Switching Concepts

The primary purpose of a switch is to make forwarding decisions based on destination MAC address. The MAC address table is created with a list of destination MAC address for each connected device. In addition the switch port assigned and VLAN membership. The Gigabit Ethernet ports are full-duplex that define a single collision domain per switch port.

The following is a list of network services provided by switches:

- Switches only read Ethernet frame header and forward traffic.
- Switches create and maintain the MAC address table.
- Switches create separate collision domains per Gigabit port.
- Switches create separate broadcast domains per VLAN.

The Gigabit Ethernet (or faster) switch port supports full-duplex traffic between the host and network switch. That eliminates collisions and creates a collision domain per port. The fact that there are no collisions increases data rate and decreases network latency for host connections.

Microsegmentation

Gigabit Ethernet switch port interfaces enable both full-duplex operation and microsegmentation. That eliminates collisions on the switch port and dedicates all port bandwidth to the connected host. CSMA/CD is a method for detecting Ethernet collisions on older hubs and bridges. It is no longer required with full-duplex switch ports.

VLAN creates a broadcast domain that is defined by assigning switch port/s to the same VLAN. All hosts connected to assigned switch ports are part of the same broadcast domain. Creating multiple VLANs will then define multiple broadcast domains. Switches do not forward broadcast or multicast traffic between VLANs minimizing bandwidth utilization.

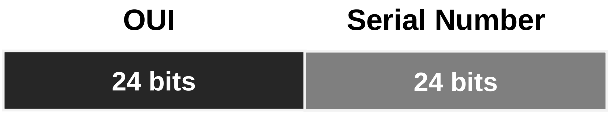
MAC Address Table

Every Ethernet network interface is assigned a unique manufacturer assigned physical hardware address called a MAC address. In addition, there is a MAC address assigned to all network devices. The MAC address provides a unique Layer 2 identifier. That enables communication between devices of the same or different VLAN. The switch forwards frames based on the MAC address and assigned port.

- Enable data forwarding between hosts in the same VLAN.
- Unique identifier associated with a network device or interface.

MAC (physical) address is 48 bits of hexadecimal numbers. The first 24 bits is a manufacturer OUI and the last 24 bits is a unique serial number (SN). There is a base MAC address assigned to each network device and unique MAC address per Ethernet interface.

Figure 1 MAC Physical Address



0000.ab + cd.1234 = 0000.abcd.1234

The switch builds a MAC address table comprised of MAC address, switch port and VLAN membership for each connected host. The switch creates a separate MAC address table for each configured VLAN. Any unicast flooding of a frame to learn a MAC address is for the assigned VLAN only. The following IOS show command will list the contents of the MAC address table for a switch. Where there are multiple VLANs configured, the switch will list all MAC address tables for all VLANs in a single table listing.

```
switch# show mac address-table
```

MAC Address Lookup

All hosts and network devices have MAC addressing that is used for Layer 2 connectivity. Each data message contains a frame with both source and destination MAC address. The host sending data is the source MAC address. The destination MAC address is the Layer 3 next hop. The switch builds a MAC address table with MAC addresses, assigned switch port and VLAN membership.

Layer 2 network switches does not rewrite the frame header MAC addressing. It examines the source MAC address and destination MAC address. The source MAC address and associated port is added to the MAC address table if it isn’t listed. The switch then does a lookup of the destination MAC address.in the MAC address table to makes a forwarding decision. The frame is forwarded out the switch port associated with the destination MAC address.

Broadcast Frame

The host first sends an ARP request packet to learn the MAC address of a server. That occurs whether they are assigned to the same VLAN or different VLAN (subnet). ARP broadcast frame is forwarded by switch out all ports to learn the MAC address of default gateway. This only occurs when the host has first started and there is no entry in host ARP table. The switch forwards broadcast frame with destination MAC address **FFFF:FFFF:FFFF** out all ports and eventually arrives at default gateway (router or L3 switch). The router responds to host with the MAC address of LAN interface (default gateway). The host then creates an IP packet with destination IP address of server and frame with MAC address of default gateway.

From there, router will send a proxy ARP broadcast on network to learn MAC address of a server on a remote subnet. ARP response is sent from server with MAC address to router that forwards onto host. All ARP tables are updated per Layer 3 hop between source and destination.

MAC Learning and Aging

MAC address learning occurs when the destination MAC address is not in the MAC address table. MAC learning is triggered as well when the aging time expires for an address. The switch removes MAC address table entries every 300 seconds as a default. Configuring the MAC aging timer to zero disables aging of MAC addresses. The switch will unicast flood (duplicate) a frame that has an unknown destination MAC address, to all ports except inbound port where frame was learned. This occurs when a MAC address has been flushed from table via aging timer.

MAC Flooding

The purpose of flooding is to learn the MAC address of a destination server that is not in the MAC address table. The switch will flood or duplicate the frame out all ports except where the frame was learned. Anything connected to the switch will read the frame destination MAC address and will drop it unless there is a match. The server for example, with the requested MAC address will respond to switch that updates the MAC address table.

The host sends packets with an IP header encapsulated in a frame. The source and destination IP address are required for end-to-end connectivity. Layer 2 switch does not examine or understand IP addressing. They can only examine Layer 2 frame within a data message for source and destination MAC address.

The following explains what happens when a host sends data to a server for an already established network session.

1. The switch adds the source MAC address of the incoming frame if it is not listed in the MAC address table. That is a destination MAC address for any frames destined for that host. This is how the MAC address table is initially populated.

2. The switch does a MAC address table lookup for the server destination MAC address and forwarding port. The packet is forwarded to router if server is on a different subnet than the host.

3. The switch floods the frame out of all switch ports except the port where the source MAC address was learned. **This only occurs when the destination MAC address is no longer in the MAC address table**.

4. The local server with the matching destination MAC address responds to the switch with a frame that has server MAC address.

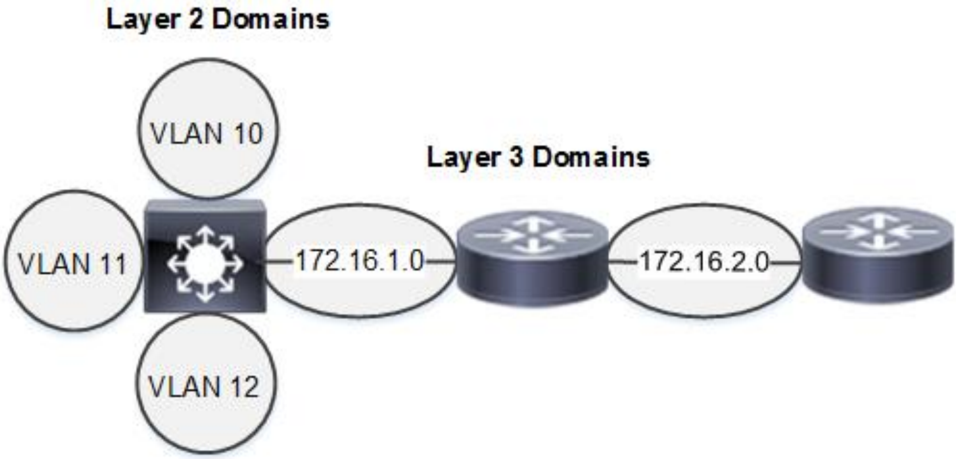
5. The default gateway would respond to switch with server MAC address from an ARP table lookup, if the server is on a remote subnet.

6. The switch then updates MAC address table with MAC address of server and forwarding port.

Broadcast Domain

The VLAN creates a broadcast domain that is defined by assigning switch port/s to the same VLAN. All hosts connected to switch ports of the same VLAN are part of the same broadcast domain. Creating multiple VLANs defines multiple broadcast domains. Switches do not forward broadcast or multicast traffic between VLANs minimizing bandwidth utilization compared with hubs and bridges. The switch only forwards unicasts, broadcasts and multicasts on the same segment (VLAN).

Figure 2 Layer 2 and Layer 3 Broadcast Domains



Cut-Through Switching

This switching technique optimizes performance by examining only the first six bytes (destination MAC address) of an Ethernet frame before making a forwarding decision. The switch does a MAC address table lookup for the destination MAC address and forwards the frame. The advantage is forwarding decision is made before all of the frame arrives and thereby minimizes latency.

Store-and-Forward Switching

The store-and-forward method is traditional switching where the frame is not forwarded until all of the frame has arrived. The switch copies the frame to memory before examining the destination MAC address.

Cisco Express Forwarding (CEF)

CEF is a layer 3 switching technique that creates FIB and adjacency tables for optimized forwarding. It is only available on routers and switch platforms with routing enabled and the required hardware.

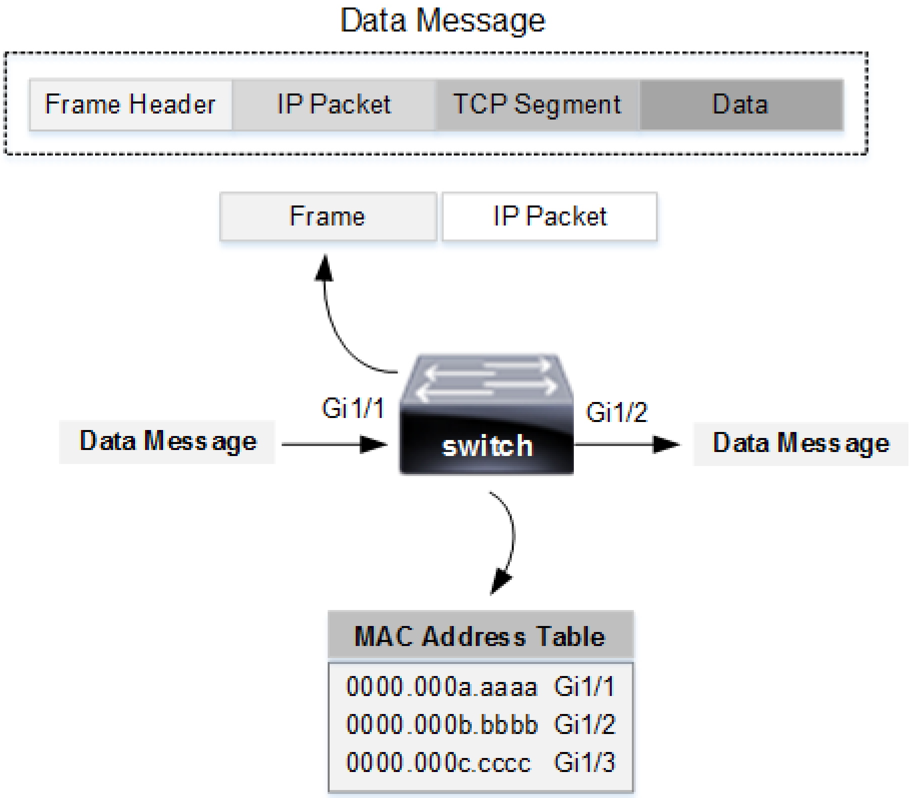
Table 1 Network Broadcasts

Broadcast Type	Destination Address	Examples
Layer 2	FFFF.FFFF.FFFF	ARP requests
Layer 3	255.255.255.255	DHCP, subnet only
Multicast	Reserved IP address	CDP, routing protocols

Frame Switching

Layer 2 switches only read the frame header within a data message to make a forwarding decision.

Figure 3 Frame Switching Operation



The switch examines the frame header for the destination MAC address and does a MAC address table lookup to make a forwarding decision. The frame is then forwarded out the switch port associated with the destination MAC address where the host is connected.

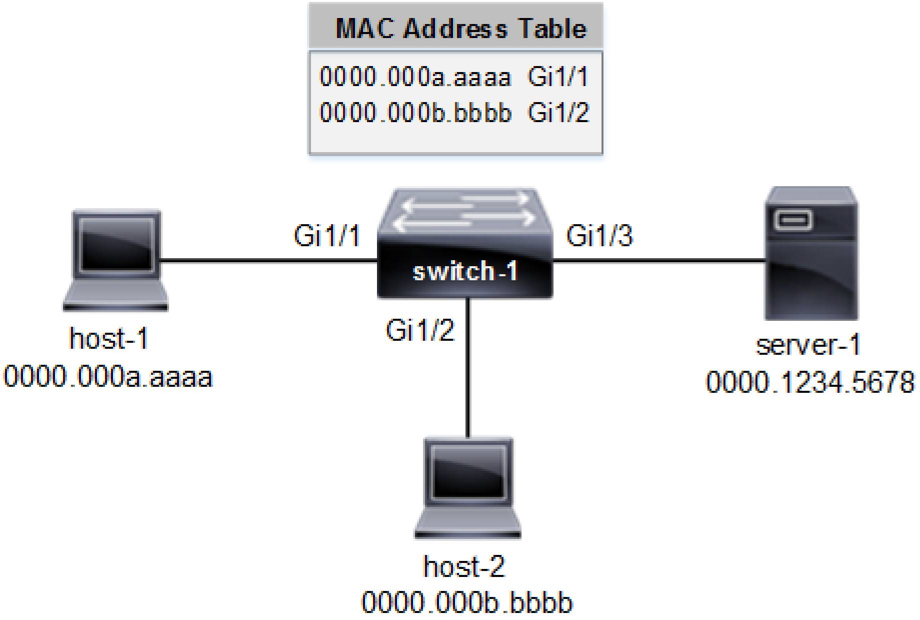
- Switches use MAC address in a frame to make forwarding decisions.
- Switches forward frames and do not frame rewrite MAC addressing.

Switches and access points make forwarding decisions based on the destination MAC address in a frame. They do not rewrite MAC addressing in the frame header. **It is only routers, Layer 3 switches and wireless controllers that do frame rewrite.** Wireless access points are essentially bridges that examine source and destination MAC address. The source MAC address of incoming frame is added to the MAC address table if it is not listed.

Frame Switching: Example 1

Refer to the network drawing where host-1 is sending data to server-1. The destination MAC address is not in the MAC address table (unknown). The switch will unicast flood (learning) the frame out all ports except the port where the frame was learned from (Gi1/1).

Figure 4 Frame Switching Example 1



Server-1 with the matching destination MAC address receives the frame and sends a frame to switch-1. The switch then updates MAC address table with the MAC address of server-1 and associated port (Gi1/3).

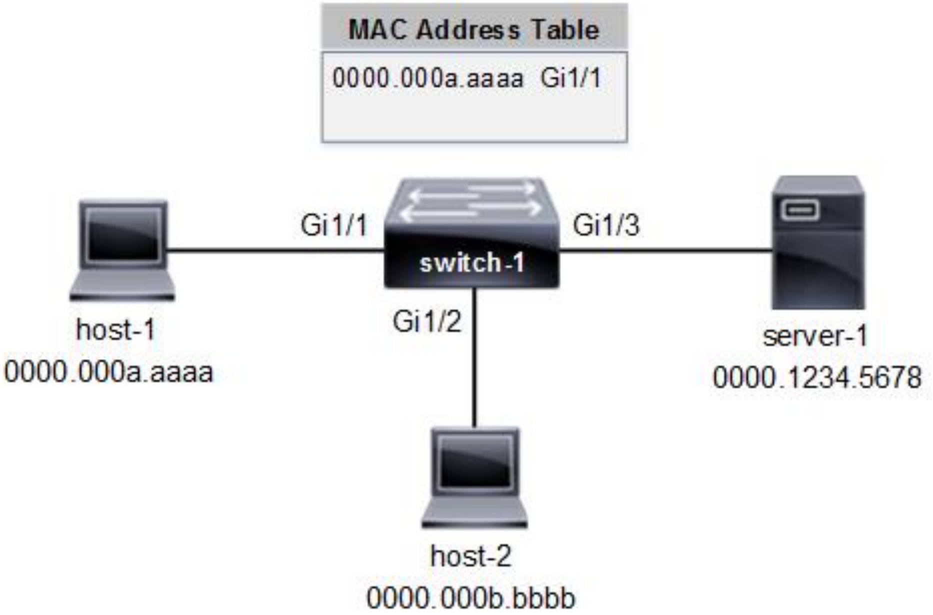
Frame Switching: Example 2

Refer to the drawing where host-2 sends data to server-1. The switch will examine the source and destination MAC address of the frame arriving on port Gi1/2 from host-2. The MAC address table has no entry for either source or destination MAC address. The switch then adds the source MAC address (host-2) to the MAC table. In addition the switch will unicast flood (MAC learning) a frame out all ports except the port where the frame was learned (Gi1/2). That broadcast frame contains only a destination MAC address.

Server-1 with the matching destination MAC address receives the frame and sends a reply frame to the switch. The switch updates the MAC address table with the MAC address of server-1.

- 0000.000b.bbbb will be added to the MAC address table.
- Frame is forwarded out all active switch ports except port Gi1/2.

Figure 5 Frame Switching Example 2



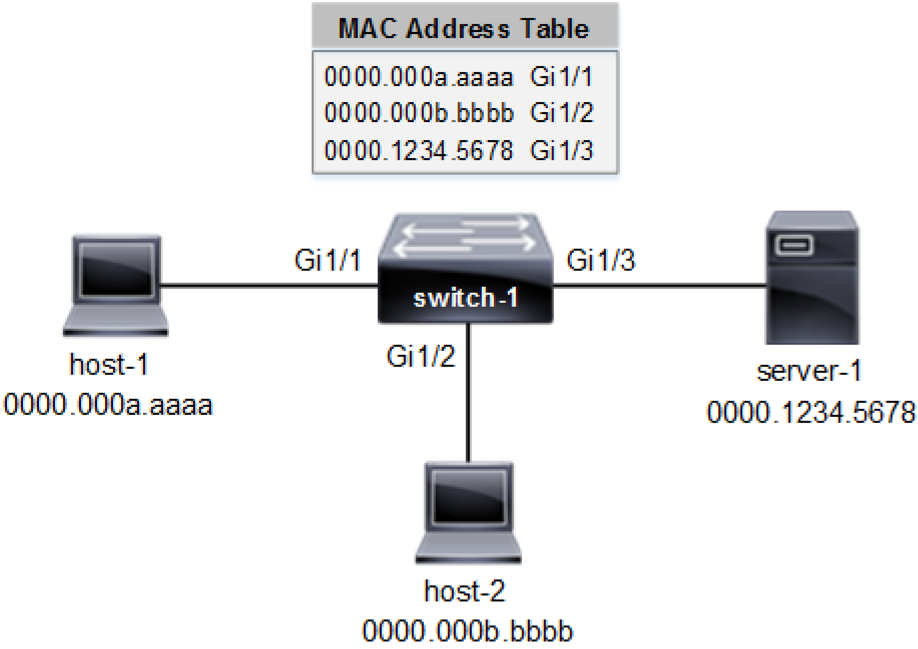
Frame Switching: Example 3

Refer to the network drawing where host-2 is sending to data to server-1. In this example, switch-1 will examine the incoming frame from host-2 arriving on port Gi1/2. The switch will do a MAC table lookup based on the destination MAC address (0000.1234.5678).

The destination MAC address is assigned to server-1 and frame is forwarded out switch port Gi1/3 associated with server-1.

- Switch will examine the frame and do a MAC address table lookup.
- Frame is forwarded out switch port Gi1/3.

Figure 6 Frame Switching Example 3



MAC Address Table	
0000.000a.aaaa	Gi1/1
0000.000b.bbbb	Gi1/2
0000.1234.5678	Gi1/3