WILEY

SYBEX
A Wiley Brand

CCENT Study Guide

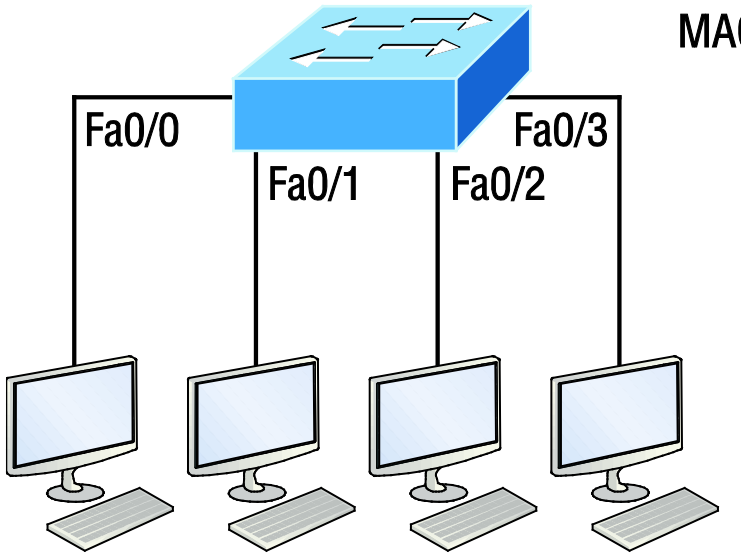
Chapter 10

Layer 2 Switching

Chapter 10 Objectives

- The CCENT Topics Covered in this chapter include:
- **2.0 LAN Switching Technologies**
- 2.1 Describe and verify switching concepts.
- 2.1.a MAC learning and aging
- 2.1.b Frame switching
- 2.1.c Frame flooding
- 2.1.d MAC address table
- 2.7 Configure, verify, and troubleshoot port security.
- 2.7.a Static
- 2.7.b Dynamic
- 2.7.c Sticky
- 2.7.d Max MAC addresses
- 2.7.e Violation actions
- 2.7.f Err-disable recovery

Figure 10.1: Empty forward/filter table on a switch



MAC forward/filter table

Fa0/0:

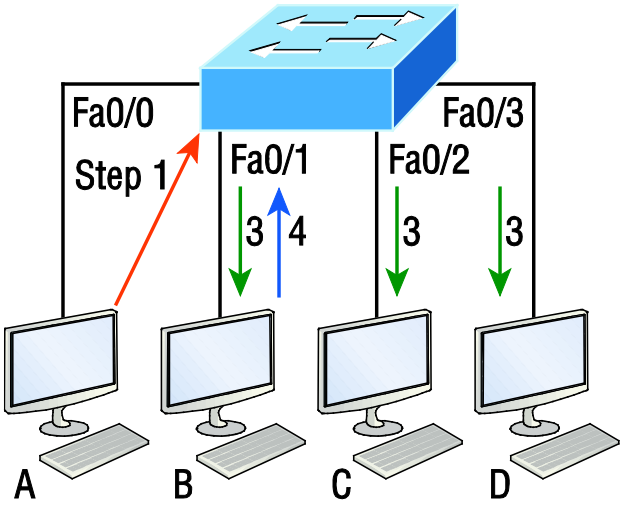
Fa0/1:

Fa0/2:

Fa0/3:

When a switch is first powered on, the MAC forward/filter table (CAM) is empty.

Figure 10.2: How switches learn hosts' locations



CAM/MAC forward/filter table

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

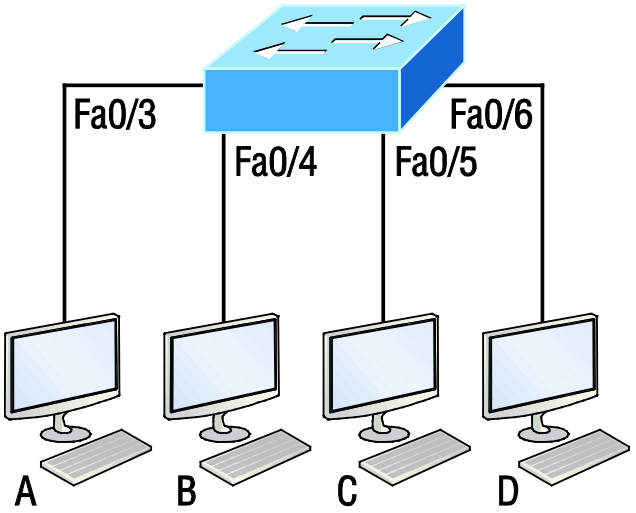
In this figure, you can see four hosts attached to a switch. When the switch is powered on, it has nothing in its MAC address forward/filter table.

Figure 10.2: How switches learn hosts' locations

Let me give you an example of how a forward/filter table is populated using Figure 10.2:

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 two, 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.

Figure 10.3: Forward/filter table

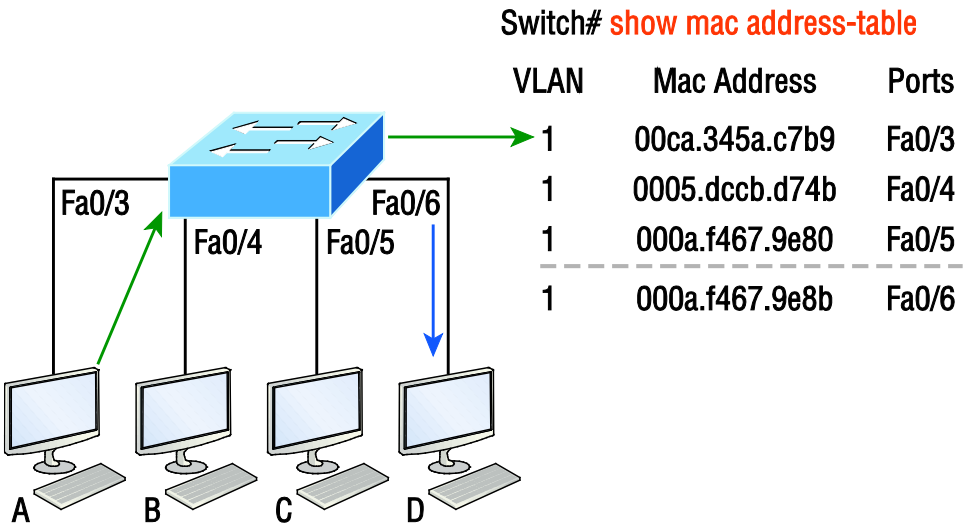


Switch# show mac address-table

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

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?

Figure 10.4: Forward/filter table 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 10.5: “Port security” on a switch port restricts port access by MAC address

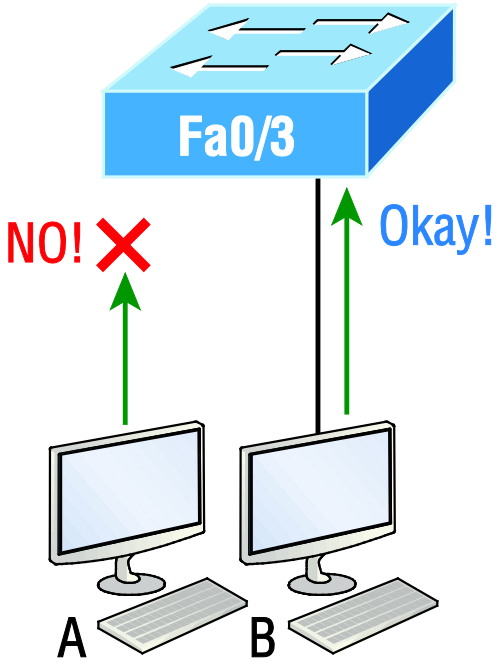


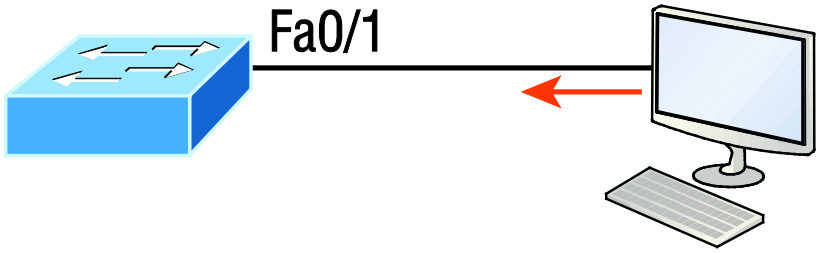
Figure 10.5 shows two hosts connected to the single switch port Fa0/3 via either a hub or access point (AP). Port Fa0/3 is configured to observe and allow only certain MAC addresses to associate with the specific port, so in this example, Host A is denied access, but Host B is allowed to associate with the port.

Port Security

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>
```

Figure 10.6: Protecting a PC in a lobby



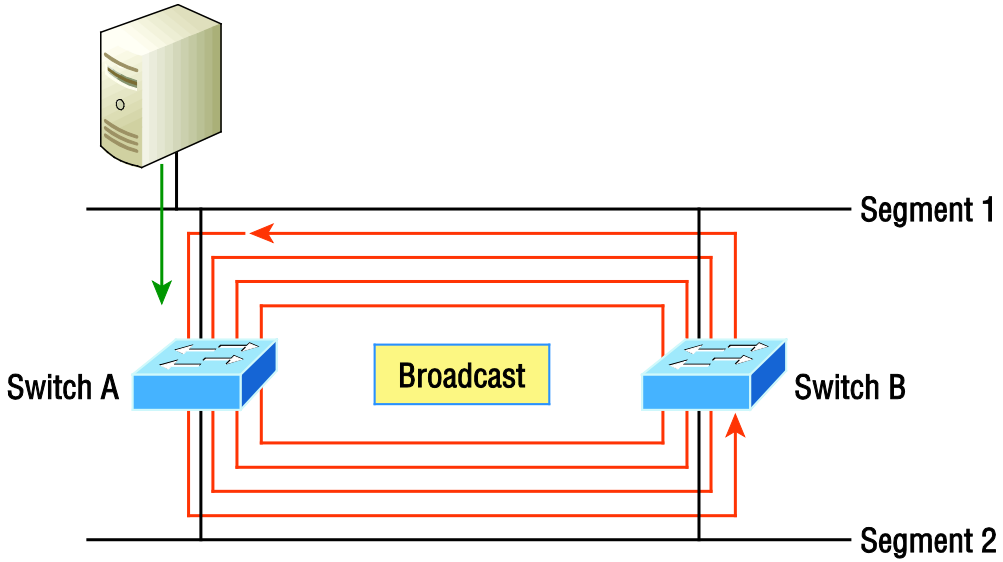
What can you do to ensure that only the MAC address of the lobby PC is allowed by switch port Fa0/1?

The solution is pretty straightforward because in this case, the defaults for port security will work well. All I have left to do is add a static MAC entry:

```
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address aa.bb.cc.dd.ee.ff
```

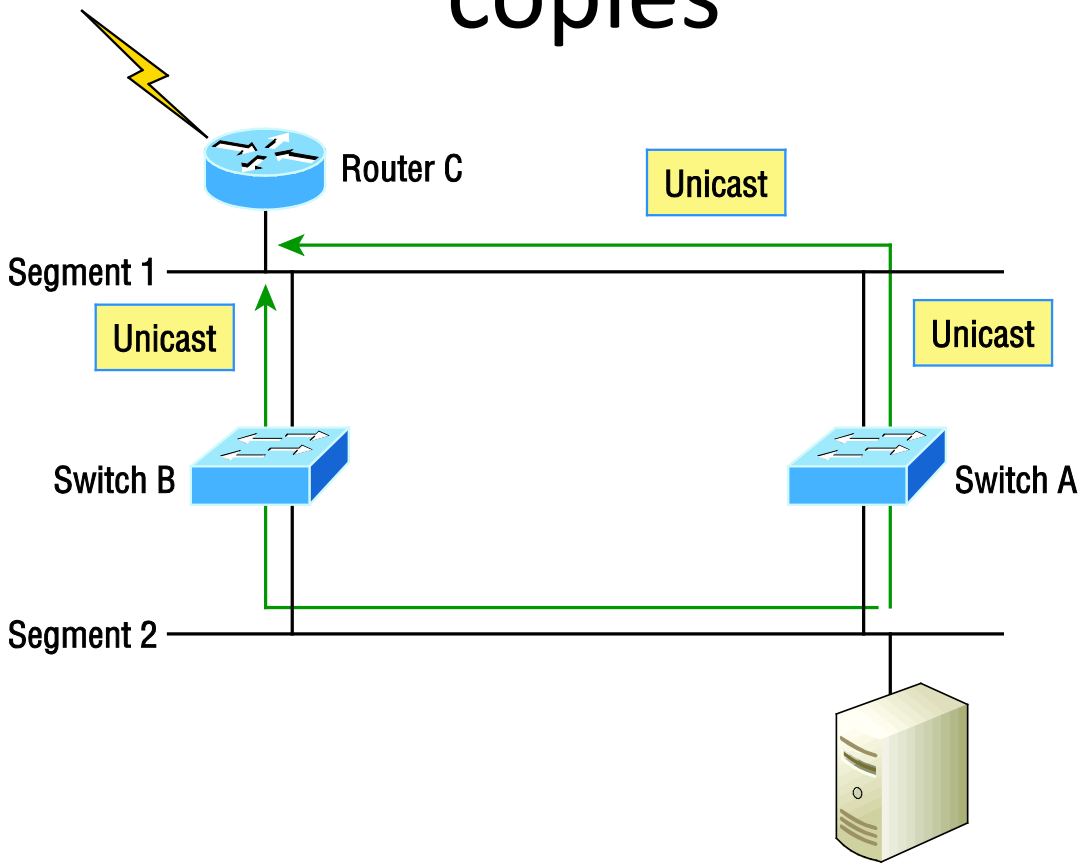
Figure 10.7: Broadcast storm

Redundant links between switches are important to have in place because they help prevent nasty network failures in the event one link stops working.



If no loop avoidance schemes are put in place, the switches will flood broadcasts endlessly throughout the internetwork. This is sometimes referred to as a *broadcast storm*.

Figure 10.8: Multiple frame copies



A device can receive multiple copies of the same frame because that frame can arrive from different segments at the same time. Figure 10.8 demonstrates how a whole bunch of frames can arrive from multiple segments simultaneously. The server in the figure sends a unicast frame to Router C.

SYBEX
A Wiley Brand

Figure 10.9: A Cisco Catalyst switch

WILEY

```
Switch>en
Switch#config t
Switch(config)#hostname S1
S1(config)#enable secret todd
S1(config)#int f0/1
S1(config-if)#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]
```

Verifying IOS Switches

- Show mac address-table
- Show interface vlan 1
- Show ip interface brief

Written Labs and Review Questions

- Read through the Exam Essentials section together in class.
- Open your books and go through all the written labs and the review questions.
- Review the answers in class.