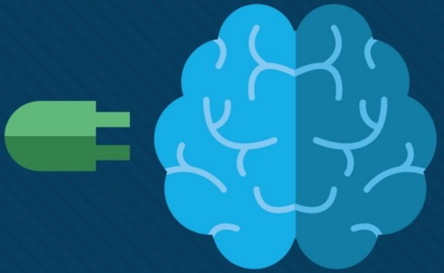


# Module 4: Physical Layer

Introduction to Networks v7.0
(ITN)

# Module Objectives

**Module Title:** Physical Layer

**Module Objective**: Explain how physical layer protocols, services, and network media support communications across data networks.

| Topic Title | Topic Objective |
|---|---|
| **Purpose of the Physical Layer** | Describe the purpose and functions of the physical layer in the network. |
| **Physical Layer Characteristics** | Describe characteristics of the physical layer. |
| **Copper Cabling** | Identify the basic characteristics of copper cabling. |
| **UTP Cabling** | Explain how UTP cable is used in Ethernet networks. |
| **Fiber-Optic Cabling** | Describe fiber optic cabling and its main advantages over other media. |
| **Wireless Media** | Connect devices using wired and wireless media. |

# 4.1 Purpose of the Physical Layer

## Purpose of the Physical Layer

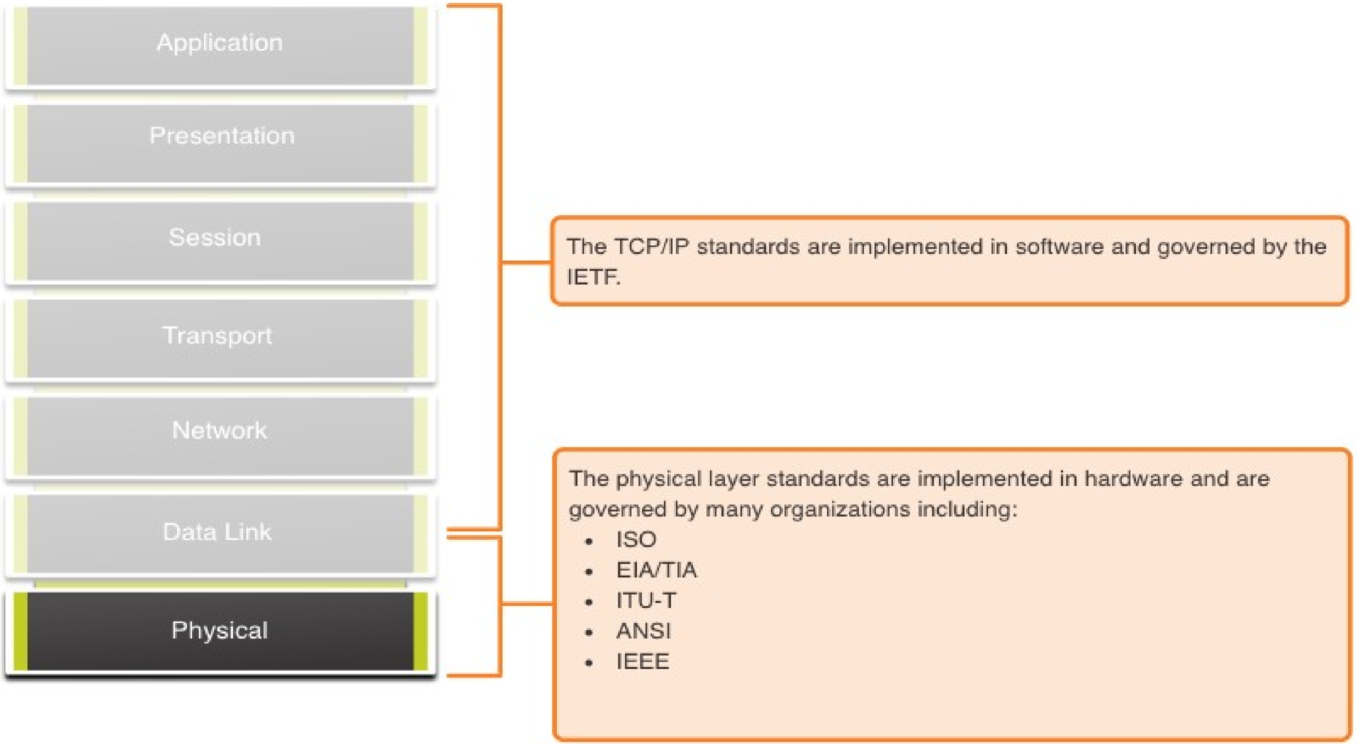
# The Physical Connection

- Before any network communications can occur, a physical connection to a local network must be established.
- This connection could be **wired or wireless**, depending on the setup of the network.
- This generally applies whether you are considering a corporate office or a home.
- A **Network Interface Card (NIC)** connects a device to the network.
- Some devices may have just one NIC, while others may have multiple NICs (Wired and/or Wireless, for example).
- Not all physical connections offer the same level of performance.

# 4.2 Physical Layer Characteristics

## Physical Layer Characteristics

# Physical Layer Standards



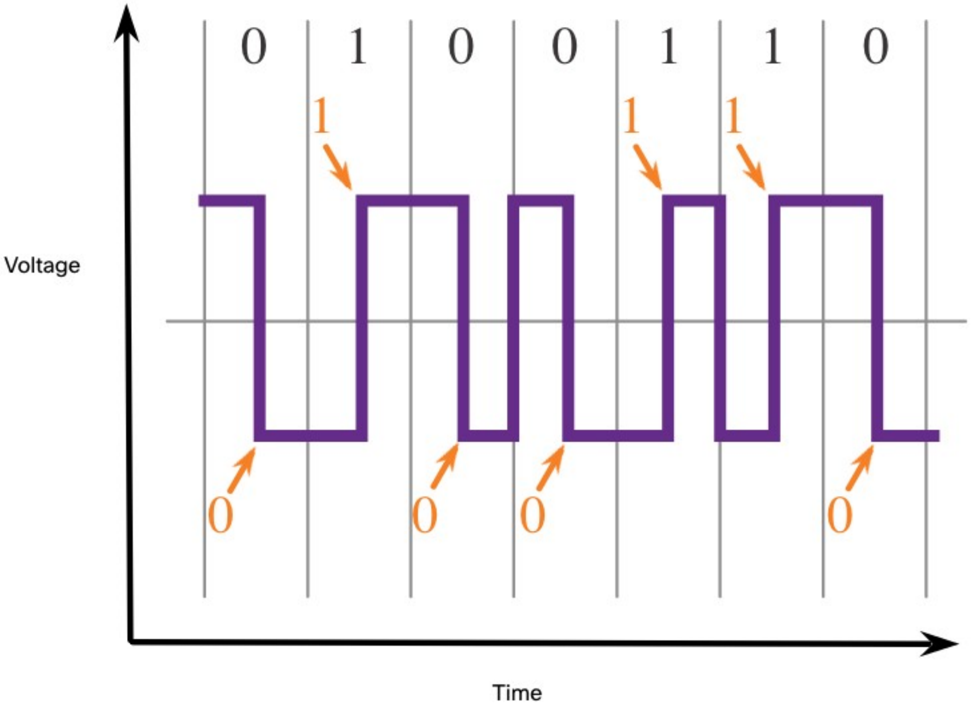
The TCP/IP standards are implemented in software and governed by the IETF.

The physical layer standards are implemented in hardware and are governed by many organizations including:

- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

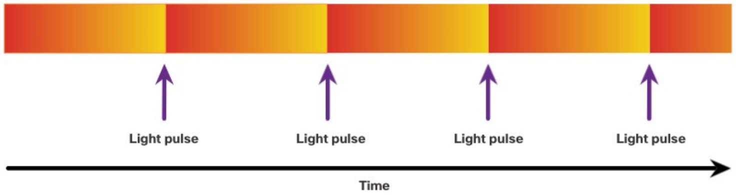
# Encoding

- Encoding converts the stream of bits into a format recognizable by the next device in the network path.
- This ‘coding’ provides predictable patterns that can be recognized by the next device.
- Examples of encoding methods include **Manchester** (shown in the figure, 0: H → L, 1: L→ H), **4B/5B, and 8B/10B**.

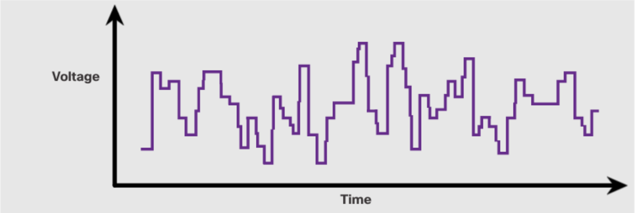


## Physical Layer Characteristics
# Signaling

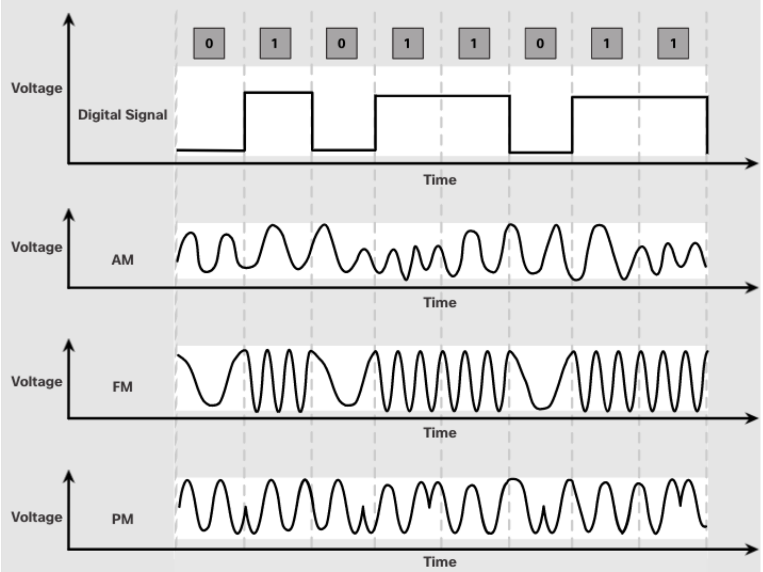
- The signaling method is how the bit values, “1” and “0” are represented on the physical medium.
- The method of signaling will vary based on the type of medium being used.



Light Pulses Over Fiber-Optic Cable



Electrical Signals Over Copper Cable



Microwave Signals Over Wireless

## Physical Layer Characteristics
# Bandwidth

- Bandwidth is the capacity at which a medium can carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time; how many bits can be transmitted in a second.
- Physical media properties, current technologies, and the laws of physics play a role in determining available bandwidth.

| Unit of Bandwidth | Abbreviation | Equivalence |
|---|---|---|
| Bits per second | bps | 1 bps = fundamental unit of bandwidth |
| Kilobits per second | Kbps | 1 Kbps = 1,000 bps = $10^3$ bps |
| Megabits per second | Mbps | 1 Mbps = 1,000,000 bps = $10^6$ bps |
| Gigabits per second | Gbps | 1 Gbps – 1,000,000,000 bps = $10^9$ bps |
| Terabits per second | Tbps | 1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps |

Physical Layer Characteristics

# Bandwidth Terminology

## Latency

- Amount of time, including delays, for data to travel from one given point to another

## Throughput

- The measure of the transfer of bits across the media over a given period of time

## Goodput

- The measure of usable data transferred over a given period of time
- Goodput = Throughput - traffic overhead

# 4.3 Copper Cabling

## Copper Cabling

# Characteristics of Copper Cabling

Copper cabling is the most common type of cabling used in networks today. It is inexpensive, easy to install, and has low resistance to electrical current flow.

Limitations:

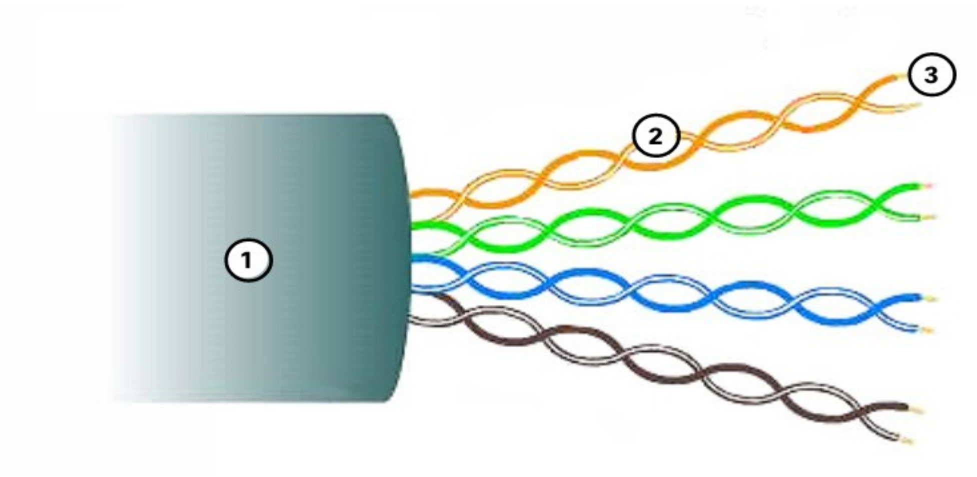
- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

Mitigation:

- Strict adherence to cable length limits will mitigate attenuation.
- Some kinds of copper cable mitigate EMI and RFI by using metallic shielding and grounding.
- Some kinds of copper cable mitigate crosstalk by twisting opposing circuit pair wires together.

Copper Cabling

# Unshielded Twisted Pair (UTP)



- UTP is the most common networking media.
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices.

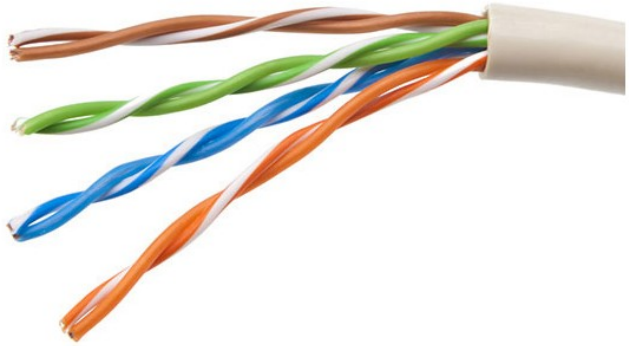
Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

# Properties of UTP Cabling

UTP has **four pairs** of color-coded copper wires twisted together and encased in a flexible plastic sheath. **No shielding** is used. UTP relies on the following properties to limit crosstalk:

- Cancellation - Each wire in a pair of wires uses opposite polarity. One wire is negative, the other wire is positive. They are twisted together and the **magnetic fields effectively cancel each other and outside EMI/RFI**.
- Variation in twists per foot in each wire - Each wire is twisted a different amount, which helps prevent crosstalk amongst the wires in the cable.



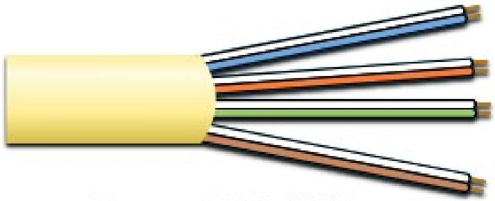
# UTP Cabling Standards and Connectors

Standards for UTP are established by the TIA/EIA. TIA/EIA-568 standardizes elements like:

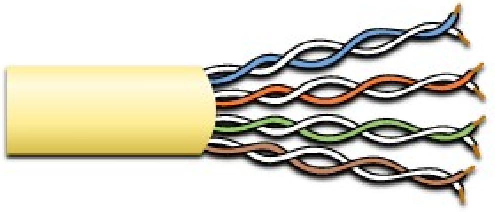
- Cable Types
- Cable Lengths
- Connectors
- Cable Termination
- Testing Methods

Electrical standards for copper cabling are established by the IEEE, which rates cable according to its performance. Examples include:

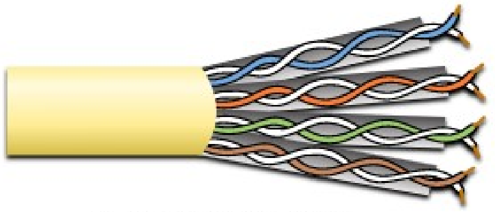
- Category 3
- Category 5 and 5e
- Category 6



Category 3 Cable (UTP)



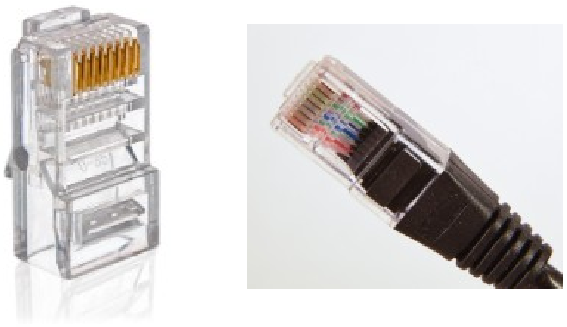
Category 5 and 5e Cable (UTP)



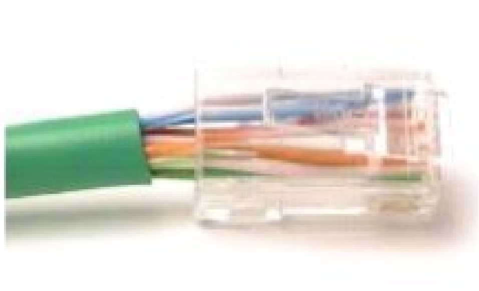
Category 6 Cable (UTP)

## UTP Cabling

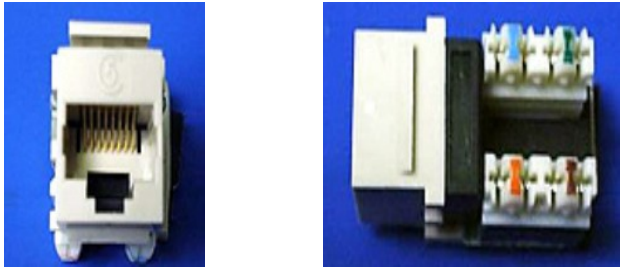
# UTP Cabling Standards and Connectors (Cont.)



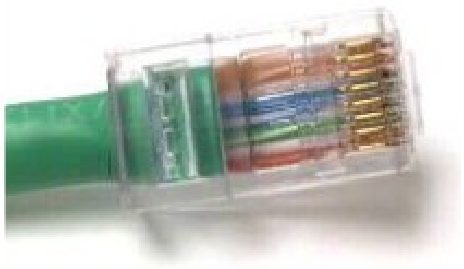
RJ-45 Connector



Poorly terminated UTP cable



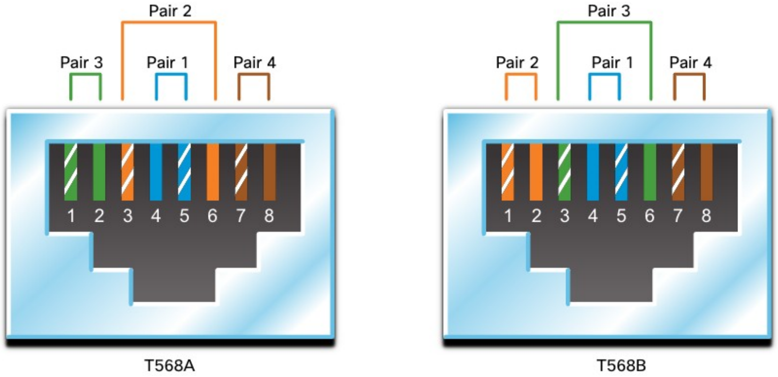
RJ-45 Socket



Properly terminated UTP cable

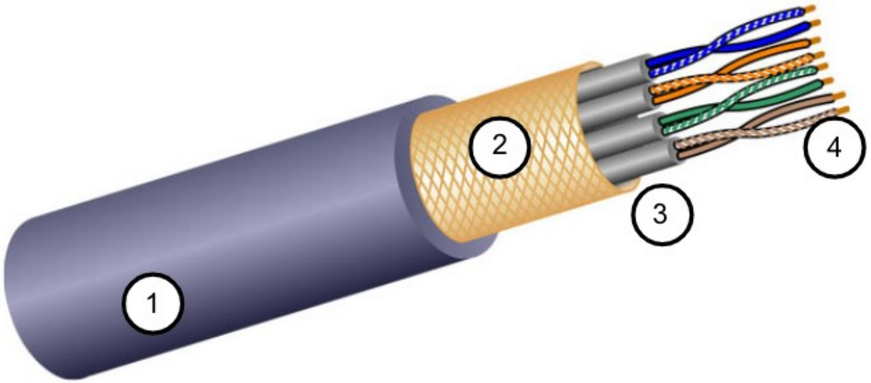
## UTP Cabling

# Straight-through and Crossover UTP Cables



| Cable Type | Standard | Application |
|---|---|---|
| Ethernet **Straight-through** | Both ends T568A or T568B | Host to Network Device |
| Ethernet **Crossover** * | One end T568A, other end T568B | Host-to-Host, Switch-to-Switch, Router-to-Router |
| * Considered Legacy due to most NICs using Auto-MDIX to sense cable type and complete connection | | |
| Rollover | Cisco Proprietary | Host serial port to Router or Switch Console Port, using an adapter |

# Shielded Twisted Pair (STP)



- **Better noise protection than UTP**
- More **expensive** than UTP
- **Harder to install than UTP**
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

## Copper Cabling

# Coaxial Cable

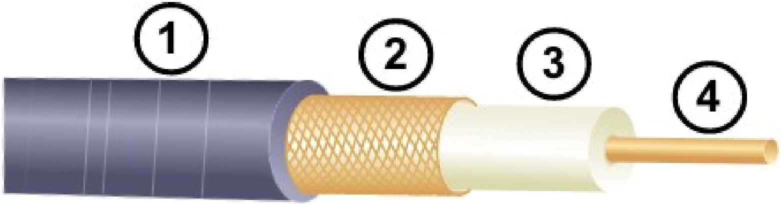
Consists of the following:

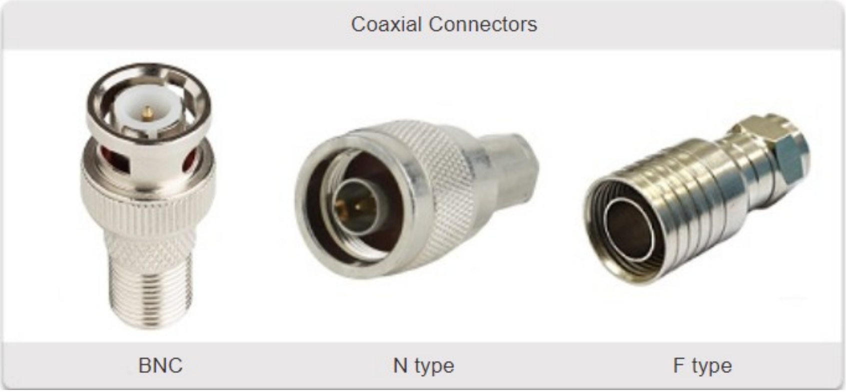
1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.

There are different types of connectors used with coax cable.

Commonly used in the following situations:

- Wireless installations - attach antennas to wireless devices
- Cable internet installations - customer premises wiring





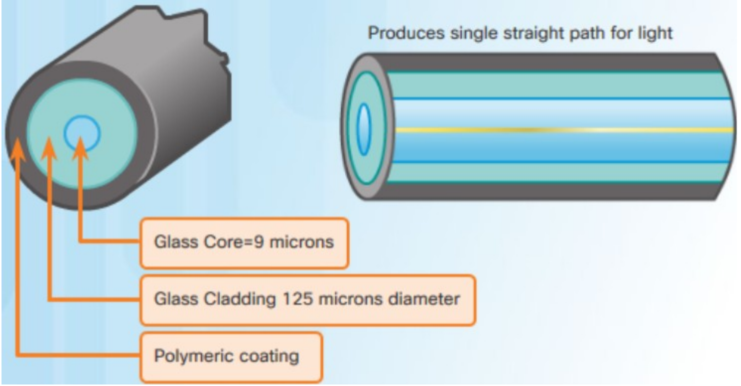
# 4.5 Fiber-Optic Cabling

# Properties of Fiber-Optic Cabling

- Not as common as UTP because of the **expense** involved
- Ideal for some networking scenarios
- Transmits data over **longer distances at higher bandwidth** than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

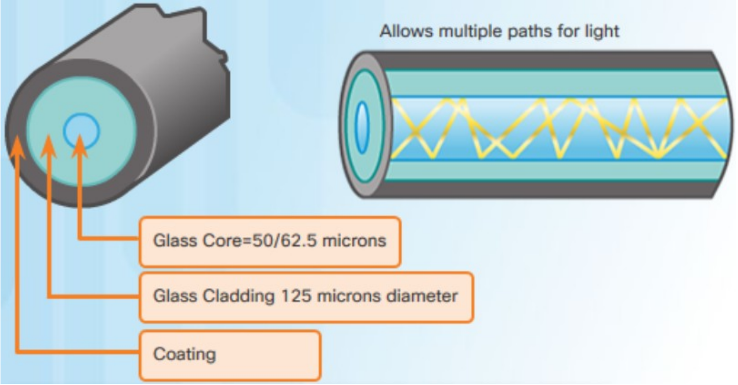
# Types of Fiber Media

## **Single-Mode** Fiber


Produces single straight path for light
Glass Core=9 microns
Glass Cladding 125 microns diameter
Polymeric coating

- Very small core
- Uses expensive lasers
- **Long-distance applications**

## **Multimode** Fiber


Allows multiple paths for light
Glass Core=50/62.5 microns
Glass Cladding 125 microns diameter
Coating

- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to **10 Gbps over 550 meters**

Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has greater dispersion than SMF, with a the maximum cable distance for MMF is 550 meters.

# Fiber-Optic Cabling Usage

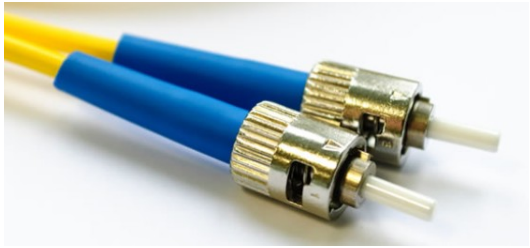
Fiber-optic cabling is now being used in four types of industry:

1. **Enterprise Networks -** Used for **backbone** cabling applications and interconnecting infrastructure devices
2. **Fiber-to-the-Home (FTTH) -** Used to provide always-on broadband services to homes and small businesses
3. **Long-Haul Networks -** Used by service providers to connect countries and cities
4. **Submarine Cable Networks -** Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh undersea environments at up to transoceanic distances.

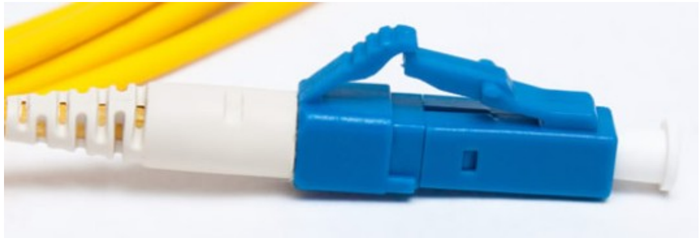
**Our focus in this course is the use of fiber within the enterprise.**

## Fiber-Optic Cabling

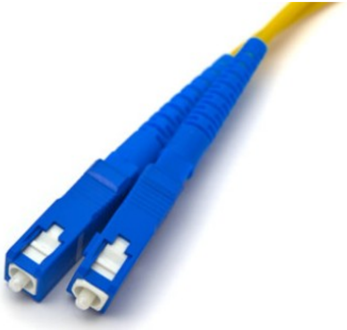
# Fiber-Optic Connectors



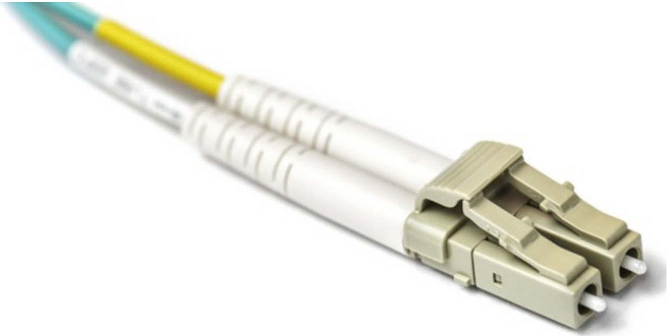
Straight-Tip (ST) Connectors



Lucent Connector (LC) Simplex Connectors

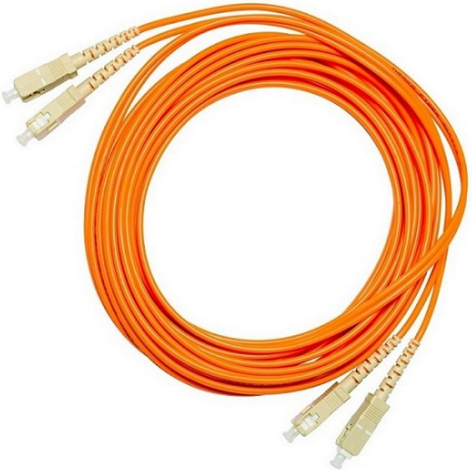


Subscriber Connector (SC) Connectors

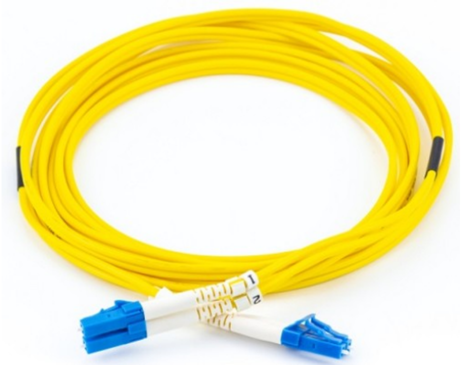


Duplex Multimode LC Connectors

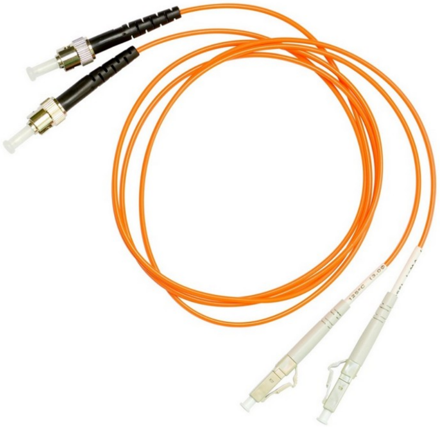
# Fiber Patch Cords



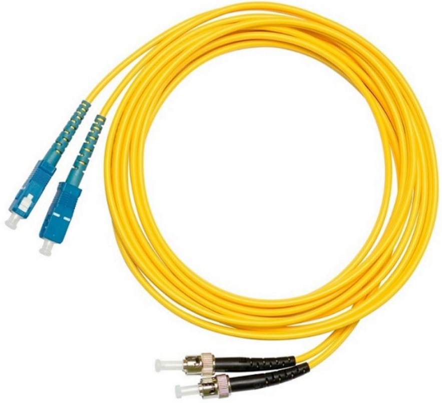
SC-SC **MM** Patch Cord



LC-LC **SM** Patch Cord



ST-LC **MM** Patch Cord



ST-SC **SM** Patch Cord

A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

## Fiber-Optic Cabling

# Fiber versus Copper

Optical fiber is primarily used as backbone cabling for high-traffic, point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

| Implementation Issues | UTP Cabling | Fiber-Optic Cabling |
|---|---|---|
| Bandwidth supported | 10 Mb/s - 10 Gb/s | 10 Mb/s - 100 Gb/s |
| Distance | Relatively short (1 - 100 meters) | Relatively long ( 1 - 100,000 meters) |
| Immunity to EMI and RFI | Low | High (Completely immune) |
| Immunity to electrical hazards | Low | High (Completely immune) |
| Media and connector costs | Lowest | Highest |
| Installation skills required | Lowest | Highest |
| Safety precautions | Lowest | Highest |

# 4.6 Wireless Media

# Properties of Wireless Media

It carries electromagnetic signals representing binary digits using radio or microwave frequencies. This provides the greatest mobility option. Wireless connection numbers continue to increase.

Some of the limitations of wireless:

- **Coverage area** - Effective coverage can be significantly impacted by the physical characteristics of the deployment location.
- **Interference** - Wireless is susceptible to interference and can be disrupted by many common devices.
- **Security** - Wireless communication coverage requires no access to a physical strand of media, so anyone can gain access to the transmission.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

# Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications dictate:

- Data to radio signal encoding methods
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

Wireless Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology
- **Bluetooth (IEEE 802.15)** - Wireless Personal Area network (WPAN) standard
- **WiMAX (IEEE 802.16)** - Uses a point-to-multipoint topology to provide broadband wireless access
- **Zigbee (IEEE 802.15.4)** - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications

# Wireless LAN

In general, a Wireless LAN (WLAN) requires the following devices:

- **Wireless Access Point (AP)** - Concentrate wireless signals from users and connect to the existing copper-based network infrastructure
- **Wireless NIC Adapters** - Provide wireless communications capability to network hosts

There are a number of WLAN standards. When purchasing WLAN equipment, ensure compatibility, and interoperability.

Network Administrators must develop and apply stringent security policies and processes to protect WLANs from unauthorized access and damage.

# 4.8 Summary

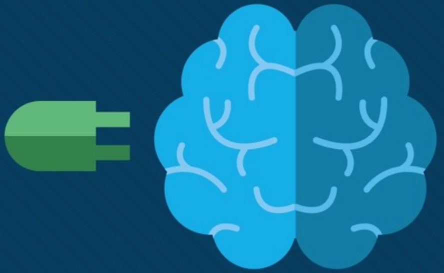
# What did I learn in this module?

- Before any network communications can occur, a physical connection to a local network, either wired or wireless, must be established.
- The physical layer consists of electronic circuitry, media, and connectors developed by engineers.
- The physical layer standards address three functional areas: physical components, encoding, and signaling.
- Three types of copper cabling are: UTP, STP, and coaxial cable (coax).
- UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE).
- The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover.

Module Practice and Quiz

# What did I learn in this module (Cont.)?

- Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media.
- There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC.
- Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode, and SC-ST single-mode.
- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations, including coverage area, interference, security, and the problems that occur with any shared medium.
- Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4).
- Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.



# Module 6: Data Link Layer

Introduction to Networks v7.0
(ITN)

# Module Objectives

**Module Title:** Data Link Layer

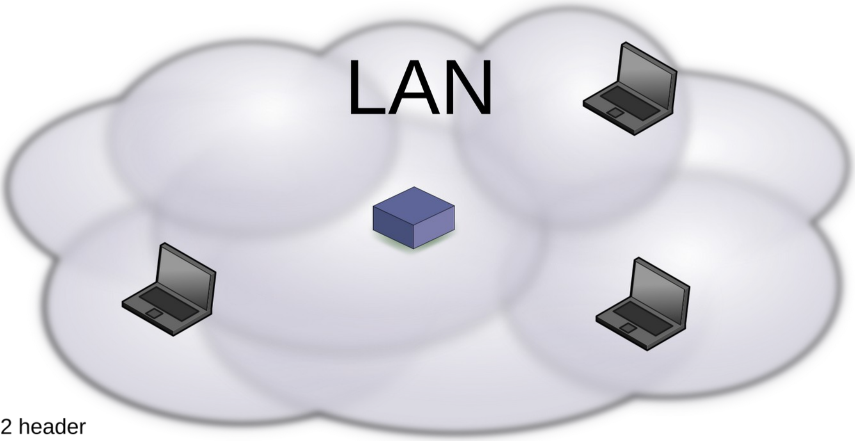
**Module Objective**: Explain how media access control in the data link layer supports communication across networks.

| Topic Title | Topic Objective |
|---|---|
| **Purpose of the Data Link Layer** | Describe the purpose and function of the data link layer in preparing communication for transmission on specific media. |
| **Topologies** | Compare the characteristics of media access control methods on WAN and LAN topologies. |
| **Data Link Frame** | Describe the characteristics and functions of the data link frame. |

# 6.1 Purpose of the Data Link Layer

# The Data Link Layer

- The Data Link layer is responsible for communications between end-device network interface cards.
- It allows upper layer protocols to access the physical layer media and encapsulates Layer 3 packets (IPv4 and IPv6) into Layer 2 Frames.
- It also performs error detection and rejects corrupts frames.



L2 header

| | | | |
|---|---|---|---|
| Source NIC | Destination NIC | Data | Frame Control Sequence |

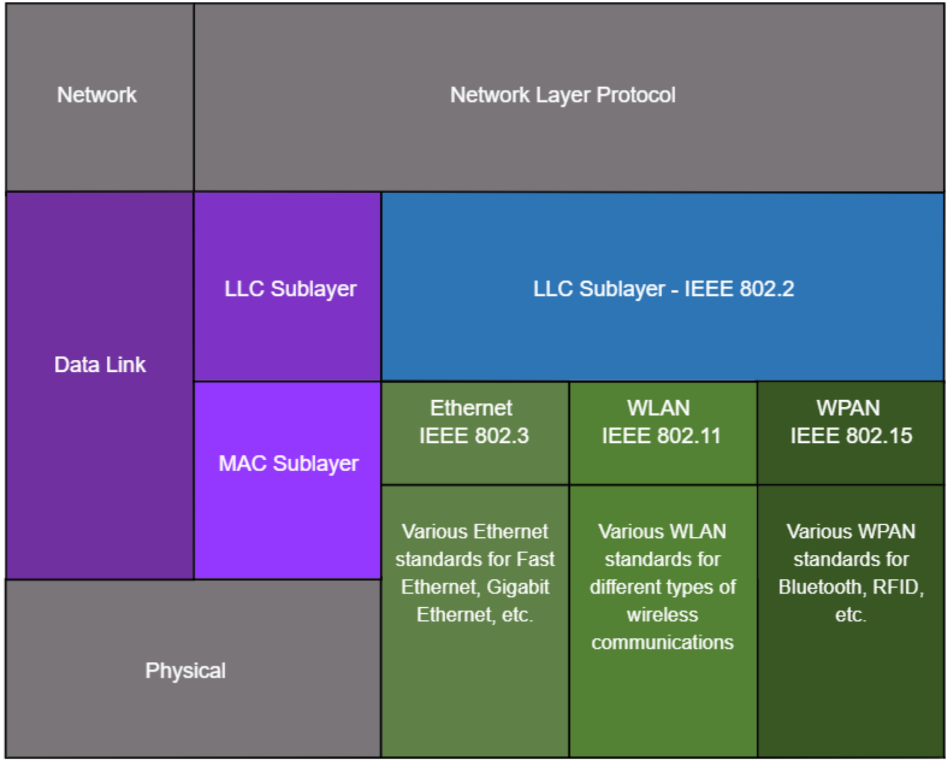
## Purpose of the Data Link Layer

# IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to the type of network (Ethernet, WLAN, WPAN, etc).

The Data Link Layer consists of two sublayers. **Logical Link Control (LLC)** and **Media Access Control (MAC).**

- The LLC sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- The MAC sublayer is responsible for data encapsulation and media access control.



Network

Network Layer Protocol

Data Link

LLC Sublayer

LLC Sublayer - IEEE 802.2

MAC Sublayer

Ethernet
IEEE 802.3

WLAN
IEEE 802.11

WPAN
IEEE 802.15

Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.

Various WLAN standards for different types of wireless communications

Various WPAN standards for Bluetooth, RFID, etc.

Physical

## Purpose of the Data Link Layer

# Data Link Layer Standards

Data link layer protocols are defined by engineering organizations:

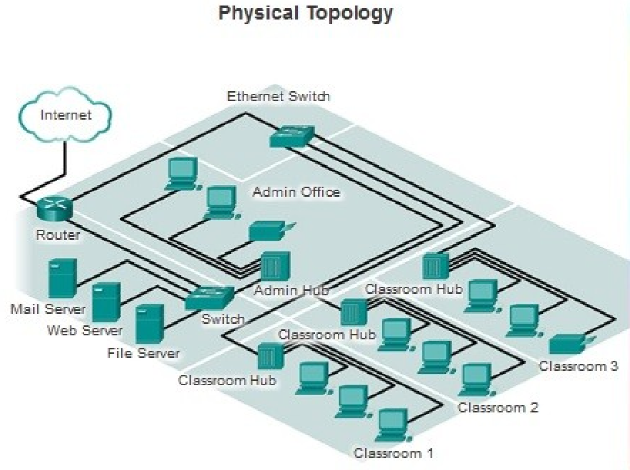
- Institute for Electrical and Electronic Engineers (IEEE).
- International Telecommunications Union (ITU).
- International Organizations for Standardization (ISO).
- American National Standards Institute (ANSI).

# 6.2 Topologies

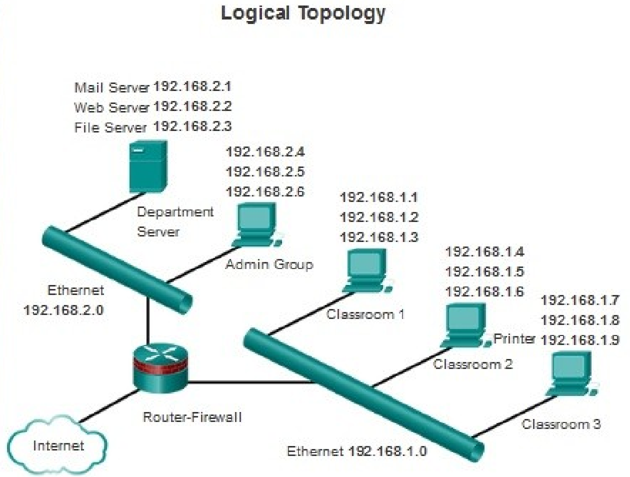
# Physical and Logical Topologies

The topology of a network is the arrangement and relationship of the network devices and the interconnections between them.

- **Physical topology** – shows physical connections and how devices are interconnected.
- **Logical topology** – identifies the virtual connections between devices using device interfaces and IP addressing schemes.

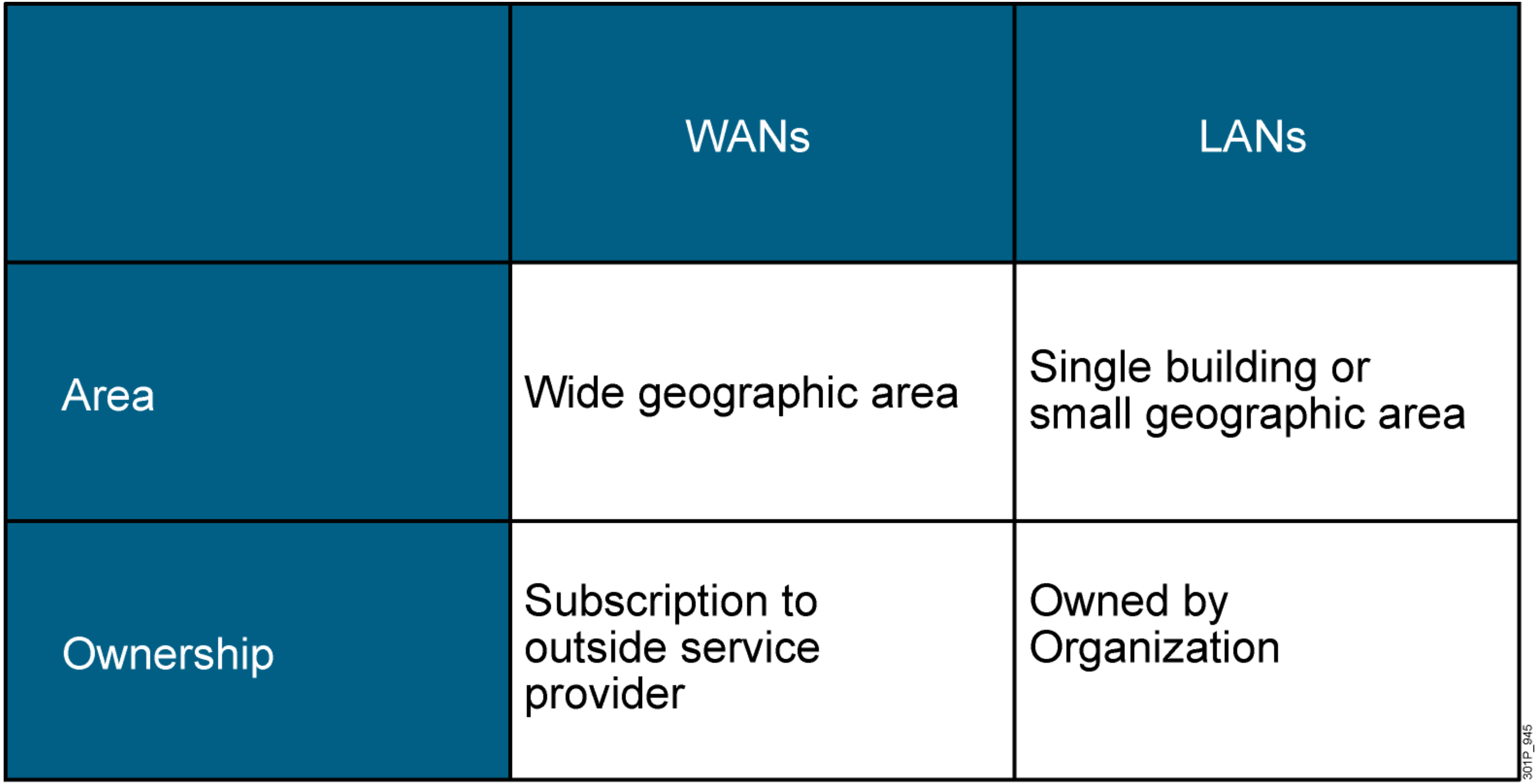


Physical Topology



Logical Topology

# WANs vs. LANs



| | WANs | LANs |
|---|---|---|
| Area | Wide geographic area | Single building or small geographic area |
| Ownership | Subscription to outside service provider | Owned by Organization |

## Topologies

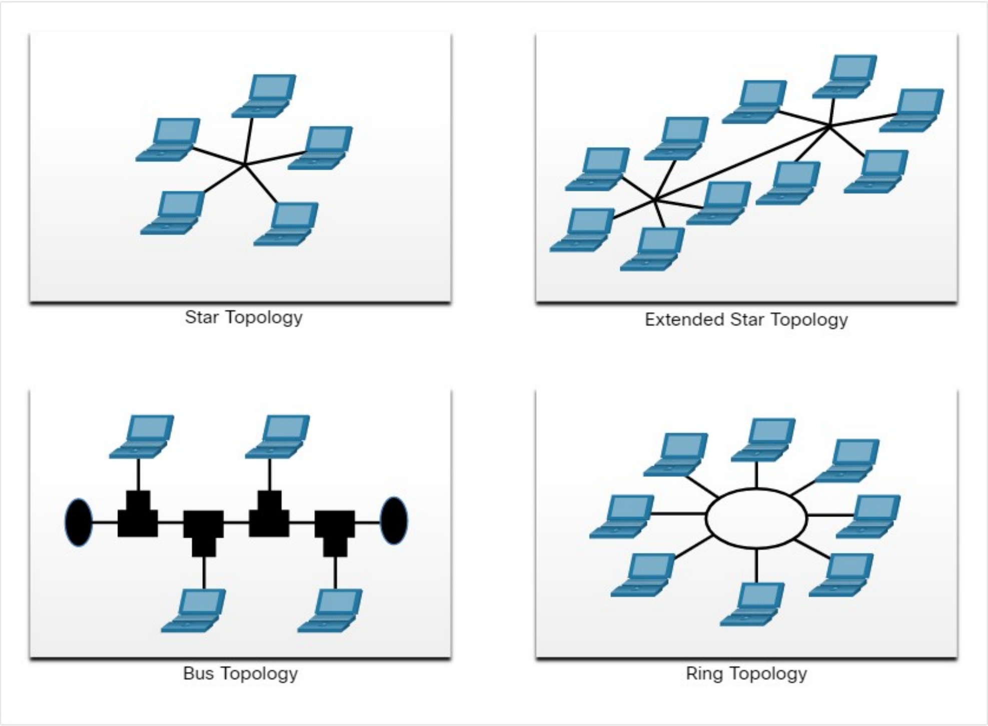
# LAN Topologies

End devices on **LANs** are typically interconnected using a star or extended star topology. Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.

Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

- **Bus** – All end systems chained together and terminated on each end.
- **Ring** – Each end system is connected to its respective neighbors to form a ring.

Physical Topologies



Star Topology

Extended Star Topology

Bus Topology

Ring Topology

Topologies

# WAN Topologies

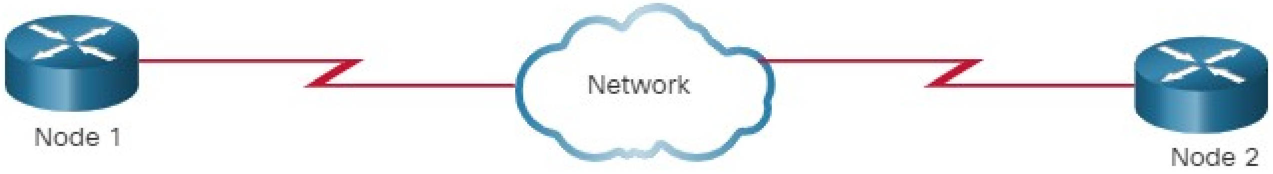
There are three common physical **WAN** topologies:

- **Point-to-point** – the simplest and most common WAN topology. Consists of a permanent link between two endpoints.
- **Hub and spoke** – similar to a star topology where a central site interconnects branch sites through point-to-point links.
- **Mesh** – provides high availability but requires every end system to be connected to every other end system.

Topologies

# Point-to-Point WAN Topology

- Physical point-to-point topologies directly connect two nodes.
- The nodes may not share the media with other hosts.
- Because all frames on the media can only travel to or from the two nodes, **Point-to-Point WAN** protocols can be very simple.



# Half and Full Duplex Communication

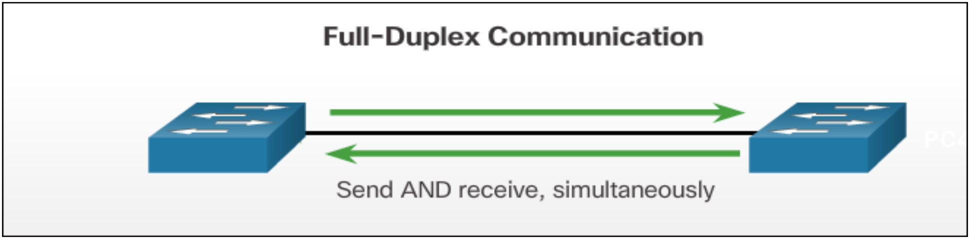
**Half-duplex communication**

- Only allows one device to send or receive at a time on a shared medium.
- Used on WLANs and legacy bus topologies with Ethernet hubs.

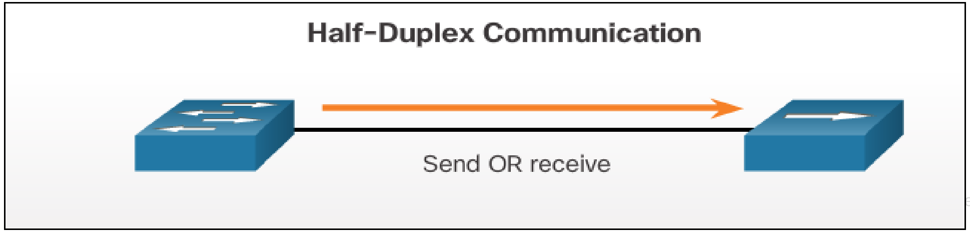
**Full-duplex communication**

- Allows both devices to simultaneously transmit and receive on a shared medium.
- Ethernet switches operate in full-duplex mode.

Bidirectional communication



Unidirectional communication



## Topologies

# Access Control Methods

### Contention-based access

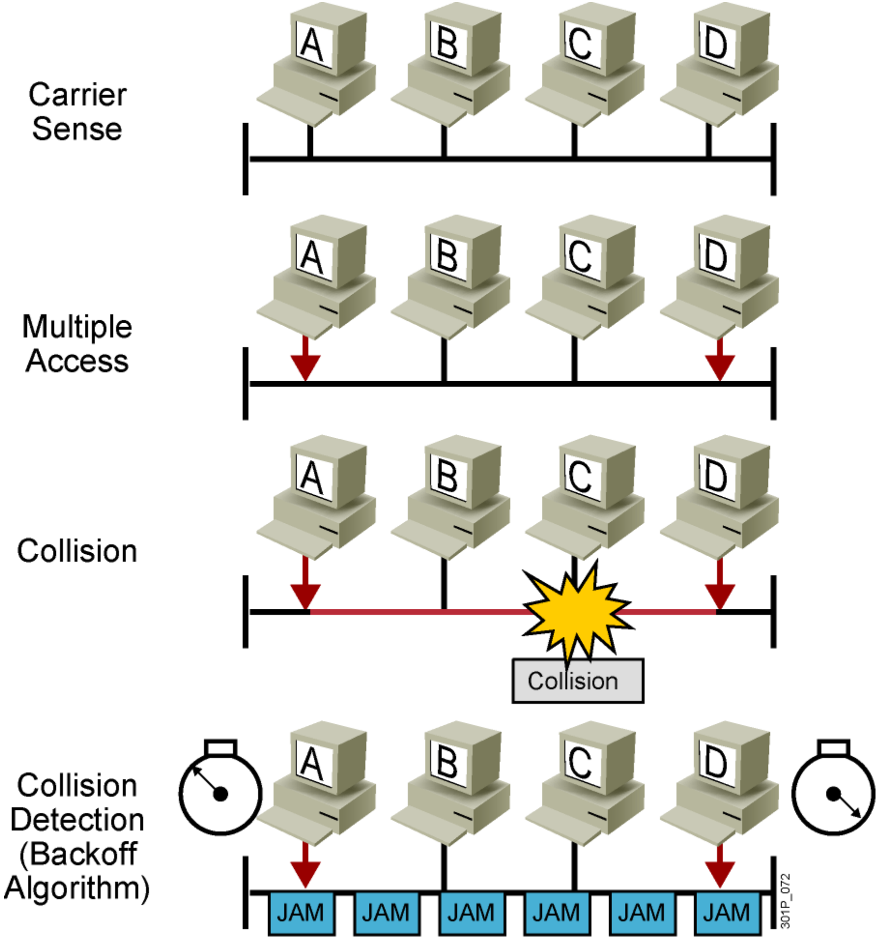
**All nodes operating in half-duplex**, competing for use of the medium. Examples are:

- Carrier sense multiple access with collision detection (**CSMA/CD**) as used on **legacy bus-topology Ethernet**.
- Carrier sense multiple access with collision avoidance (**CSMA/CA**) as used on **Wireless LAN**s.

### Controlled access

- **Deterministic** access where each node has its own time on the medium.
- Used on legacy networks such as **Token Ring** and **ARCNET**.

# CSMA/CD



Carrier Sense Multiple Access Collision Detection (CSMA/CD)

Topologies

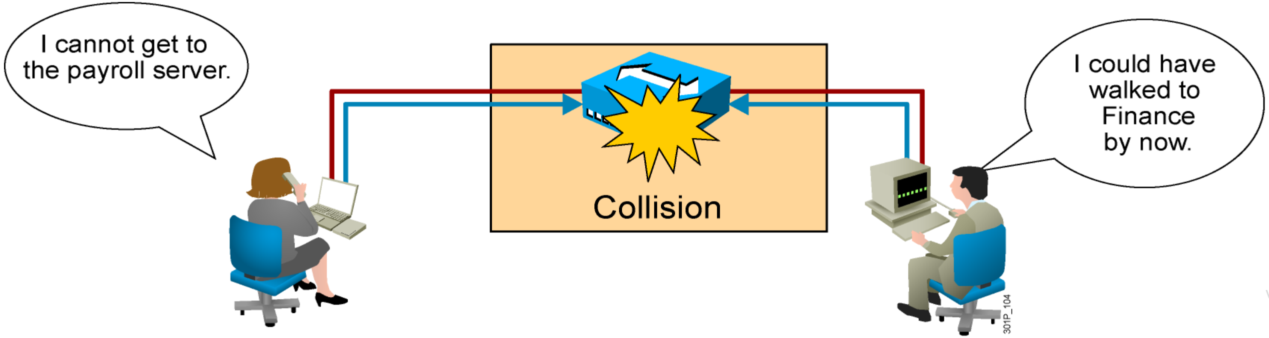
# Contention-Based Access – CSMA/CD

**CSMA/CD**

- Used by legacy Ethernet LANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision detection process to govern when a device can send and what happens if multiple devices send at the same time.

**CSMA/CD collision detection process**:

- Devices transmitting simultaneously will result in a signal collision on the shared media.
- Devices detect the collision.
- Devices wait a random period of time and retransmit data.


I cannot get to the payroll server.
Collision
I could have walked to Finance by now.
301P_104

Topologies

# Contention-Based Access – CSMA/CA

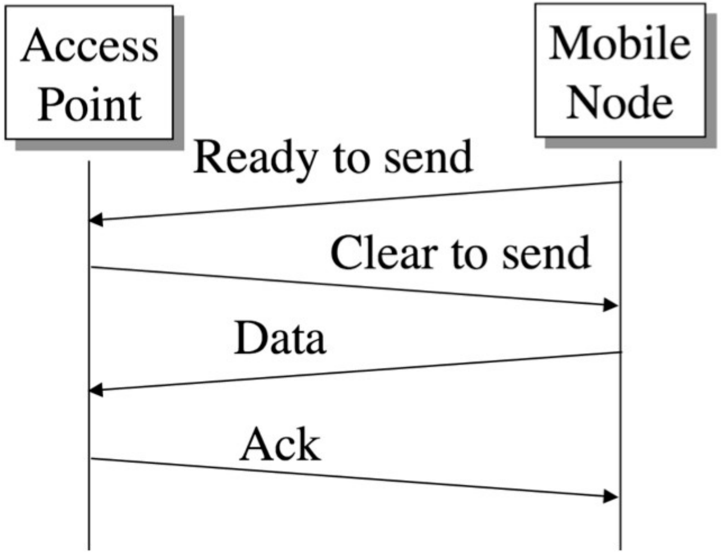
**CSMA/CA**

- Used by IEEE 802.11 WLANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.

**CSMA/CA collision avoidance process**:

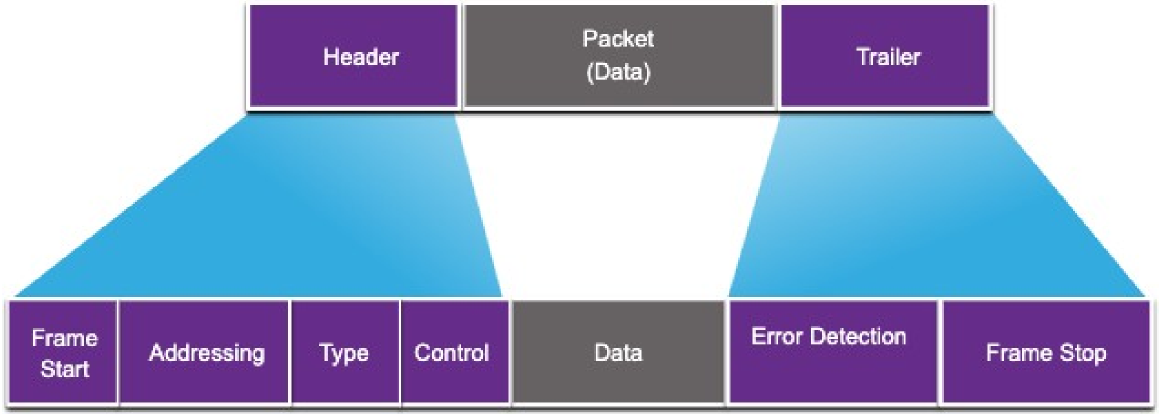
- When transmitting, devices also include the time duration needed for the transmission.
- Other devices on the shared medium receive the time duration information and know how long the medium will be unavailable.

**4-Way Handshake**



# 6.3 Data Link Frame

# Frame Fields

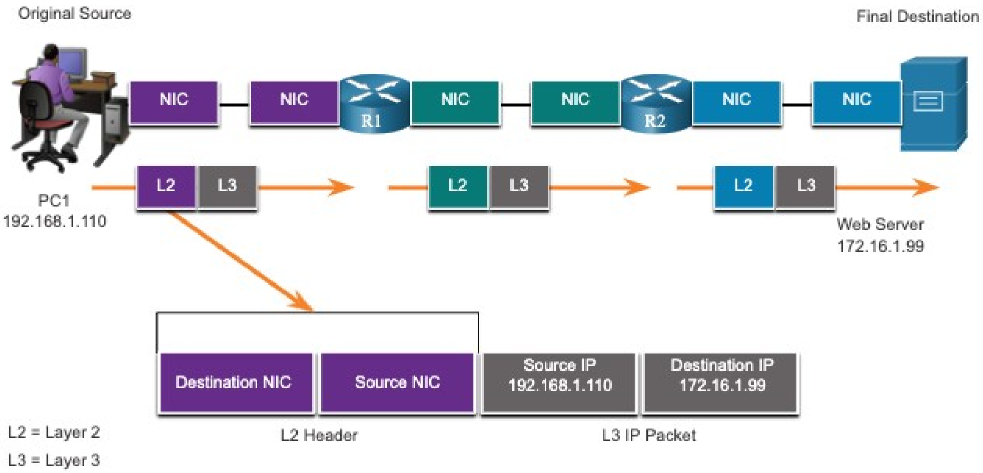


| Field | Description |
|---|---|
| Frame Start and Stop | Identifies beginning and end of frame |
| Addressing | Indicates source and destination nodes |
| Type | Identifies encapsulated Layer 3 protocol |
| Control | Identifies flow control services |
| Data | Contains the frame payload |
| Error Detection | Used for determine transmission errors |

## Data Link Frame

# Layer 2 Addresses

- Also referred to as a physical address.
- Contained in the frame header.
- Used only for local delivery of a frame on the link.
- Updated by each device that forwards the frame.



# LAN and WAN Frames

The logical topology and physical media determine the data link protocol used:

- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame-Relay

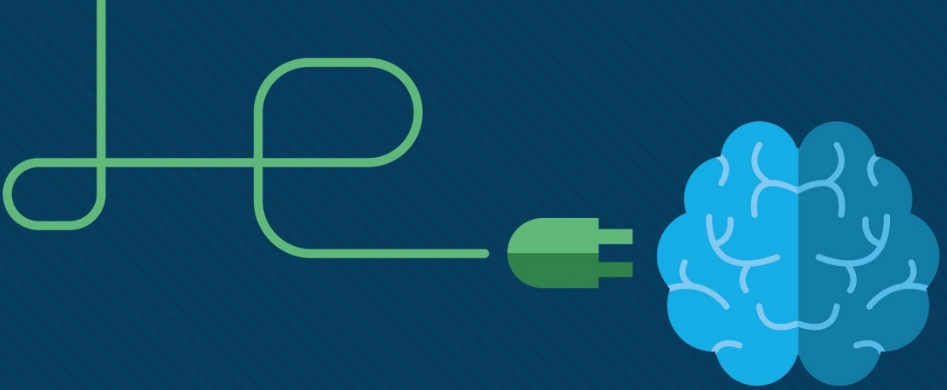
Each protocol performs media access control for specified logical topologies.

# 6.4 Module Practice and Quiz

Module Practice and Quiz

# What did I learn in this module?

- The data link layer of the OSI model (Layer 2) prepares network data for the physical network.
- The data link layer is responsible for network interface card (NIC) to network interface card communications.
- The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC.
- The two types of topologies used in LAN and WAN networks are physical and logical.
- Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh.
- Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously.
- In contention-based multi-access networks, all nodes are operating in half-duplex.
- Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.
- The data link frame has three basic parts: header, data, and trailer.
- Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection.
- Data link addresses are also known as physical addresses.
- Data link addresses are only used for link local delivery of frames.



# Module 7: Ethernet Switching

Introduction to Networks v7.0
(ITN)

# Module Objectives

**Module Title:** Ethernet Switching

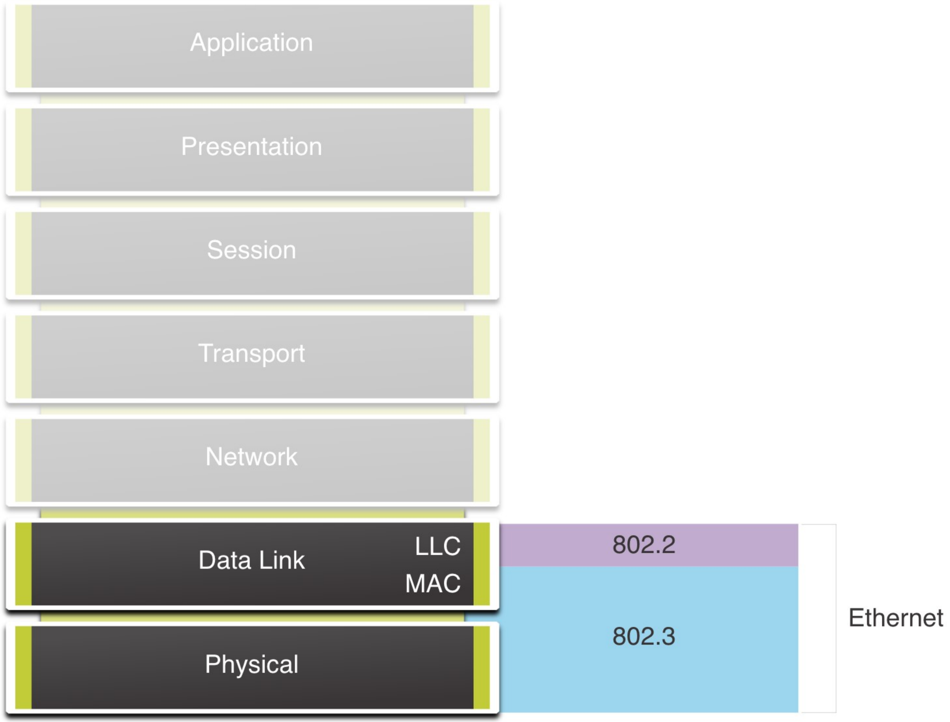
**Module Objective**: Explain how Ethernet works in a switched network.

| 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

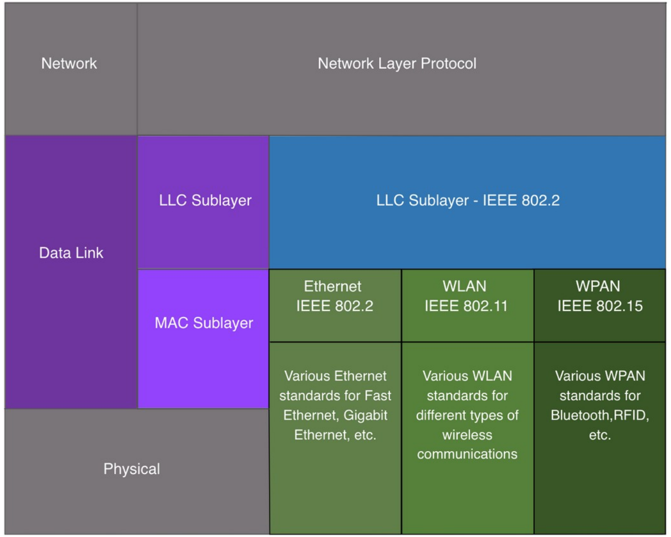
- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.



# 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.



Network

Network Layer Protocol

Data Link

LLC Sublayer

LLC Sublayer - IEEE 802.2

MAC Sublayer

Ethernet
IEEE 802.2

WLAN
IEEE 802.11

WPAN
IEEE 802.15

Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.

Various WLAN standards for different types of wireless communications

Various WPAN standards for Bluetooth,RFID, etc.

Physical

Ethernet Frames

# MAC Sublayer

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

**Data Encapsulation**

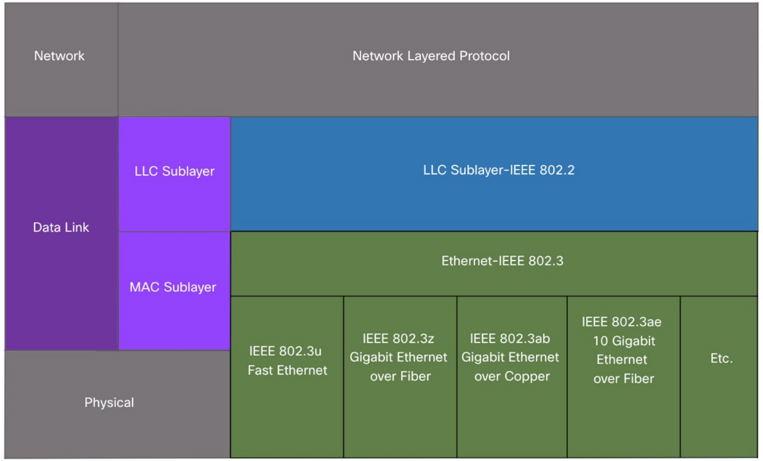
IEEE 802.3 data encapsulation includes the following:

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

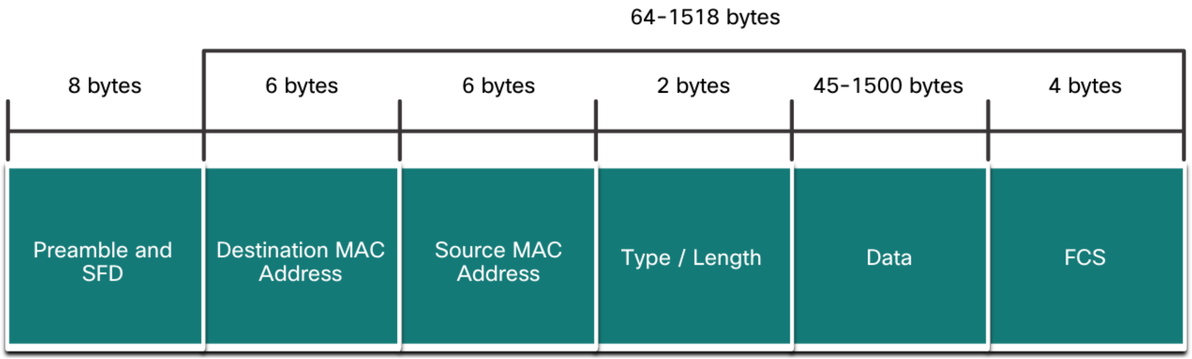
**Media Access**

- 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.


Network
Network Layered Protocol
Data Link
LLC Sublayer
LLC Sublayer-IEEE 802.2
MAC Sublayer
Ethernet-IEEE 802.3
Physical
IEEE 802.3u Fast Ethernet
IEEE 802.3z Gigabit Ethernet over Fiber
IEEE 802.3ab Gigabit Ethernet over Copper
IEEE 802.3ae 10 Gigabit Ethernet over Fiber
Etc.

# 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.

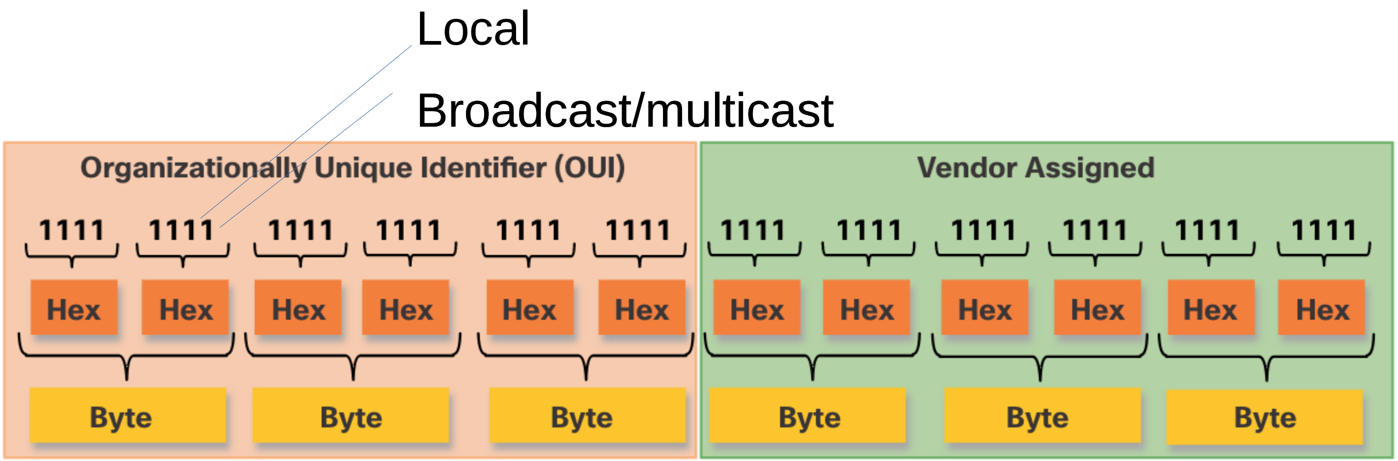


64-1518 bytes

| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 45-1500 bytes | 4 bytes |
|---|---|---|---|---|---|
| Preamble and SFD | Destination MAC Address | Source MAC Address | Type / Length | Data | FCS |

# 7.2 Ethernet MAC Address

# MAC Address



Local

Broadcast/multicast

Organizationally Unique Identifier (OUI)
Vendor Assigned
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111
Hex Hex Hex Hex Hex Hex Hex Hex Hex Hex Hex Hex
Byte Byte Byte Byte Byte Byte

00:AA:22:33:44:55

00-AA-22-33-44-55

## Ethernet MAC Addresses

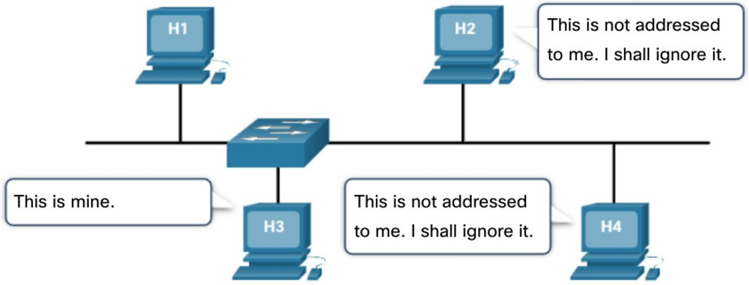
# Frame Processing

- 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.

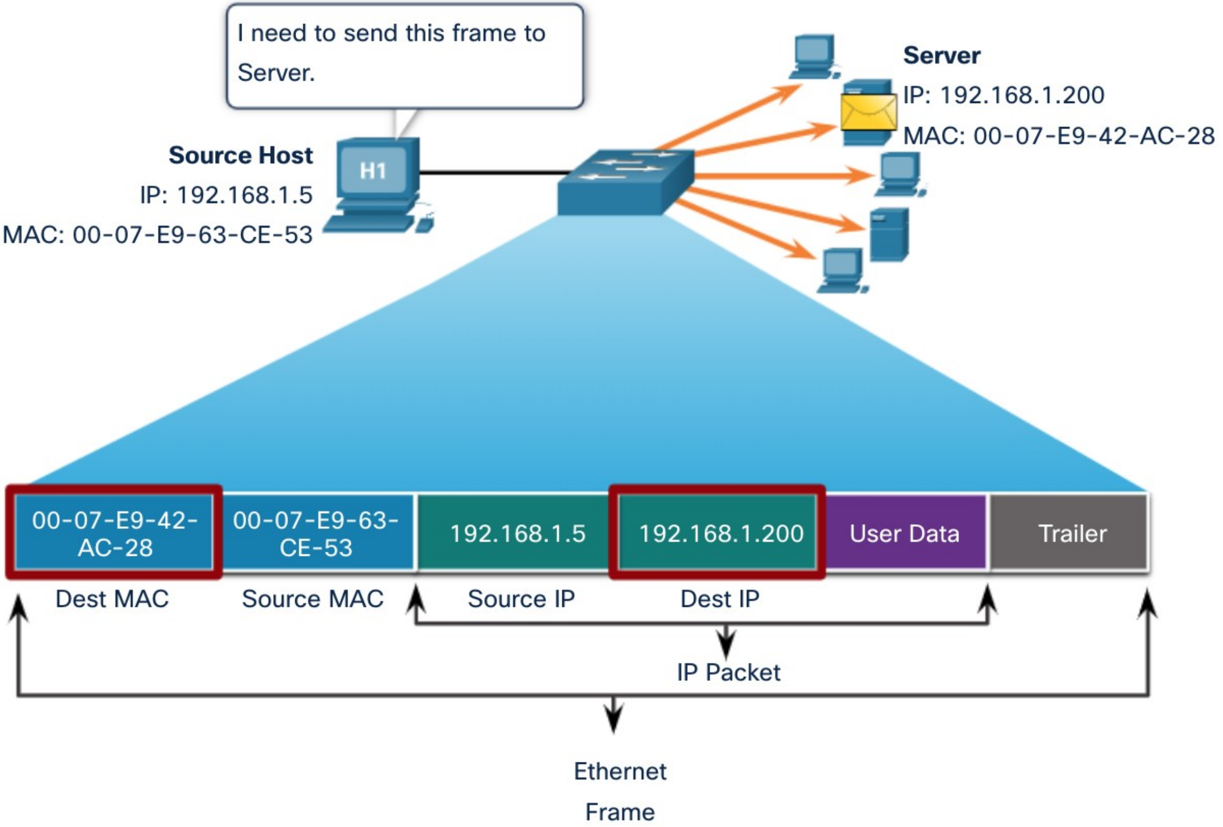
**Note:** Ethernet NICs will also accept frames if the destination MAC address is a **broadcast or a multicast** group of which the host is a member.

- 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 | | |

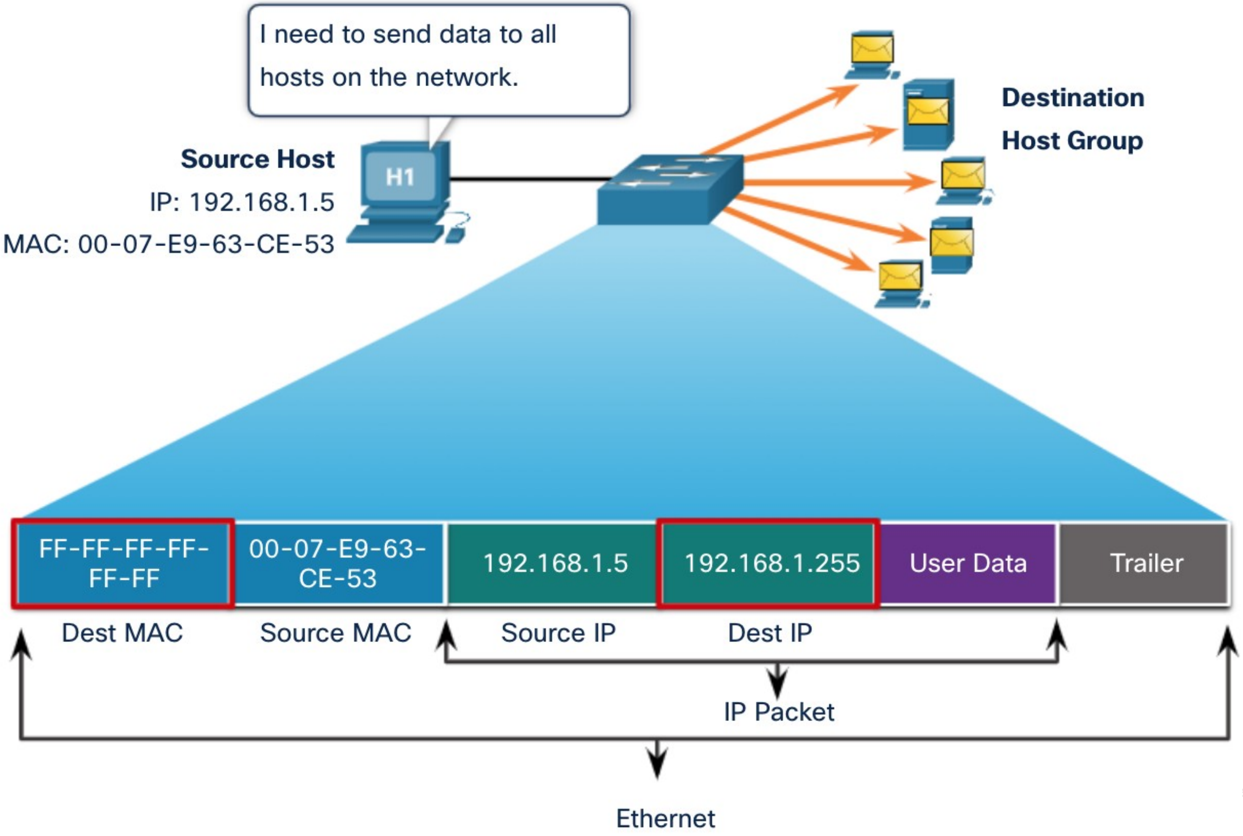

H1
H2
This is not addressed to me. I shall ignore it.
This is mine.
H3
This is not addressed to me. I shall ignore it.
H4

# Unicast MAC Address



## Ethernet MAC Addresses

# Broadcast MAC Address



I need to send data to all hosts on the network.

**Source Host**

IP: 192.168.1.5

MAC: 00-07-E9-63-CE-53

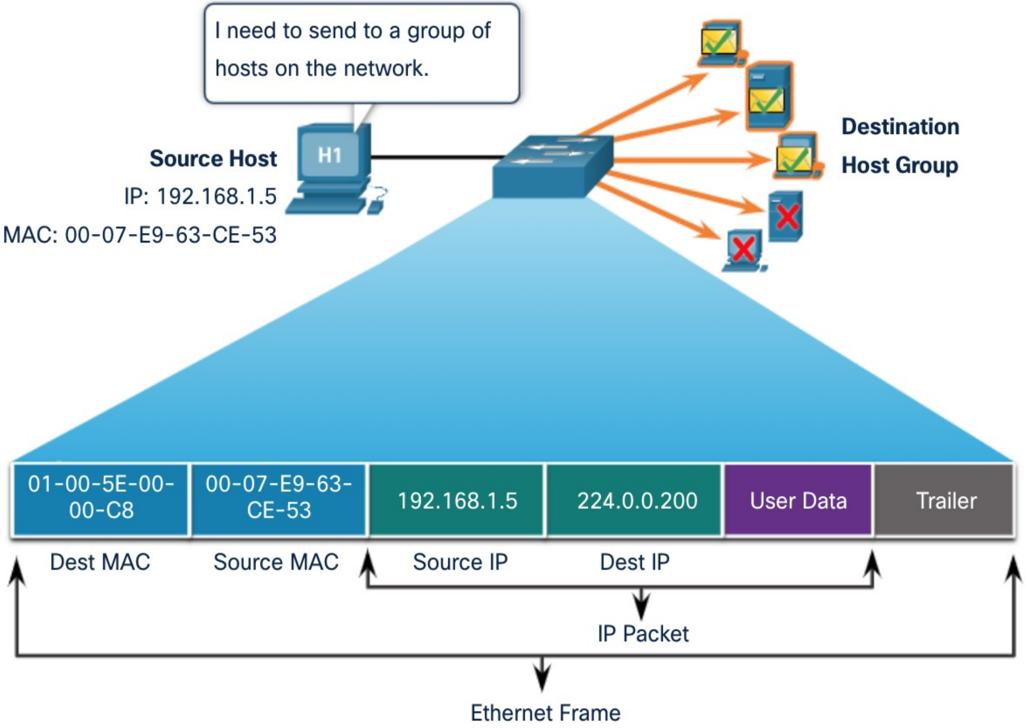
**Destination Host Group**

| Dest MAC | Source MAC | Source IP | Dest IP | | |
|---|---|---|---|---|---|
| FF-FF-FF-FF-FF-FF | 00-07-E9-63-CE-53 | 192.168.1.5 | 192.168.1.255 | User Data | Trailer |

## Ethernet MAC Addresses

# Multicast MAC Address

Multicast bit set
Not FF:FF:FF:FF:FF:FF



# 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**

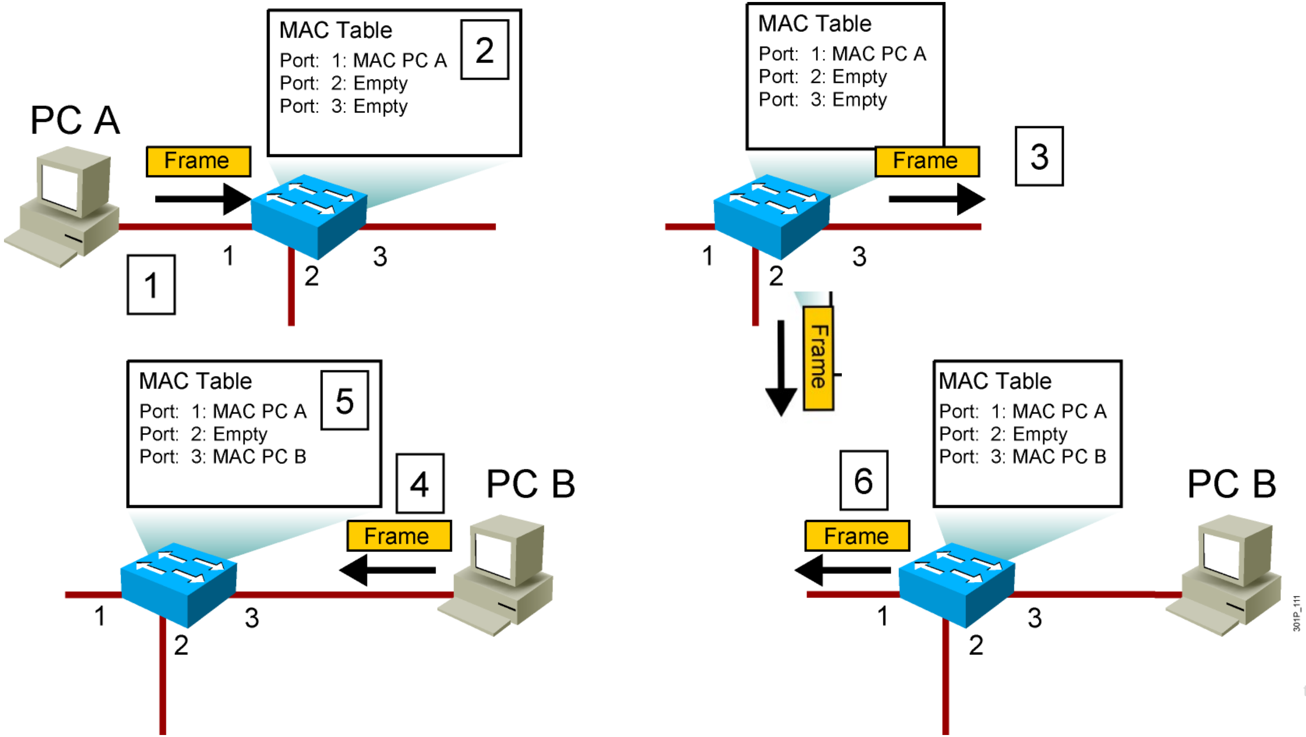
**Note**: The MAC address table is sometimes referred to as a content addressable memory **(CAM) table.**

## The MAC Address Table

# Switch Learning and Forwarding

**Examine the Source MAC Address (Learn)**

**Find the Destination MAC Address (Forward)**



MAC Table
Port: 1: MAC PC A
Port: 2: Empty
Port: 3: Empty

MAC Table
Port: 1: MAC PC A
Port: 2: Empty
Port: 3: Empty

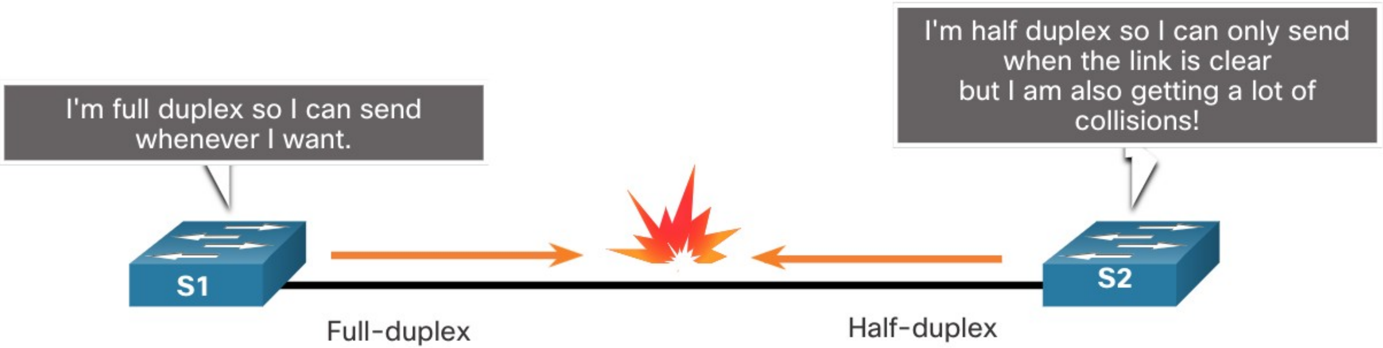
MAC Table
Port: 1: MAC PC A
Port: 2: Empty
Port: 3: MAC PC B

MAC Table
Port: 1: MAC PC A
Port: 2: Empty
Port: 3: MAC PC B

# 7.4 Switch Speeds and Forwarding Methods

# 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.


I'm full duplex so I can send whenever I want.
I'm half duplex so I can only send when the link is clear but I am also getting a lot of collisions!
S1
S2
Full-duplex
Half-duplex

## Switch Speeds and Forwarding Methods

# 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

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.