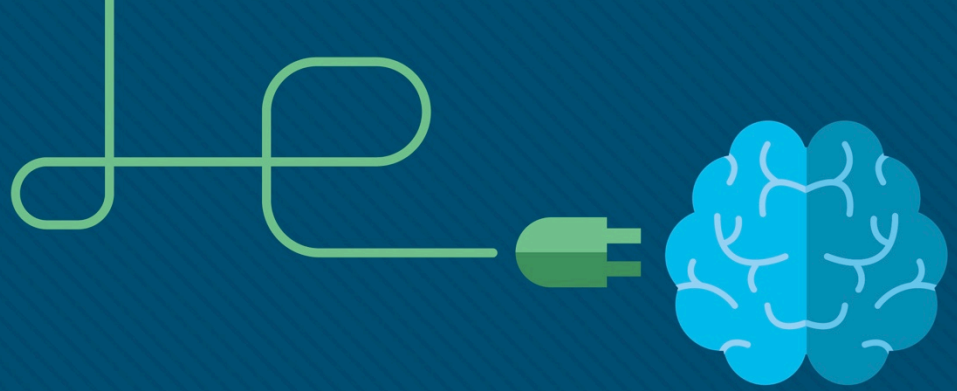


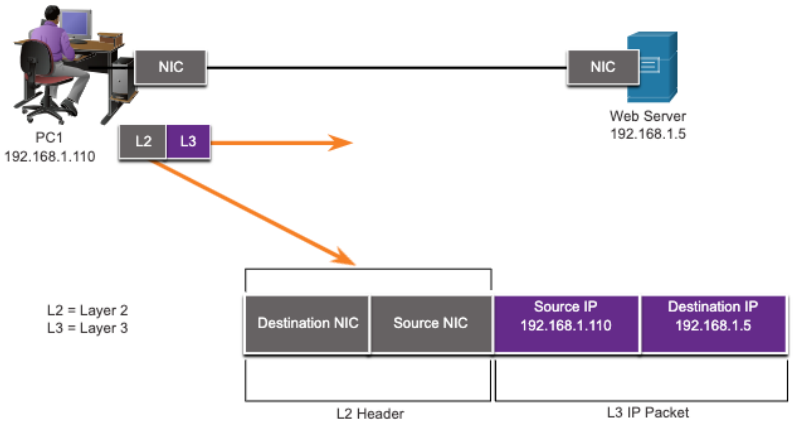
Module 4: Data Link Layer

Introduction to Networks v7.0
(ITN)

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.



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).**

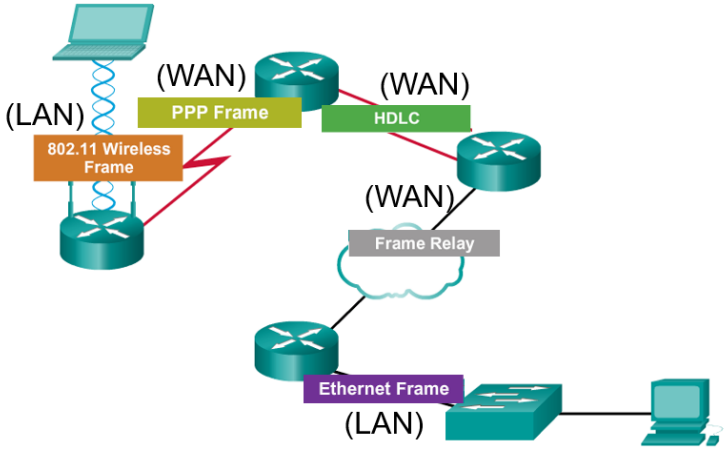
- The LLC sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- The MAC sublayer is responsible for data encapsulation and media access control.

Providing Access to Media

Packets exchanged between nodes may experience numerous data link layers and media transitions.

At each hop along the path, a router performs four basic Layer 2 functions:

- Accepts a frame from the network medium.
- De-encapsulates the frame to expose the encapsulated packet.
- Re-encapsulates the packet into a new frame.
- Forwards the new frame on the medium of the next network segment.



Topologies

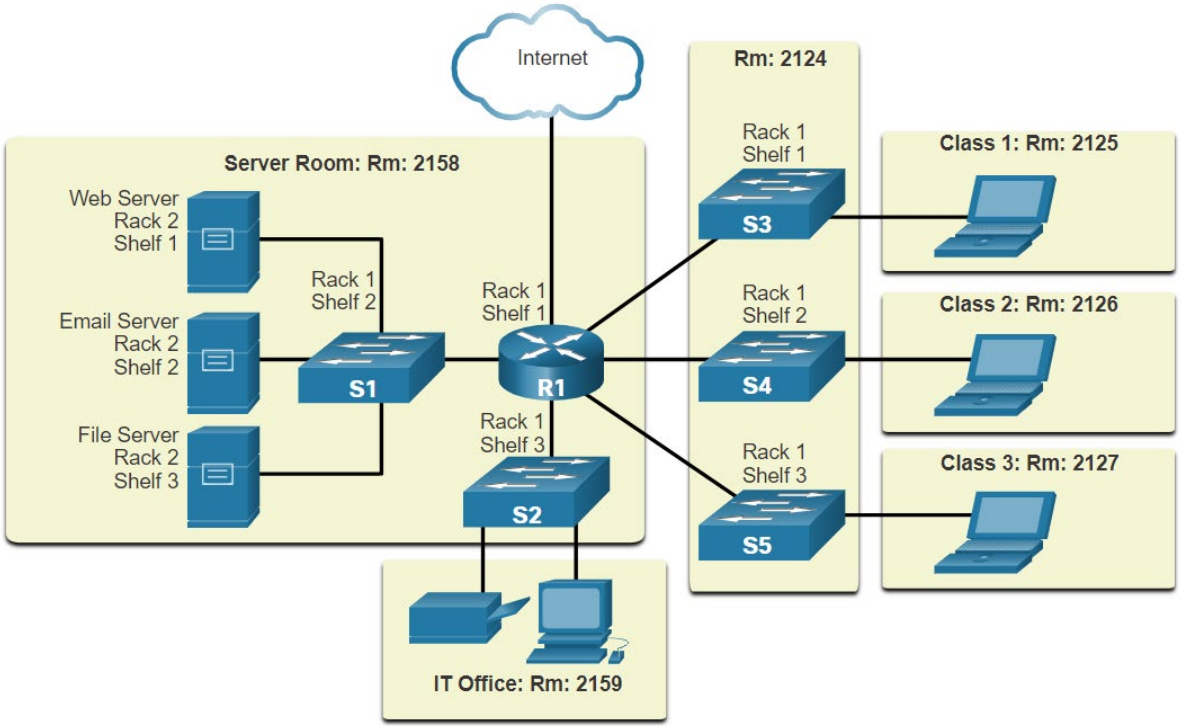
Physical and Logical Topologies

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

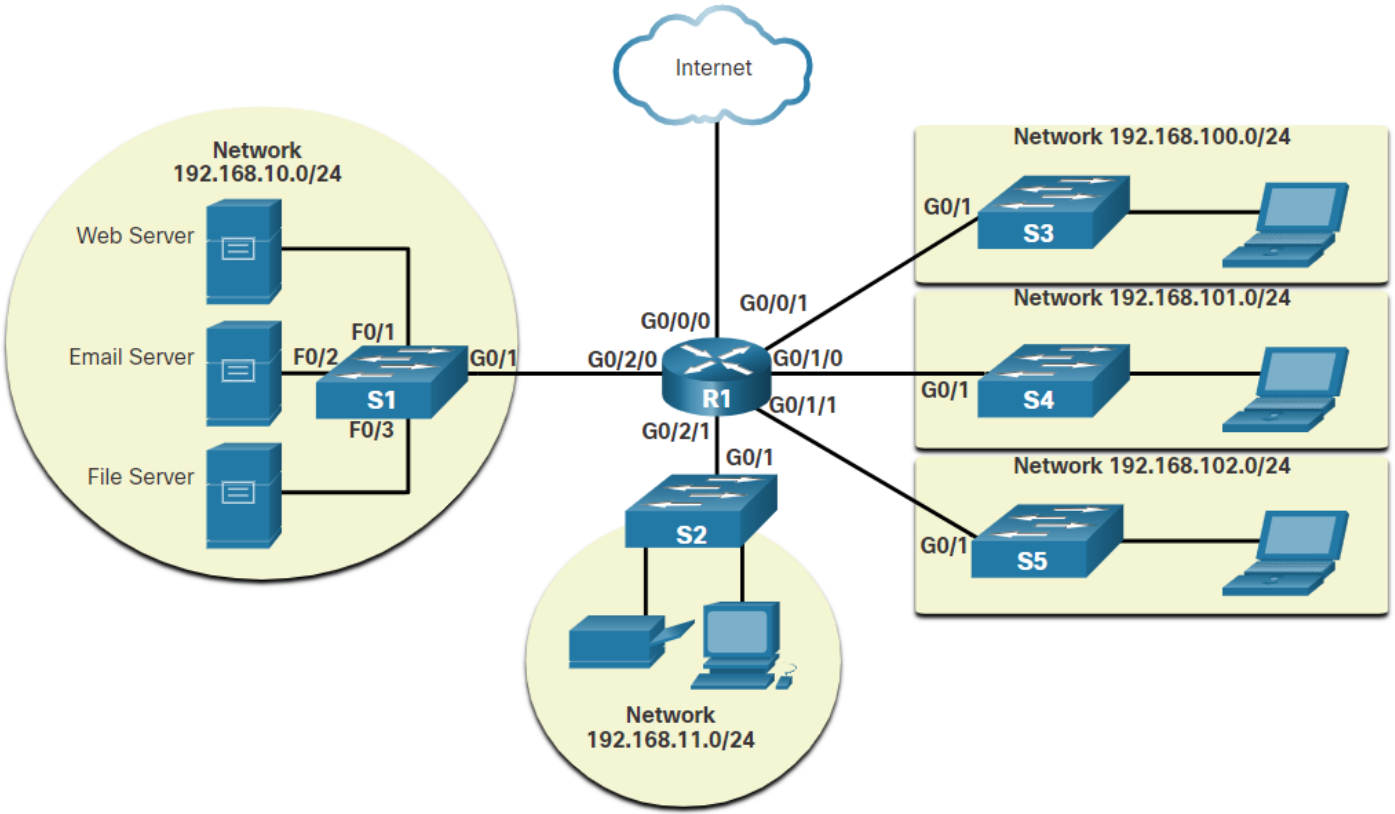
There are two types of topologies used when describing networks:

- **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



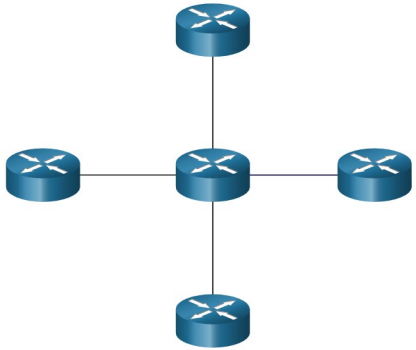
Logical Topology

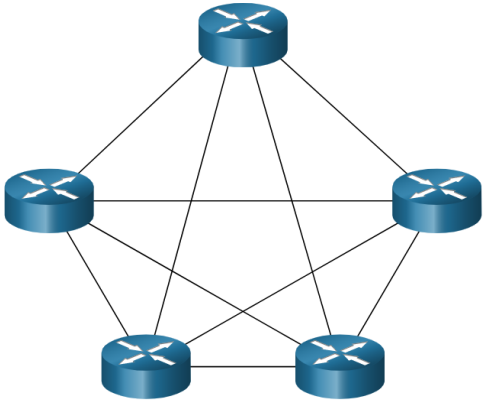


WAN Topologies

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.





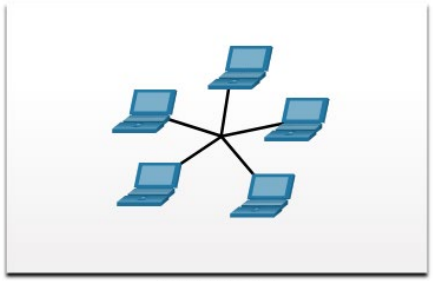
LAN Topologies

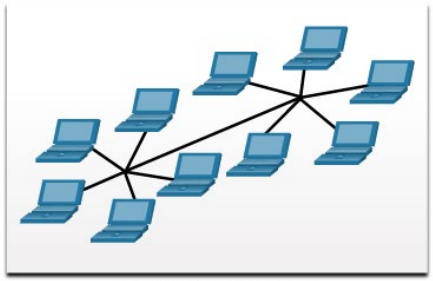
End devices on LANs are typically interconnected using a star or extended star topology. Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.

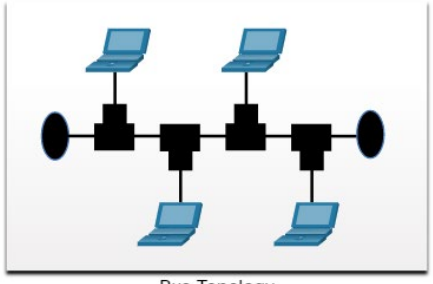
Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

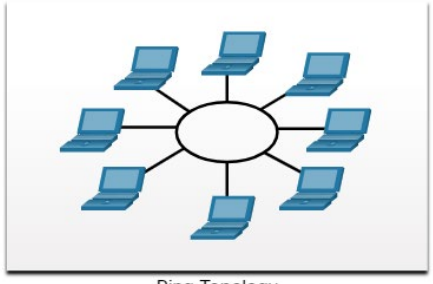
- **Bus** – All end systems chained together and terminated on each end.
- **Ring** – Each end system is connected to its respective neighbors to form a ring.

Physical Topologies


Star Topology


Extended Star Topology


Bus Topology


Ring Topology

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.

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 LANs.

Controlled access

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

Data Link Frame

The Frame

Data is encapsulated by the data link layer with a header and a trailer to form a frame.

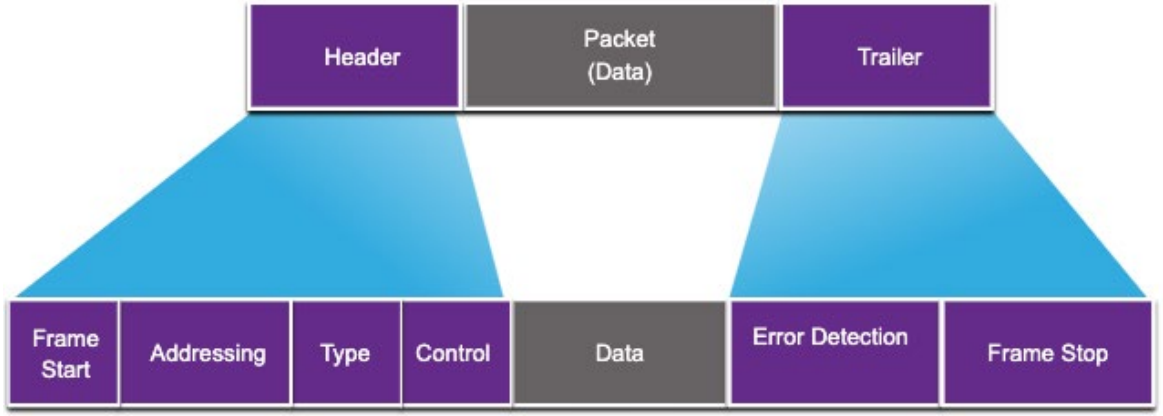
A data link frame has three parts:

- Header
- Data
- Trailer

The fields of the header and trailer vary according to data link layer protocol.

The amount of control information carried with in the frame varies according to access control information and logical topology.

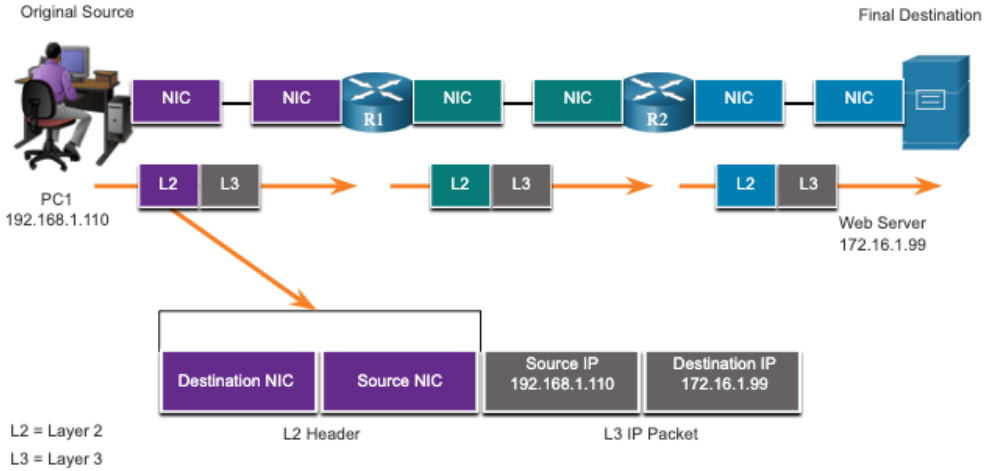
Frame Fields



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

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:

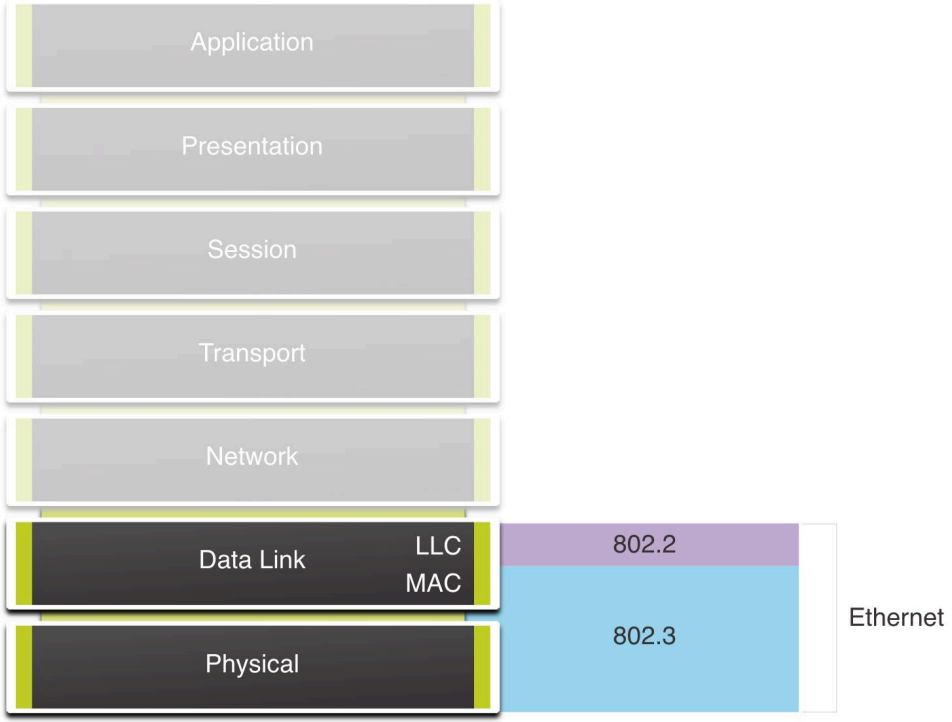
- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame-Relay

Each protocol performs media access control for specified logical topologies.

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.



MAC Sublayer

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

Data Encapsulation

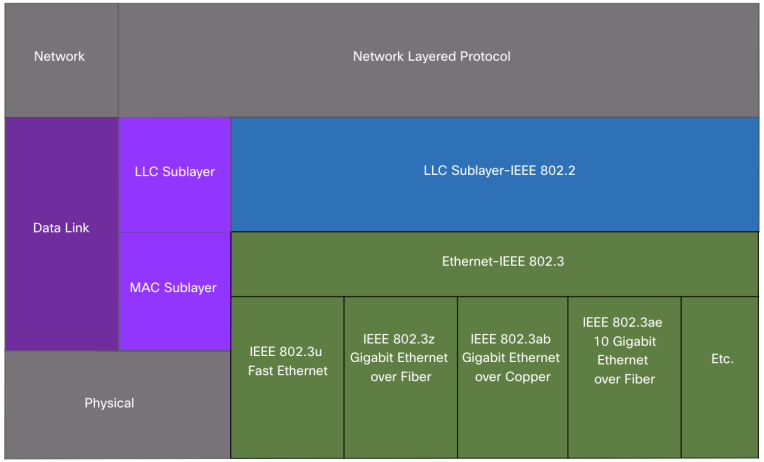
IEEE 802.3 data encapsulation includes the following:

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

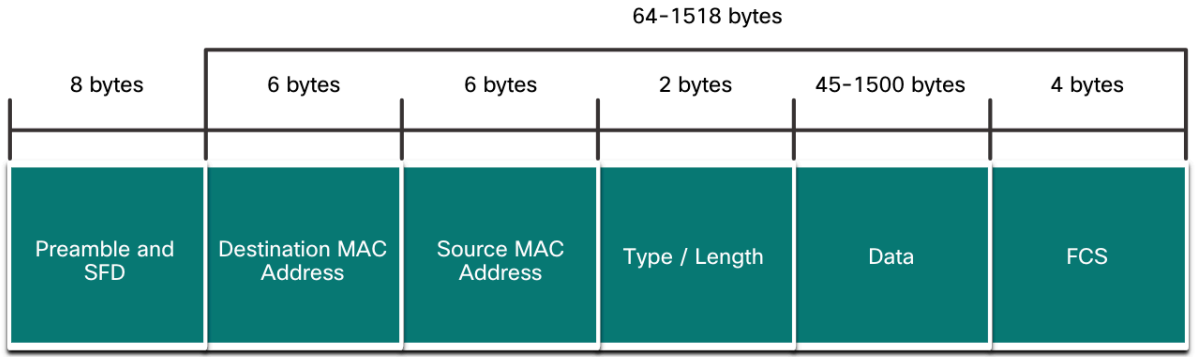
Media Access

- 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.



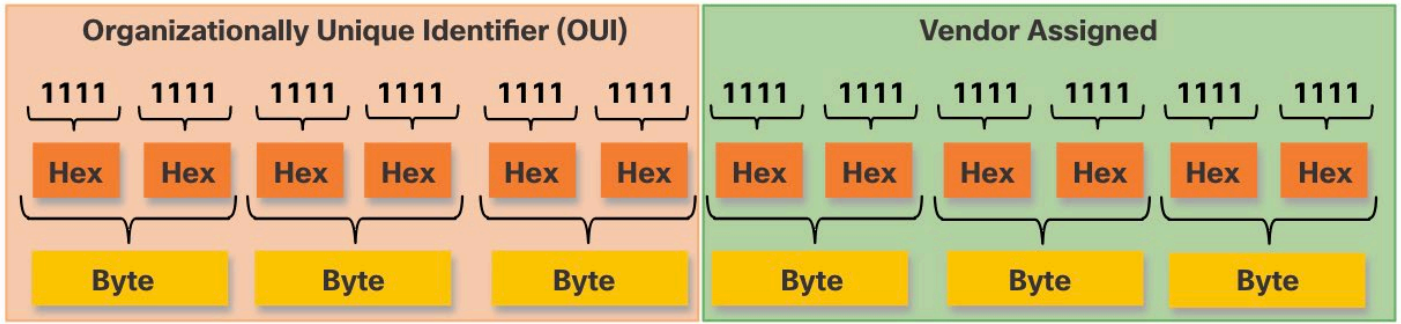
Ethernet MAC Address

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.

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.

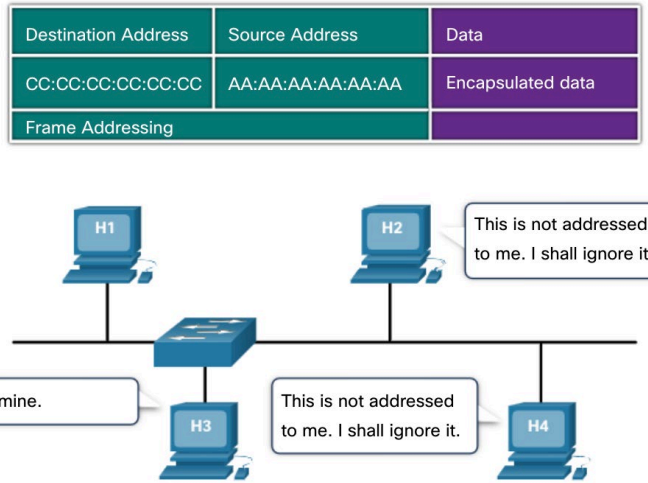


Frame Processing

- 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.

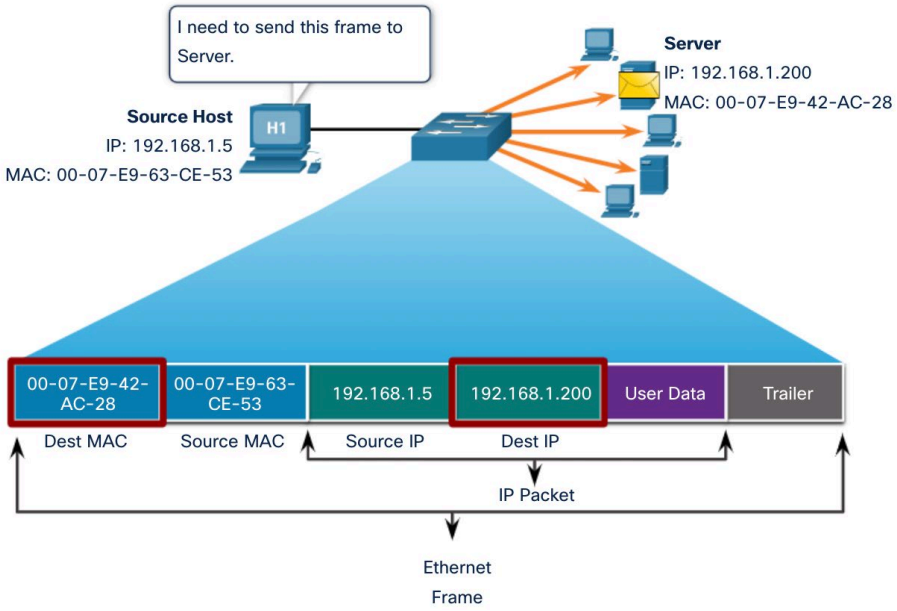


Unicast MAC Address

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).

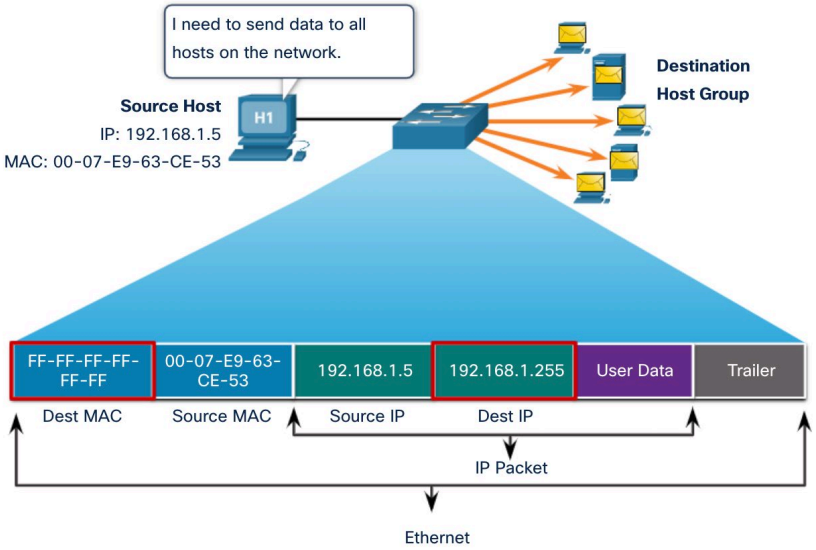
Note: The source MAC address must always be a unicast.



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.




CISCO