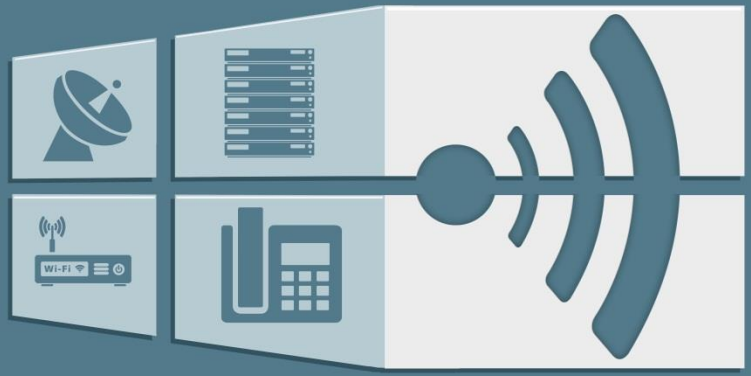


Introduction to CCNA® Routing and Switching

Lesson 10

Layer 2 Switching

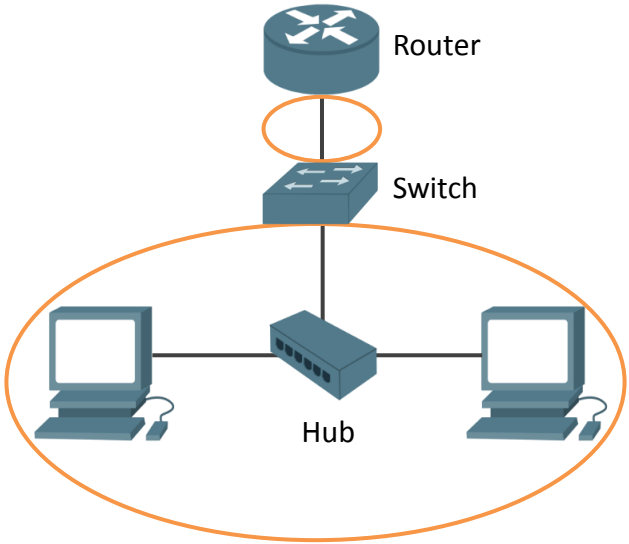
By the end of this lesson, you will be able to:

- Explain the aspects of collision and broadcast domains
- Explain switch management
- Configure and verify port security

A hub:

- is a layer 1 device.
- does not use any addressing logic.
- broadcasts all frames.

All the links attached to a hub form one collision domain.

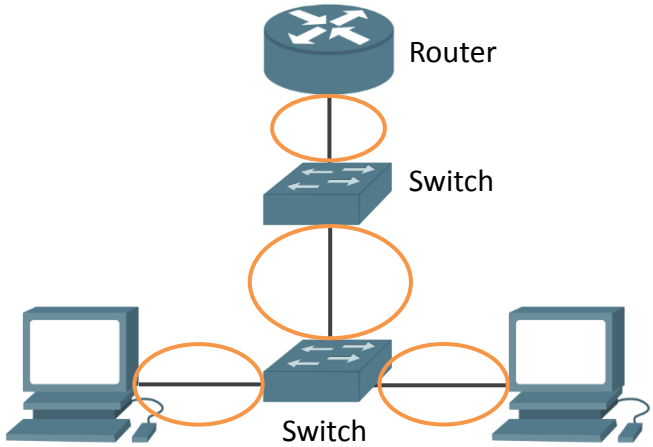


A switch:

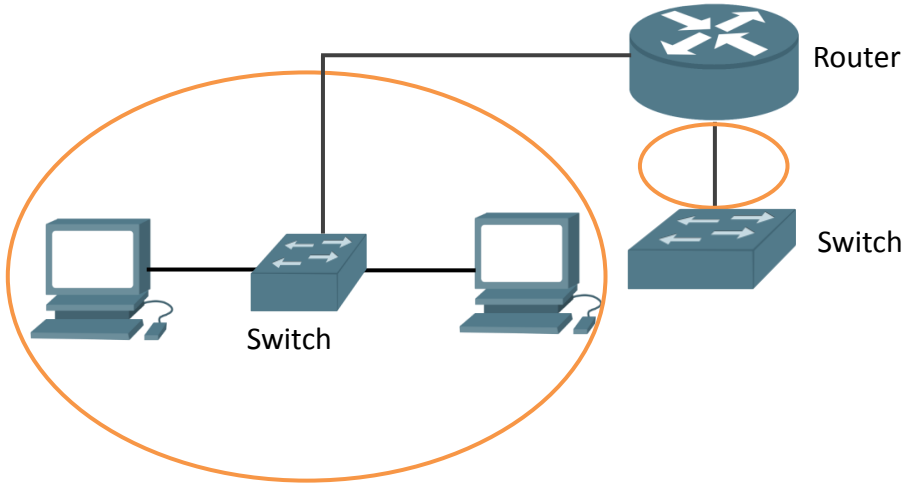
- is a layer 2 device.
- is different from a hub.

Each switch port is its own collision domain.

Frames sent to a device and attached to a switch are received by the intended device only.



A broadcast domain is a subnet. This is why there is a broadcast address in each subnet.



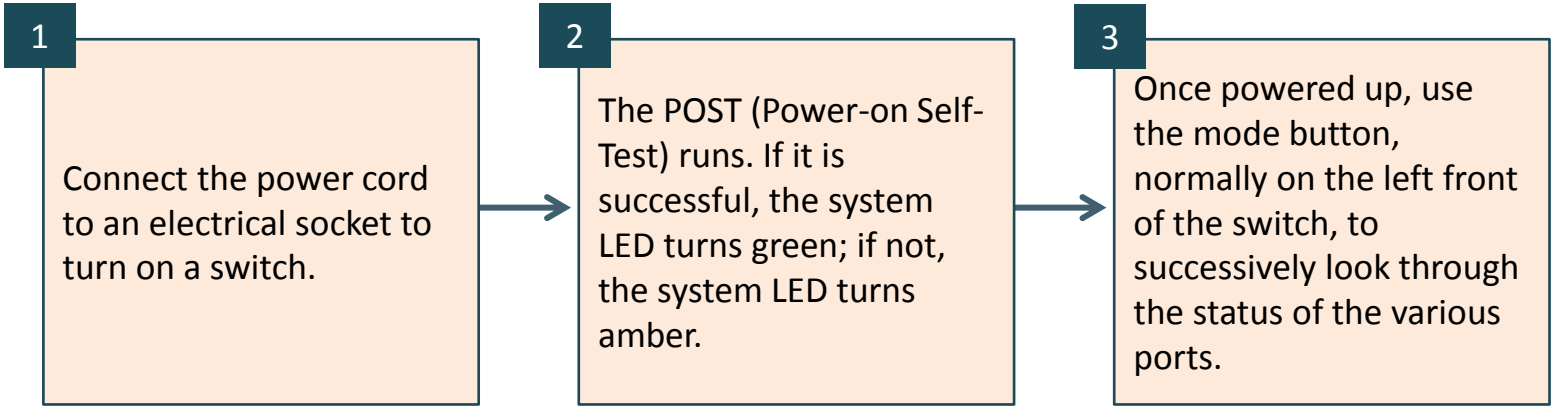
Separating traffic is desirable because:

- it increases network security.
- it decreases the amount of traffic in a section of the network.
- it cuts down on the control protocol traffic in a section of the network.
- network problems will tend to be confined to a smaller portion of the network.

The following are the advantages of switches:

- Bridging is accomplished via hardware.
- Offers low latency.
- Offers nearly wire-speed switching capabilities.

The process flow for booting a switch is given below:



To manage a switch, it must be accessible through Telnet or SSH. It requires an IP address.

Command to configure the address:

```
interface vlan 1
ip address ip-address mask
no shutdown
```

A Layer 2 switch needs a default gateway to get to the router interface that will service its routing needs. The command for the default gateway is as follows:

```
ip default-gateway IP-address
```

A switch performs the following functions:

- It learns Layer 2 addresses of attached devices.
- It forwards or filters Layer 2 frames.
- It uses Spanning Tree Protocol (STP) to prevent loops from forming in the Layer 2 domain.

Whenever a frame is received, the switch looks up the source MAC address in the MAC address table. If it is not found, the source MAC address and the source port are added to the MAC address table, along with the associated Virtual Local Area Network (VLAN) and address type.

Depending on the IOS, the command to show the MAC address table is either of the following:

```
Sw1#show mac-address-table
```

OR

```
Sw1#show mac address-table
```

```
Sw1#show mac-address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

 All    0280.a200.b000    STATIC      CPU
   1    0000.0000.0001    DYNAMIC     Fa0/1
   1    0000.0000.0011    DYNAMIC     Fa0/11
   2    0000.0000.0002    DYNAMIC     Fa0/2
   2    0000.0000.0012    DYNAMIC     Fa0/12
   2    0000.0000.0022    DYNAMIC     Fa0/22
Total Mac Addresses for this criterion: 6
```

The switch looks up the Layer 2 destination address in the MAC address table.

- If the address is found, the MAC address table provides the correct egress interface and the frame is only sent out of that interface.
- If the address is not found, the switch floods the frame; it sends the frame out of all active interfaces with the same VLAN except the interface on which it was received.
- All broadcast addresses are flooded to all interfaces regardless of VLAN.

Enabling port security can help protect switch interfaces from such a situation.

The command to configure port security:

```
Interface Fa0/1
switchport mode access
switchport access vlan 2
switchport port-security
```

The command to set the number of MAC addresses that can be assigned to interface Fa0/1 to 2:

switchport port-security maximum *number*

The command to verify port security:

show port-security interface f0/3

The default violation mode is **shutdown**. The port becomes **err-disabled** upon violation.

The following command can be entered in interface configuration mode:

Sw1(config-if)# **switchport port-security violation** *violation-mode*

Violation Mode	Violation Counter Increases	Port is Shut Down
Protect	N	N
Restrict	Y	N
Shutdown	Y	Y

The different types of MAC addresses are as follows:

- Static secure: These are manually configured addresses that become part of the MAC address table.
- Dynamic secure: These become part of only the MAC address table, not the running configuration.
- Sticky secure: These are dynamically learned and stored to running configuration.

The interface configuration command to manually configure static secure MAC address:

switchport port-security mac-address *mac-address*

The following command can be used to enable sticky address learning.

```
switchport port-security mac-address sticky
```

The following command can be used to disable sticky address learning.

```
no switchport port-security mac-address sticky
```

Sticky address learning has the following effects:

- The MAC addresses learned become static secure addresses.
- They also become a part of the running configuration.

Quiz

For hardware switching, Cisco uses _____.

a. ASICs
b. ROMs
c. POST
d. RAMs

For hardware switching, Cisco uses _____.

a. ASICs
b. ROMs
c. POST
d. RAMs

Answer: a.

Explanation: Cisco uses Application Specific Integrated Circuits (ASICs) for hardware switching.

Which command is used on a switch port to limit the number of MACs that are learned?

a. switchport port-security violation
b. switchport port-security maximum
c. switchport port security maximum
d. switchport port-security mac-number

Which command is used on a switch port to limit the number of MACs that are learned?

a. switchport port-security violation
b. switchport port-security maximum
c. switchport port security maximum
d. switchport port-security mac-number

Answer: b.

Explanation: The **switchport port-security maximum** command is used on a switch port to limit the number of MACs that are learned.

_____ MAC address types do not become part of the running configuration.

a. Dynamic secure
b. Sticky static
c. Static secure
d. Sticky secure

_____ MAC address types do not become part of the running configuration.

a. Dynamic secure
b. Sticky static
c. Static secure
d. Sticky secure

Answer: a.

Explanation: Dynamic secure MAC address types do not become part of the running configuration.

The default port security violation mode is _____.

a. restrict
b. limit
c. protect
d. shutdown

The default port security violation mode is _____.

a. restrict
b. limit
c. protect
d. shutdown

Answer: d.

Explanation: The default port security violation mode is **shutdown**.

All of the following commands display the CAM except _____.

a. show cam-table
b. show mac-address-table
c. show mac address table
d. sh mac add

All of the following commands display the CAM except _____.

a. show cam-table
b. show mac-address-table
c. show mac address table
d. sh mac add

Answer: b.

Explanation: Although it is called the CAM, use a variation of the **show mac-address-table** command to display it.

Here is a quick recap of what was covered in this lesson:

- The fewer collision and broadcast domains in a network, the better.
- Switching offers fast hardware forwarding.
- The MAC address table keeps track of Layer 2 forwarding information.
- The default violation mode for port security is shutdown.