Module 7: Ethernet Switching

Introduction to Networks v7.0
(ITN)

Module Objectives

Module Title: Ethernet Switching

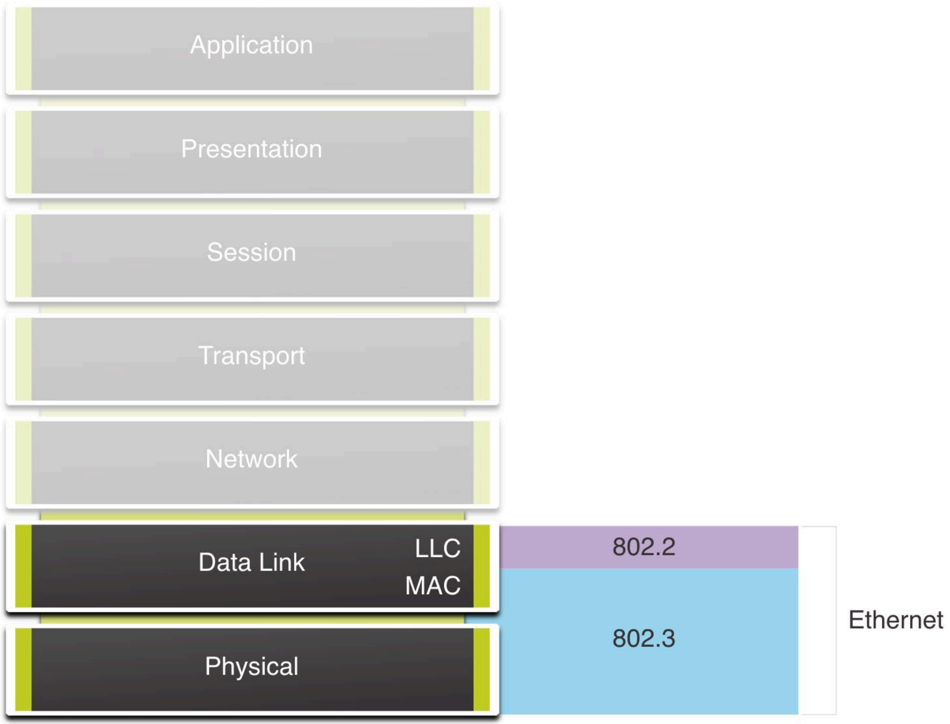
Module Objective: Explain how Ethernet works in a switched network.

Topic Title	Topic Objective
Ethernet Frame	Explain how the Ethernet sublayers are related to the frame fields.
Ethernet MAC Address	Describe the Ethernet MAC address.
The MAC Address Table	Explain how a switch builds its MAC address table and forwards frames.
Switch Speeds and Forwarding Methods	Describe switch forwarding methods and port settings available on Layer 2 switch ports.

7.1 Ethernet Frames

Ethernet Encapsulation

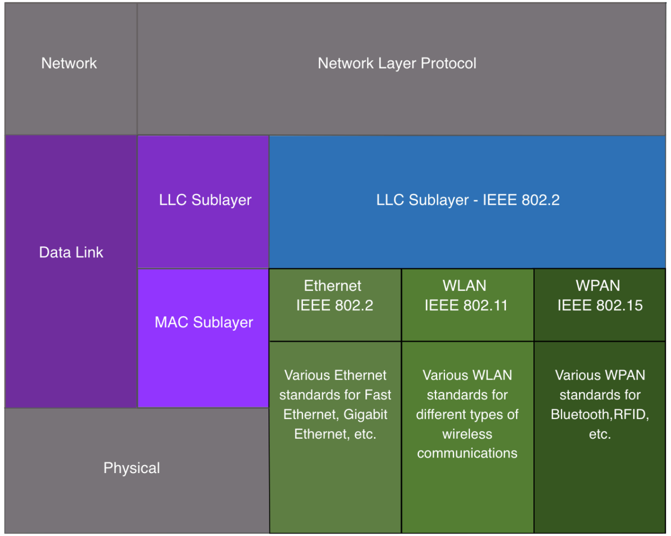
- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.



Data Link Sublayers

The 802 LAN/MAN standards, including Ethernet, use two separate sublayers of the data link layer to operate:

- **LLC Sublayer**: (IEEE 802.2) Places information in the frame to identify which network layer protocol is used for the frame.
- **MAC Sublayer**: (IEEE 802.3, 802.11, or 802.15) Responsible for data encapsulation and media access control and provides data link layer addressing.



MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

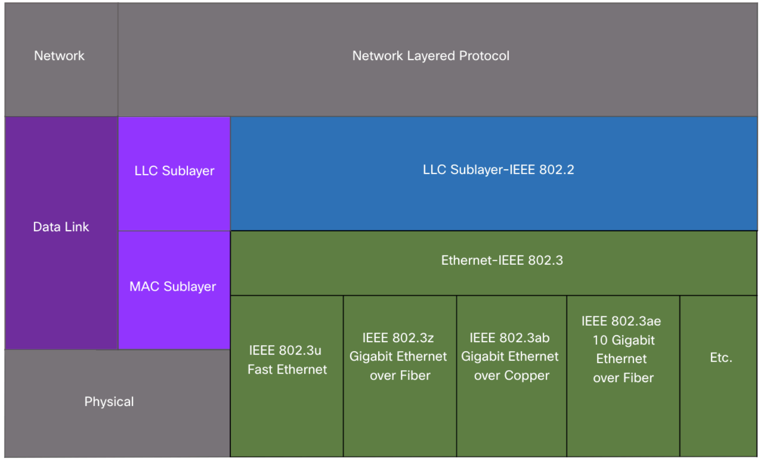
IEEE 802.3 data encapsulation includes the following:

1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

MAC Sublayer

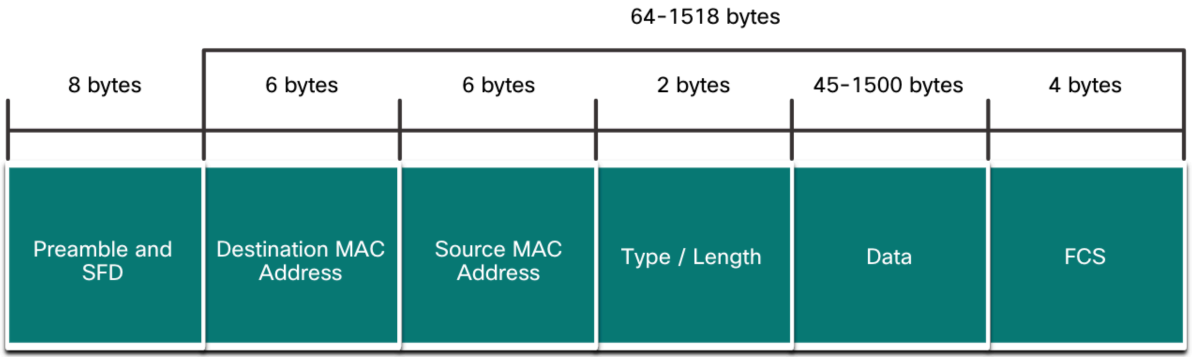
Media Access

- The IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.
- Legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD).
- Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.



Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. The preamble field is not included when describing the size of the frame.
- Any frame less than 64 bytes in length is considered a "collision fragment" or "runt frame" and is automatically discarded. Frames with more than 1500 bytes of data are considered "jumbo" or "baby giant frames".
- If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



Lab – Use Wireshark to Examine Ethernet Frames

In this lab, you will complete the following objectives:

- Part 1: Examine the Header Fields in an Ethernet II Frame
- Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

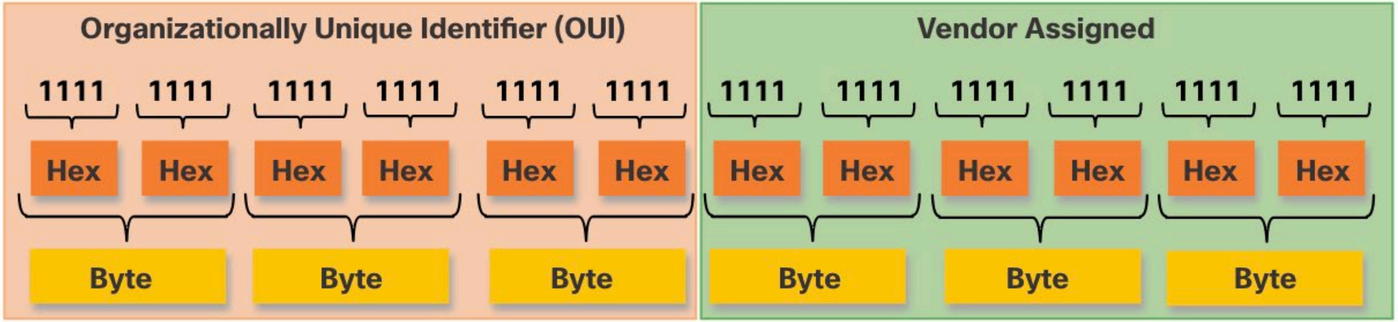
7.2 Ethernet MAC Address

MAC Address and Hexadecimal

- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example the binary value 0000 1010 is represented in hexadecimal as 0A.
- Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.
- Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media. MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.
- All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).
- An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value.



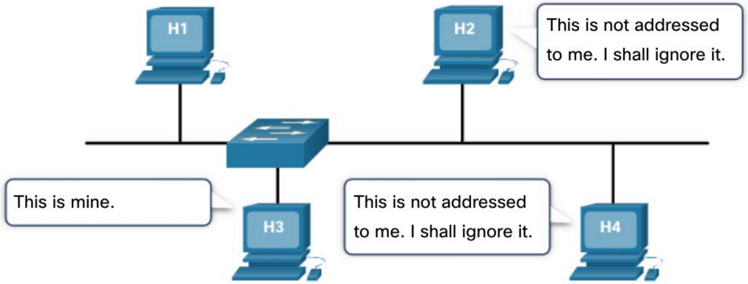
Ethernet MAC Addresses
Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header include a Source MAC address and a Destination MAC address.
- When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

- Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.

Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		

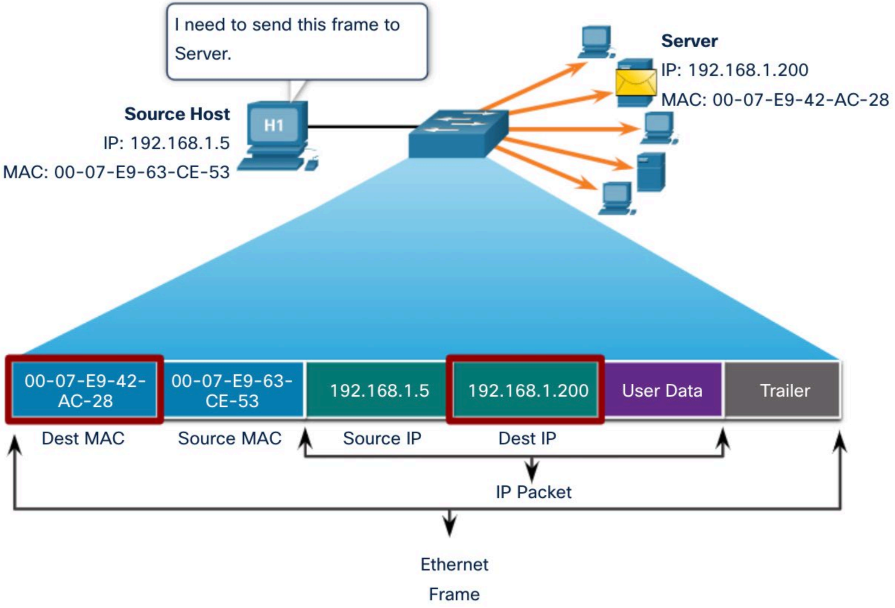


Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.
- The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

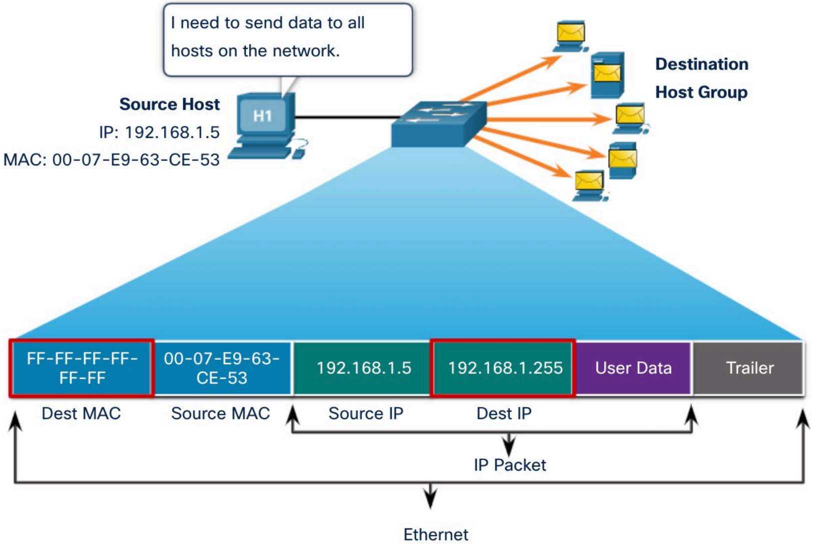
Note: The source MAC address must always be a unicast.



Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

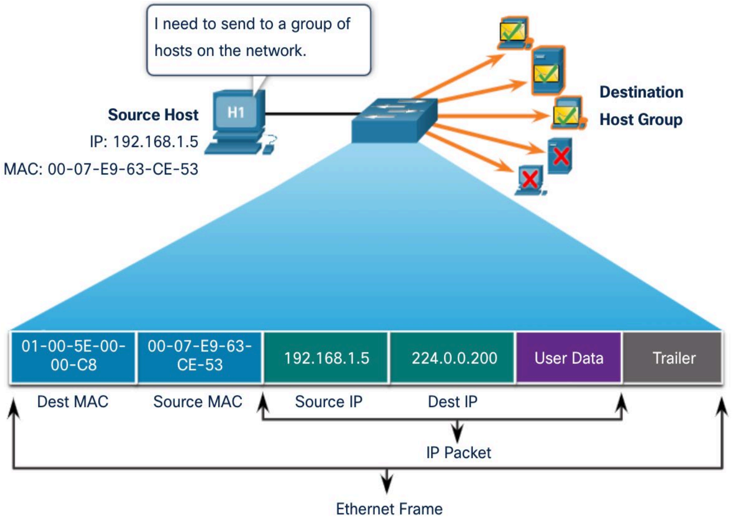
- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the **host portion**. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.



Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices that belong to the same multicast group.

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP).
- It is flooded out all Ethernet switch ports except the incoming port, **unless** the switch is configured for multicast snooping. It is not forwarded by a router, **unless** the router is configured to route multicast packets.
- Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.
- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address.



Lab – View Network Device MAC Addresses

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display, Describe, and Analyze Ethernet MAC Addresses

7.3 The MAC Address Table

Switch Fundamentals

- A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 ND packet. The switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- An Ethernet switch examines its **MAC address table** to make a forwarding decision for each frame, unlike legacy Ethernet hubs that repeat bits out all ports except the incoming port.
- When a switch is turned on, the MAC address table is empty

Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.

Switch Learning and Forwarding

Examine the Source MAC Address (Learn)

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the port number where the frame entered the switch. If the source MAC address **does not exist**, it is added to the table along with the incoming port number. If the source MAC address **does exist**, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for 5 minutes.

Note: If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

Switch Learning and Forwarding (Contd.)

Find the Destination MAC Address (Forward)

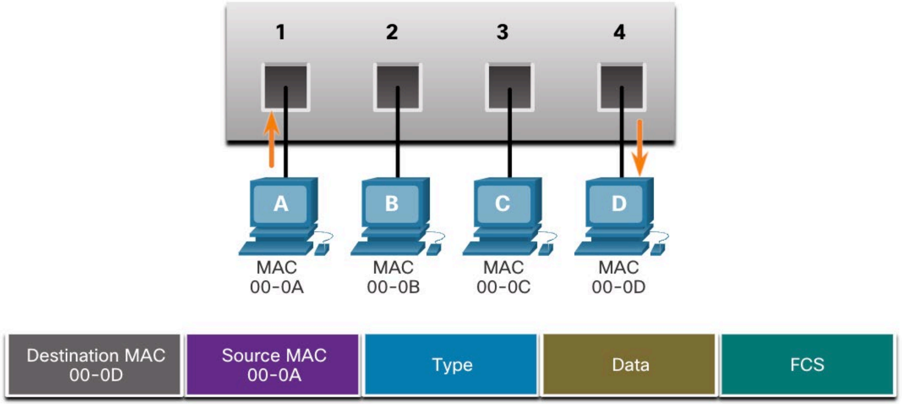
If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is **in** the table, it will forward the frame out the specified port. If the destination MAC address is **not** in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

Note: If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.

Filtering Frames

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.

MAC Address Table	
Port	**MAC Address**
1	00-0A
4	00-0D



Video – MAC Address Tables on Connected Switches

This video will cover the following:

- How switches build MAC address tables
- How switches forward frames base on the content of their MAC address tables

Video – Sending the Frame to the Default Gateway

This video will cover the following:

- What a switch does when the destination AMC address is not listed in the switch’s MAC address table.
- What a switch does when the source AMC address is not listed in the switch’s MAC address table

Lab – View the Switch MAC Address Table

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table

7.4 Switch Speeds and Forwarding Methods

Frame Forwarding Methods on Cisco Switches

Switches use one of the following forwarding methods for switching data between network ports:

- **Store-and-forward switching** - This frame forwarding method receives the entire frame and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. Then the frame is forwarded out of the correct port.
- **Cut-through switching** - This frame forwarding method forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

- A big advantage of store-and-forward switching is that it determines if a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data.
- Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.

Cut-Through Switching

In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port it should forward out the data. The switch does not perform any error checking on the frame.

There are **two variants** of cut-through switching:

- **Fast-forward switching** - Offers the lowest level of latency by immediately forwarding a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. The destination NIC discards the faulty packet upon receipt. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching** - A compromise between the high latency and high integrity of store-and-forward switching and the low latency and reduced integrity of fast-forward switching, the switch stores and performs an error check on the first 64 bytes of the frame before forwarding. Because most network errors and collisions occur during the first 64 bytes, this ensures that a collision has not occurred before forwarding the frame.

Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them or when the destination port is busy because of congestion.

Method	Description
Port-based memory	•Frames are stored in queues that are linked to specific incoming and outgoing ports. •A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted. •It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. •This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	•Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer memory required by a port is dynamically allocated. •The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.

- Shared memory buffering also results in larger frames that can be transmitted with fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports. Therefore, more bandwidth can be dedicated to certain ports (e.g., server port).

Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth (“speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices.

There are two types of duplex settings used for communications on an Ethernet network:

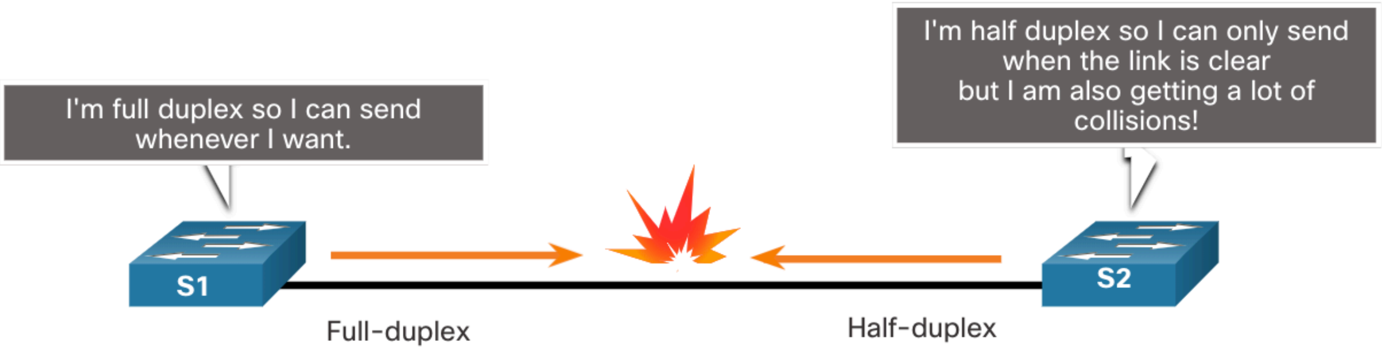
- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

Note: Gigabit Ethernet ports only operate in full-duplex.

Duplex and Speed Settings

- Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.
- This can occur when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration.
- It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.



Auto-MDIX

Connections between devices once required the use of either a crossover or straight-through cable. The type of cable required depended on the type of interconnecting devices.

Note: A direct connection between a router and a host requires a cross-over connection.

- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.
- The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature.
- Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

7.5 Module Practice and Quiz

What did I learn in this module?

- Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet uses the LLC and MAC sublayers of the data link layer to operate.
- The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.
- MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes.
- When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

What did I learn in this module? (Contd.)

- A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port.
- The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.
- Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free.
- Two methods of memory buffering are port-based memory and shared memory.
- There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex.

New Terms and Commands

- Store-and-Forward Switching
- Cut-through Switching
- Fast-Forward Switching
- Fragment-free Switching
- OUI (Organizationally Unique Identifier)
- ARP (Address Resolution Protocol)
- ND (Neighbor Discovery)
- Port-based memory
- Shared memory
- Auto-MDIX

CISCO