Layer 2 Switching

CNW 4541

Department of Computer Science & Engineering
ITER, Siksha 'O' Anusandhan Deemed To Be University
Jagamohan Nagar, Jagamara, Bhubaneswar, Odisha - 751030

Book(s)

Text Book(s)

Todd Lammle

CCNA Routing & Switching

Secound Edition

SYBEX

Talk Flow

1. Switching Services
2. Describe and verify switching concepts
3. Configure, verify, and troubleshoot port security
4. Configuring Catalyst Switches

Switching Services

- Unlike old bridges, which used software to create and manage a Content Addressable Memory (CAM) filter table, our new, fast **switches** use application-specific integrated circuits (ASICs) to build and maintain their MAC filter tables.
- Layer 2 **switches** and bridges are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses before deciding to either forward, flood, or drop the frame.
- Unlike hubs, **switches** create private, dedicated collision domains and provide independent bandwidth exclusive on each port.

Switching Services (contd.)

Here's a list of four important advantages we gain when using layer 2 switching:

- Hardware-based bridging (ASICs)
- Wire speed
- Low latency
- Low cost

A big reason layer 2 switching is so efficient is that no modification to the data packet takes place. The device only reads the frame encapsulating the packet, which makes the switching process considerably faster and less error-prone than routing processes are.

Describe and verify switching concepts

Three Switch Functions at Layer 2

There are three distinct functions of layer 2 switching that are vital:

1. **Address learning:** Layer 2 switches remember the source hardware address of each frame received on an interface and enter this information into a MAC database called a forward/filter table.

2. **Forward/filter decisions:** When a frame is received on an interface, the switch looks at the destination hardware address, then chooses the appropriate exit interface for it in the MAC database. This way, the frame is only forwarded out of the correct destination port.

3. **Loop avoidance:** If multiple connections between switches are created for redundancy purposes, network loops can occur. Spanning Tree Protocol (STP) is used to prevent network loops while still permitting redundancy.

Describe and verify switching concepts (contd.)

Address learning (contd.)

- When a switch is first powered on, the MAC forward/filter table (CAM) is empty, as shown in Figure 1

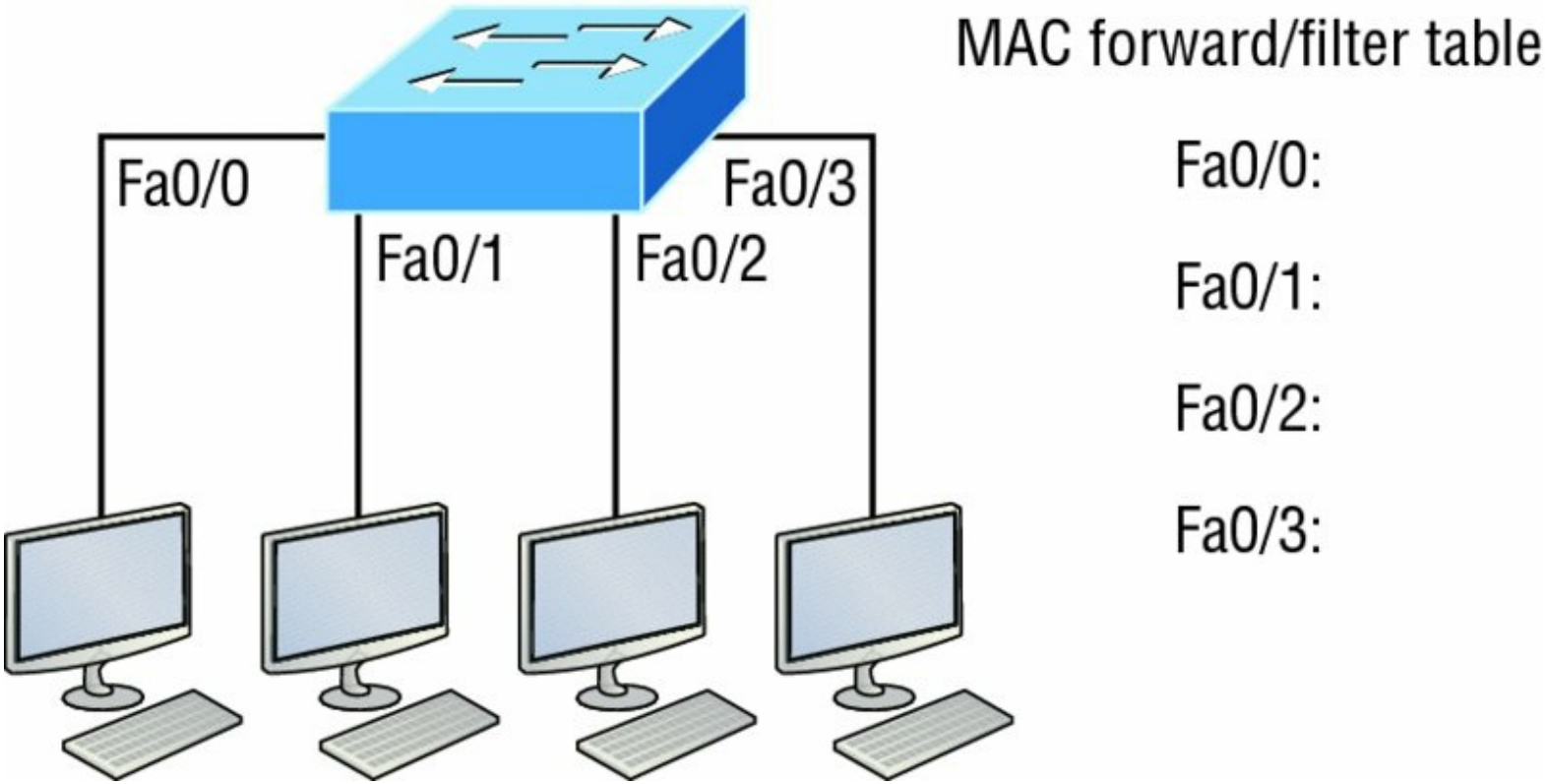
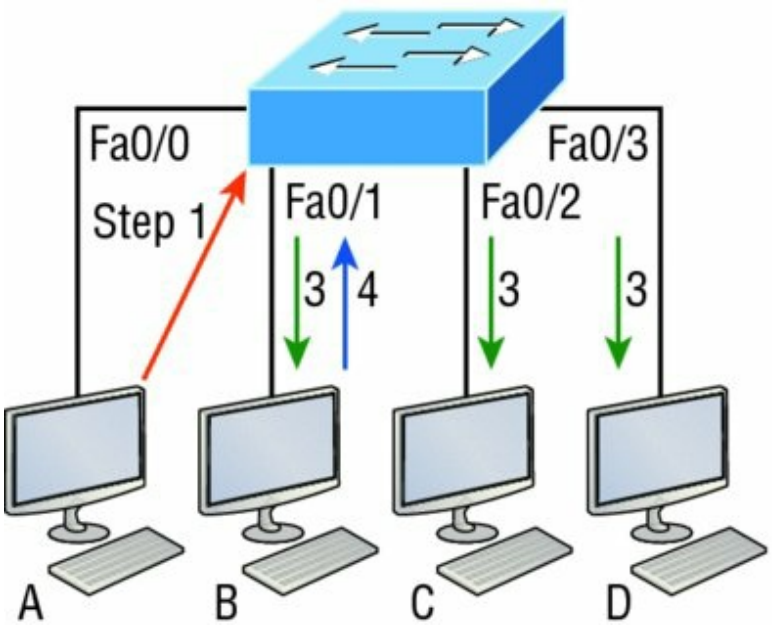


Figure 1: Empty forward/filter table on a switch

Describe and verify switching concepts (contd.)

Address learning (contd.)

- In this figure, you can see four hosts attached to a switch. When the switch is powered on, it has nothing in its MAC address forward/filter table, just as in Figure 1. But when the hosts start communicating, the switch places the source hardware address of each frame into the table along with the port that the frame's source address corresponds to.



CAM/MAC forward/filter table

Fa0/0:	0000.8c01.000A	Step 2
Fa0/1:	0000.8c01.000B	Step 4
Fa0/2:		
Fa0/3:		

Figure 2: How switches learn hosts' locations

Describe and verify switching concepts (contd.)

Address learning (contd.)

Example of how a forward/filter table is populated using Fig 2.

1. Host A sends a frame to Host B. Host A's MAC address is 0000.8c01.000A; Host B's MAC address is 0000.8c01.000B.
2. The switch receives the frame on the Fa0/0 interface and places the source address in the MAC address table.
3. Since the destination address isn't in the MAC database, the frame is forwarded out all interfaces except the source port.
4. Host B receives the frame and responds to Host A. The switch receives this frame on interface Fa0/1 and places the source hardware address in the MAC database.
5. Host A and Host B can now make a point-to-point connection and only these specific devices will receive the frames. Hosts C and D won't see the frames, nor will their MAC addresses be found in the database because they haven't sent a frame to the switch yet.

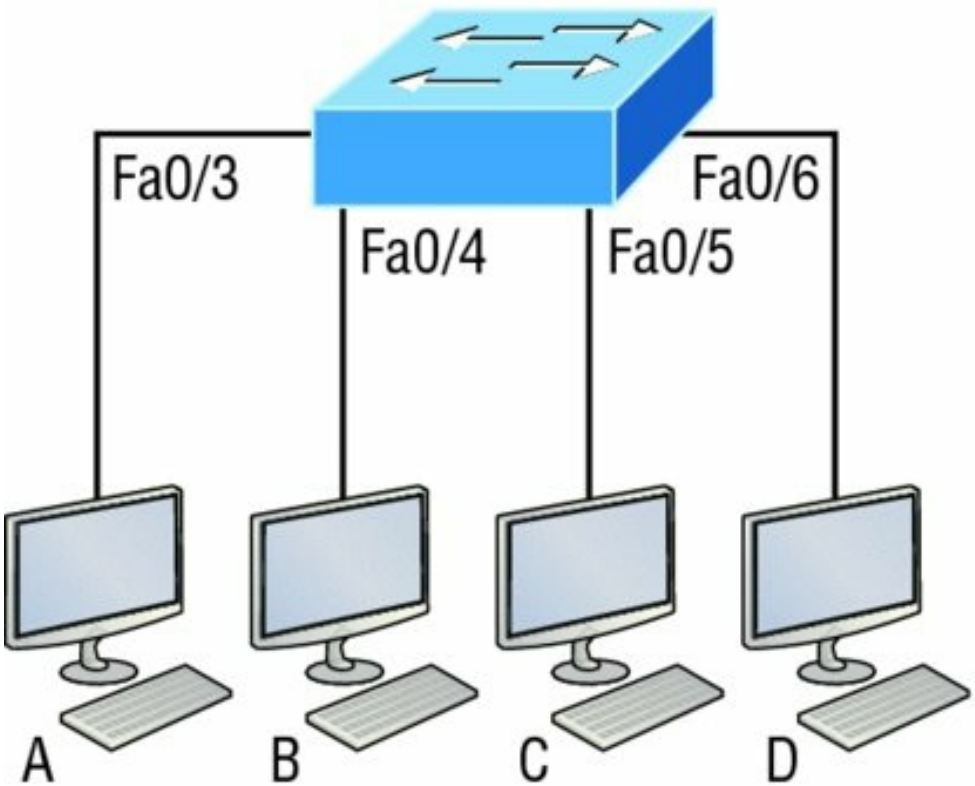
Describe and verify switching concepts (contd.)

Forward/Filter Decisions

- When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is only sent out of the appropriate exit interface.
- But if the destination hardware address isn't listed in the MAC database, then the frame will be flooded out all active interfaces except the interface it was received on.
- If a host or server sends a broadcast on the LAN, by default, the switch will flood the frame out all active ports except the source port.

Forward/Filter Decisions(contd.)

- In Figure 3, Host A sends a data frame to Host D. What do you think the switch will do when it receives the frame from Host A?



Switch# show mac address-table

VLAN	Mac Address	Ports
1	0005.dccb.d74b	Fa0/4
1	000a.f467.9e80	Fa0/5
1	000a.f467.9e8b	Fa0/6

Figure 3: Forward/Filter table

Forward/Filter Decisions(contd.)

- Let's examine Figure 4 to find the answer.Since Host A's MAC address is not in the forward/filter table, the switch will add the source address and port to the MAC address table, then forward the frame to Host D.

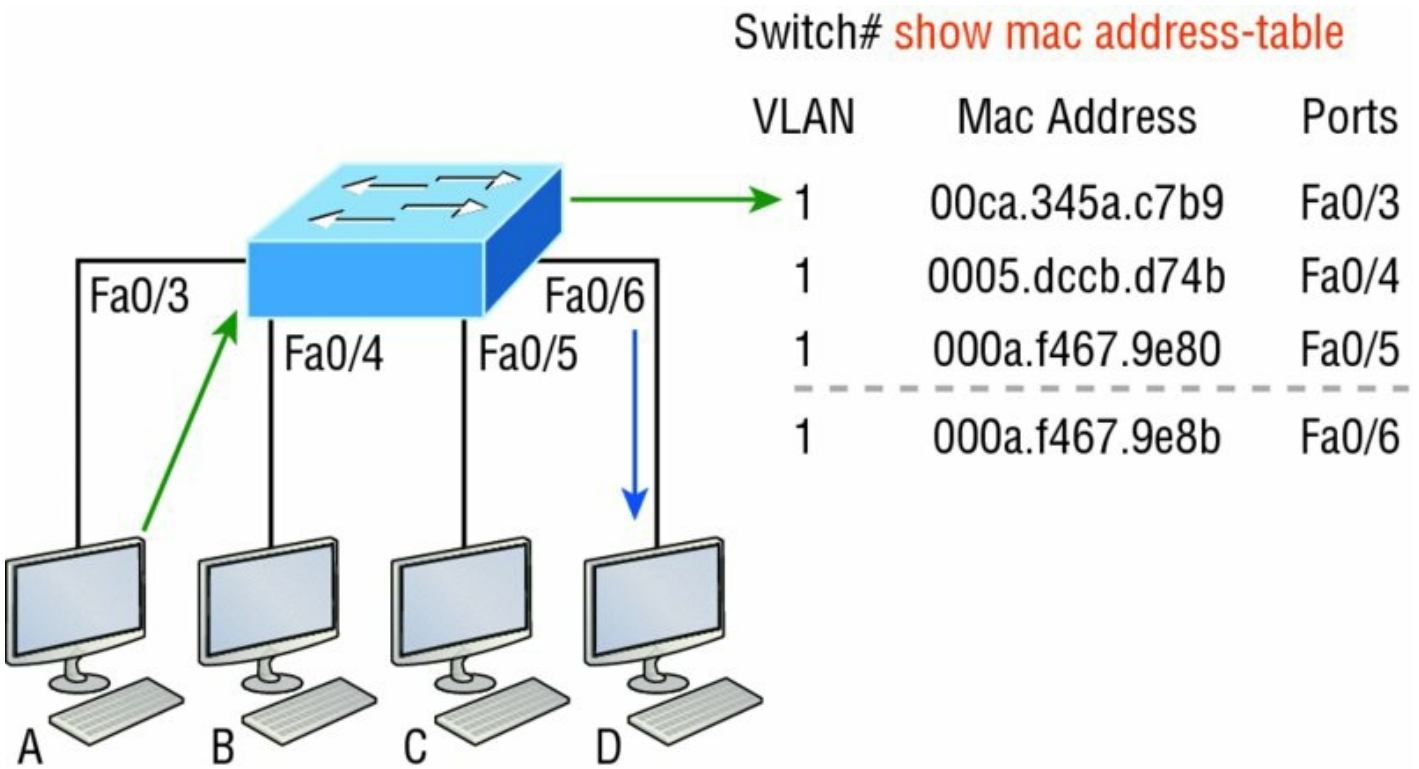


Figure 4: Forward/Filter table answer

Describe and verify switching concepts (contd.)

Loop Avoidance

- Redundant links between switches are important to have in place because they help prevent nasty network failures in the event that one link stops working.
- But they can also cause more problems than they solve! This is because frames can be flooded down all redundant links simultaneously, creating network loops as well as other evils.
- **Here's a list of some of the problems that can occur:**
  1. If no loop avoidance schemes are put in place, the switches will flood broadcasts endlessly throughout the inter-network. This is sometimes referred to as a **broadcast storm**.

Describe and verify switching concepts (contd.)

Loop Avoidance(contd.)

2. A device can receive multiple copies of the same frame because that frame can arrive from different segments at the same time.

3. The MAC address filter table could be totally confused about the source device's location because the switch can receive the frame from more than one link. Worse, the bewildered switch could get so caught up in constantly updating the MAC filter table with source hardware address locations that it will fail to forward a frame! This is called **thrashing** the MAC table.

4. One of the most vile events is when multiple loops propagate throughout a network. Loops can occur within other loops, and if a broadcast storm were to occur simultaneously, the network wouldn't be able to perform frame switching—period!

Describe and verify switching concepts (contd.)

Loop Avoidance(contd.)

- **Figure 5** illustrates how a broadcast can be propagated throughout the network. Observe how a frame is continually being flooded through the internetwork's physical network media.

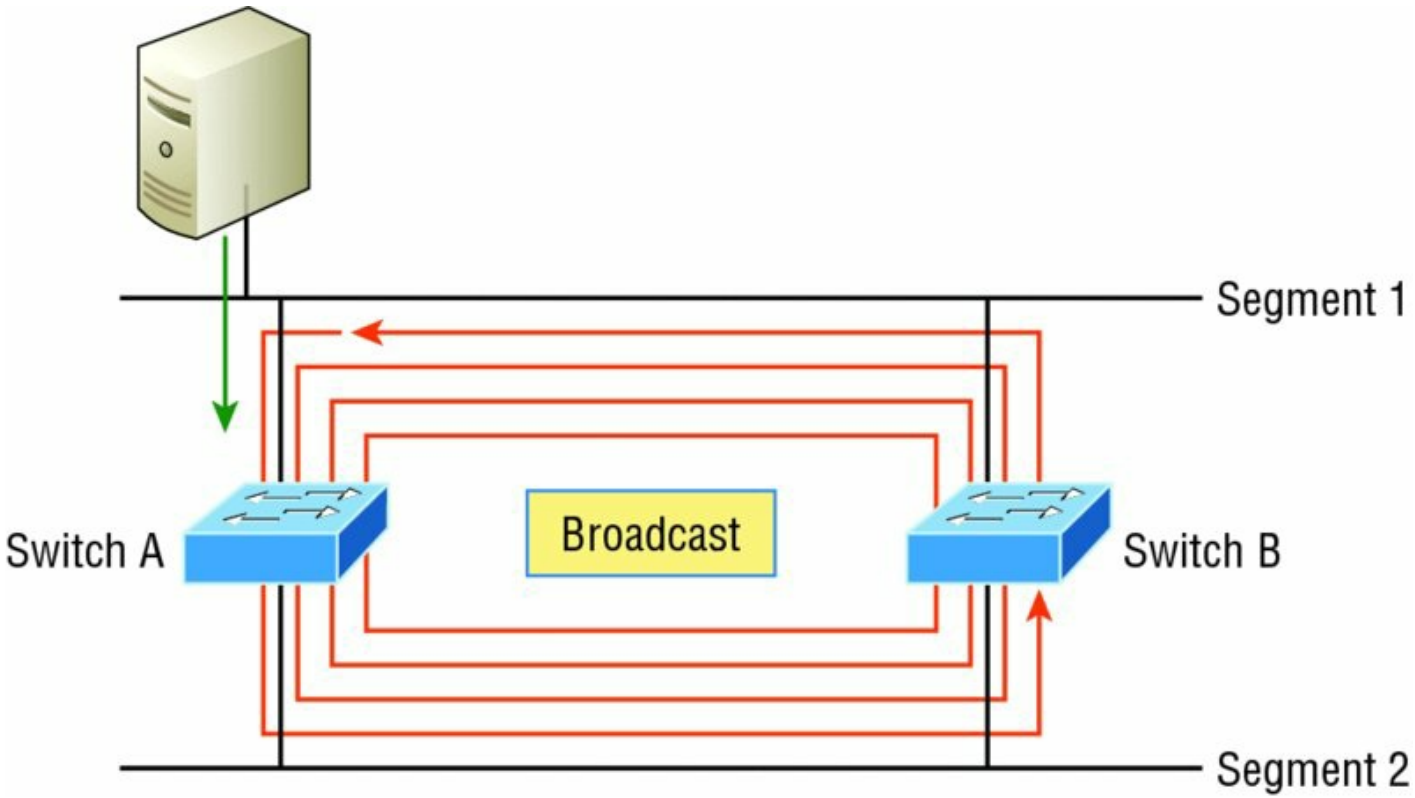


Figure 5: Broadcast Storm

Loop Avoidance(contd.)

1. **Figure 6** demonstrates how a whole bunch of frames can arrive from multiple segments simultaneously.

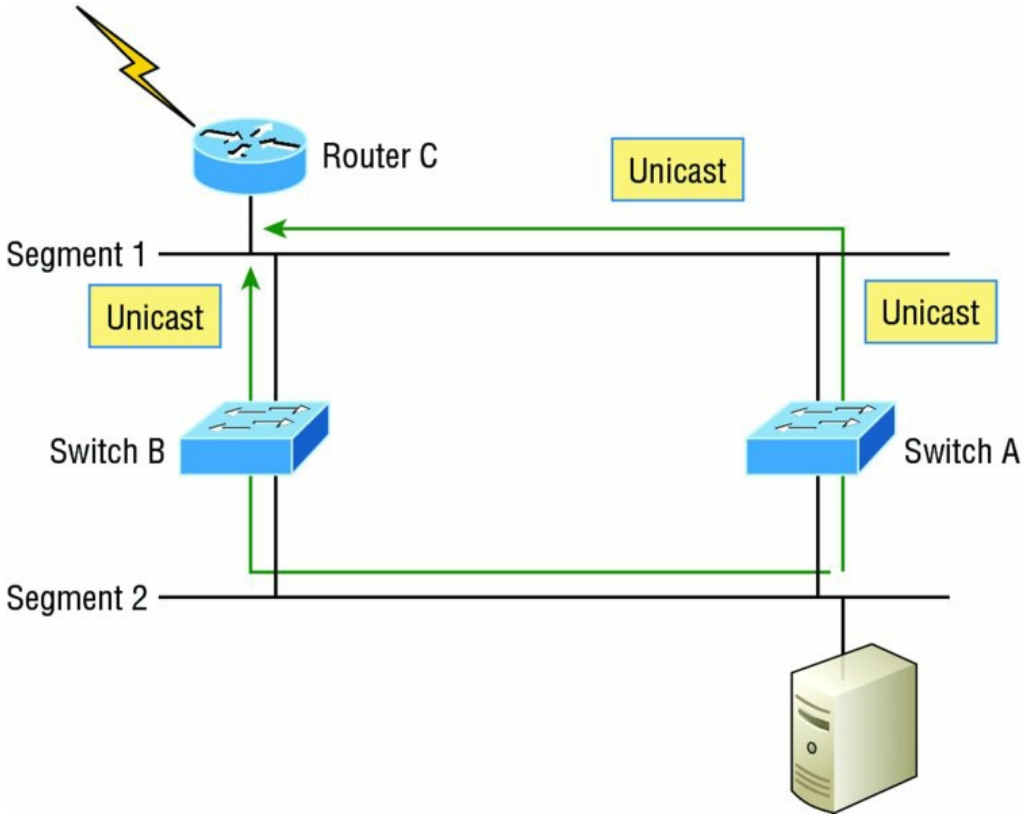


Figure 6: Multiple frame copies

Configure, verify, and troubleshoot port security

Port Security

- By using port security, you can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses.

- If you want to set up a switch port to allow only one host per port and make sure the port will shut down if this rule is violated, use the following commands like this:
  Switch(config-if)#switchport port-security maximum 1
  Switch(config-if)#switchport port-security violation shutdown

- Also with the **sticky command** you can provide static MAC address security without having to type in absolutely everyone's MAC address on the network.
  Switch(config-if)#switchport port-security mac-address sticky
  Switch(config-if)#switchport port-security maximum 2
  Switch(config-if)#switchport port-security violation shutdown

Configure, verify, and troubleshoot port security(contd.)

Port Security(contd.)

- This is all good, but you still need to balance your particular security needs with the time that implementing and managing them will realistically require.
- Always remember to shut down unused ports or assign them to an unused VLAN. All ports are enabled by default, so you need to make sure there's no access to unused switch ports!
- Here are your options for configuring port security:

Configure, verify, and troubleshoot port security(contd.)

Port Security(contd.)

```
Switch#config t
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
aging                Port-security aging commands
mac-address          Secure mac address
maximum              Max secure addresses
violation            Security violation mode
<cr>
```

Configure, verify, and troubleshoot port security (contd.)

Port Security(contd.)

You can configure the device to take one of the following actions when a security violation occurs by using the **switchport port-security** command:

- **Protect**: The protect violation mode drops packets with unknown source addresses until you remove enough secure MAC addresses to drop below the maximum value.
- **Restrict**: The restrict violation mode also drops packets with unknown source addresses until you remove enough secure MAC addresses to drop below the maximum value.
- **Shutdown**: Shutdown is the default violation mode. The shutdown violation mode puts the interface into an error-disabled state immediately. The entire port is shut down. To make the interface usable, you must perform a shut/no shut on the interface.

Configuring Catalyst Switches

Catalyst Switch Configuration

It's time to show you how to start up and configure a Cisco Catalyst switch(3850) using the command-line interface (CLI).
Here's a list of the basic tasks we'll be covering next:

- Administrative functions
- Configuring the IP address and subnet mask
- Setting the IP default gateway
- Setting port security
- Testing and verifying the network

Configuring Catalyst Switches(contd.)

Figure 7 shows a typical Cisco Catalyst switch.

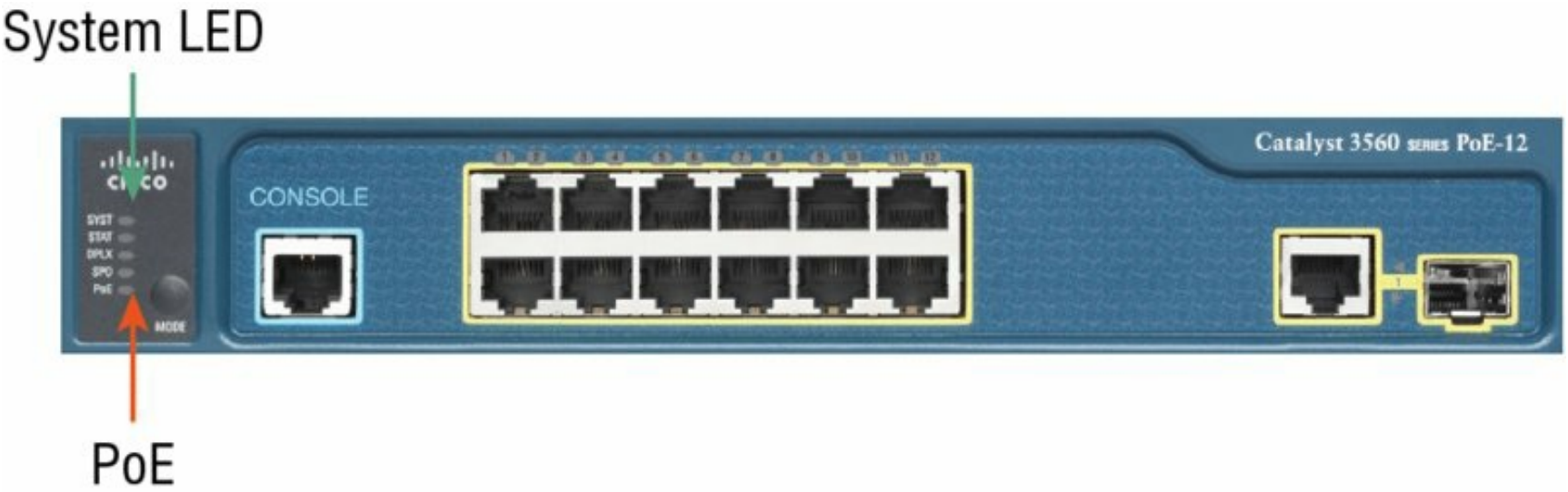


Figure 7: A Cisco Catalyst switch

Configuring Catalyst Switches(contd.)

- **Figure 8** shows the switched network.Now if we connect our switches to each other, as shown in Figure 8, remember that first we'll need a crossover cable between the switches.

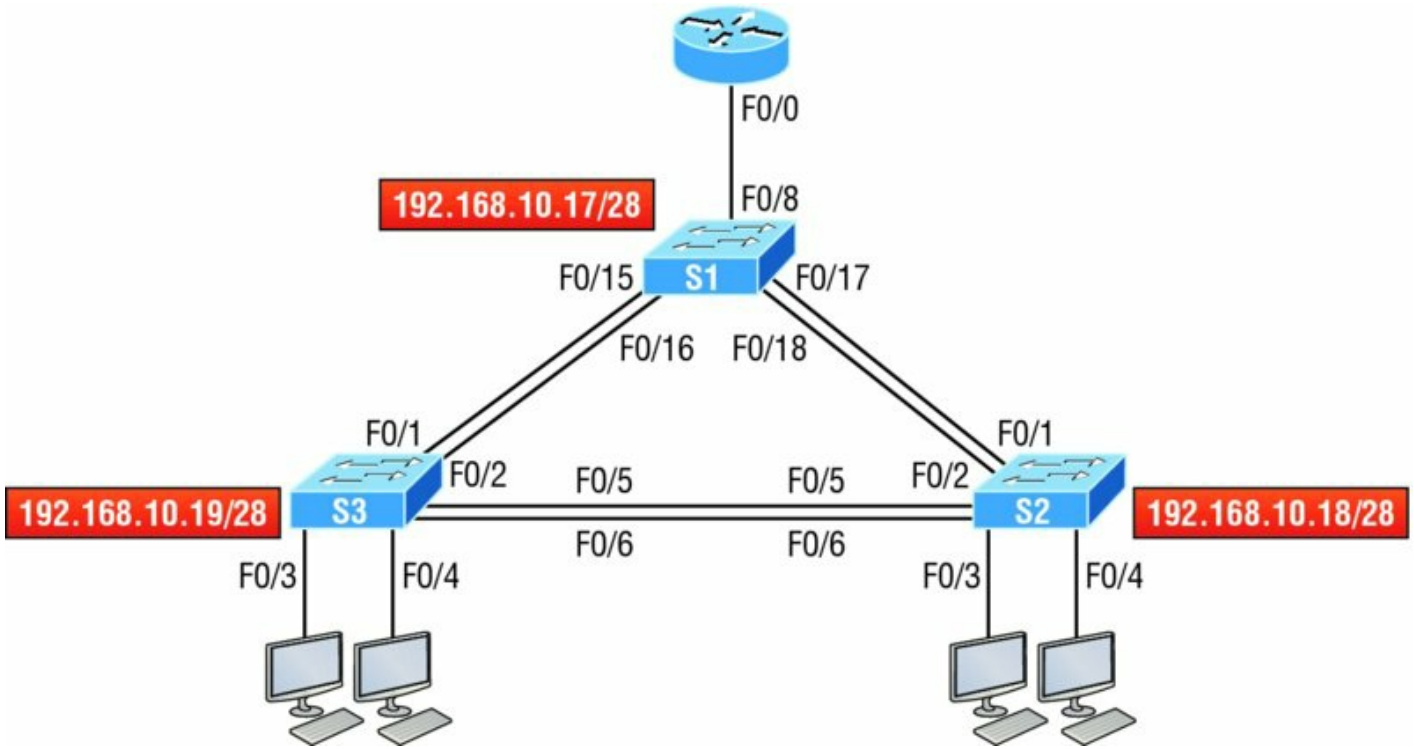


Figure 8: A Cisco Catalyst switch

Configuring Catalyst Switches(contd.)

- When you first connect the switch ports to each other, the link lights are amber and then turn green, indicating normal operation.
- **Do We Need to Put an IP Address on a Switch?**
  Absolutely not! Switches have all ports enabled and ready to rock. Take the switch out of the box, plug it in, and the switch starts learning MAC addresses in the CAM. So why would I need an IP address since switches are providing layer 2 services? Because you still need it for in-band management purposes! Telnet, SSH, SNMP, etc. all need an IP address in order to communicate with the switch through the network (in-band).
- Let's configure our switches now so you can watch how I configure the management interfaces on each switch.

Configuring Catalyst Switches(contd.)

- We're going to begin our configuration by connecting into each switch and setting the administrative functions. We'll also assign an IP address to each switch.

```
Switch>en
Switch#config t
Switch(config)#hostname S1
S1(config)#enable secret todd
S1(config)#int f0/15
S1(config-if)#description 1st connection to
S3 S1(config-if)#int f0/16
S1(config-if)#description 2nd connection to S3
S1(config-if)#int f0/17
S1(config-if)#description 1st connection to S2
S1(config-if)#int f0/18
```

Configuring Catalyst Switches(contd.)

```
S1(config-if)#description 2nd connection to S2
S1(config-if)#int f0/8
S1(config-if)#desc Connection to IVR
S1(config-if)#line con 0
S1(config-line)#password console
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password telnet
S1(config-line)#login
S1(config-line)#int vlan 1
S1(config-if)#ip address 192.168.10.17 255.255.255.240
S1(config-if)#no shut
S1(config-if)#exit
```

Configuring Catalyst Switches(contd.)

S1(config)#banner motd this is my S1 switch#
S1(config)#exit
S1#copy run start
Destination filename [startup-config]? [enter]
Building configuration... [OK]
S1#

- In the same way we will configure the **S2** and **S3** switch also.

Configuring Catalyst Switches(contd.)

- Now let's ping to S1 and S2 from the S3 switch and see what happens:

S3#**ping 192.168.10.17**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds: .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/9 ms
S3#**ping 192.168.10.18**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.18, timeout is 2 seconds: .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/9 ms
S3#**sh ip arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.10.17	0	001c.575e.c8c0	ARPA	Vlan1

Configuring Catalyst Switches (contd.)

Port Security

So let's set port security on our S3 switch now. Ports Fa0/3 and Fa0/4 will have only one device connected in our lab. By using port security, we're assured that no other device can connect once our hosts in ports Fa0/3 and in Fa0/4 are connected. Here's how to easily do that with just a couple commands:

S3**#config t**
S3(config)**#int range f0/3-4**
S3(config-if-range)**#switchport mode access**
S3(config-if-range)**#switchport port-security**
S3(config-if-range)**#do show port-security int f0/3**

Port Security	**: Enabled**
Port Status	**: Secure-down**
Violation Mode	**: Shutdown**
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled

Configuring Catalyst Switches (contd.)

Port Security (contd.)

Maximum MAC Addresses	**: 1**
Total MAC Addresses	: 0
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0000.0000.0000:0
Security Violation Count	: 0

Configuring Catalyst Switches (contd.)

Verifying Cisco Catalyst Switches

- To verify router and switches run this command:
  show running-config
  This command provide really great overview of each device.
- We can run other cammnad, to verify the IP address set on a switch, we can use the **show interface command:**
  S3**#sh int vlan 1**
- We can use this command to displays the forward filter table, also called a content addressable memory (CAM) table
  S3**#sh mac address-table**
- we can assign **Static MAC Addresses** via this command.
  S3(config)**#mac address-table ?**
  S3(config)**#mac address-table static aaaa.bbbb.cccc vlan 1 int fa0/7**
  S3(config)**#do show mac address-table**.

Practice Questions(contd.)

1. If a destination MAC address is not in the forward/filter table, what will the switch do with the frame?
2. What does the sticky keyword in the port-security command provide?
3. What command will show you the forward/filter table?
4. Write the command that would limit the number of MAC addresses allowed on a port to 2.
5. What are the three switch functions at layer 2?