



Configure a Switch



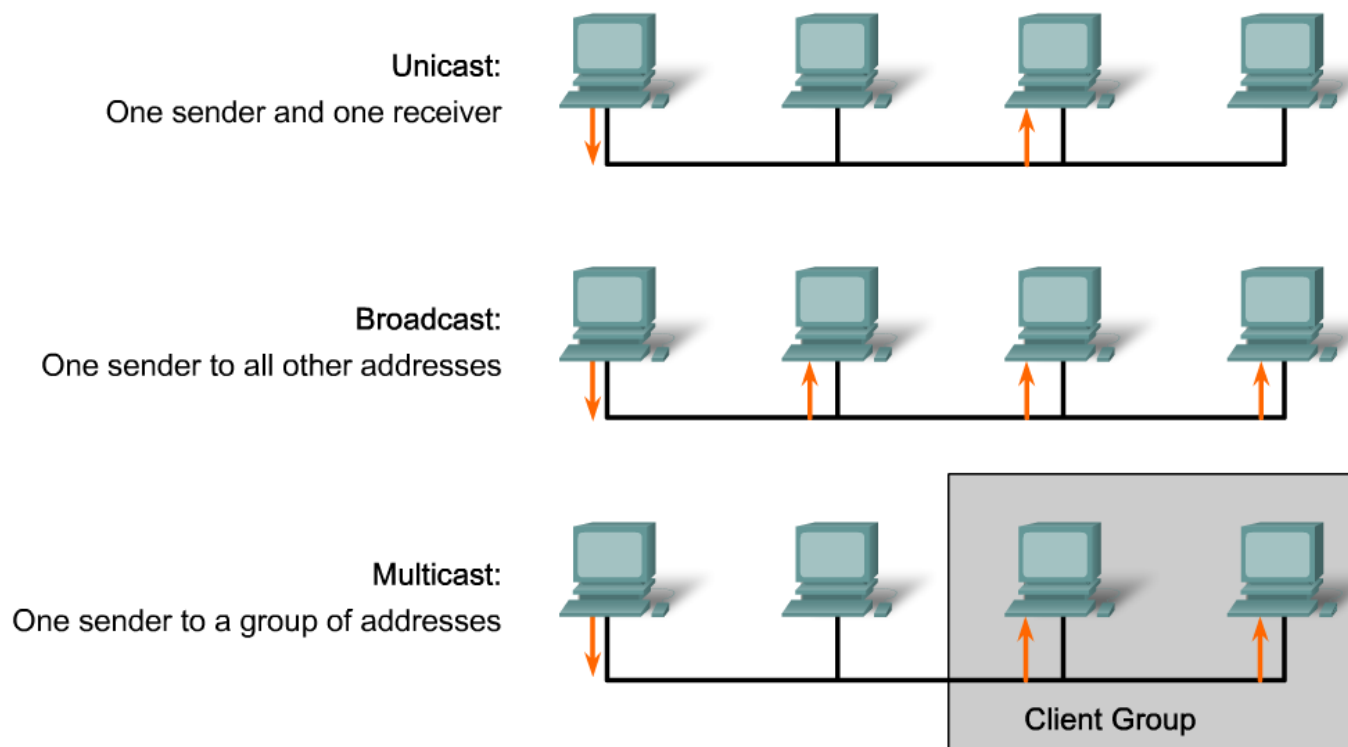
LAN Switching and Wireless – Chapter 2

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.

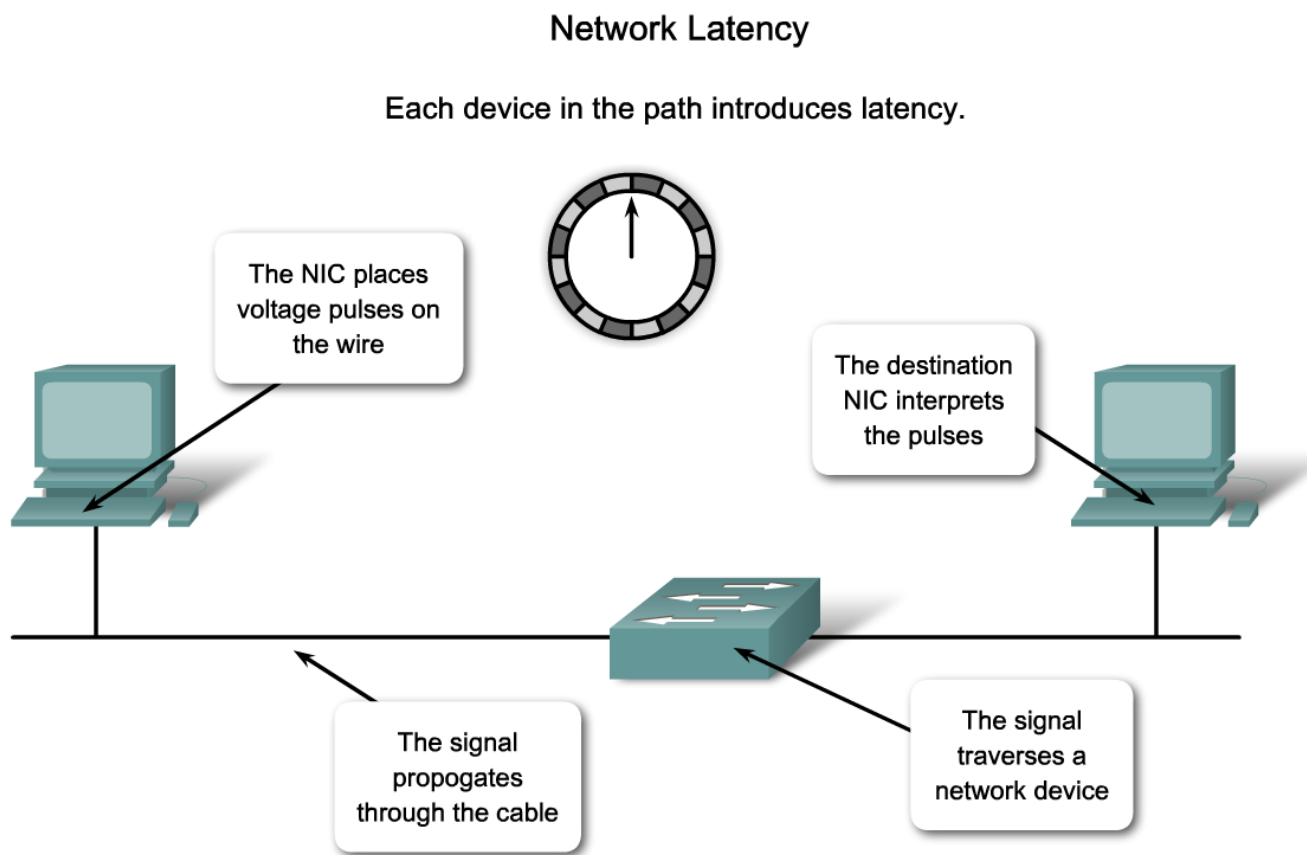
Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

- Describe the key elements of Ethernet/802.3 networks



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



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.

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.

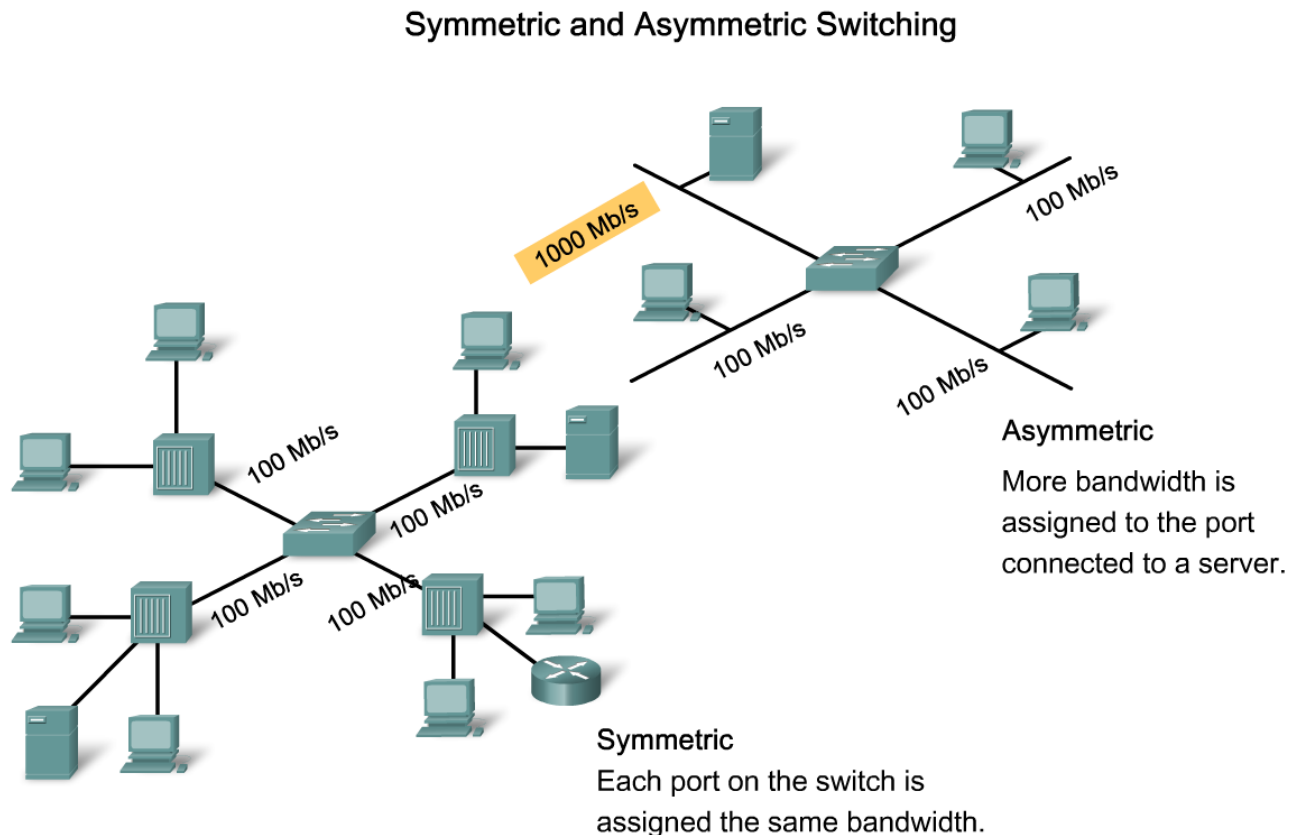
Cut-through



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

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

- Explain symmetric and asymmetric Switching



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.

SWITCH

- Asymmetric switching
- Symmetric switching
- Port base memory buffering
- Shared memory buffering
- Store and forward switching method
- Cut-through switching method

Asymmetric vs symmetric switching

- Asymmetric switching adalah ketika switch mampu melakukan transfer data dengan kecepatan yang berbeda-beda, misalnya switch 100/1000 Mbps.
- Symmetric switching adalah ketika switch hanya mendukung kecepatan pengiriman paket data yang sama, misalnya hanya mendukung 100 Mbps.
- Asymmetric switching sangat berperan penting untuk tipe komunikasi client-server, karena sekarang switch sudah beragam, dan dalam satu jaringan sangat mungkin ada switch yg berbeda jenis.

Memory buffering: port based vs shared

- Port based memory buffering: paket-paket data yang hendak dikirimkan menuju suatu port akan di-queue di port tsb. Setiap port dialokasikan bagian memory. Paket data baru akan dikirim jika antrian/queue di port tsb sudah available.
- Shared memory buffering: ketika ada alokasi memory buffering pada memory lain, maka bisa dimanfaatkan untuk mengolah paket data untuk segera dikirimkan. Hal ini memungkinkan pengiriman paket-paket data yg lebih cepat.

Switching method: store and forward vs cut-through

- Store and forward adalah metode switching dimana paket data baru akan dikirimkan bila hasil perhitungan menunjukkan paket tsb adalah paket data yang valid. Dengan kata lain, harus diperiksa sampai, baru bisa dikirim.

Switching method: store and forward vs cut-through

- Cut-through terdiri dari 2 field:
 1. fast forward yaitu metode switching dimana latency paling kecil karena paket data akan langsung dikirim begitu destination address diketahui. Tidak ada pengecekan error pada paket sehingga paket yang error pun akan tetap dikirim.
 2. fragment-free metode switching dimana paket data baru akan dikirim bila hasil pemeriksaan awal dari 64 byte pertama tidak menunjukkan adanya error.
64 byte itu field: preamble source addr+destination addr+sdikit data

Switching method: store and forward vs cut-through

- Adaptive cut-through adalah pengembangan dari metode cut through dimana paket data akan dikirimkan secara cut-through. Namun bila terjadi error pada paket yang dikirim sampai batas jumlah tertentu (threshold) maka metode switching akan diubah menjadi store and forward.

Switch Configuration

- Manageble switch dpt diberikan IP. IP ini diberikan bukan kepada setiap int fast ethernet yg dimilikinya, namun kpd interface VLAN.
- VLAN (Virtual LAN) adalah fitur switch yg memungkinkan end user device untuk terhubung ke dalam sebuah LAN tanpa terbatas pada geografis (ruangan atau gedung).
- Switch mempunyai default VLAN yaitu VLAN 1.

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#

Configure a Switch for Operation in a Network

- Describe the Cisco IOS help facilities

Configuring Port Security on a Cisco Catalyst Switch

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	S1# configure terminal
Specify the type and number of the physical interface to configure, for example fastEthernet F0/18, and enter interface configuration mode. Use this Cisco IOS command:	S1(config)# interface fastEthernet 0/18
Set the interface mode as access. An interface in the dynamic desirable default mode cannot be configured as a secure port. Use this Cisco IOS command:	S1(config-if)# switchport mode access
Enable port security on the interface. Use this Cisco IOS command:	S1(config-if)# switchport port-security
Return to privileged EXEC mode. Use this Cisco IOS command:	S1(config-if)# end

Port Security Configuration Script

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	S1# configure terminal
Specify the type and number of the physical interface to configure. Use this Cisco IOS command:	S1(config)# interface fastEthernet 0/18
Set the interface mode as access. Use this Cisco IOS command:	S1(config-if)# switchport mode access
Enable port security on the interface. Use this Cisco IOS command:	S1(config-if)# switchport port-security
Set the maximum number of secure addresses to 50. Use this Cisco IOS command:	S1(config-if)# switchport port-security maximum 50
Enable sticky learning. Use this Cisco IOS command:	S1(config-if)# switchport port-security mac-address sticky
Return to privileged EXEC mode. Use this Cisco IOS command:	S1(config-if)# end

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
```

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:

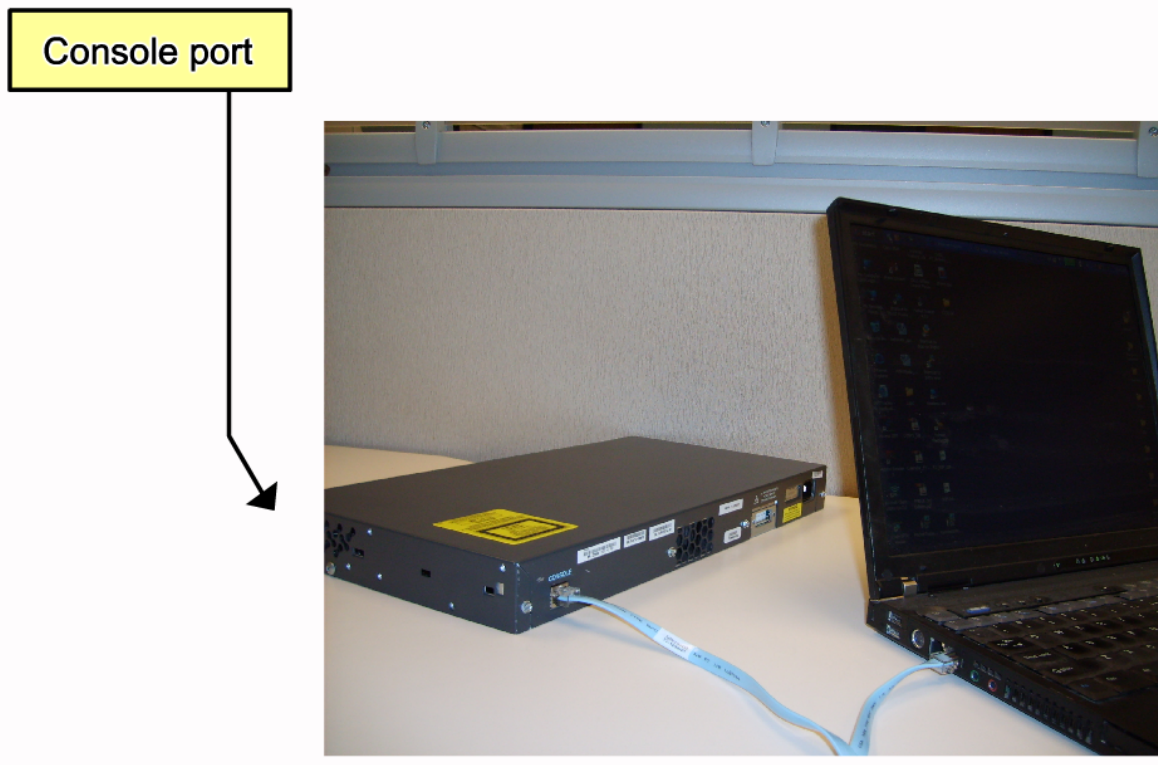
- The switch loads the boot loader software from NVRAM.
- The boot loader:
 - Performs low-level CPU initialization.
 - Performs POST for the CPU subsystem.
 - Initializes the flash file system on the system board.
 - Loads a default operating system software image into memory and boots the switch.
-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

Configure a Switch for Operation in a Network

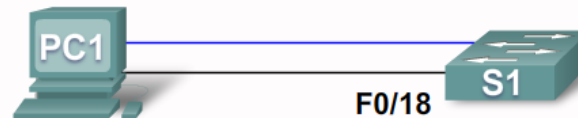
- Describe how to prepare the switch to be configured



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

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.	<code>show interfaces [interface-id]</code>
Displays contents of startup configuration.	<code>show startup-config</code>
Displays current operating configuration.	<code>show running-config</code>
Displays information about flash: file system.	<code>show flash:</code>
Displays system hardware and software status.	<code>show version</code>
Display the session command history.	<code>show history</code>
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.	<code>show ip {interface http arp}</code>
Displays the MAC forwarding table.	<code>show mac-address-table</code>

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 Ctrl+C key combination to cancel.	<pre>S1#copy system:running-config flash:startup-config Destination filename [startup-config]?</pre>
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.	<pre>S1#copy running-config startup-config Destination filename [startup-config]?</pre>
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.	<pre>S1#copy startup-config flash:config.bak1 Destination filename [config.bak1]?</pre>

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 <i>password</i>
Configures the enable secret password to enter privileged EXEC mode.	S1(config)# enable secret <i>password</i>
Exit from line configuration mode and return to privileged EXEC mode.	S1(config)# end

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.	<code>S1#configure terminal</code>
Configure a login banner.	<code>S1(config)#banner login "Authorized Personnel Only!"</code>

Configure a MOTD Banner

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

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

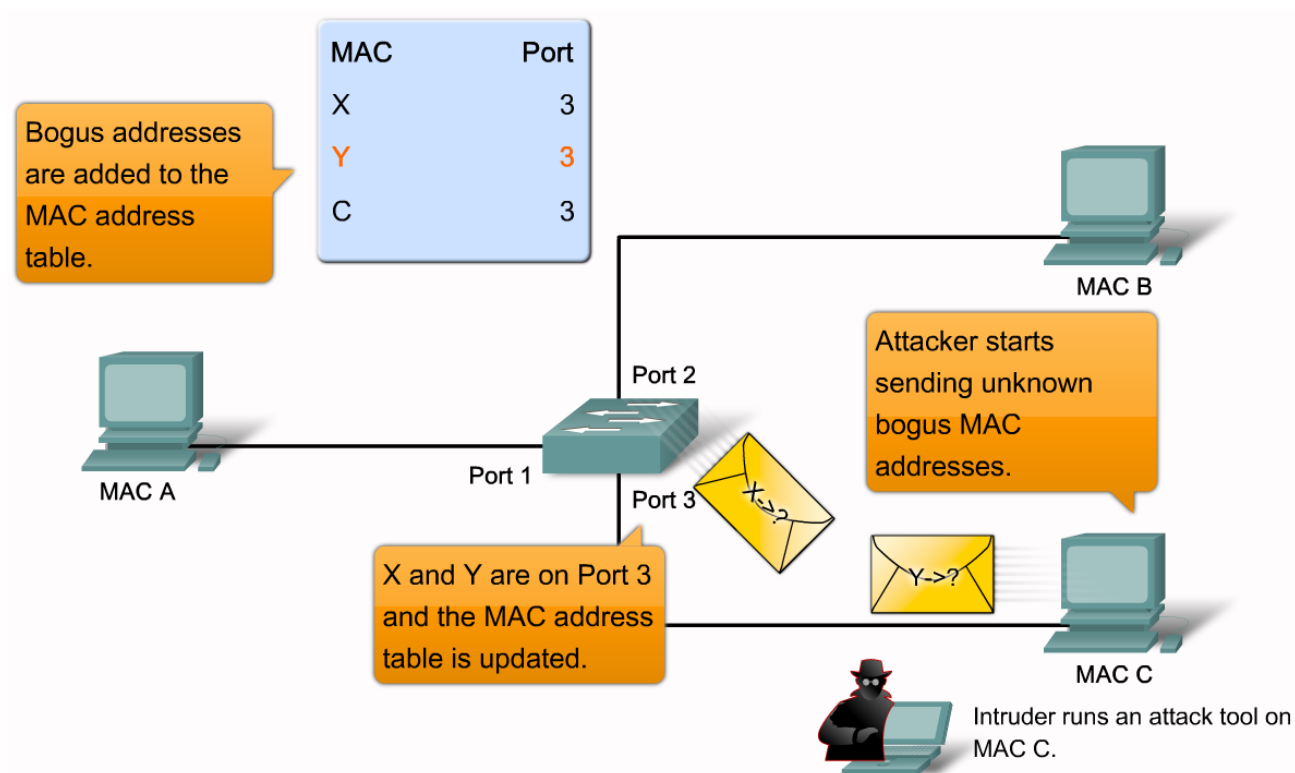
```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

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
```

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



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.

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

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.

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

Summary

- Switch forwarding methods

Store & forward – used by Cisco Catalyst switches

Cut through – 2 types

Cut through

Fast forwarding

Summary

- Symmetric switching

Switching is conducted between ports that have the same bandwidth

- Asymmetric switching

Switching is conducted between ports that have unlike bandwidth

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

