Configure a Switch

LAN Switching and Wireless – Chapter 2

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

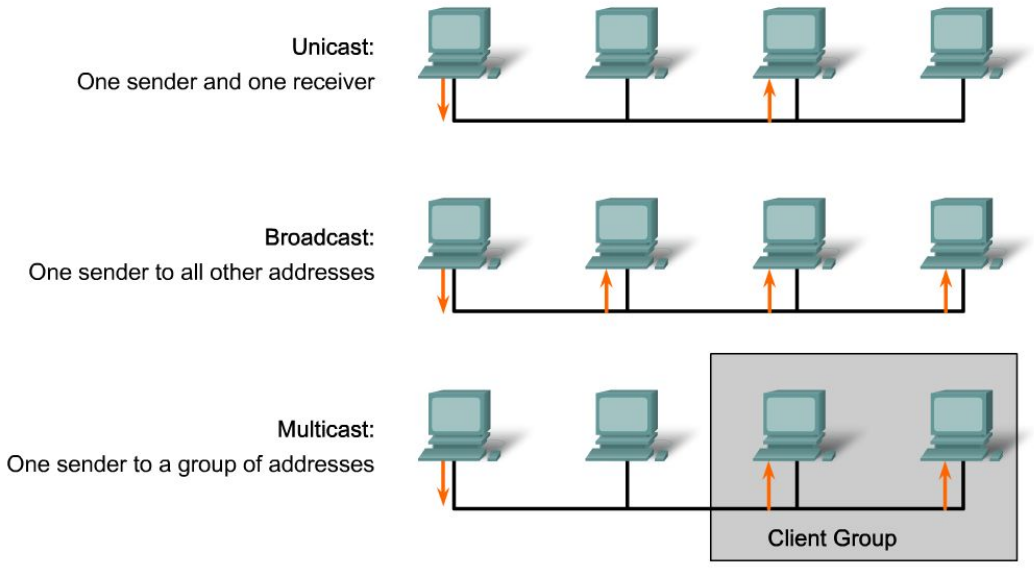
Objectives

- Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard.
- Explain the functions that enable a switch to forward Ethernet frames in a LAN.
- Configure a switch for operation in a network designed to support voice, video, and data transmissions.
- Configure basic security on a switch that will operate in a network designed to support voice, video, and data transmissions.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

- Describe the key elements of Ethernet/802.3 networks



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

MAC Address

Broadcast	Local	OUI Number	"Vendor Number"
"OUI"			Vendor Assignment

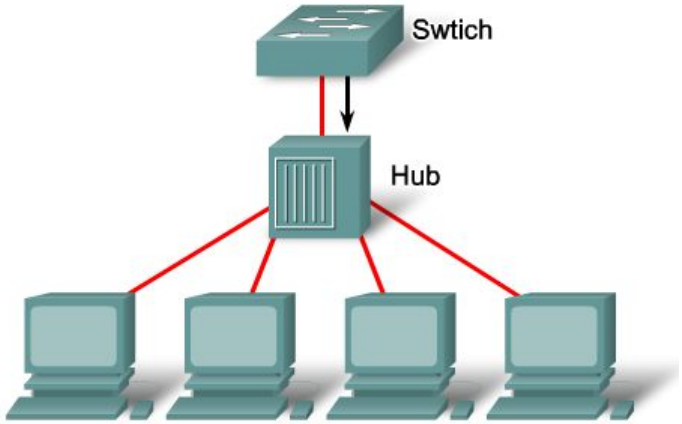
© 2006 Cisc

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

Duplex Settings

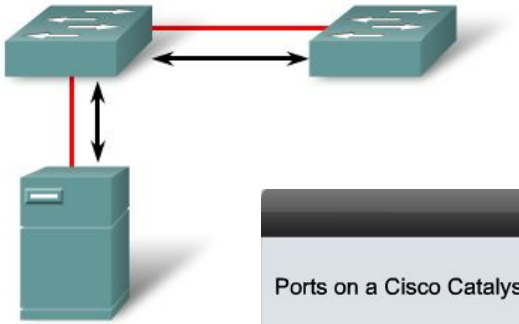
Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity



Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled



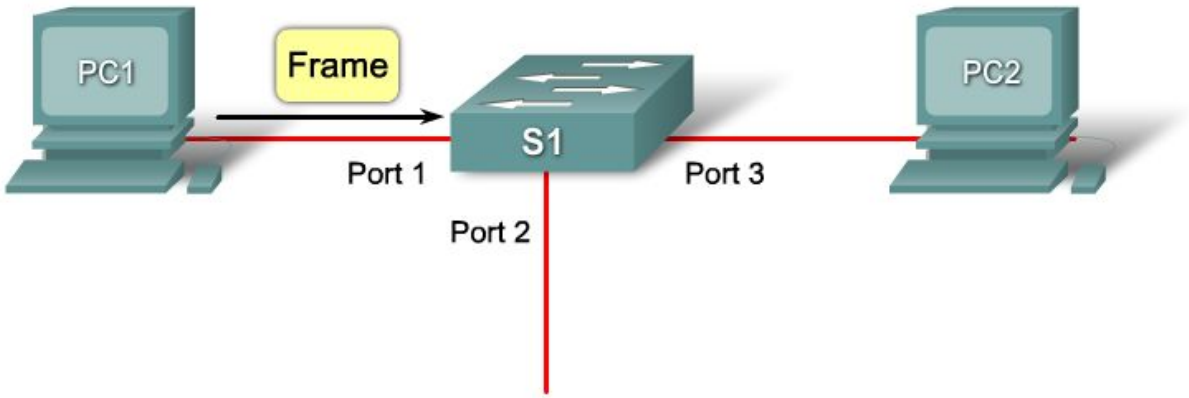
Ports on a Cisco Catalyst 2960 Series switch can be configured with these settings:

- `auto` option allows the two ports to communicate in order to decide the mode.
- `full` option sets full-duplex mode.
- `half` option sets half-duplex mode.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables

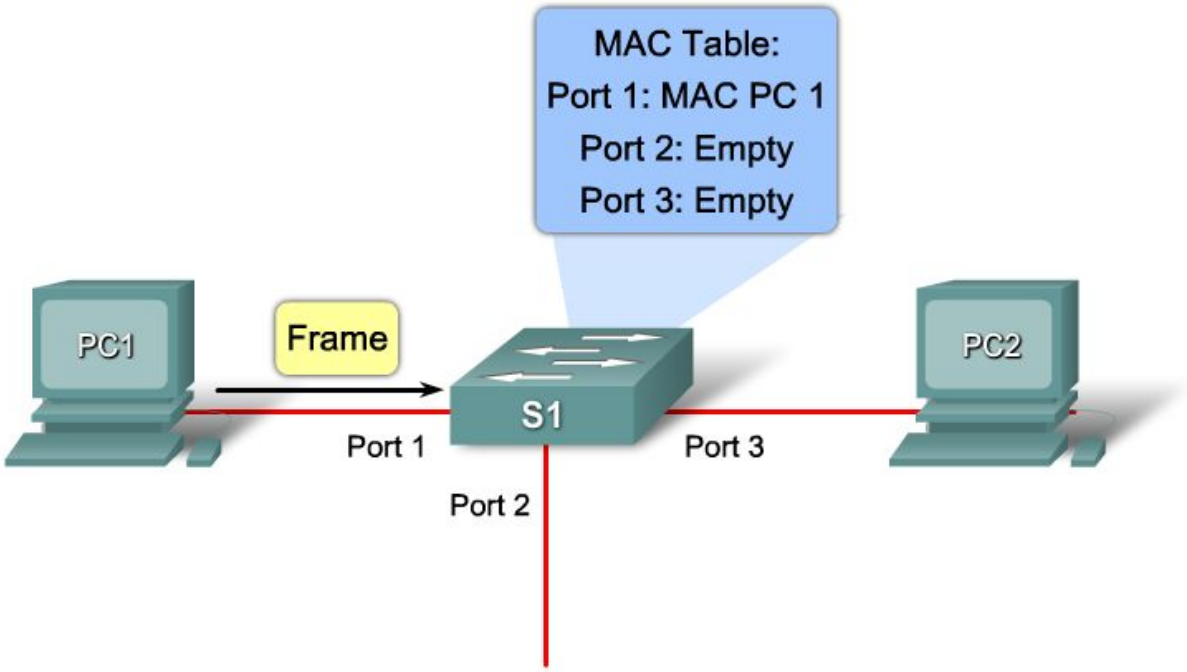


Step 1: The switch receives a frame destined for PC2 on Port 1 from PC1.

1 2 3 4 5 6

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables



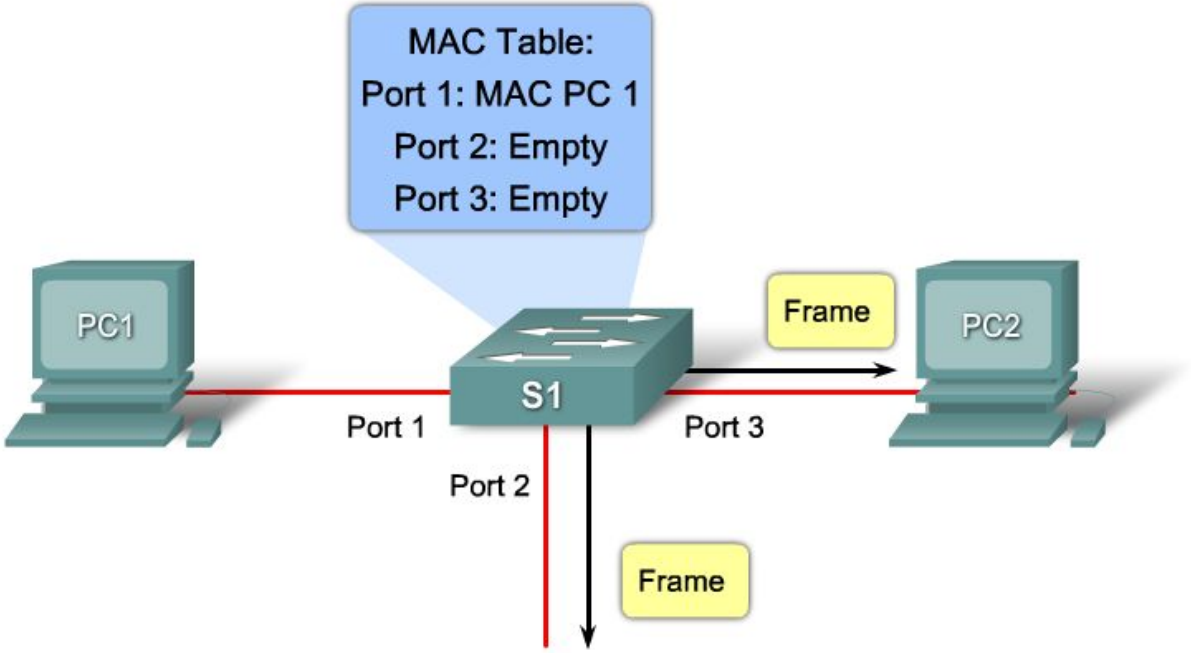
Step 2: The switch enters the source MAC address and the switch port that received the frame into the MAC table.

1 2 3 4 5 6

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables



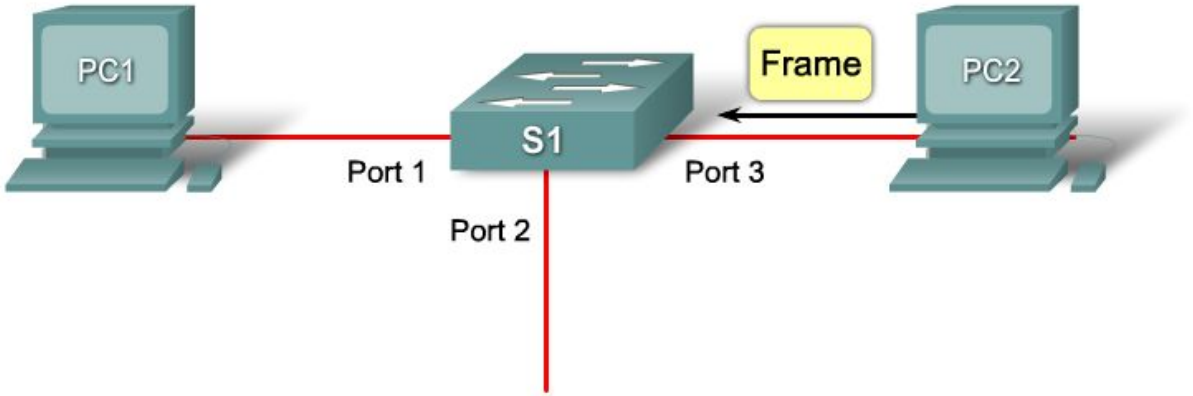
Step 3: Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.

1 2 3 4 5 6

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables



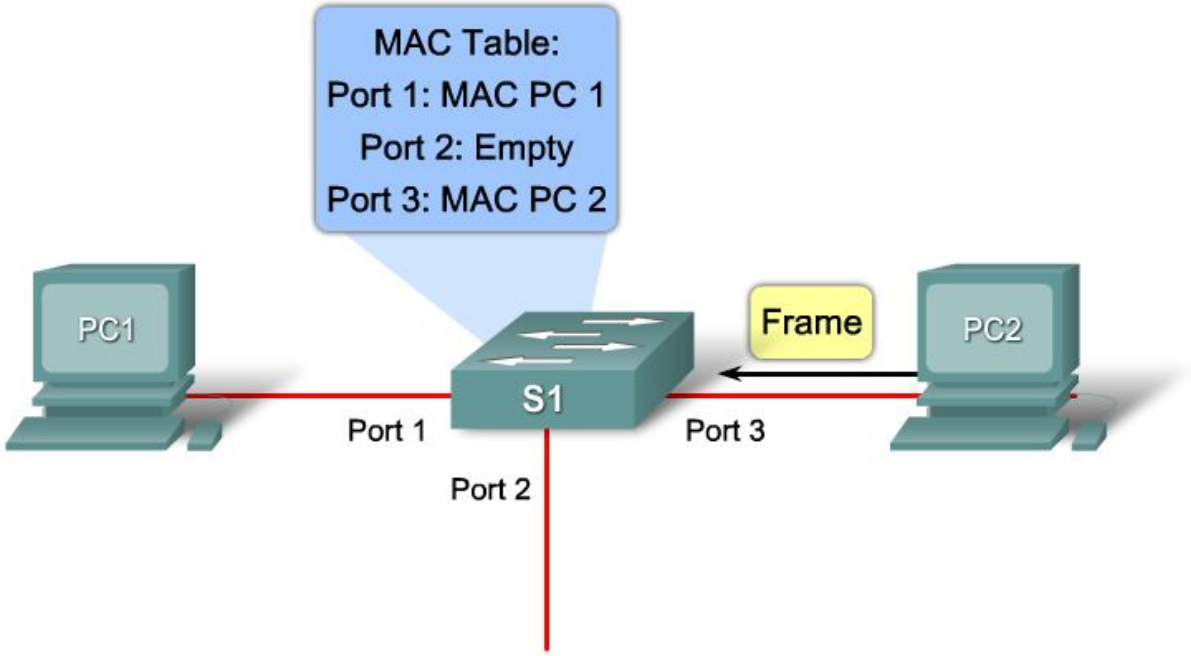
Step 4: The destination device replies to the broadcast with a unicast frame addressed to PC 1.

1 2 3 4 5 6

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables



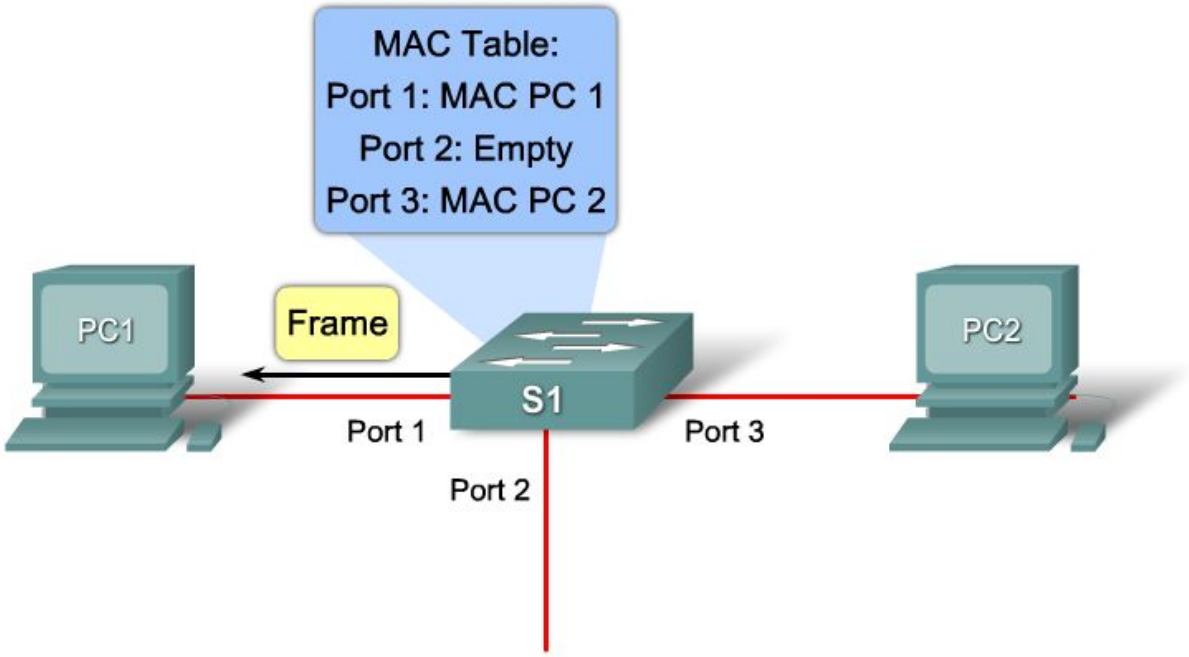
Step 5: The switch enters the source MAC address of PC 2 and port number of the switch port that received the frame into the MAC table. The destination address of the frame and its associated port is found in the MAC table.

1 2 3 4 5 6

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

MAC Addressing and Switch MAC Tables

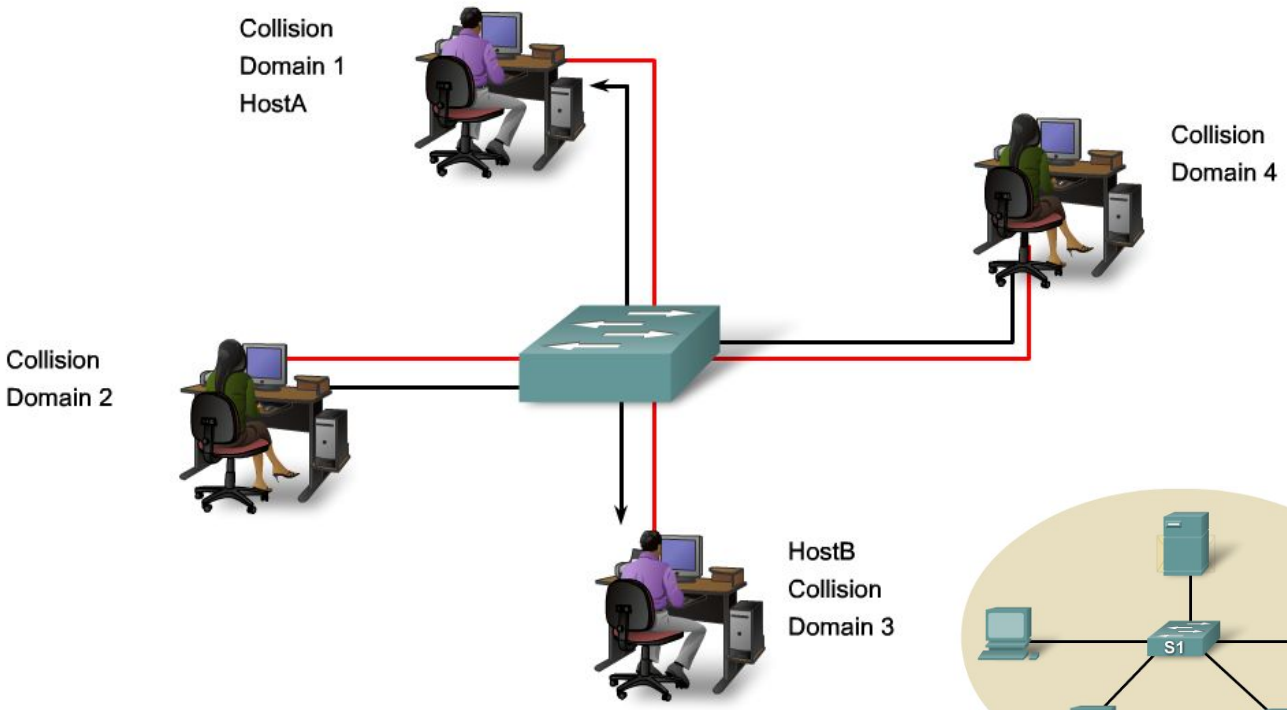


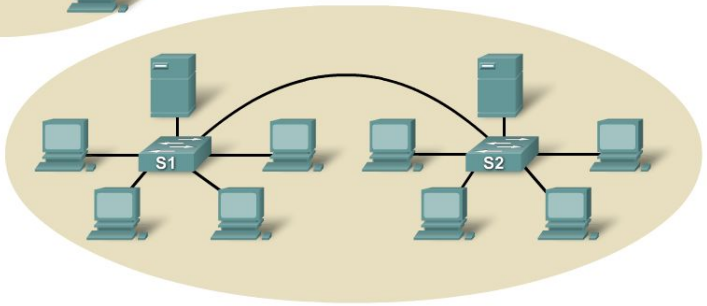
Step 6: The switch can now forward frames between source and destination devices without flooding, because it has entries in the MAC table that identify the associated ports.

1 2 3 4 5 6

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



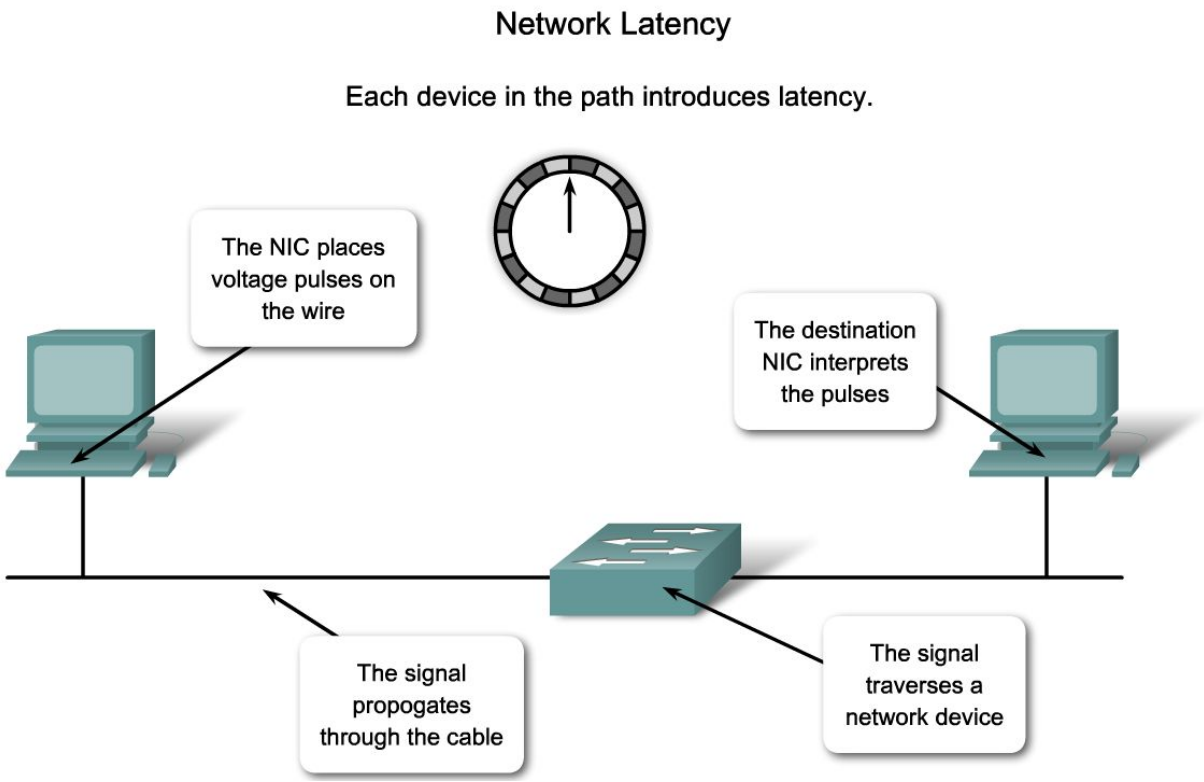


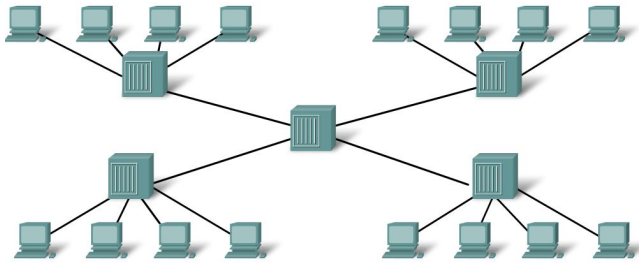
Bandwidth and Throughput
Collision Domains
Broadcast Domains

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

- Describe the design considerations for Ethernet/802.3 networks

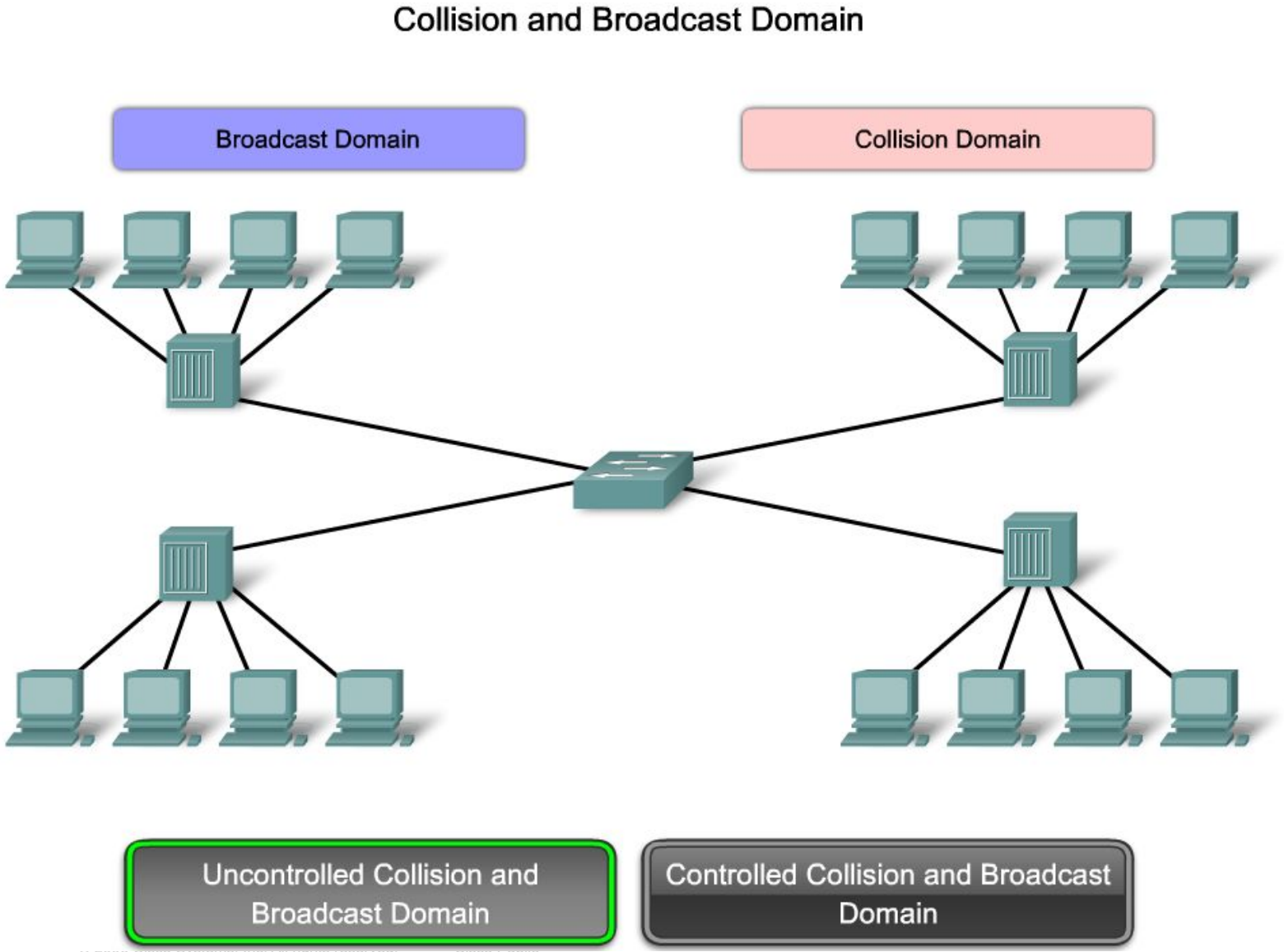




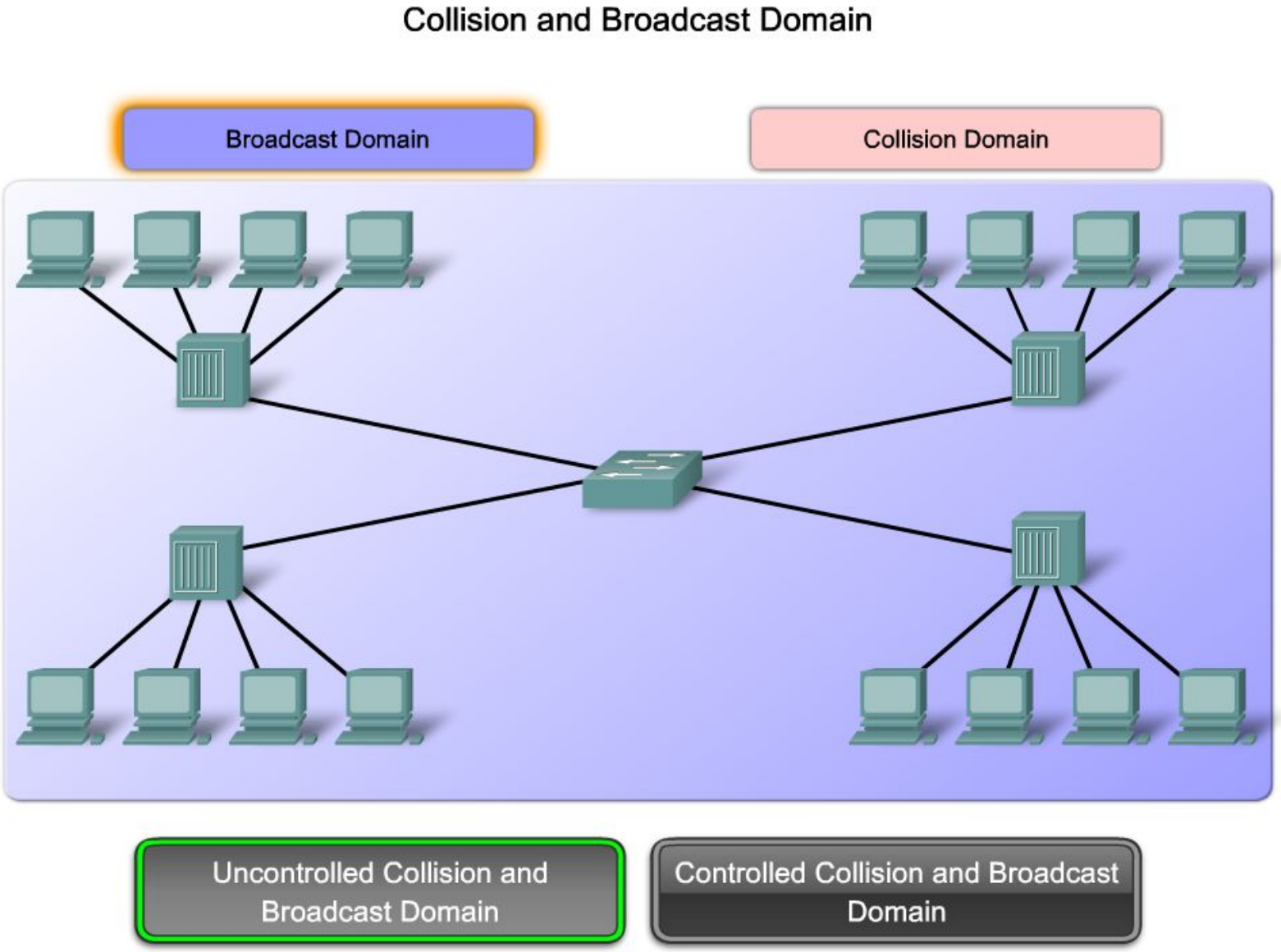
Network Latency
Network Congestion

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

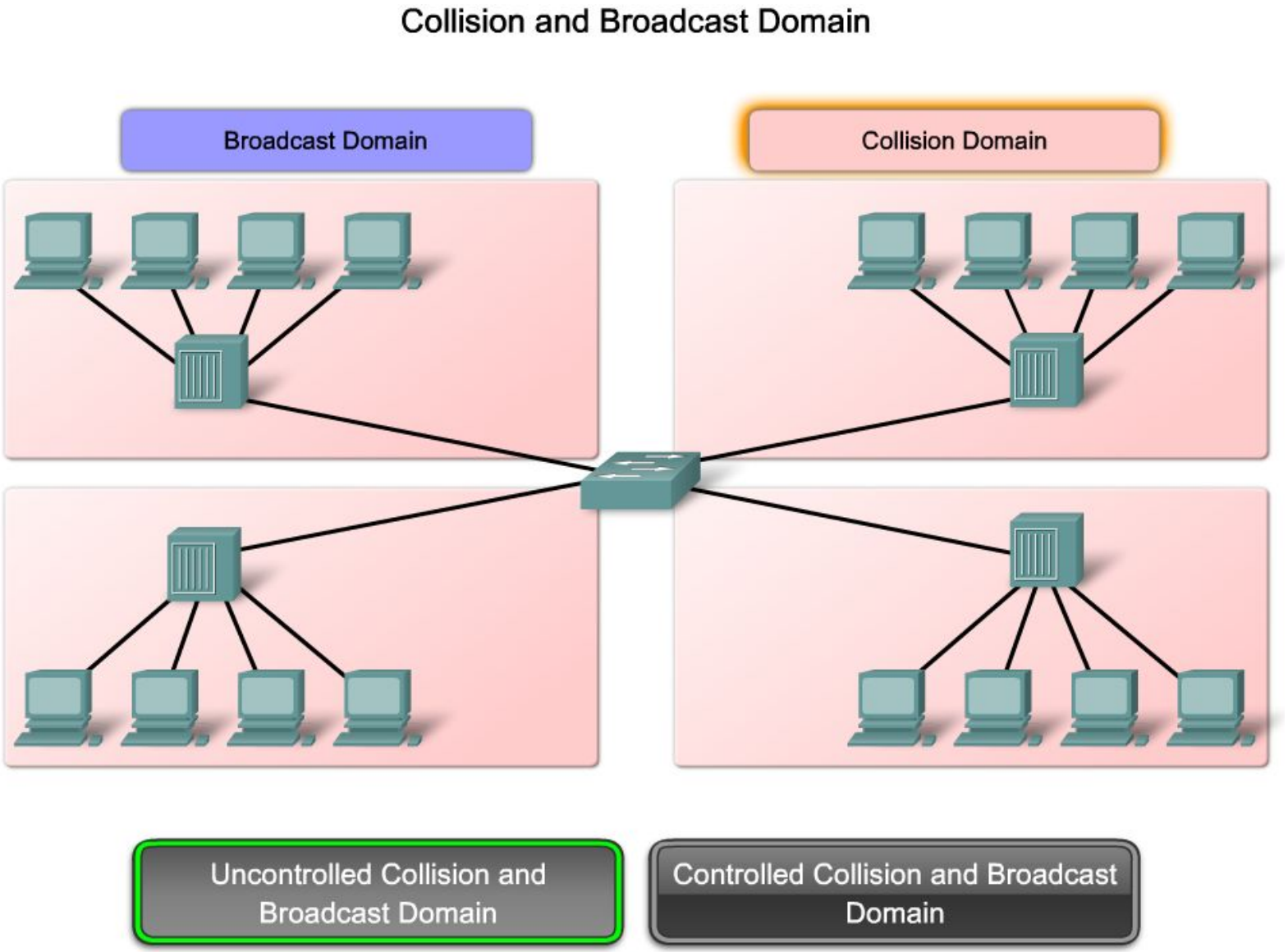
Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



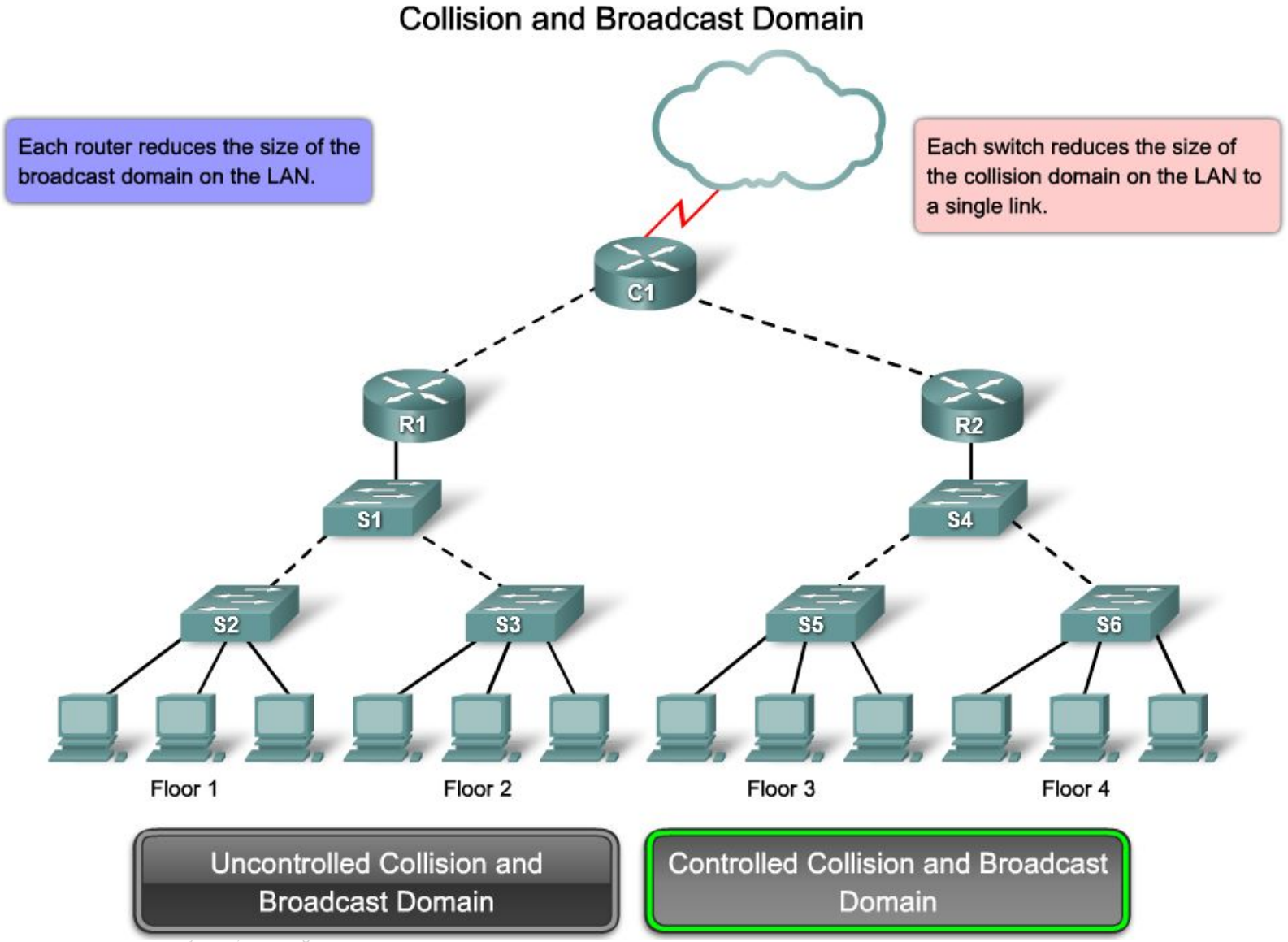
Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



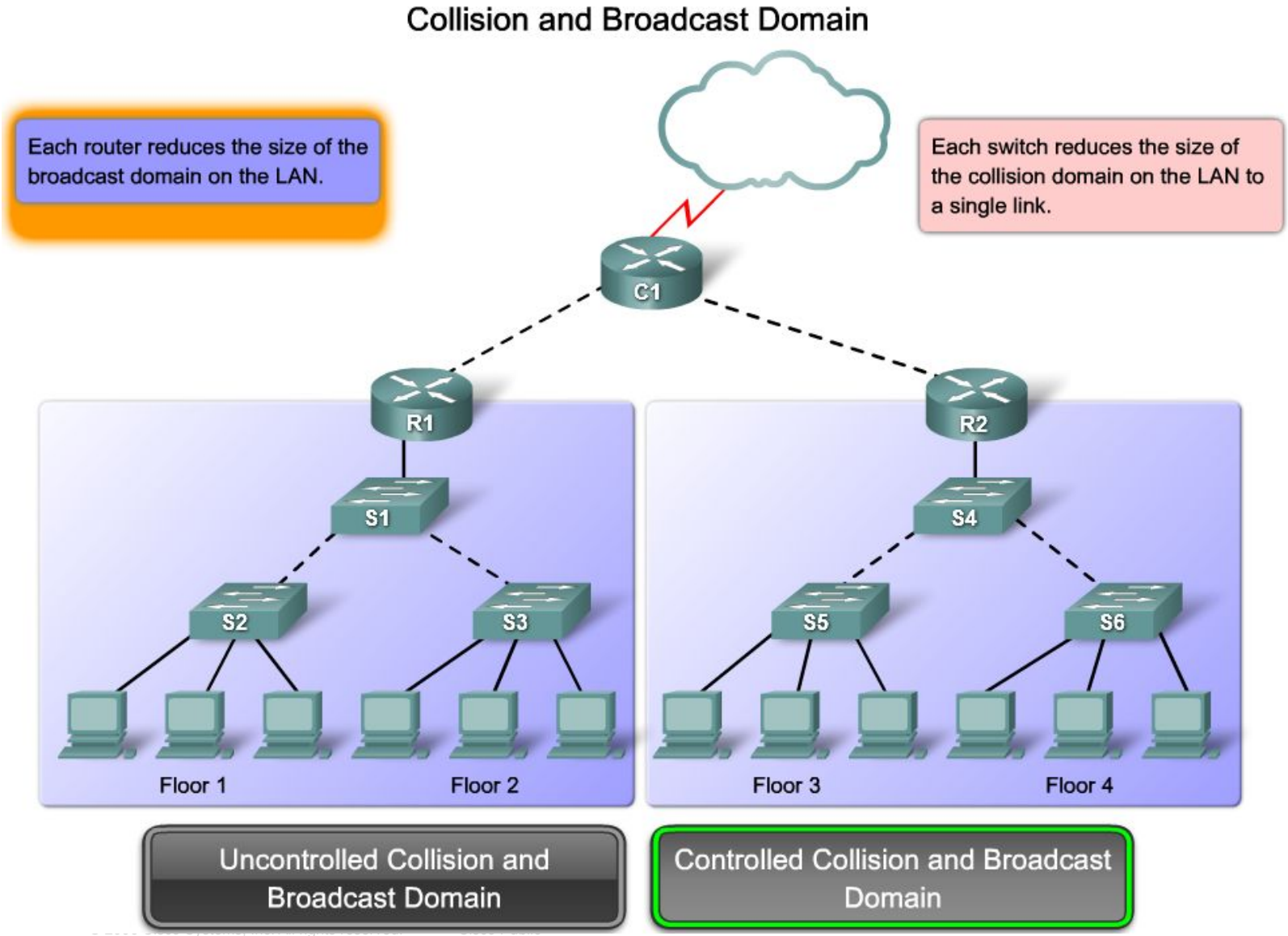
Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



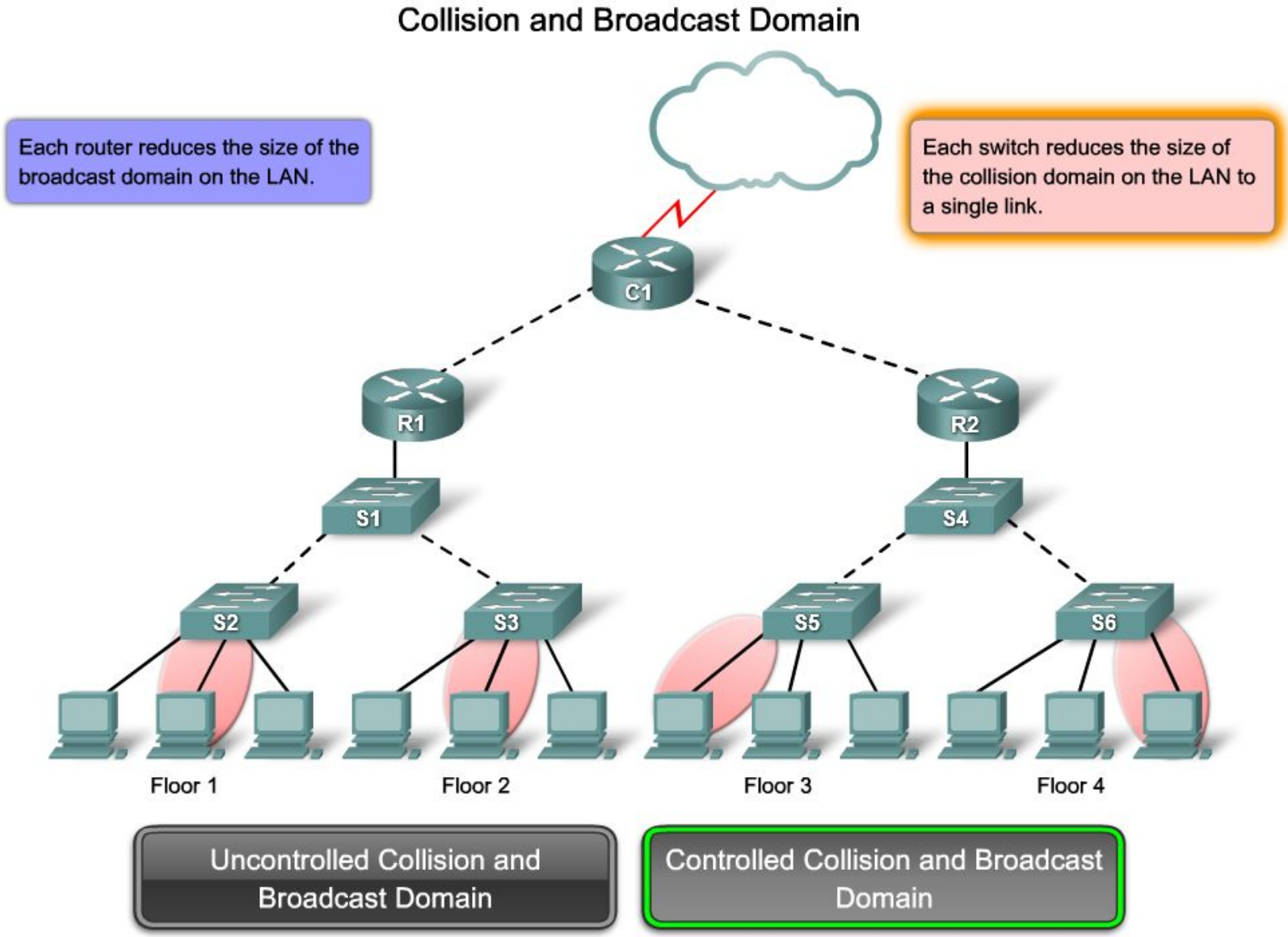
Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

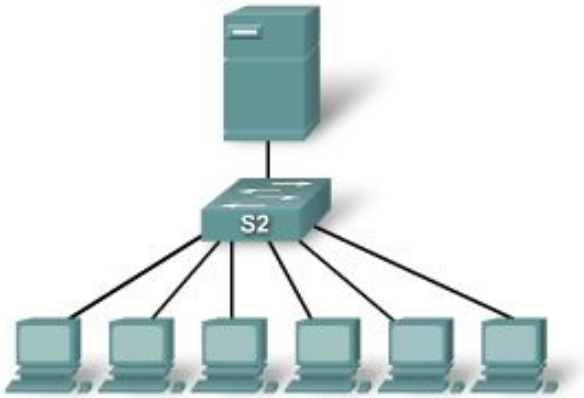
- Describe the LAN design considerations to reduce network latency

Controlling Network Latency

- Consider the latency caused by each device on the network.
  - A core level switch supporting 48 ports, running at 1000 Mb/s full duplex requires 96 Gb/s internal throughput if it is to maintain full wirespeed across all ports simultaneously.

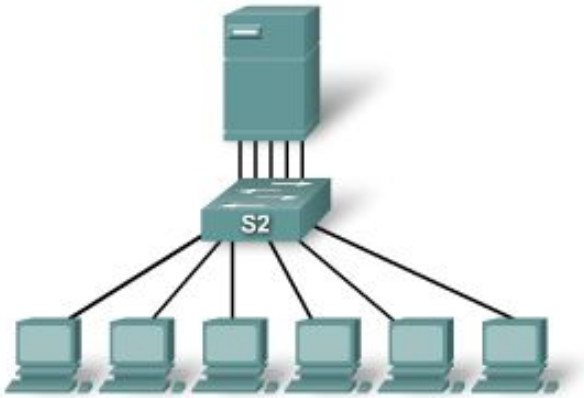
- Higher OSI layer devices can also increase latency on a network.
  - A router must strip away the Layer 2 fields in a frame in order to interpret layer 3 addressing information. The extra processing time causes latency.
  - Balance the use of higher layer devices to reduce network latency with the need to prevent contention from broadcast traffic or the high collision rates.

Server with one 1000 Mb/s NIC



NIC Bandwidth of 167 Mb/s per computer

Server with five 1000 Mb/s NICs



NIC Bandwidth of 833 Mb/s per computer

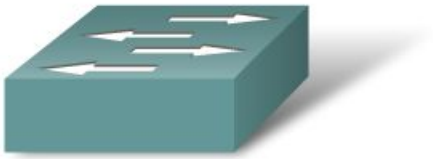
© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Describe the switch forwarding methods

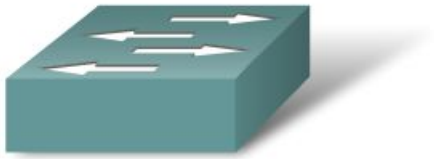
Switch Packet Forwarding Methods

Store-and-forward

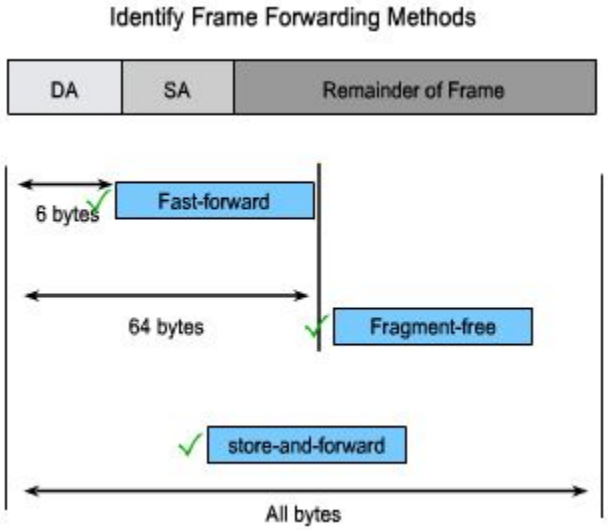


Complete frame is received before forwarding.

Cut-through



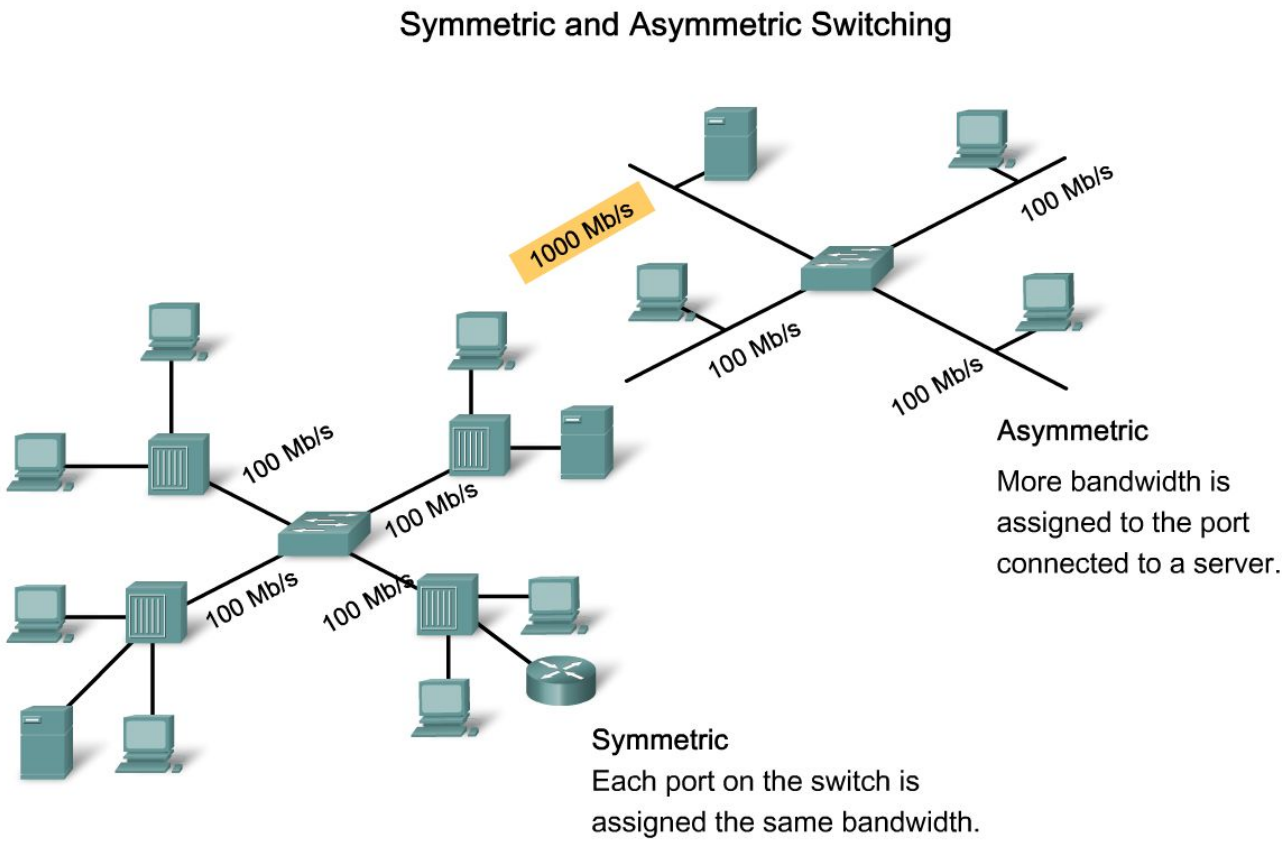
The frame is forwarded through the switch before the entire frame is received.



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Explain symmetric and asymmetric Switching



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Describe how memory buffering works

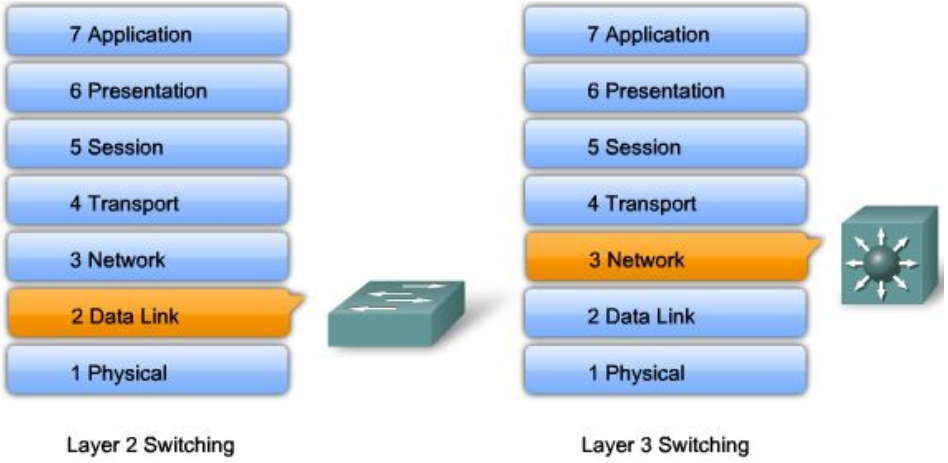
Port-Based and Shared Memory Buffering

Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Compare Layer 2 with Layer 3 switching



Layer 3 Switch and Router Comparison

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

Configure a Switch for Operation in a Network

- Describe the Cisco IOS commands used to navigate the command-line

The Command Line Interface Modes

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#`

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure a Switch for Operation in a Network

- Describe the Cisco IOS help facilities

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`

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.

© 2006 Cisco Systems, Inc. All rights re

Configure a Switch for Operation in a Network

- Describe the Cisco IOS commands used to access the command history

The Command History Buffer

```
switch#show history
  enable
  show history
  enable
  config
  t
  confi
  t
  show history
switch#
```

Use the **show history** command to view recently entered EXEC commands.

Configure the Command History buffer

Cisco IOS CLI Command Syntax	
Enable terminal history. This command can be run from either user or privileged EXEC mode.	switch#**terminal history**
Configures the terminal history size. The terminal history can maintain 0 to 256 command lines.	switch#**terminal history size 50**
Resets the terminal history size to the default value of 10 command lines.	switch#**terminal no history size**
Disables terminal history.	switch#**terminal no history**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure a Switch for Operation in a Network

- Describe the boot sequence of a Cisco switch

Describe the Boot Sequence

The boot sequence of a Cisco switch:

-The switch loads the boot loader software from NVRAM.

-The boot loader:

- Performs low-level CPU initialization.
- Performs POST for the CPU subsystem.
- Initializes the flash file system on the system board.
- Loads a default operating system software image into memory and boots the switch.

-The operating system runs using the config.text file, stored in the switch flash storage.

The boot loader can help you recover from an operating system crash:

-Provides access into the switch if the operating system has problems serious enough that it cannot be used.

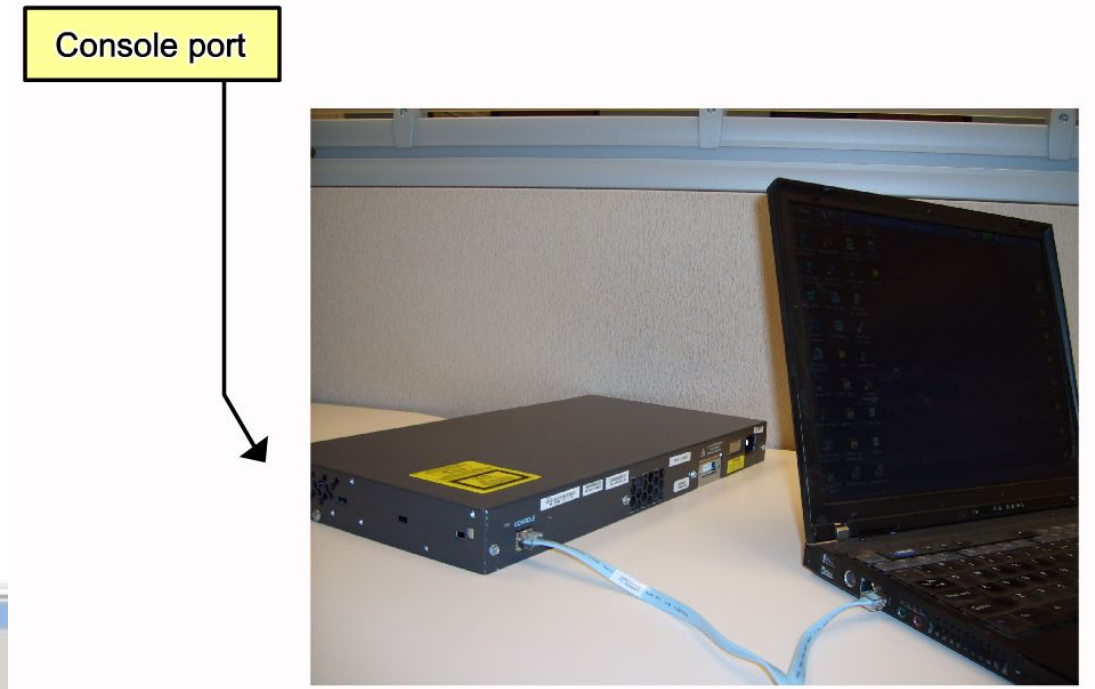
-Provides access to the files stored on flash before the operating system is loaded.

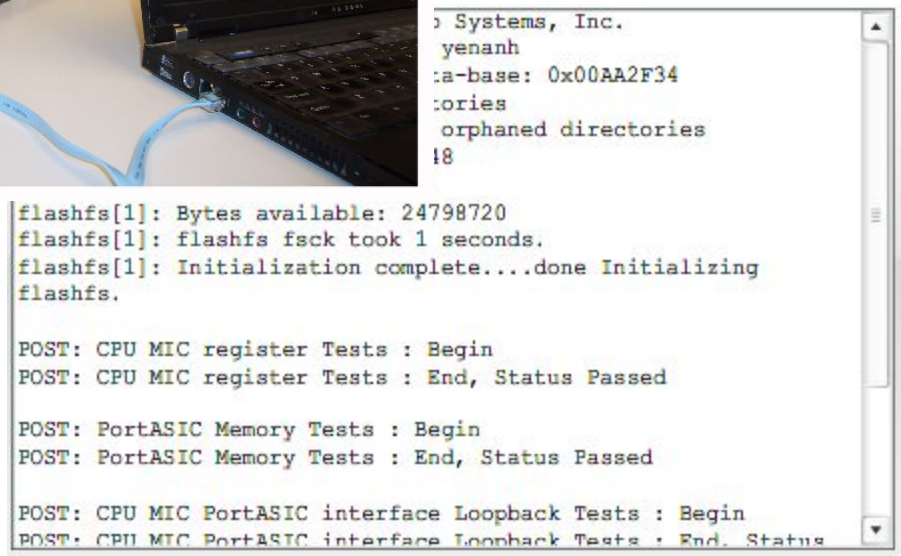
-Use the boot loader command line to perform recovery operations.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure a Switch for Operation in a Network

- Describe how to prepare the switch to be configured

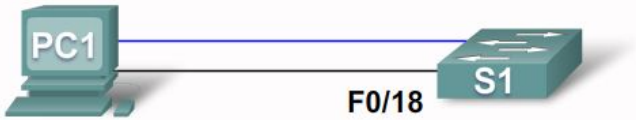




Configure a Switch for Operation in a Network

- Describe how to perform a basic switch configuration

Configure IP Connectivity



PC1:
- IP address - 172.17.99.12
- Connected to Console port
- Connected to port F0/18 on S1

S1:
- VLAN 99
- the management VLAN
- IP address -172.17.99.11
- Port F0/18 assigned to VLAN 99

- For TCP/IP management a Layer 3 address must be assigned to the switch.
- VLAN 1 is the default management interface for all switches
- There are security risks associated with using VLAN 1
- Create another VLAN, for example VLAN 99 or VLAN 150
- Assign that VLAN to an appropriate port, for example F0/18

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure a Switch for Operation in a Network

- Describe how to verify the Cisco IOS configuration using the Show command

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`

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure a Switch for Operation in a Network

- Describe how to manage the Cisco IOS configuration files

Backup and Restore Switch Configurations

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 Crtl+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 Crtl+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 Crtl+C key combination to cancel.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to configure password options

Configure EXEC Mode Passwords

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Configures the **enable password** to enter privileged EXEC mode.	`S1(config)#enable password` *password*
Configures the **enable secret** password to enter privileged EXEC mode.	`S1(config)#enable secret` *password*
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config)#end`

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to configure a login banner

Configure a Login Banner

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configure a login banner.	S1(config)#**banner login "Authorized Personnel Only!"**

Configure a MOTD Banner

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configure a MOTD login banner.	S1(config)#**banner motd "Device maintenance will be occurring on Friday!"**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe the how to configure Telnet and SSH on a switch

Telnet and SSH

Telnet
-Most common access method
-Sends clear text message streams
-Is not secure

SSH
-Should be the common access method
-Sends encrypted message stream
-Is secure

Configuring Telnet

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

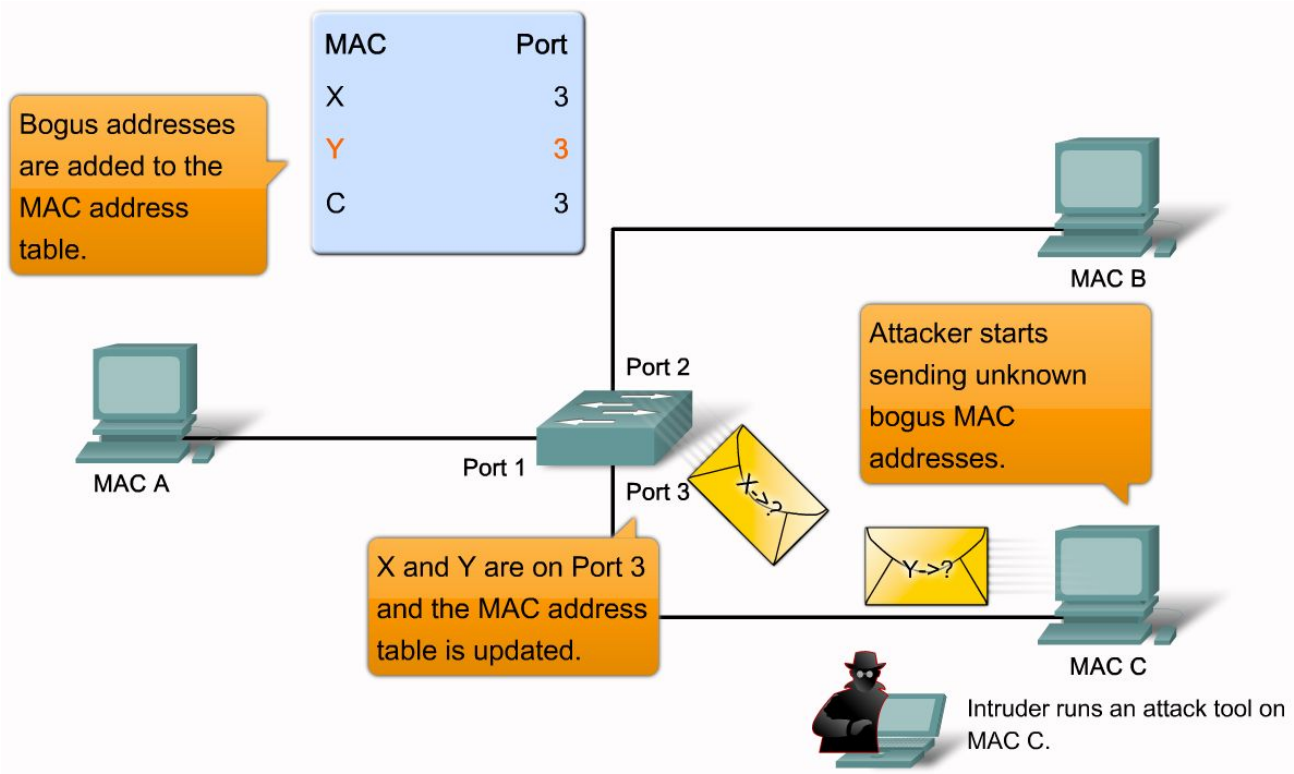
Configuring SSH

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe the key switch security attacks. The description should include, MAC address flooding, spoofing attacks, CDP attacks, and Telnet attacks



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe how network security tools are used to improve network security

Security Tools

Network Security Tools perform these functions:

-Network Security Audits help you to

- Reveal what sort of information an attacker can gather simply by monitoring network traffic.
- Determine the ideal amount of spoofed MAC addresses to remove.
- Determine the age-out period of the MAC Address table.

-Network Penetration Testing helps you to

- Identify weaknesses within the configuration of your networking devices.
- Launch numerous attacks to test your network.
- Caution: Plan penetration tests to avoid network performance impacts.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe why you need to secure ports on a switch

Network Security Tools Features

Common features of a modern network security tool include:

-Service Identification
-Support of SSL Services
-Non-destructive and Destructive Testing
-Database of Vulnerabilities

You can use network security tools to:

-Capture chat messages
-Capture files from NFS traffic
-Capture HTTP requests in Common Log Format
-Capture mail messages in Berkeley mbox format
-Capture passwords
-Display capture URLs in Netscape in real-time
-Flood a switched LAN with random MAC addresses
-Forge replies to DNS address and pointer queries
-Intercept packets on a switched LAN

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to disable unused ports

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, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summary

- LAN Design

  Process that explains how a LAN is to be implemented

  Factors to consider in LAN design include

    Collision domains

    Broadcast domains

    Network latency

    LAN segmentation

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summary

- Switch forwarding methods
  - Store & forward – used by Cisco Catalyst switches
  - Cut through – 2 types
    - Cut through
    - Fast forwarding

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summary

- Symmetric switching

  Switching is conducted between ports that have the same bandwidth

- Asymmetric switching

  Switching is conducted between ports that have unlike bandwidth

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

Summary

- CISCO IOS CLI includes the following features
  - Built in help
  - Command history/options
- Switch security
  - Password protection
  - Use of SSH for remote access
  - Port security

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public