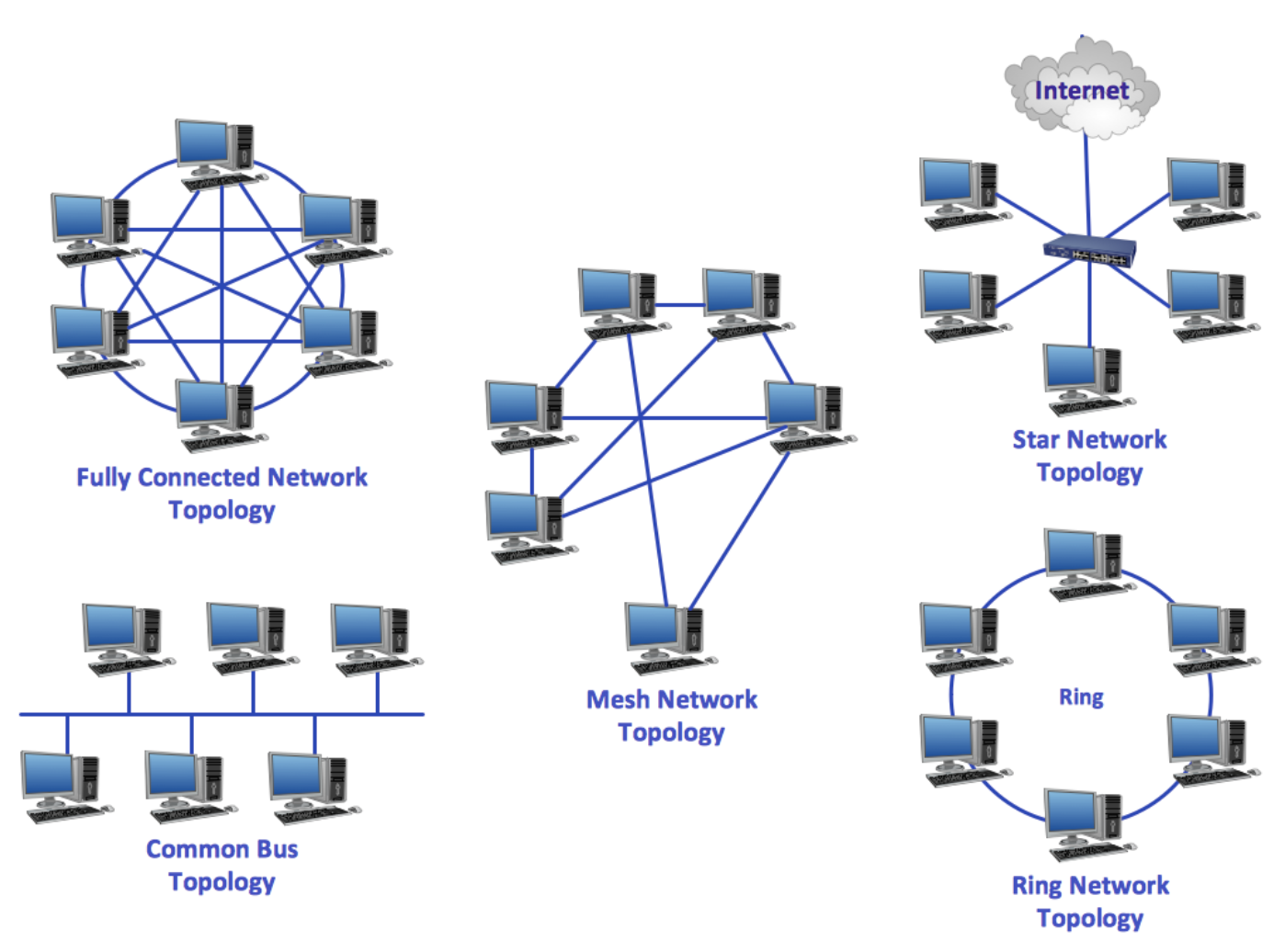
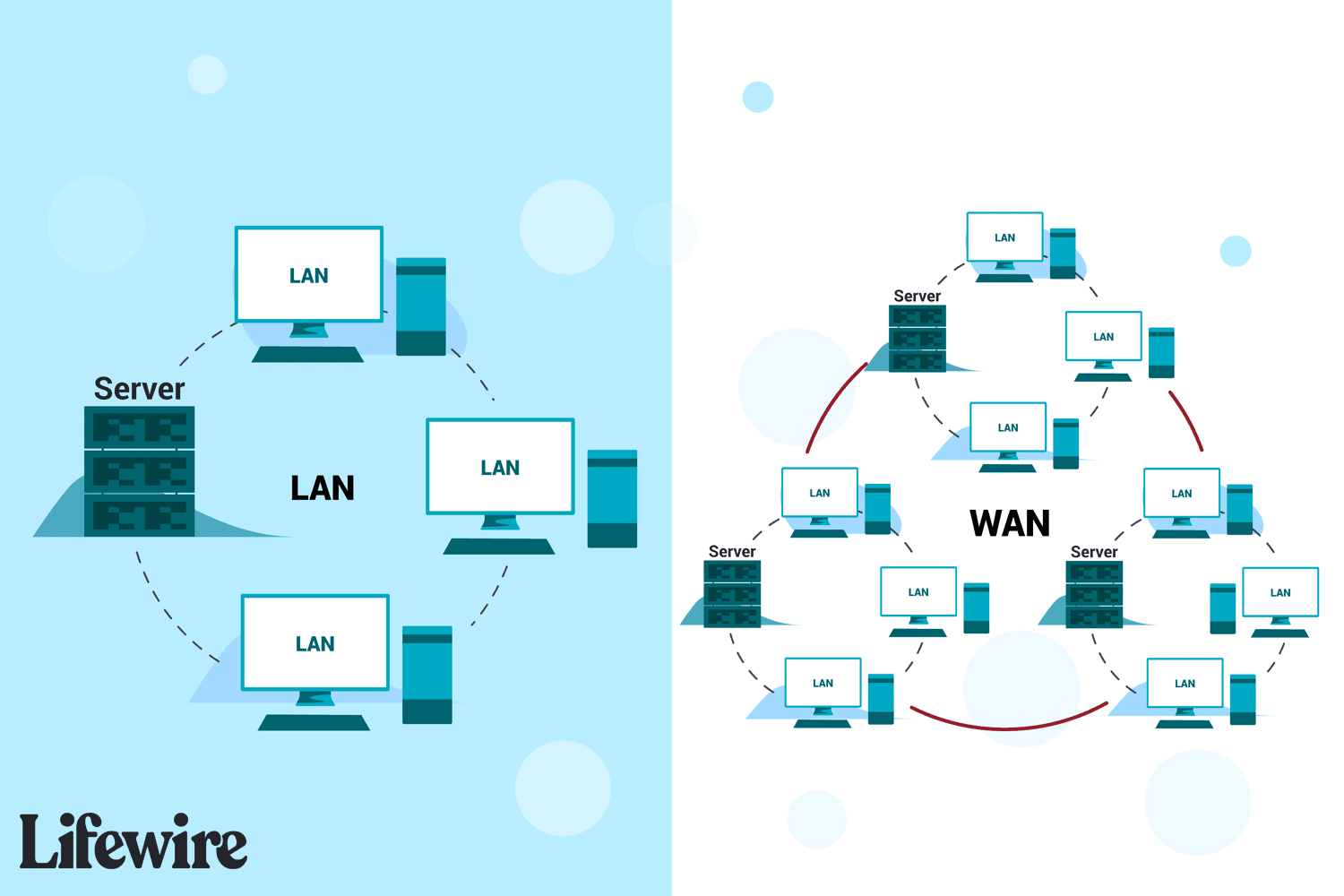
**TERM-2 CCNA Assignment**

Module 7 Network fundamentals

1. **Explain Network Topologies:**
   * Network topologies are how devices in a network are physically or logically arranged.
   * Common topologies include Bus, Ring, Star, Mesh, and Hybrid many other like point-to-point tree.
   * Each has its advantages, like simplicity or fault tolerance.

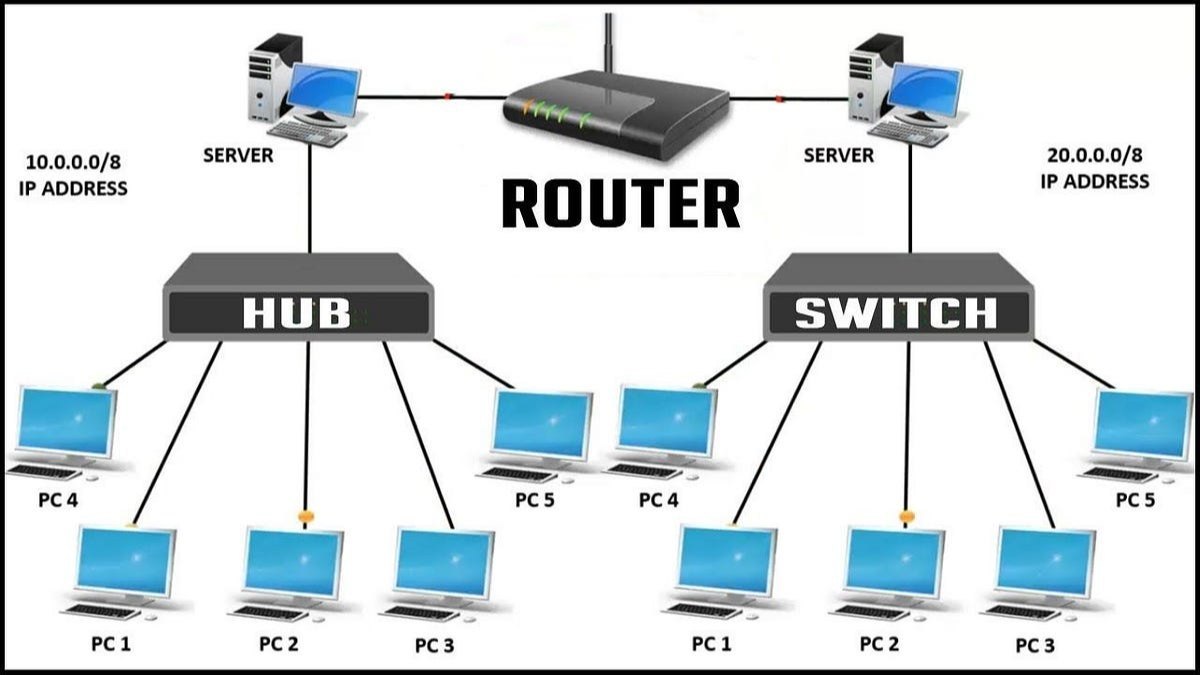


1. **Explain TCP/IP Networking Model:**
   * TCP/IP is a protocol suite for internet communication.
   * It consists of four layers: Application, Transport, Internet, and Link.
   * Each layer handles specific tasks, ensuring reliable data transmission.
2. **Explain LAN and WAN Networks:**
   * LAN (Local Area Network) is a network in a limited geographic area, like a building.
   * WAN (Wide Area Network) spans larger distances, connecting LANs across cities or countries.



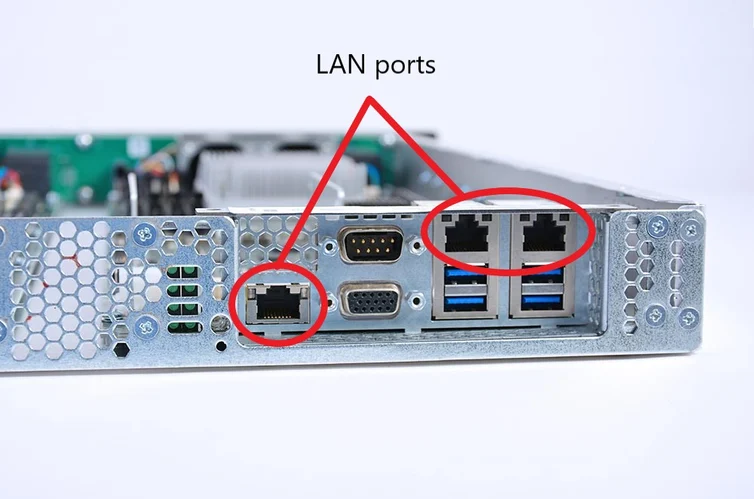


1. **Explain Operation of Switch:**
   * A switch connects devices in a LAN and uses MAC addresses to forward data.
   * It operates at the Data Link layer, making data transmission more efficient.



1. **Describe the Purpose and Functions of Various Network Devices:**
   * Routers connect different networks, directing data between them.
   * Hubs and switches connect devices within a network.
   * Modems enable communication between digital and analog systems.
2. **Make a List of the Appropriate Media, Cables, Ports, and Connectors to Connect Switches:**
   * Media: Ethernet cables.
   * Cables: Cat5e or Cat6 Ethernet cables.
   * Ports: Ethernet ports on switches.
   * Connectors: RJ45 connectors for Ethernet cables.





1. **Define Network Devices and Hosts:**
   * Network devices are hardware facilitating communication (routers, switches).
   * Hosts are devices, like computers, connected to a network.
   * Both play roles in data exchange within a network

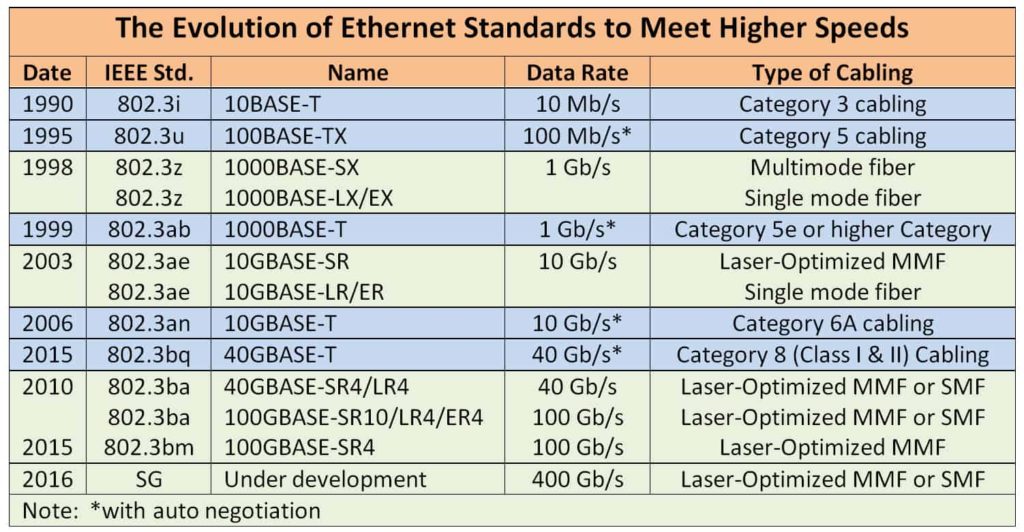
**What are Ethernet Standard (802.3) and Frame Formats?**

**Ethernet Standard (802.3):**

* **Definition:** IEEE 802.3 is the standard that defines the operation of Ethernet networks.
* **Purpose:** It specifies the rules for how devices in a network communicate and share the transmission medium.
* **Key Features:** Includes specifications for the physical layer (e.g., cable types) and the data link layer (e.g., frame format).
* **Variations:** Different versions exist, such as 10BASE-T (10 Mbps over twisted pair cables) and 1000BASE-T (1 Gbps over twisted pair cables).

**Frame Formats:**

* **Definition:** In networking, a frame is a unit of data transmitted over a network.
* **Ethernet Frame Components:**
  + **Preamble:** Synchronization bits to alert the receiving device.
  + **Destination and Source MAC Addresses:** Identifies the devices sending and receiving the frame.
  + **Type/Length Field:** Specifies the type of data or the length of the frame.
  + **Data:** The actual payload being transmitted.
  + **FCS (Frame Check Sequence):** Error-checking information to ensure data integrity.
* **Purpose:** Frames organize data for efficient transmission and provide error-checking mechanisms.



**Comparison between UTP, MM, and SM Ethernet Cabling:**

* **UTP (Unshielded Twisted Pair):** Common, affordable, suitable for short distances.
* **MM (Multimode):** Moderate cost, suitable for medium distances, uses multiple paths for light.
* **SM (Single-mode):** Higher cost, longer distances, uses a single path for light, suitable for long-range connections.
* **Making Cross Cable:**

**Materials Needed:**

1. Ethernet cable
2. RJ45 connectors
3. Crimping tool

**Steps:**

1. Strip about 1.5 inches (3-4 cm) of the outer insulation from both ends of the Ethernet cable.
2. Untwist and arrange the color-coded wires according to the T568A or T568B standard on one end of the cable.
3. Crimp the RJ45 connector onto the arranged wires using a crimping tool.
4. Repeat steps 2 and 3 for the other end, but this time use the opposite wiring standard (T568A or T568B).

**Result:** You have created a Cross cable, suitable for connecting two devices of the same type (e.g., PC to PC or switch to switch).

* **Making Straight-Through Cable:**

**Materials Needed:**

1. Ethernet cable
2. RJ45 connectors
3. Crimping tool

**Steps:**

1. Strip about 1.5 inches (3-4 cm) of the outer insulation from both ends of the Ethernet cable.
2. Untwist and arrange the color-coded wires according to the T568A or T568B standard on both ends of the cable. Make sure both ends follow the same standard.
3. Crimp the RJ45 connector onto the arranged wires at both ends using a crimping tool.

**Result:** You have created a Straight-Through cable, suitable for connecting devices of different types (e.g., PC to switch, router to computer).

**Differentiate between LAN/WAN Operation and Features:**

* + **LAN (Local Area Network):** Limited to a small geographic area like a building. Features high data transfer rates, low latency, and often used within an organization.
  + **WAN (Wide Area Network):** Spans larger distances, connecting LANs across cities or countries. Features lower data transfer rates due to the extended distance.

**Explain ARP, ICMP, and Domain Name:**

* + **ARP (Address Resolution Protocol):** Maps IP addresses to MAC addresses in a local network, facilitating communication between devices.
  + **ICMP (Internet Control Message Protocol):** Manages error messages and network diagnostics, including tools like Ping.
  + **Domain Name:** A human-readable name for internet resources, translating to IP addresses (e.g., [www.example.com](http://www.example.com/) to 192.168.1.1).

**Describe the Components Required for Network and Internet Communications:**

* + Devices (computers, routers, switches).
  + Cabling (Ethernet cables).
  + Protocols (TCP/IP).
  + Software (network operating systems, browsers).
  + Servers (DNS servers, web servers).

**Explain Encapsulation and Decapsulation in OSI Reference Model:**

* + **Encapsulation:** Data is wrapped with headers and trailers at each OSI layer during transmission.
  + **Decapsulation:** Headers and trailers are removed layer by layer upon receipt, revealing the original data.

**Explain Network Segmentation and Basic Traffic Management Concepts:**

* + **Network Segmentation:** Dividing a network into smaller segments to improve performance, security, and manageability.
  + **Traffic Management:** Controlling the flow of data to avoid congestion, ensuring efficient network utilization.

**What is Flow Control and Acknowledgment?**

* + **Flow Control:** Mechanisms to regulate data transmission speed, preventing congestion and ensuring a smooth flow of information across a network.
  + **Acknowledgment:** Confirmation signals sent by the receiver to the sender, indicating successful receipt of data packets. This ensures data integrity and helps manage the flow of information.

Use the OSI and TCP/IP models and their associated protocols to explain how data Flows in a network

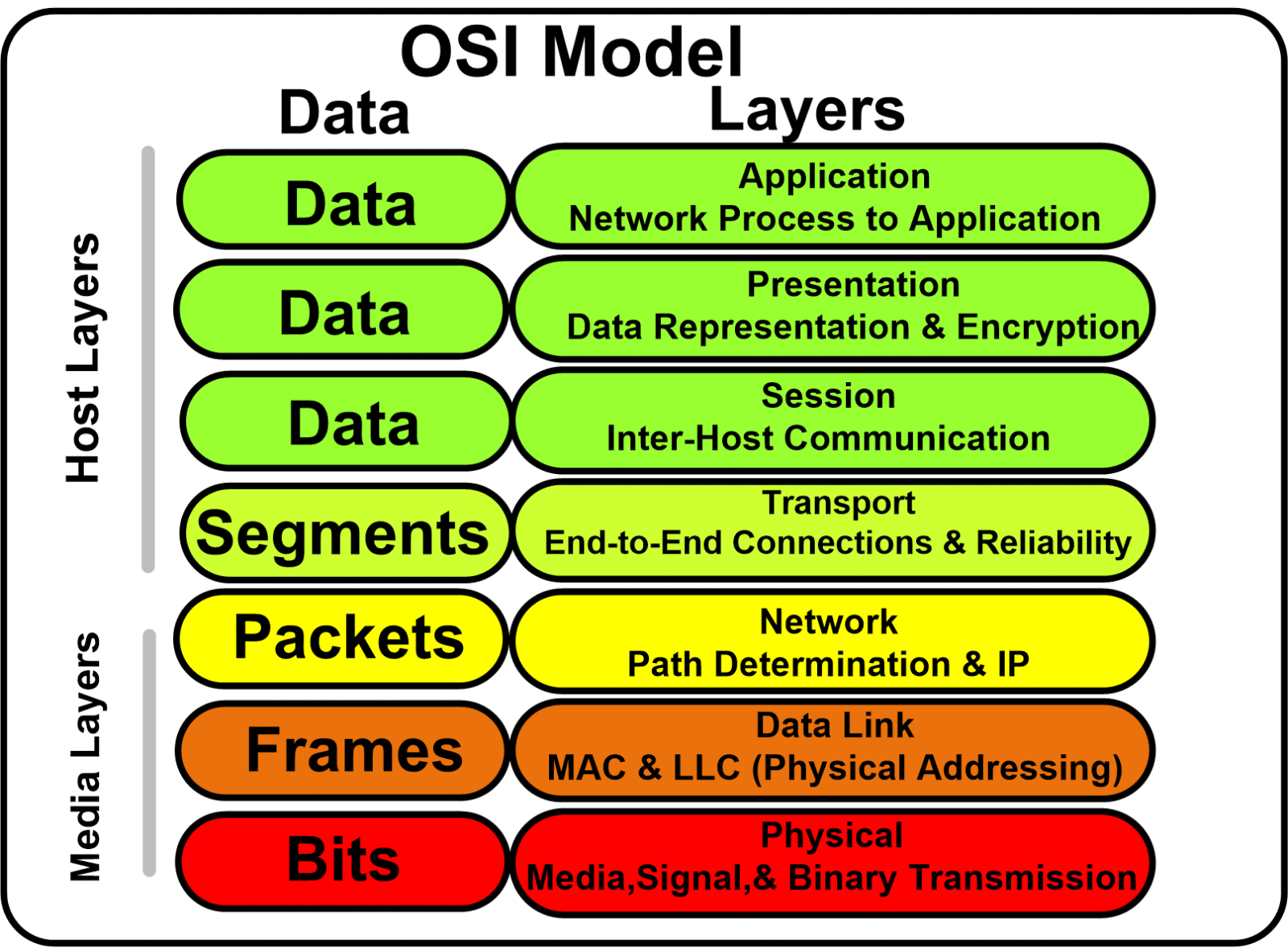
**Data Flow in a Network**:

* + OSI Model: The OSI (Open Systems Interconnection) model conceptualizes network communication into seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical layers. Each layer has its own set of protocols and functions. Data flows through these layers by encapsulating and de-encapsulating information as it moves through the network.
  + TCP/IP Model: The TCP/IP model, which is more commonly used in practical networking, consists of four layers: Application, Transport, Internet, and Network Access. Each layer corresponds to similar functions as the OSI model but with different terminology and protocols.

Identify and explain at layers 1, 2, 3, and 7 using a layered model approach

**Layers 1, 2, 3, and 7 Explained**:

* + Layer 1: The Physical layer deals with the physical aspects of data transmission, such as cables, connectors, and electrical signals.
  + Layer 2: The Data Link layer ensures reliable data transfer across the physical layer. It includes functions like framing, error detection, and MAC (Media Access Control) addressing.
  + Layer 3: The Network layer focuses on logical addressing and routing. It determines the best path for data packets to travel from the source to the destination across different networks.
  + Layer 7: The Application layer provides services directly to end-users and applications. It includes protocols for activities like file transfers, email, and web browsing.

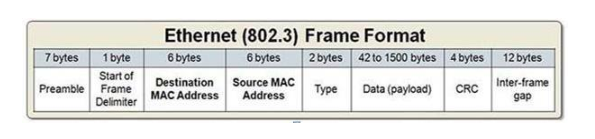


**Explain CSMA/CD and CSMA/CA**

**CSMA/CD and CSMA/CA**:

1. **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**:
   * CSMA/CD is a protocol used in Ethernet networks to govern how devices access the network medium.
   * "Carrier Sense" means that devices listen for a clear channel before attempting to transmit data.
   * "Multiple Access" indicates that multiple devices share the same communication medium.
   * "Collision Detection" refers to the process of detecting when two devices transmit data simultaneously, causing a collision.
   * If a collision occurs, devices stop transmitting, wait for a random amount of time, and then attempt to retransmit.
   * CSMA/CD is primarily used in wired Ethernet networks where collisions are possible due to shared communication channels.
2. **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:
   * CSMA/CA is a protocol used in wireless networks to avoid collisions.
   * Like CSMA/CD, CSMA/CA also involves "Carrier Sense," where devices listen for the channel's availability before transmitting.
   * However, in CSMA/CA, devices attempt to avoid collisions by waiting for a random period after detecting the channel is busy.
   * If the channel is clear for a predetermined time (the Distributed Inter-Frame Space), the device can transmit its data.
   * CSMA/CA is used in wireless networks where collisions are more prevalent due to the shared nature of the wireless medium and the hidden node problem.

Explain this frame and find layer



Based on the provided frame description, let's break it down:

7 bytes: Preamble - Helps the receiving device synchronize its clock with the incoming bitstream.

1 byte: Start of Frame Delimiter - Marks the start of the frame.

6 bytes: Destination MAC Address - Identifies the intended recipient of the frame.

6 bytes: Source MAC Address - Identifies the sender of the frame.

2 bytes: Type - Indicates the type of protocol data being carried in the payload.

42 to 1500 bytes: Data (Payload) - Actual information being transmitted.

4 bytes: CRC (Cyclic Redundancy Check) - Used for error detection in the frame.

Inter-frame gap - Period of silence between frames to allow for proper frame reception.

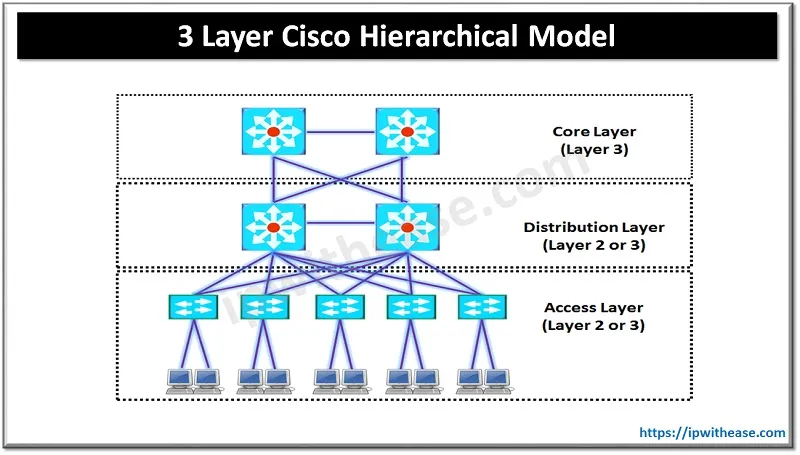
This frame format is associated with the Ethernet (802.3) frame format, which is used primarily in Ethernet networks.

Considering the elements described, this frame operates at the Data Link layer (Layer 2) of the OSI model. It includes MAC addresses (both source and destination) for addressing at the Data Link layer, along with a CRC for error detection, which are characteristics of Layer 2 protocols like Ethernet. Therefore, this frame belongs to Layer 2 of the OSI model.

**Draw and explain Cisco hierarchical modeTop of Form**

**Cisco Hierarchical Model**:

* + The Cisco hierarchical model divides a network infrastructure into three layers: Core, Distribution, and Access layers. The Core layer focuses on high-speed backbone connections, the Distribution layer provides routing, filtering, and WAN access, while the Access layer connects end-user devices to the network.
  + Core Layer: This layer is responsible for high-speed and reliable data transportation across the network. It typically involves high-end routers and switches optimized for fast data forwarding. The core layer ensures high availability and low latency for critical network services.
  + Distribution Layer: The distribution layer aggregates traffic from access layer switches and provides services like routing, filtering, and policy enforcement. It acts as an intermediary between the core and access layers, offering segmentation and security services.
  + Access Layer: The access layer provides connectivity for end-user devices such as computers, printers, and IP phones to the network. It involves switches that connect directly to end-user devices and enforce security policies. The access layer is where VLANs (Virtual Local Area Networks) are implemented to segment network traffic efficiently.

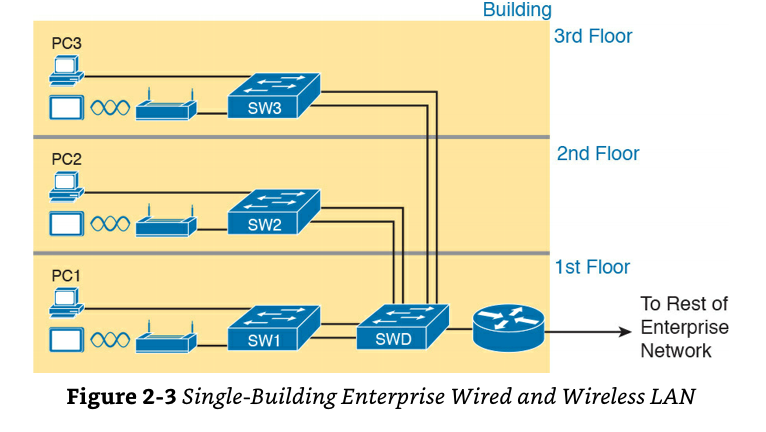




Drawing of a typical wired and wireless enterprise LAN

**Typical Wired and Wireless Enterprise LAN**:

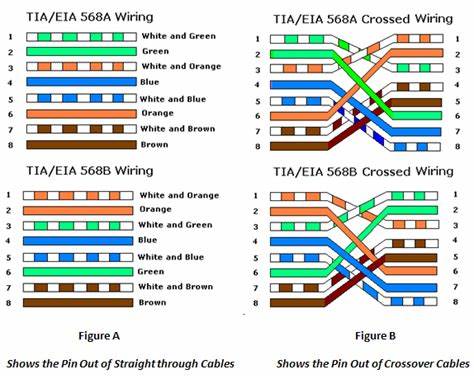
* + A typical wired LAN uses Ethernet cables to connect devices to switches or routers. These cables may include Cat5e, Cat6, or Cat6a cables for data transmission.
  + A wireless LAN utilizes wireless access points (APs) to provide connectivity to devices without physical cables. Devices communicate with APs using Wi-Fi protocols.



Describe the uses of straight-through and crossover Ethernet cables

**Straight-through and Crossover Ethernet Cables**:

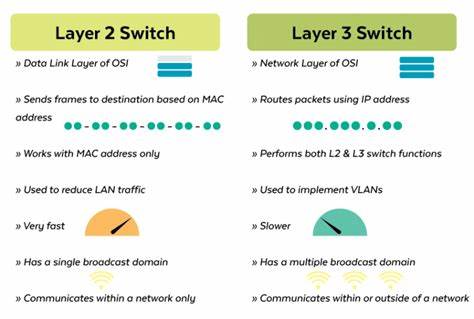
* + Straight-through cables have the same pin configuration on both ends and are used to connect devices of different types (e.g., a computer to a switch).
  + Crossover cables have different pin configurations on each end and are used to connect similar devices (e.g., switch to switch, or computer to computer).



Explain Layer 2 and Layer 3 Switch

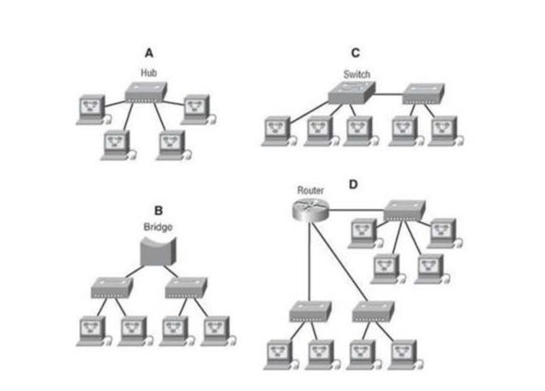
**Layer 2 and Layer 3 Switch**:

* + A Layer 2 switch operates at the Data Link layer (Layer 2) of the OSI model and makes forwarding decisions based on MAC addresses.
  + A Layer 3 switch operates at the Network layer (Layer 3) and can perform routing functions based on IP addresses in addition to Layer 2 switching.



Identifying Collision and Broadcast Domains

* **Hub**: A hub operates at the physical layer (Layer 1) of the OSI model. It does not create separate collision domains; all devices connected to a hub are in the same collision domain.
* **Switch**: A switch operates at the data link layer (Layer 2) of the OSI model. It creates separate collision domains for each port, which means that each port on a switch represents its own collision domain.
* **Router**: A router operates at the network layer (Layer 3) of the OSI model. It separates broadcast domains, meaning that it doesn't pass broadcast packets between different network segments, effectively containing broadcast traffic within each segment.
* **Bridge**: A bridge operates at the data link layer (Layer 2) of the OSI model. Similar to a switch, it creates separate collision domains for each port



Explain Spanning Tree Protocol

**Spanning Tree Protocol (STP)**:

* STP is a network protocol used to prevent loops in Ethernet networks. It works by dynamically shutting down redundant links between switches while keeping one link active for data transmission. This prevents the formation of network loops, which can lead to broadcast storms and network congestion. STP uses a distributed algorithm to select the best path through the network while blocking redundant paths.

Explain uncast Multicast and Broadcast

**Unicast, Multicast, and Broadcast**:

* **Unicast**: Unicast transmission sends data from one sender to one receiver. It is the most common type of communication in networks, where a single packet is delivered to a specific destination.
* **Multicast**: Multicast transmission sends data from one sender to multiple specific receivers. It is used for one-to-many communication where data is delivered simultaneously to a group of hosts interested in receiving it.
* **Broadcast**: Broadcast transmission sends data from one sender to all devices within a network segment. It is used for one-to-all communication, where data is sent to all devices in the broadcast domain.

Explain CAM (Content Addressable Memory)

**Content Addressable Memory (CAM)**:

* CAM is a type of memory used in networking devices like switches to store MAC addresses and associated port numbers. It allows for quick lookups of MAC addresses, enabling switches to forward frames to the correct port based on destination MAC addresses.

Explain CAM (Ternary Content Addressable Memory)

**Ternary Content Addressable Memory (TCAM)**:

* TCAM is an advanced form of CAM that provides more flexibility in matching patterns. It allows for ternary searches, where a search key can have three states: 0, 1, or "don't care." TCAM is commonly used in networking devices for implementing access control lists (ACLs) and Quality of Service (QoS) policies.

Which command use of Show MAC TABLE?

**Show MAC TABLE Command**:

* The "show mac address-table" command is used in Cisco IOS devices to display the MAC address table, also known as the MAC address forwarding table. This table contains information about MAC addresses learned by the switch and the associated switch ports. It shows which MAC addresses are reachable via which switch ports. This command is useful for troubleshooting network connectivity issues and verifying MAC address learning and forwarding behavior on the switch.