forward switching.
    - Fragment-free switching.

Switch Forwarding Methods

- Store-and forward:



Switch Forwarding Methods

- Store-and forward:
  - Receives the entire frame.
  - Computes the CRC and checks the frame length.
  - If valid, checks the switch table for the destination address and forwards the frame.
  - If invalid, the frame is dropped.

  - *Store-and forward is the only method used on current Cisco Catalyst switches.*
    - Needed for QoS on converged networks.

Switch Forwarding Methods

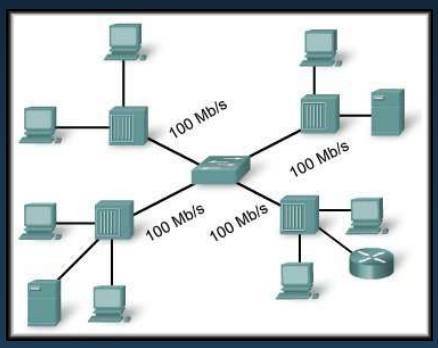
- Cut-through:
  - Forwards a frame before it is entirely received.
  - At a minimum, it must read the destination and source MAC addresses.
  - Faster than store-and-forward.
  - No error checking.
    - *Any corrupt frames are still forwarded and consume network bandwidth.*

Switch Forwarding Methods

- Cut-through – Fast-forward:
  - Typical method of cut-through.
  - Forwards a frame immediately after it reads and finds the destination address.
- Cut-through – Fragment-free:
  - Stores the first 64 bytes of the frame before forwarding.
    - The first 64 bytes of the frame is where most network errors and collisions occur.
    - Checks for a collision before forwarding the frame.
- Some switches are configured to use cut-through on each port until a user defined error threshold is reached. At that time, they change to store-and forward.

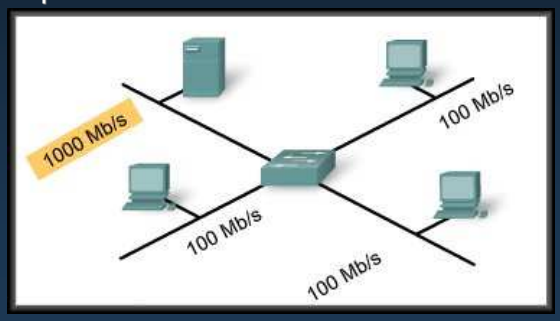
Symmetric and Asymmetric Switching

- Symmetric:
  - All ports are of the same bandwidth.
  - Optimized for a reasonably distributed traffic load.
  - For example, a peer-to-peer network.



Symmetric and Asymmetric Switching

- Asymmetric:
  - Provides switched connections between ports of unlike bandwidth.
  - For example, more bandwidth can be assigned to a server to prevent bottlenecks.



Memory Buffering

- A switch analyzes some or all of a packet before it forwards it to the destination host based on the forwarding method.
- It stores the packet for the brief time in a memory buffer.
- Built into the hardware
  - Two types:
    - Port based.
    - Shared.

Memory Buffering

- Port Based:
  - Frames are stored in queues that are linked to specific incoming and outgoing ports.
  - A frame is transmitted to the outgoing port only when all the frames ahead of it in the queue have been successfully transmitted.
  - It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port.

Memory Buffering

- **Shared:**
  - Deposits all frames into a common memory buffer that all the ports on the switch share.
  - The amount of buffer memory required by a port is dynamically allocated.
  - The frames in the buffer are linked dynamically to the destination port.
  - Allows the packet to be received on one port and then transmitted on another port, without moving it to a different queue.

Layer 2 and Layer 3 Switching

- **Layer 2 Switching:**
  - Performs switching and filtering based **only on the OSI Data Link layer** (Layer 2) MAC address.
  - Completely transparent to network protocols and user applications.
  - Remember that a Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.

Cisco Catalyst 2960 Series

Layer 2 and Layer 3 Switching

- **Layer 3 Switching:**
  - Functions similarly to a Layer 2 switch but instead of using only the Layer 2 MAC address a Layer 3 switch can also use IP address information.
  - A Layer 3 switch can also learn which IP addresses are associated with its interfaces.
  - This allows the Layer 3 switch to direct traffic throughout the network based on IP address information.

Cisco Catalyst 3560 Series

Layer 2 and Layer 3 Switching

- **Layer 3 Switching:**
  - ***However, Layer 3 switches do not completely replace the need for routers on a network.***
    - Routers perform additional Layer 3 services that Layer 3 switches are not capable of performing.

Feature	Layer 3 Switch	Router
Layer 3 Routing	Supported	Supported
Traffic Management	Supported	Supported
WIC Support		Supported
Advanced Routing Protocols		Supported
Wirespeed routing	Supported	

Switch Concepts and Configuration

Switch Management Configuration

Cisco IOS CLI Command Syntax	
Switch from user EXEC to privileged EXEC mode.	switch>**enable**
If a password has been set for privileged EXEC mode you will be prompted to enter it now.	Password:**password**
The # prompt signifies privileged EXEC mode.	switch#
Switch from privileged EXEC to user E	
The > prompt signifies user EXEC mo	

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	switch#**configure terminal**
The (config)# prompt signifies that the switch is in global configuration mode.	switch(config)#
Switch from global configuration mode to interface configuration mode for fast ethernet interface 0/1.	switch(config)#**interface fastethernet 0/1**
The (config-if)# prompt signifies that the switch is in the interface configuration mode.	switch(config-if)#
Switch from interface configuration mode to global configuration mode.	switch(config-if)#**exit**
The (config)# prompt signifies that the switch is in global configuration mode.	switch(config)#
Switch from global configuration mode to privileged EXEC mode.	switch(config)#**exit**
The # prompt signifies that the switch is in privileged EXEC mode.	switch#

Navigating Command-Line Interface Modes

- CLI itself is basically the same as a router:
  - Access modes with a password.
  - Help Facility and Command History
  - Configure console and telnet access.
  - Commands to configure options for each interface.
  - Commands to verify the status of the switch.
- The difference is the functions to be configured:
  - Commands to create and control VLANs (Chapter 3)
  - Configure a default gateway.
  - Manage the MAC Address table.
  - Switch security.

Navigating Command-Line Interface Modes

- Access Levels:
  - User EXEC.
  - Privileged EXEC.

Cisco IOS CLI Command Syntax	
Switch from user EXEC to privileged EXEC mode.	`switch>enable`
If a password has been set for privileged EXEC mode you will be prompted to enter it now.	`Password:password`
The # prompt signifies privileged EXEC mode.	`switch#`
Switch from privileged EXEC to user EXEC mode.	`switch#disable`
The > prompt signifies user EXEC mode.	`switch>`

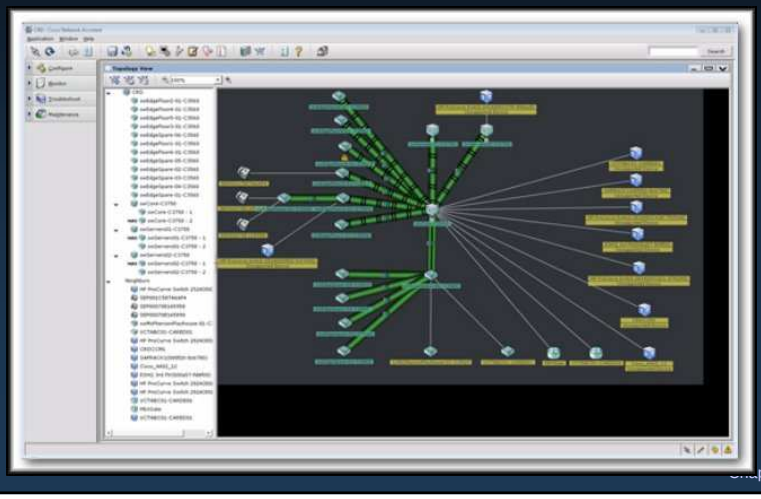
Navigating Command-Line Interface Modes

- Configuration Modes:
  - Global Configuration Mode.
  - Interface Configuration Mode (and more….)

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`switch#configure terminal`
The (config)# prompt signifies that the switch is in global configuration mode.	`switch(config)#`
Switch from global configuration mode to interface configuration mode for fast ethernet interface 0/1.	`switch(config)#interface fastethernet 0/1`
The (config-if)# prompt signifies that the switch is in the interface configuration mode.	`switch(config-if)#`
Switch from interface configuration mode to global configuration mode.	`switch(config-if)#exit`
The (config)# prompt signifies that the switch is in global configuration mode.	`switch(config)#`
Switch from global configuration mode to privileged EXEC mode.	`switch(config)#exit`
The # prompt signifies that the switch is in privileged EXEC mode.	`switch#`

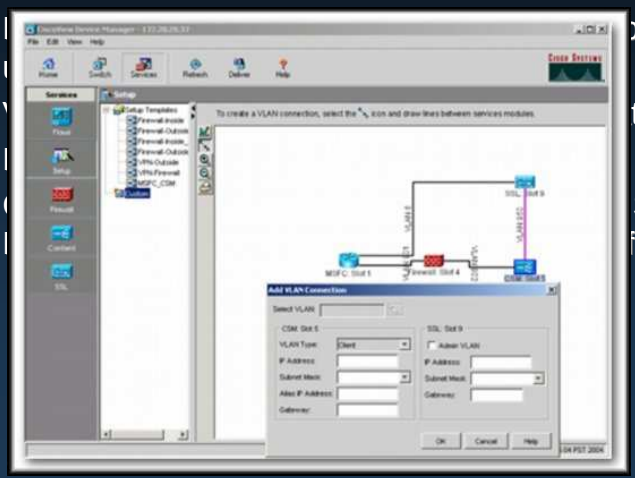
Navigating Command-Line Interface Modes

- GUI-Based Alternatives to the CLI:
  - Cisco Network Assistant.



Navigating Command-Line Interface Modes

- GUI-Based Alternatives to the CLI:
  - Cisco View.
    - ou can
    - tion.
    - Simple
    - form.

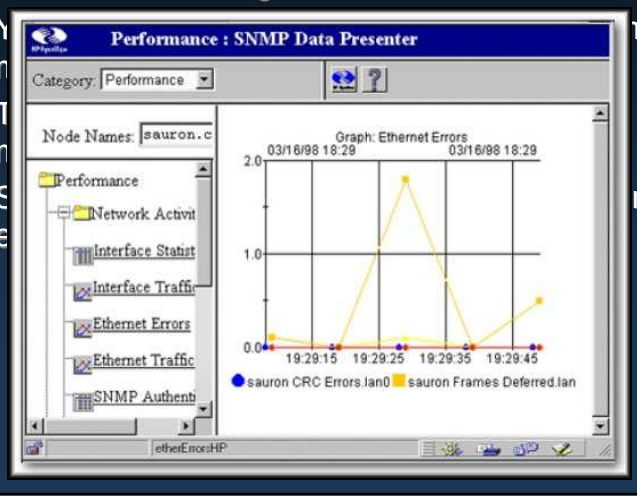


Navigating Command-Line Interface Modes

- GUI-Based Alternatives to the CLI:
  - Cisco Device Manager.
    - Web e switch mem
    - Conf
    - Acce through a web brow

Navigating Command-Line Interface Modes

- GUI-Based Alternatives to the CLI:
  - SNMP Network Management.
    - Y patible n
    - T n
    - S n in large e



Using the Help Facility

- Word / Command line syntax Help:

Cisco Switch Command Syntax	

Example of command prompting. In this example, the help function provides a list of commands available in the current mode that start with cl.	`switch#cl?`
	
	`clear  clock`

Example of incomplete command.	`switch#clock`
	
	`% Incomplete command.`

Example of symbolic translation.	`switch#colck`
	
	`% Unknown command or computer name, or unable to find computer address`

Example of command prompting. Notice the space? In this example, the help function provides a list of subcommands associated with the clock command.	`switch#clock ?`
	
	`set  Set the time and date`

In this example, the help function provides a list of command arguments required with the clock set command.	`switch#clock set ?`
	
	`hh:mm:ss  Current Time`

Using the Help Facility

- Console Error Messages:

Example Error Message	Meaning	How to Get Help
`switch#cl` `% Ambiguous command: "cl"`	You did not enter enough characters for your device to recognize the command.	Re-enter the command followed by a question mark (?), without a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`switch#clock` `% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?), with a space between the command and the question mark.

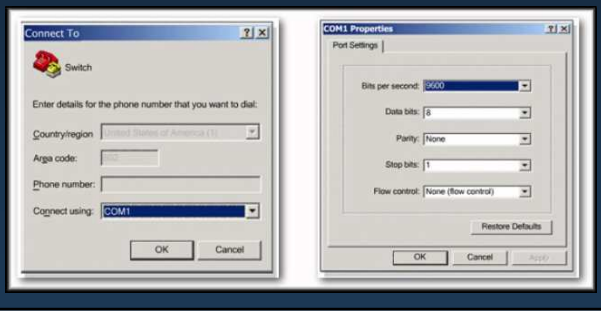
`switch#clock set aa:12:23`
`^`
`% Invalid input detected at '^' marker.`
	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands or parameters that are available.

Switch Boot Sequence

- Switch loads the Boot Loader program.
  - Small program stored in NVRAM.
    - CPU Initialization.
    - POST.
    - Initializes flash memory.
    - Loads a default OS image into memory and boots the switch.
  - The OS then initializes the interfaces using the Cisco IOS commands found in the operating system configuration file config.text, stored in the switch flash memory.

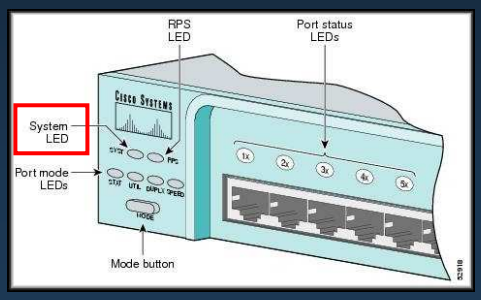
Prepare to Configure the Switch

- A PC connected to the console port.
- A terminal emulator application (e.g.. HyperTerminal) is running and configured correctly.
- Attach the power cord to the switch.
  - Some Catalyst switches, including the 2950 and 2960 series switches do not have a power button.



Prepare to Configure the Switch

- Observe the Boot Sequence.
  - When the switch is powered on, the POST begins.
  - During POST, the LEDs blink while a series of tests determine that the switch is functioning properly.
    - Successful: the SYST LED rapidly blinks green.
    - Fails: the SYST LED turns amber.



Prepare to Configure the Switch

- Obs
  -
  -

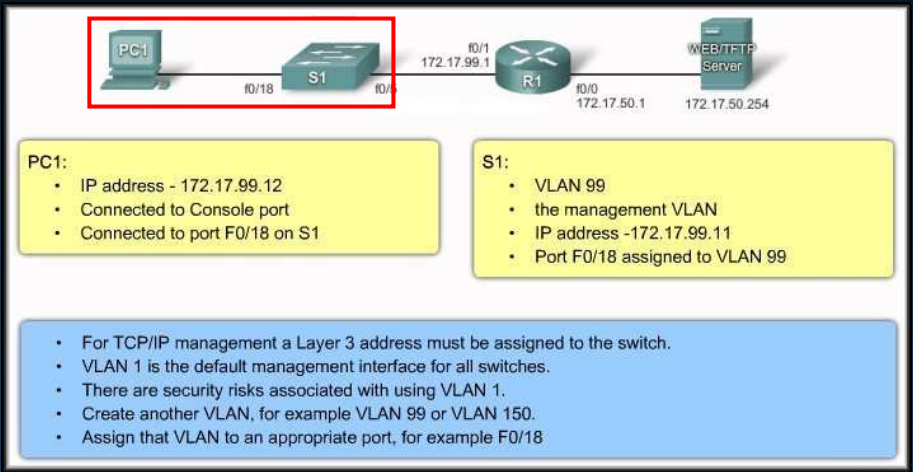
```
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34
flashfs[1]: 602 files, 19 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 32514048
flashfs[1]: Bytes used: 7715328
flashfs[1]: Bytes available: 24798720
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....done Initializing
flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status
```

Basic Switch Configuration

- Key Configuration Sequences:
  - Switch Management Interface:
    - To manage a switch remotely using TCP/IP, you need to assign the switch an IP address.
    - An access layer switch is much like a PC in that you need to configure an IP address, a subnet mask, and a default gateway.
  - Duplex and Speed of active interfaces:
    - Usually the default but can be modified.
  - Support for HTTP access.
    - We will restrict ourselves to the CLI.
  - MAC address table management.

Basic Switch Configuration

- Switch Management Interface:



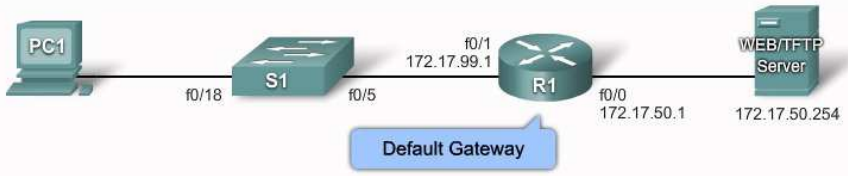
Basic Switch Configuration

- **Switch Management Interface:**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Enter the interface configuration mode for the VLAN 99 interface.	`S1(config)#interface vlan 99`
Configure the interface IP address.	`S1(config-if)#ip address 172.17.99.11 255.255.255.0`
Enable the interface.	`S1(config-if)#no shutdown`
Return to privileged EXEC mode.	`S1(config-if)#end`
Enter global configuration mode.	`S1#configure terminal`
Enter the interface to assign the VLAN.	`S1(config)#interface fastethernet 0/18`
Define the VLAN membership mode for the port.	`S1(config-if)#switchport mode access`
Assign the port to a VLAN.	`S1(config-if)#switchport acces vlan 99`
Return to privileged EXEC mode.	`S1(config-if)#end`
Save the running configuration to the switch start-up configuration.	`S1#copy running-config startup-config`

Basic Switch Configuration

- **Configure Default Gateway:**



Cisco IOS CLI Command Syntax	
Configures the default gateway on the switch.	`S1(config)#ip default-gateway 172.17.99.1`
Return to privileged EXEC mode.	`S1(config)#end`
Save the running configuration to the switch start-up configuration.	`S1#copy running-config startup-config`

from another subnet to perform maintenance or troubleshoot.

Basic Switch Configuration

- Verify Configuration:

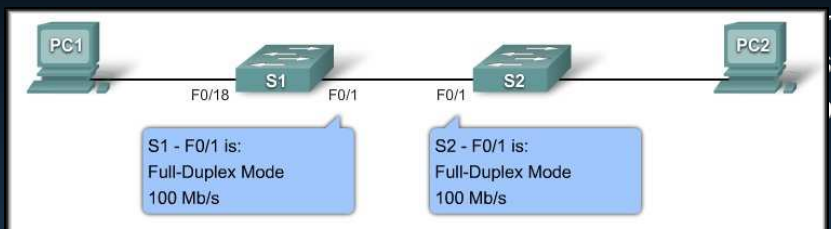
```
S1#show running-config
<output omitted>
!
```

```
S1#show ip interface brief
interface              IP-address      OK?  Method  Status  Protocol
Vlan99                 172.17.99.11    Yes  manual  up      down
<output omitted>
FastEthernet 0/18      unassigned      Yes  unset   down    down
FastEthernet 0/19      unassigned      Yes  unset   down    down
<output omitted>
S1#
```

```
!
ip default-gateway 172.17.99.1
!
<output omitted>
!
```


Basic Switch Configuration

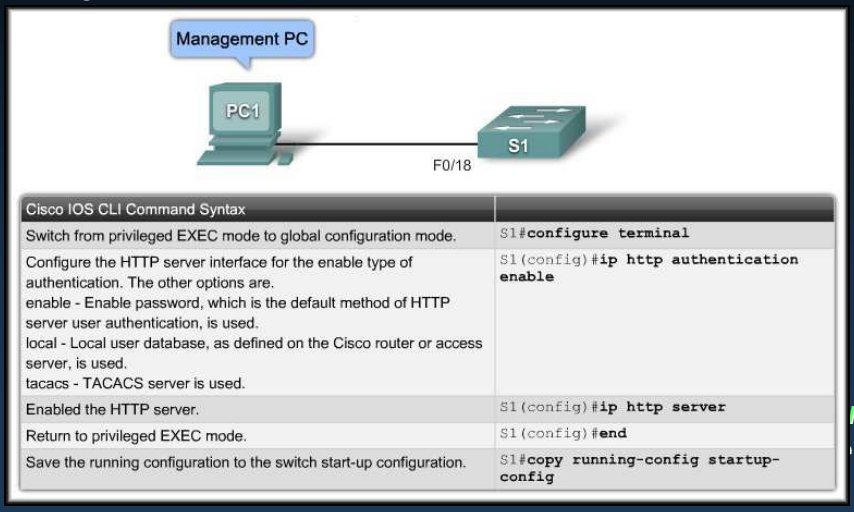
- Configure Duplex and Speed:



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Enter the interface configuration mode.	S1(config)#**Interface fastethernet 0/1**
Configure the interface duplex mode to enable AUTO duplex configuration.	S1(config-if)#**duplex auto**
Configure the interface duplex speed and enable AUTO speed configuration.	S1(config-if)#**speed auto**
Return to privileged EXEC mode.	S1(config-if)#**end**
Save the running configuration to the switch start-up configuration.	S1#**copy running-config startup-config**

Basic Switch Configuration

- Configure HTTP Access:



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configure the HTTP server interface for the enable type of authentication. The other options are. enable - Enable password, which is the default method of HTTP server user authentication, is used. local - Local user database, as defined on the Cisco router or access server, is used. tacacs - TACACS server is used.	S1(config)#**ip http authentication enable**
Enabled the HTTP server.	S1(config)#**ip http server**
Return to privileged EXEC mode.	S1(config)#**end**
Save the running configuration to the switch start-up configuration.	S1#**copy running-config startup-config**

Basic Switch Configuration

- MAC A
  - Sw
  - The

v to

esses.

```
Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c20000d      STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    000c.7671.7534    DYNAMIC     Fa0/2
   1    0013.e809.7695    DYNAMIC     Fa0/2
   1    0017.9a51.d339    DYNAMIC     Fa0/2
   1    0019.5b0a.a951    DYNAMIC     Fa0/2
   1    0060.b0af.7be4    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 25
```

Basic Switch Configuration

- Dynamic MAC Addresses:
  - The switch provides dynamic addressing by learning the source MAC address of each frame that it receives on each port.
  - It then adds the source MAC address and its associated port number to the MAC address table.
  - As devices are added or removed from the network, the switch updates the MAC address table.
    - It adds new entries and ages out those that are currently not in use.

Basic Switch Configuration

- Static MAC Addresses:
  - A network administrator can specifically assign static MAC addresses to certain ports.
  - Static addresses are not aged out.
  - The switch always knows which port to send out traffic destined for that specific MAC address.
  - To create a static mapping in the MAC address table, use the command:
    mac-address-table static <MAC address>
    vlan {1-4096, ALL}
    interface interface-id
  - To remove it, use the 'no' form of the command.

Verifying Switch Configuration

- Using the show commands:

Cisco IOS CLI Command Syntax	
Displays interface status and configuration for a single or all interfaces available on the switch.	`show interfaces [interface-id]`
Displays contents of startup configuration.	`show startup-config`
Displays current operating configuration.	`show running-config`
Displays information about flash: file system.	`show flash:`
Displays system hardware and software status.	`show version`
Display the session command history.	`show history`
Displays IP information. The interface option displays IP interface status and configuration. The http option displays HTTP information about device manager running on the switch. The arp option displays the IP ARP table.	`show ip {interface | http | arp}`
Displays the MAC forwarding table.	`show mac-address-table`

Basic Switch Management

- Backing up and Restoring Switch Configuration Files:
  - Backup to the flash drive.

Cisco IOS CLI Command Syntax	
Formal version of Cisco IOS copy command. Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy system:running-config flash:startup-config` `Destination filename [startup-config]?`
Informal version of the copy command. The assumptions are that the running-config is running on the system and that the startup-config file that will be stored in flash NVRAM. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy running-config startup-config` `Destination filename [startup-config]?`
Backup the startup-config to a file stored in flash NVRAM. Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy startup-config flash:config.bak1` `Destination filename [config.bak1]?`

Basic Switch Management

- **Backing up and Restoring Switch Configuration Files:**
  - Restore from the flash drive.

Cisco IOS CLI Command Syntax	
Copy the config.bak1 file stored in flash to the startup-configuration assumed to be stored in flash. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	S1#**copy flash:config.bak1 startup-config** Destination filename [startup-config]?
Have the Cisco IOS perform restart the switch. If you have modified the running configuration file you are asked to save it. Confirm with a 'y' or an 'n'. To confirm the reload press the Enter key to accept and use the Ctrl+C key combination to cancel.	S1#**reload** System configuration has been modified. Save? [yes/no]: n Proceed with reload? [confirm]?

Basic Switch Management

- **Backing up and Restoring Switch Configuration Files:**
  - Backup to a TFTP server.
    - Make sure that the TFTP server is running.
    - Login to the switch.
    - Upload the configuration to the TFTP server.

S1#copy system:running-config tftp://172.16.2.155/S1Rconfig.txt

or….S1#copy run tftp

Basic Switch Management

- **Backing up and Restoring Switch Configuration Files:**
  - Restore from a TFTP server.
    - Make sure that the TFTP server is running.
    - Login to the switch.
    - download the configuration to the TFTP server.

S1#copy tftp://172.16.2.155/S1Rconfig.txt **system:running-config**
S1#copy running-config startup-config
S1#reload

or….S1#copy tftp run
S1#copy run start
S1#reload

Basic Switch Management

- **Backing up and Restoring Switch Configuration Files:**
  - Clearing configuration files.

```
S1#erase nvram:
Erasing the nvram filesystem will remove all configuration
files!
Continue? [confirm]
[OK]
Erase of nvram: complete
S1#
```

  - Deleting files from the flash drive.
    - **delete** flash:filename