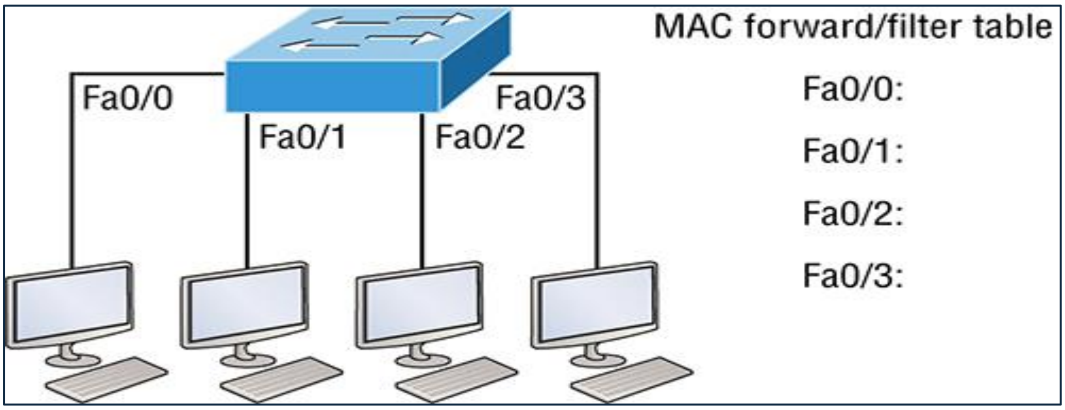
Switching Services

Bridges use software to create and manage a Content Addressable Memory (CAM) filter table. Layer 2 switches and bridges are faster than routers because they don't waste 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.

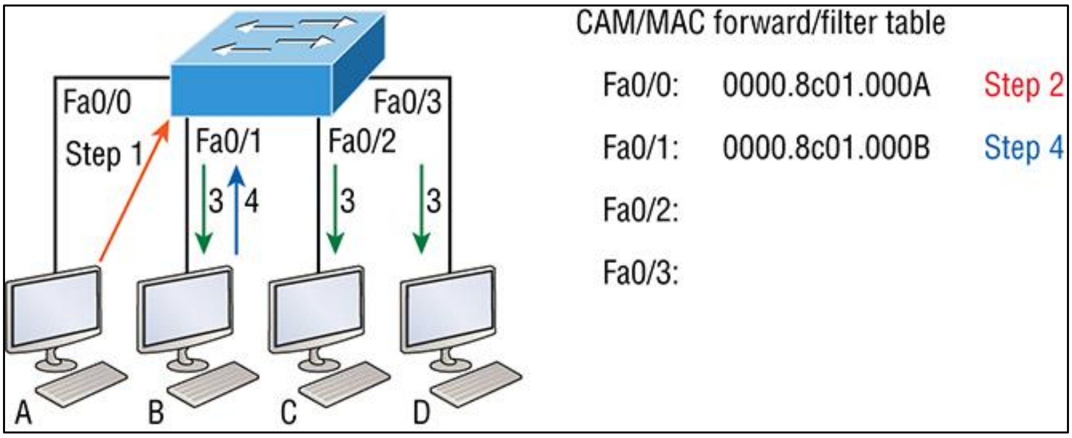
Three Switch Functions at Layer 2

There are three distinct functions of layer 2 switching you need to remember

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.



When a device transmits and an interface receives a frame, the switch places the frame's source address in the MAC forward/filter table, allowing it to refer to the precise interface the sending device is located on. The switch then has no choice but to flood the network with this frame out of every port except the source port because it has no idea where the destination device is actually located.


CAM/MAC forward/filter table
Fa0/0: 0000.8c01.000A Step 2
Fa0/1: 0000.8c01.000B Step 4
Fa0/2:
Fa0/3:
Fa0/0
Step 1
Fa0/1
Fa0/2
Fa0/3
3
4
3
3
A
B
C
D

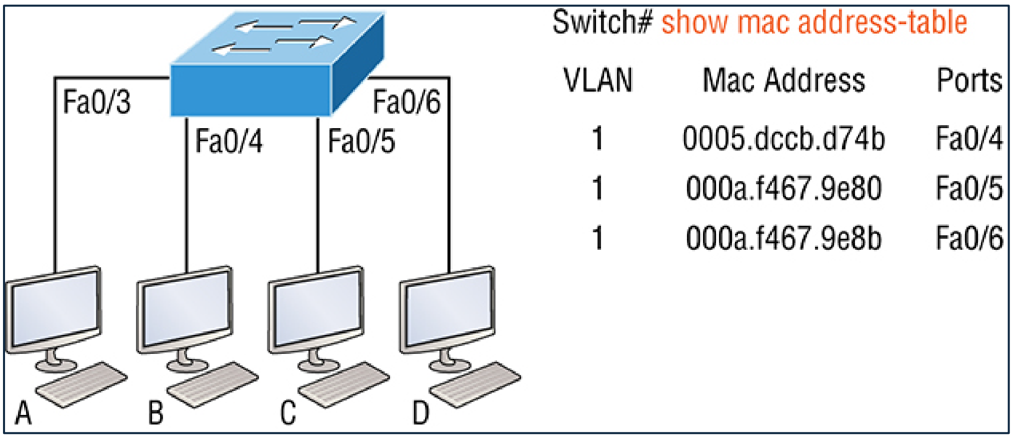
1. Host A sends a frame to Host B. Host A's MAC address is 0000.8c01.000A; Host B's MAC address is 0000.8c01.000B.
2. The switch receives the frame on the Fa0/0 interface and places the source address in the MAC address table.
3. Since the destination address isn't in the MAC database, the frame is forwarded 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.

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.

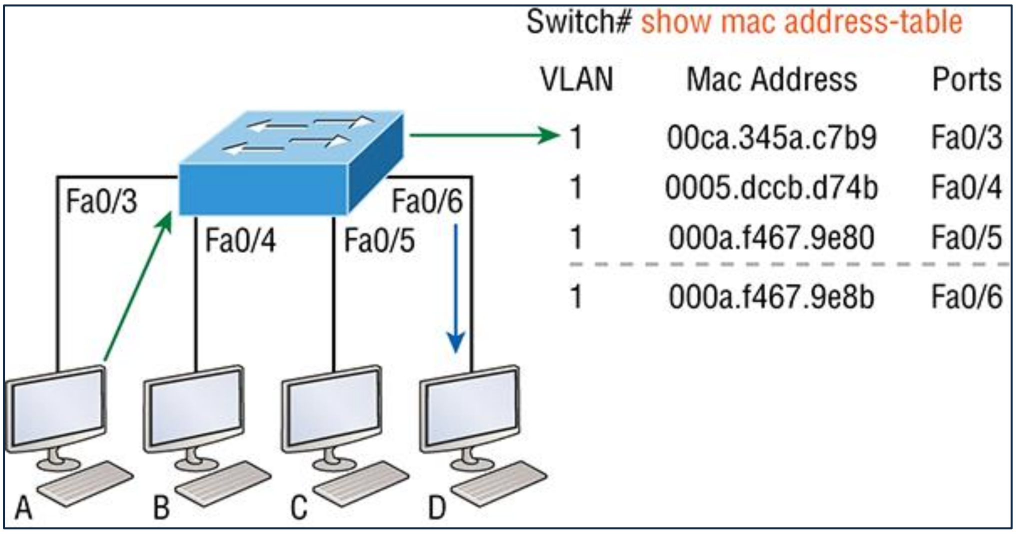
When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is only sent out of the appropriate exit interface. The switch won't transmit the frame out any interface except for the destination interface, which preserves bandwidth on the other network segments. This process is called frame filtering.

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. Remember, the switch creates smaller collision domains, but it's always still one large broadcast domain by default.

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
```



```
Switch# show mac address-table
 VLAN    Mac Address       Ports
  1      00ca.345a.c7b9    Fa0/3
  1      0005.dccb.d74b    Fa0/4
  1      000a.f467.9e80    Fa0/5
 - - - - - - - - - - - - - - - - -
  1      000a.f467.9e8b    Fa0/6
```

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. It's important to remember that the source MAC is always checked first to make sure it's in the CAM table. After that, if Host D's MAC address wasn't found in the forward/filter table, the switch would've flooded the frame out all ports except for port Fa0/3 because that's the specific port the frame was received on.

Now let's take a look at the output that results from using a `show mac address-table` command:

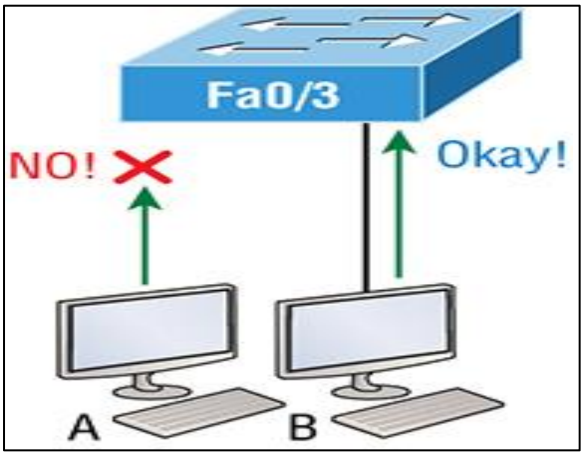
```
Switch#sh mac address-table
Vlan Mac Address Type Ports]]> ---- ----------- -------- -----
1 0005.dccb.d74b DYNAMIC Fa0/1
1 000a.f467.9e80 DYNAMIC Fa0/3
1 000a.f467.9e8b DYNAMIC Fa0/4
1 000a.f467.9e8c DYNAMIC Fa0/3
1 0010.7b7f.c2b0 DYNAMIC Fa0/3
1 0030.80dc.460b DYNAMIC Fa0/3
1 0030.9492.a5dd DYNAMIC Fa0/1
1 00d0.58ad.05f4 DYNAMIC Fa0/1
```

Now, let's say the preceding switch received a frame with the following MAC addresses:

Source MAC: **0005.dccb.d74b**

Destination MAC: **000a.f467.9e8c**

Port Security



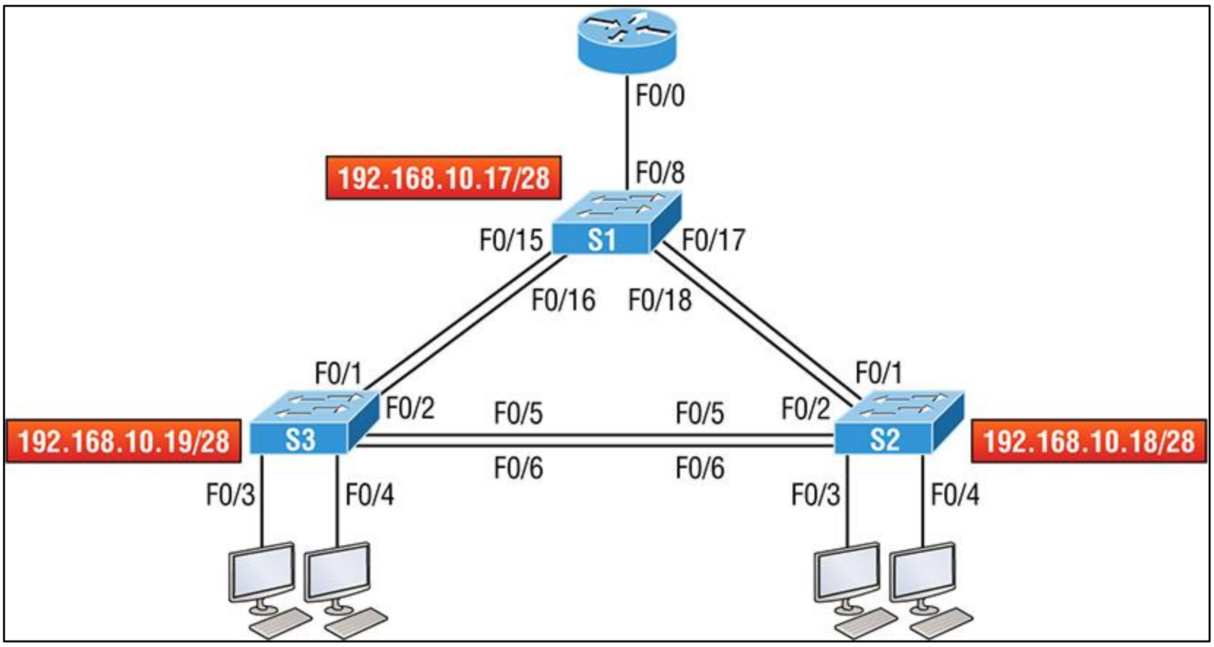
Port Fa0/3 is configured to observe and allow only certain MAC addresses to associate with the specific port. So in this example, Host A is denied access, but Host B is allowed to associate with the port. By using port security, you can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses.

Here are your options for configuring port security:

```
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>
```

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

Configuring Catalyst Switches



Let’s configure our switches now.

S1

We’re going to begin by connecting into each switch and setting the administrative functions. We’ll also assign an IP address to each switch. Let’s use a simple IP scheme like 192.168.10.16/28. This mask should be familiar to you! Check out the following output:

```
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
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
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#
```

The first thing to notice here is that there’s no IP address configured on the switch’s physical interfaces. Since all ports on a switch are enabled by default, there’s not really a whole lot to configure. The IP address is configured under a logical interface, called a management domain or VLAN. You can use the default VLAN 1 to manage a switched network just as we're doing here, but you can opt to use a different VLAN for management.

The rest of the configuration is basically the same as the process you go through for router configuration. So remember… no IP addresses on physical switch interfaces, no routing protocols, and so on. We're performing layer 2 switching at this point, not routing!

S2

Here is the S2 configuration:

```
Switch#config t
Switch(config)#hostname S2
S2(config)#enable secret todd
S2(config)#int f0/1
S2(config-if)#desc 1st connection to S1
S2(config-if)#int f0/2
S2(config-if)#desc 2nd connection to s1
S2(config-if)#int f0/5
S2(config-if)#desc 1st connection to S3
S2(config-if)#int f0/6
S2(config-if)#desc 2nd connection to s3
S2(config-if)#line con 0
S2(config-line)#password console
S2(config-line)#login
S2(config-line)#line vty 0 15
S2(config-line)#password telnet
S2(config-line)#login
S2(config-line)#int vlan 1
S2(config-if)#ip address 192.168.10.18 255.255.255.240
S2(config)#exit
S2#copy run start
Destination filename [startup-config]?[enter]
Building configuration...
[OK]
S2#
```

```
S2#ping 192.168.10.17
```

S3

Check out the S3 switch configuration:

```
Switch>en
```

```
Switch#config t
SW-3(config)#hostname S3
S3(config)#enable secret todd
S3(config)#int f0/1
S3(config-if)#desc 1st connection to S1
S3(config-if)#int f0/2
S3(config-if)#desc 2nd connection to S1
S3(config-if)#int f0/5
S3(config-if)#desc 1st connection to S2
S3(config-if)#int f0/6
S3(config-if)#desc 2nd connection to S2
S3(config-if)#line con 0
S3(config-line)#password console
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password telnet
S3(config-line)#login
S3(config-line)#int vlan 1
S3(config-if)#ip address 192.168.10.19 255.255.255.240
S3(config-if)#no shut
S3(config-if)#banner motd #This is the S3 switch#
S3(config)#exit
S3#copy run start
Destination filename [startup-config]?[enter]
Building configuration...
[OK]
S3#
```

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
Internet 192.168.10.18 0 b414.89d9.18c0 ARPA Vlan1
Internet 192.168.10.19 - ecc8.8202.82c0 ARPA Vlan1
S3#
```

There's one more command you need to know about, even though we don't really need it in our current network because we don't have a router involved yet. It's the `ip default-gateway` command. If you want to manage your switches from outside your LAN, you must set a default gateway on the switches just as you would with a host, and you do this from global config.

```
S3#config t
S3(config)#ip default-gateway 192.168.10.30
```

Port Security

A secured switch port can associate anywhere from 1 to 8,192 MAC addresses. 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 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
```

The first command sets the mode of the ports to “access” ports. These ports must be access or trunk ports to enable port security. By using the command `switchport port-security` on the interface, we enable port security with a maximum MAC address of 1 and violation of shutdown. These are the defaults, and you can see them in the highlighted output of the show port-security int `f0/3` command in the preceding code.

Port security is enabled, as displayed on the first line, but the second line shows `Secure-down` because I haven’t connected my hosts into the ports yet. Once we do, the status will show `Secure-up` and would become `Secure-shutdown` if a violation occurs.

It’s very important to remember that you can set parameters for port security but it won’t work until you enable port security at the interface level. Notice the output for port `F0/6`:

```
S3#config t
S3(config)#int range f0/6
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport port-security violation
restrict
S3(config-if-range)#do show port-security int f0/6
Port Security : Disabled
Port Status : Secure-up
Violation Mode : restrict
```

Port `Fa0/6` has been configured with a violation of restrict, but the first line shows that port security has not been enabled on the port yet. Remember, you must use this command at interface level to enable port security on a port:

```
S3(config-if-range)#switchport port-security
```

There are two other modes you can use instead of just shutting down the port. The restrict and protect modes mean that another host can connect up to the maximum MAC addresses allowed, but after the maximum has been met, all frames will just be dropped and the port won’t be shut down.

Both the restrict and shutdown violation modes alert you via SNMP that a violation has occurred on a port.

```
S3#sh port-security int f0/3
Port Security : EnabledPort Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 2
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0013:0ca69:00bb3:00ba8:1
Security Violation Count : 1
```

Here you can see that the port is in Secure-shutdown mode and the light for the port would be amber. To enable the port again, you'd need to do this:

```
S3(config-if)#shutdown
S3(config-if)#no shutdown
```

Verifying Cisco Catalyst Switches

```
S3#sh int vlan 1
Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is ecc8.8202.82c0 (bia
ecc8.8202.82c0)
Internet address is 192.168.10.19/28
```

```
S3#sh mac address-table
```

```
S2#sh mac address-table
```

Assigning Static MAC Addresses

You can set a static MAC address in the MAC address table, but like setting static MAC port security without the sticky command, it's a ton of work. Just in case you want to do it, here's how:

```
S3(config)#mac address-table ?
aging-time Set MAC address table entry maximum age
```

```
learning Enable MAC table learning feature
move Move keyword
notification Enable/Disable MAC Notification on the switch
static static keyword
S3(config)#mac address-table static aaaa.bbbb.cccc vlan 1 int fa0/7
S3(config)#do show mac address-table
Mac Address Table]]> ------------------------------------------
```