



# Introduction to Networking

CTO43-3-1 Version VD1



**A . P . U**  
ASIA PACIFIC UNIVERSITY  
OF TECHNOLOGY & INNOVATION

## Ethernet



# Topics and Structure of the lesson

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.
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.
MAC and IP	Compare the roles of MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

# Key Terms You Must Be Able To Use

If you have mastered this topic, **you should be able to use the following terms correctly in your exams:**

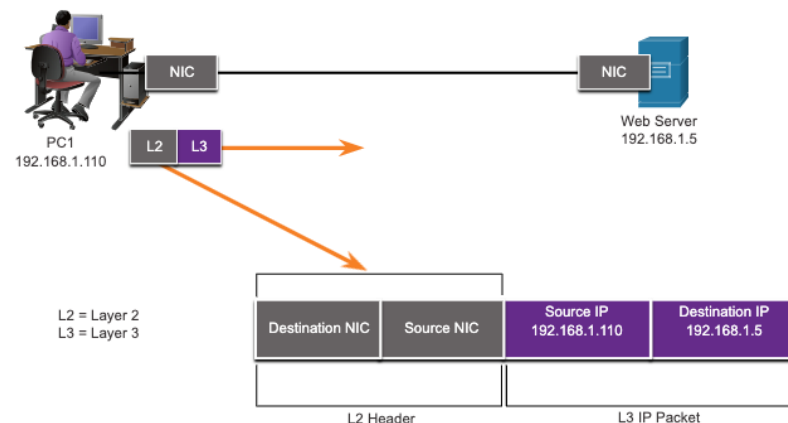
- Data Link Layer and Standards
- Topologies LAN and WAN
- Access Control Methods: CSMA/CD – CSMA/CA
- Data Link Frames
- Ethernet Encapsulation
- Data Link Sub-Layer and MAC Sub-Layer
- Ethernet Frame Fields and MAC Address
- MAC Address and Hexadecimal
- Unicast, Multicast and Broadcast MAC Address
- MAC Address Table
- Switching, Learning and Forwarding
- Frame Forwarding and Cut Through Switching
- Half and Full Duplex /Duplex and Speed Settings/AUTO-MDIX
- MAC and IP
- Address Resolution Protocol (ARP)/ARP Broadcast and ARP Spooling

# Purpose of the Data Link Layer

# 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.

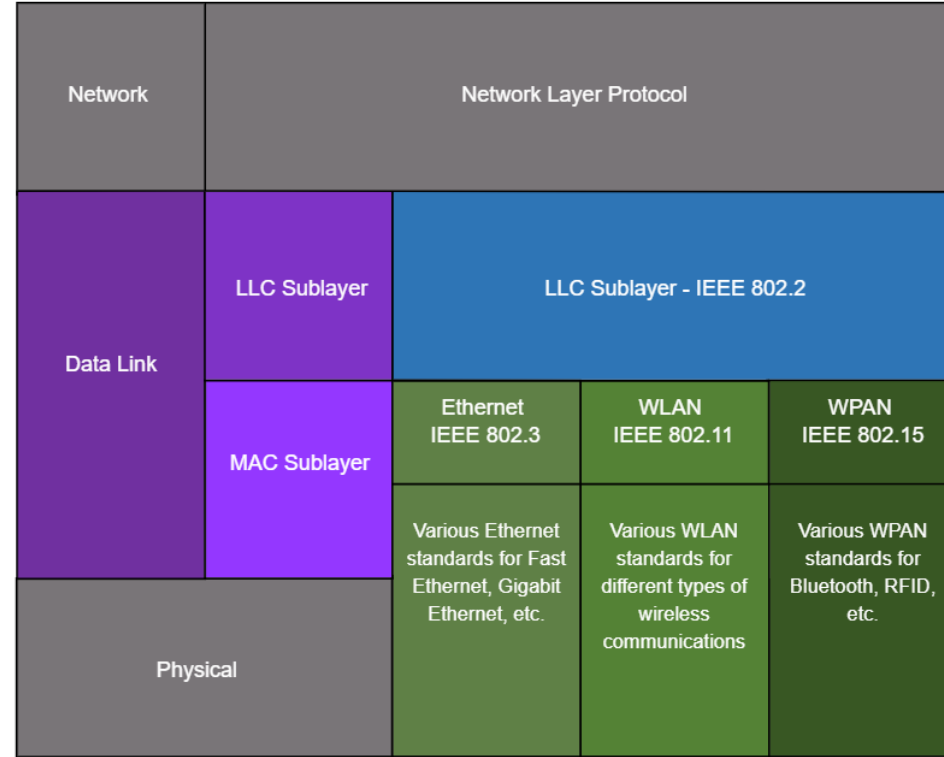


# IEEE 802 LAN/MAN Data Link Sublayers

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.



## Purpose of the Data Link Layer

# 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.

# 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).

\*IETF maintains protocols and services for TCP/IP Protocol Suite in the upper layers but it does not define functions and operation of the TCP/IP Network Access Layer





# Topologies

# 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:

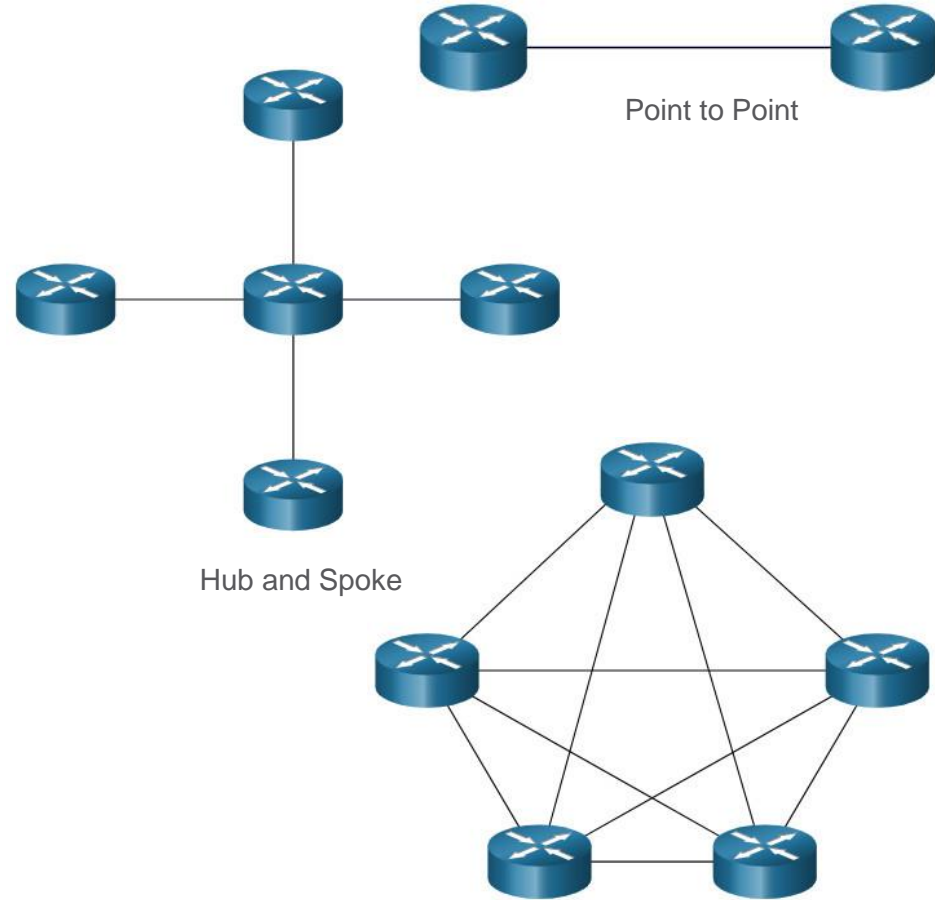
- **Physical topology** – shows physical connections and how devices are interconnected.
  - Eg. Room No, Location of the Equipment Rack
- **Logical topology** – identifies the virtual connections between devices using device interfaces and IP addressing schemes.
  - Eg IP addressing scheme

# 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.



# 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.

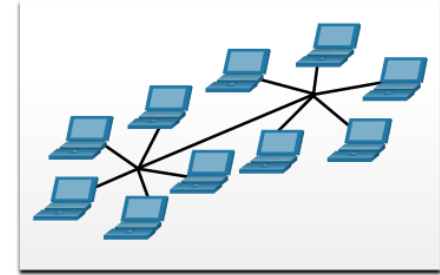
Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

- **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.

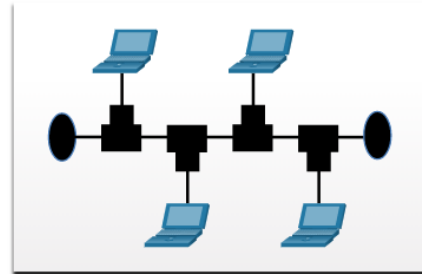
### Physical Topologies



Star Topology



Extended Star Topology



Bus Topology



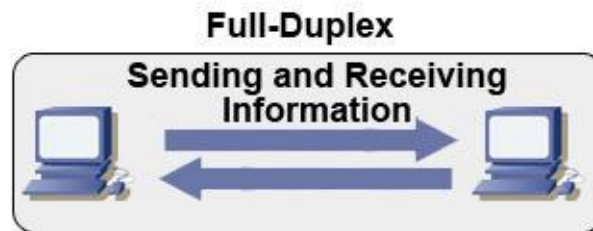
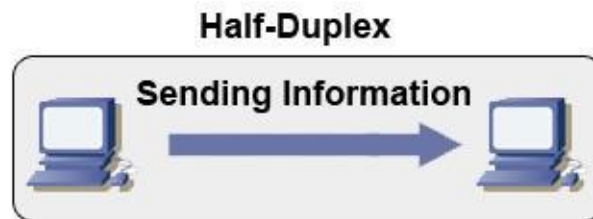
Ring Topology

# Topologies

## 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.

# Topologies

## Access Control Methods

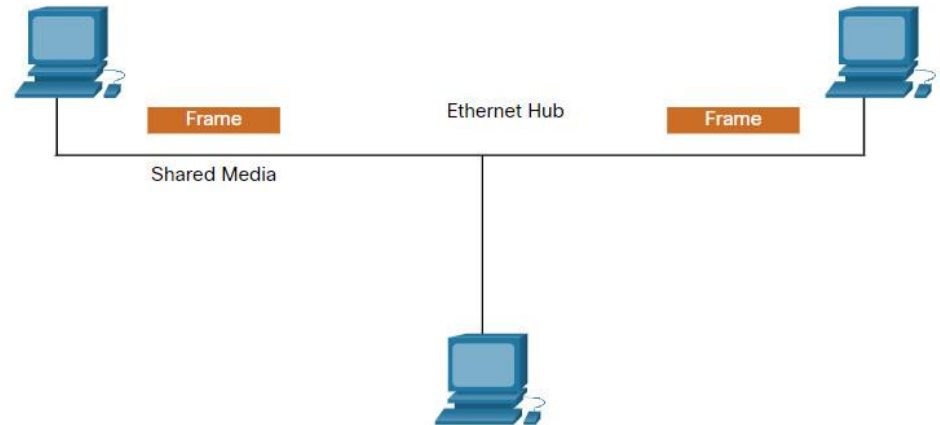
### Contention-based access

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 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.



# 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.



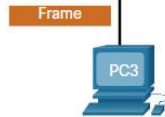
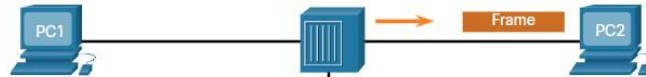
# Topologies

## Contention-Based Access – CSMA/CD

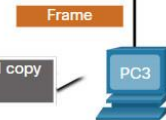
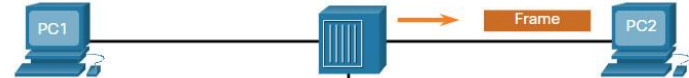
The medium is available so I will send the Ethernet frame to PC3.



I have a frame to send but I have to wait because I am receiving a frame.



This frame is not for me, so I will ignore it.



This frame is for me, so I will copy the entire frame.

# Topologies

## Contention-Based Access – CSMA/CA

### **CSMA/CA**

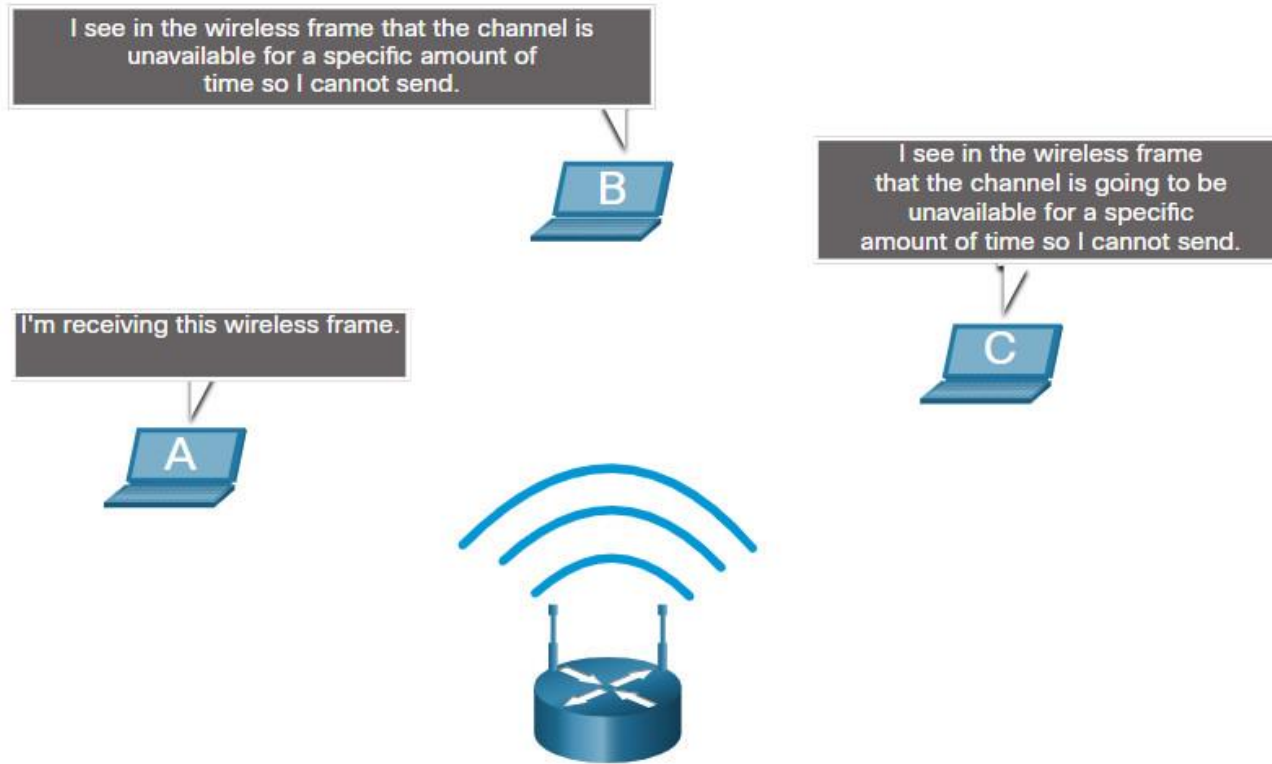
- Used by IEEE 802.11 WLANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.

### **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.

# Topologies

## Contention-Based Access – CSMA/CA



# Data Link Frame

# Data Link Frame

## The Frame

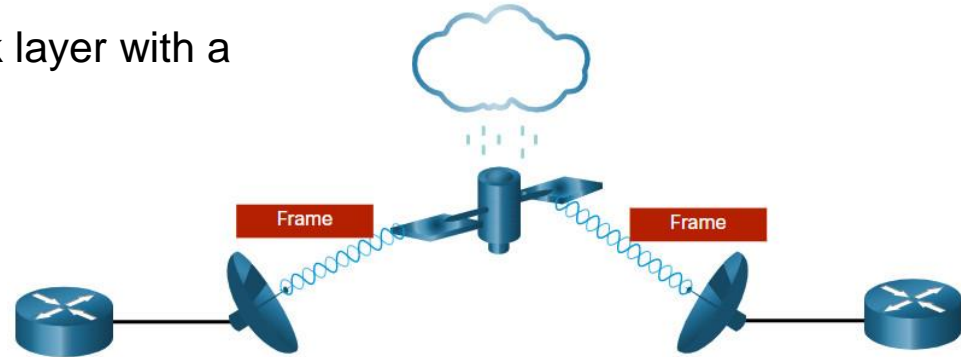
Data is encapsulated by the data link layer with a header and a trailer to form a frame.

A data link frame has three parts:

- Header
- Data
- Trailer

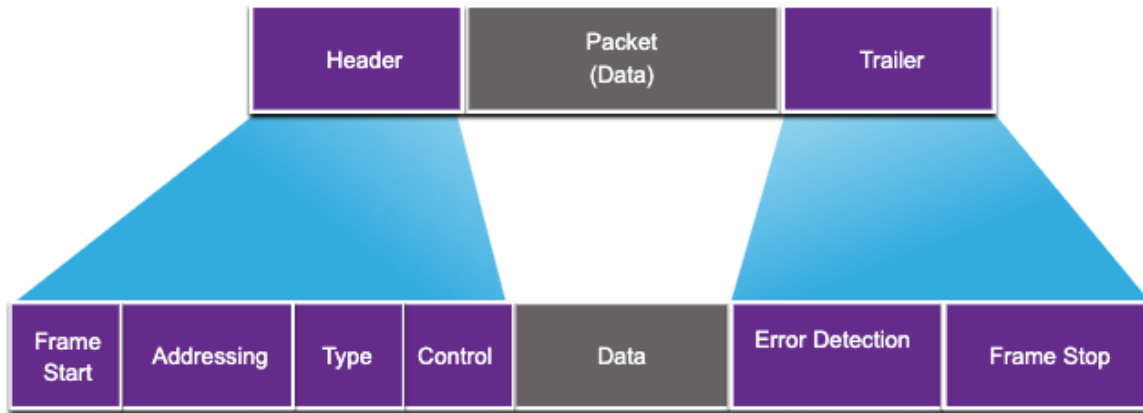
The fields of the header and trailer vary according to data link layer protocol.

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



# Data Link Frame

## Frame Fields

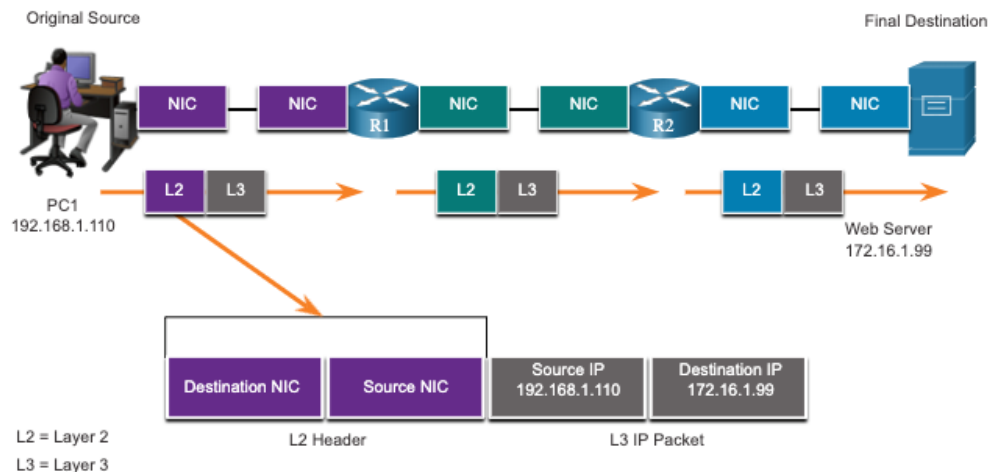


Field	Description
Frame Start and Stop	Identifies beginning and end of frame
Addressing	Indicates source and destination nodes
Type	Identifies encapsulated Layer 3 protocol
Control	Identifies flow control services
Data	Contains the frame payload
Error Detection	Used for determine transmission errors

# 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.



## Data Link 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)
  - Byte Oriented and performs faster than HDLC, does not require Cisco device on both ends
- High-Level Data Link Control (HDLC)
  - Bit Oriented and performs slower than PPP, requires Cisco devices on both ends
- Frame-Relay
  - cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in wide area networks (WANs)

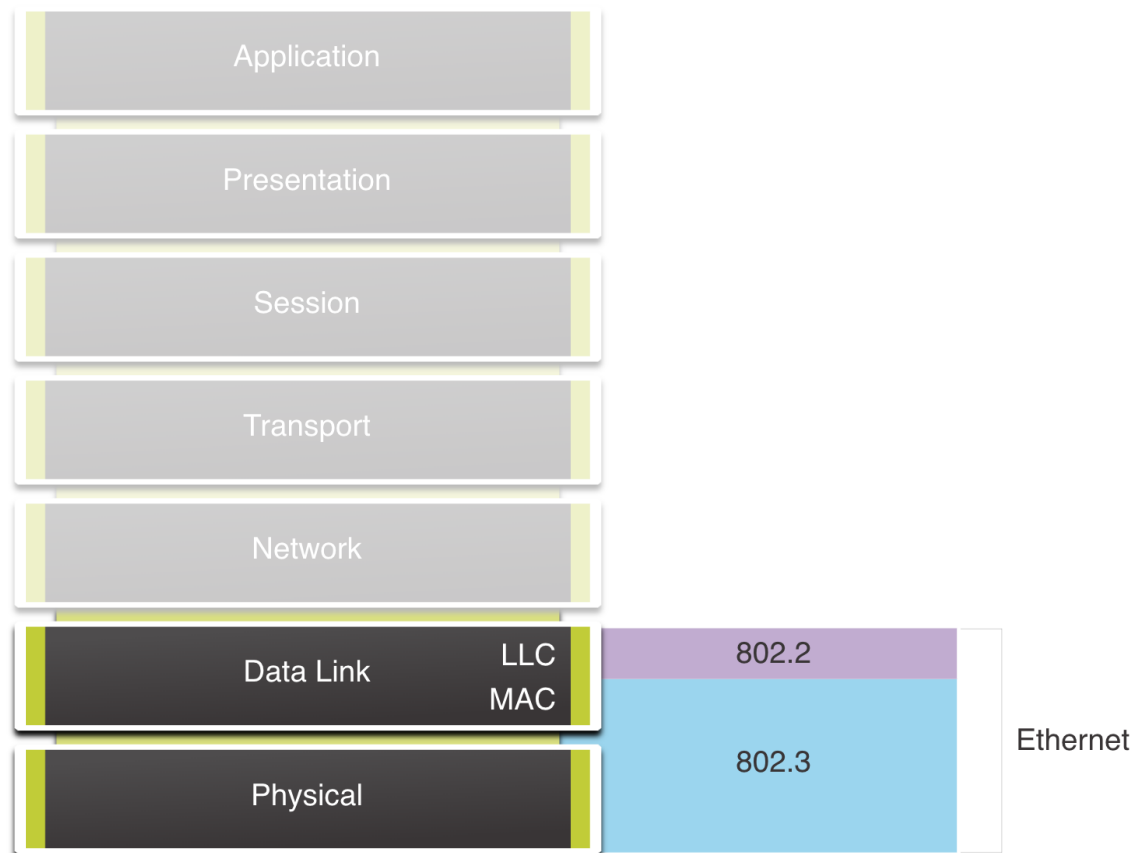
Each protocol performs media access control for specified logical topologies.



# 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.

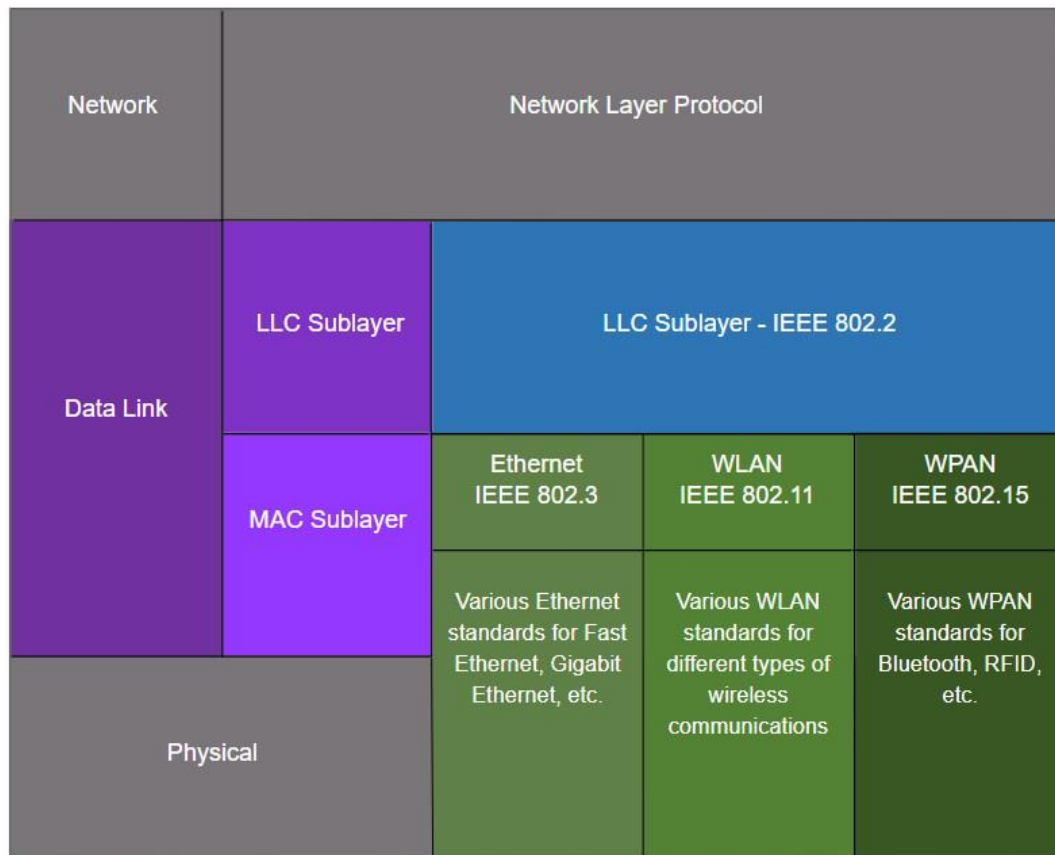


# Ethernet Frames

## 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.



# 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:

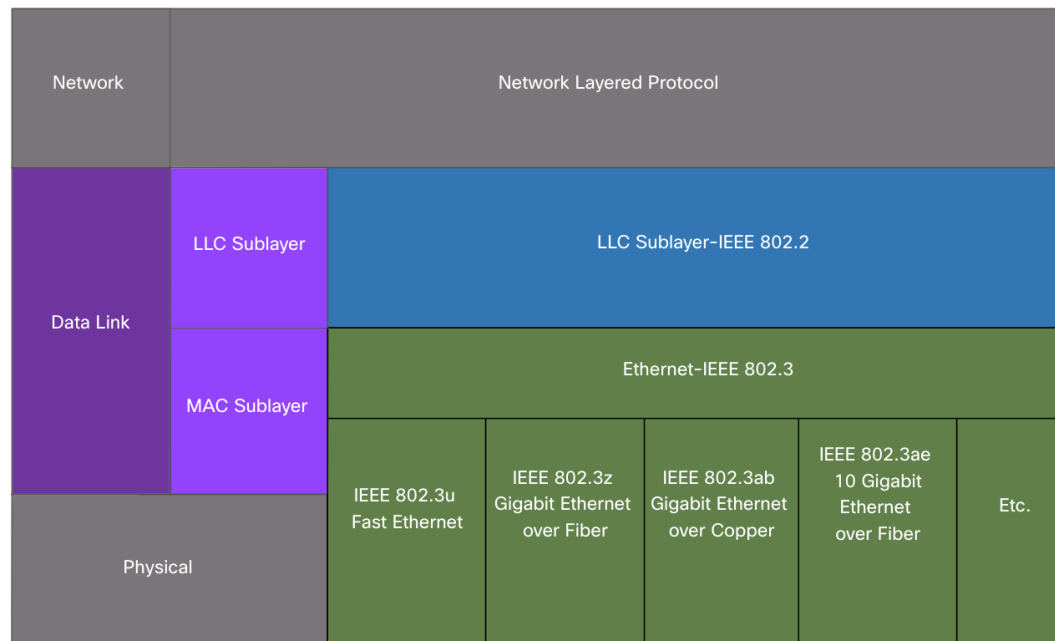
1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet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

# Ethernet Frames

## MAC Sublayer

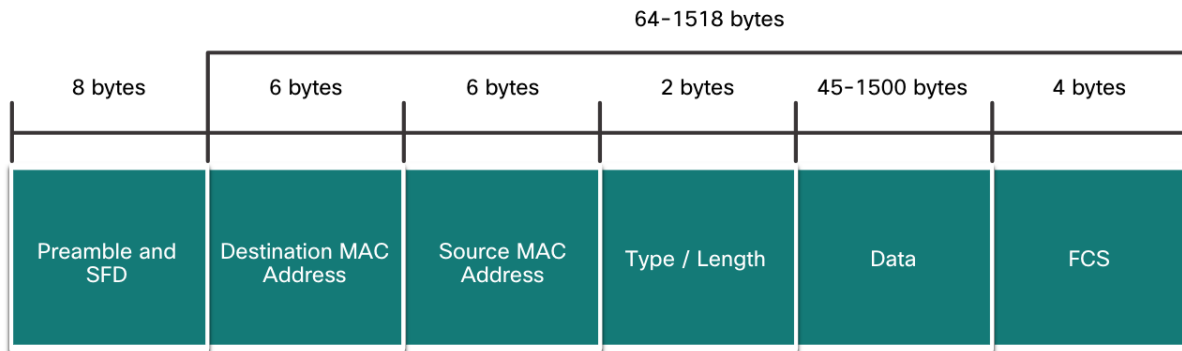
### Media Access

- 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 Frames

# Ethernet Frame Fields

## Ethernet Frame Fields Details:

Field	Description
Preamble and Start Frame Delimiter	The Preamble (7 bytes) and Start Frame Delimiter (SFD) (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes.
Destination MAC Address	This 6-byte field is the identifier for the intended recipient.
Source MAC Address Field	This 6-byte field identifies the originating NIC or interface of the frame.
Type / Length	This 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame. Eg. hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP.
Data Field	This field (46 – 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least 64 bytes long.
Frame Check Sequence Field	The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC).

# Ethernet MAC Address



# MAC Address and Hexadecimal

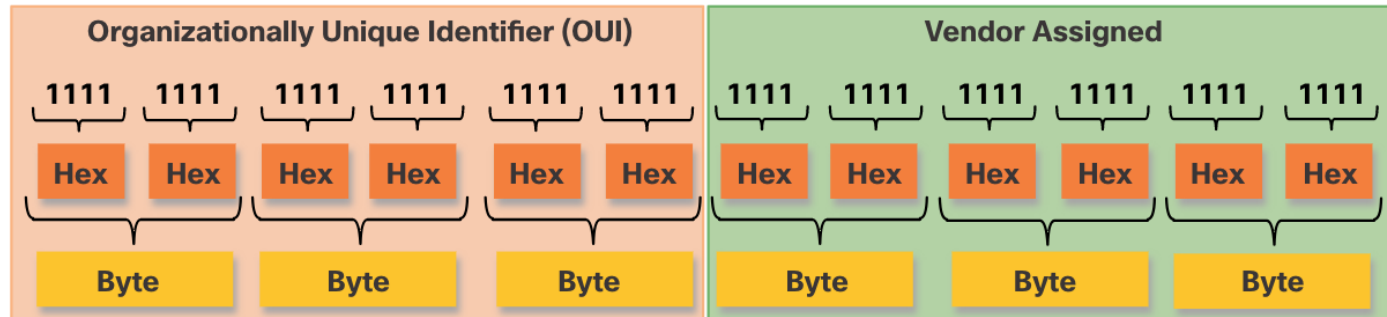
- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed 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).

Decimal (Base 10)	Binary (Base 2)	Hexadecimal (Base 16)
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

# Ethernet MAC Addresses

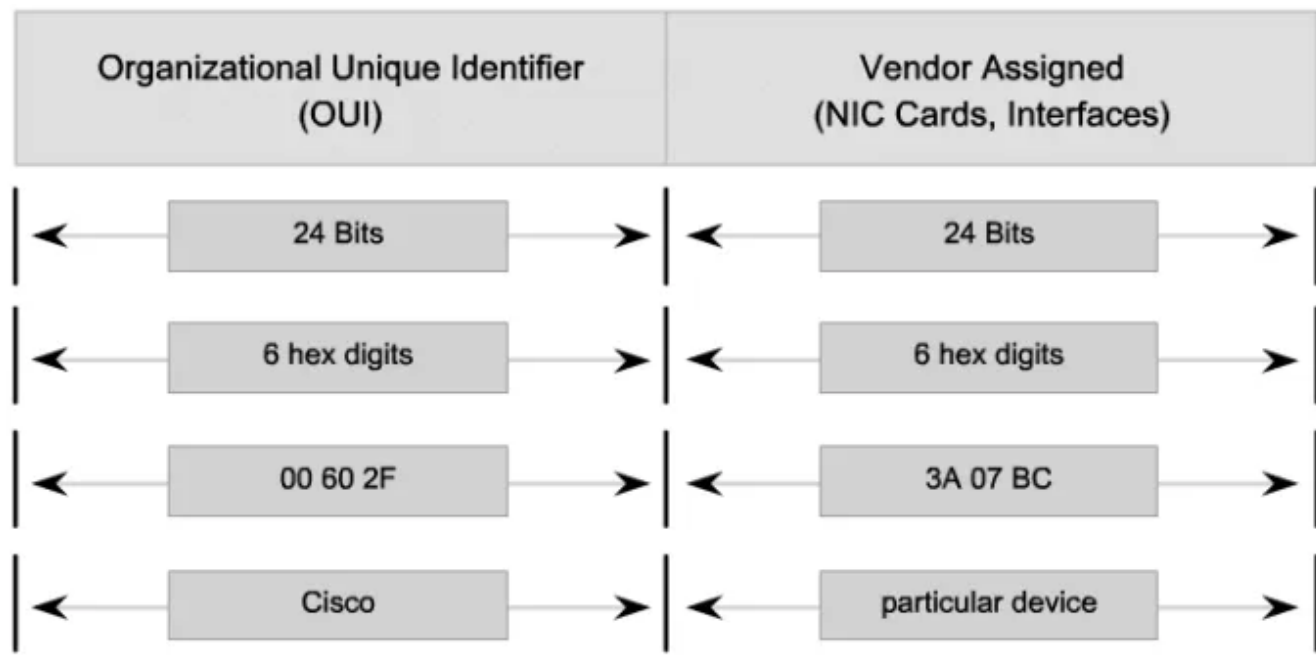
## Ethernet MAC Address

- 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

## Ethernet MAC Address



Different representations of MAC Addresses

00-60-2F-3A-07-BC  
00:60:2F:3A:07:BC  
0060.2F3A.07BC

# Ethernet MAC Addresses

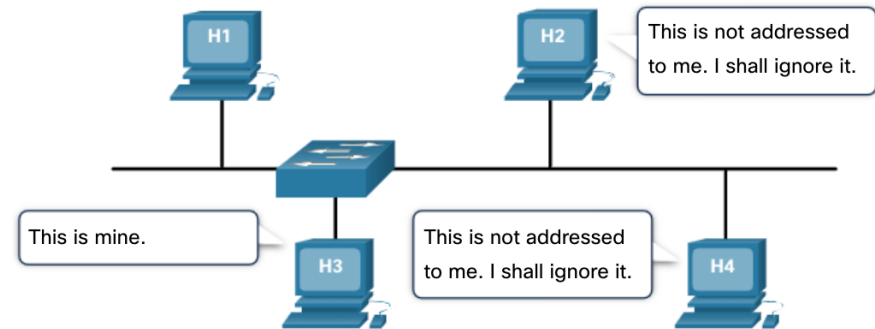
## Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header includes 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		



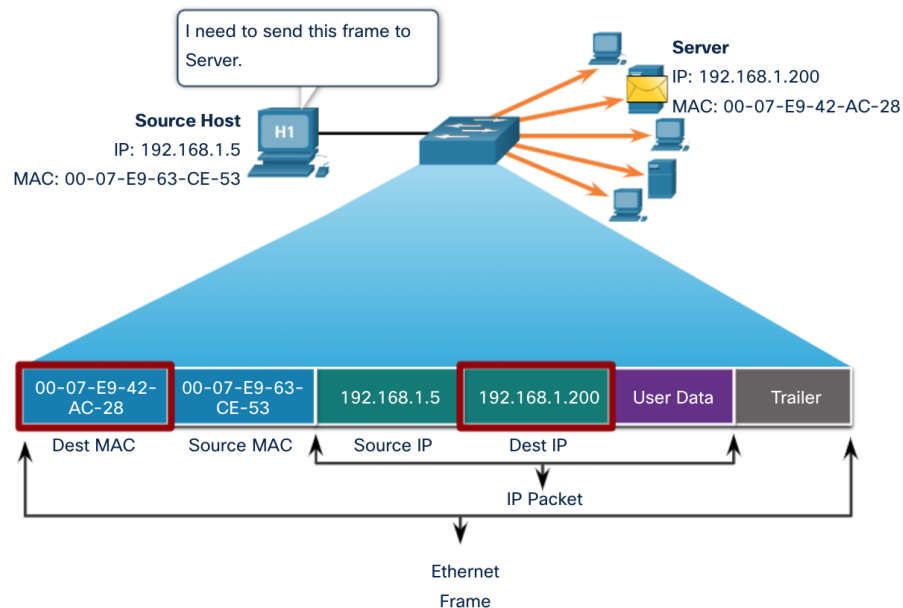
# Ethernet MAC Addresses

## 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.

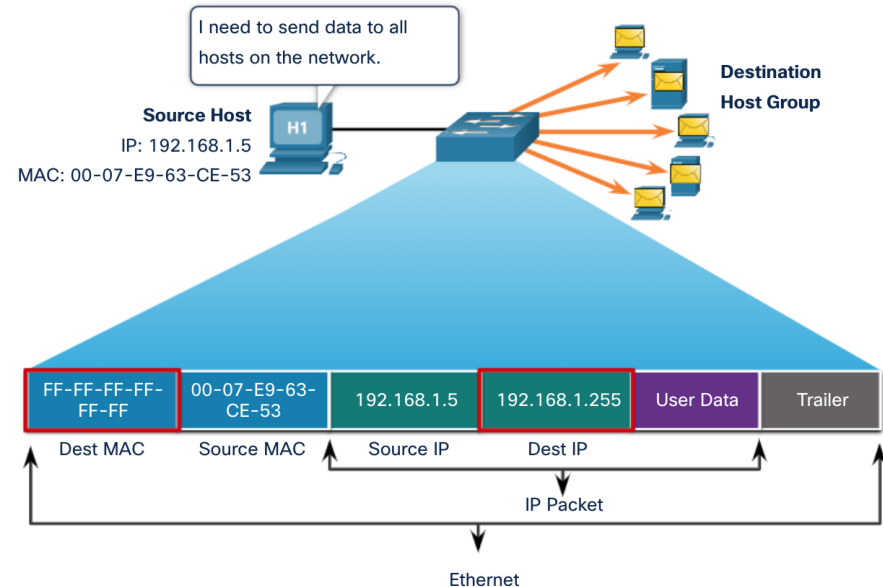


# Ethernet MAC Addresses

## 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.

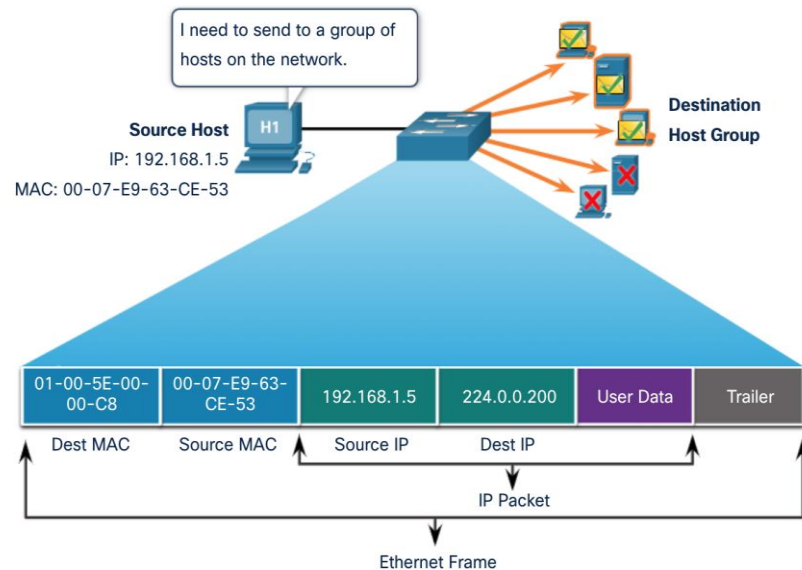


# Ethernet MAC Addresses

## 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.



\*In Spanning Tree Protocol Broadcast PDUs (BPDUs) are sent to Multicast MAC Address 01-80-c2-00-00-00 for the native VLANs and 01-00-0c-cc-cc-cd for other VLANs.

# The MAC Address Table

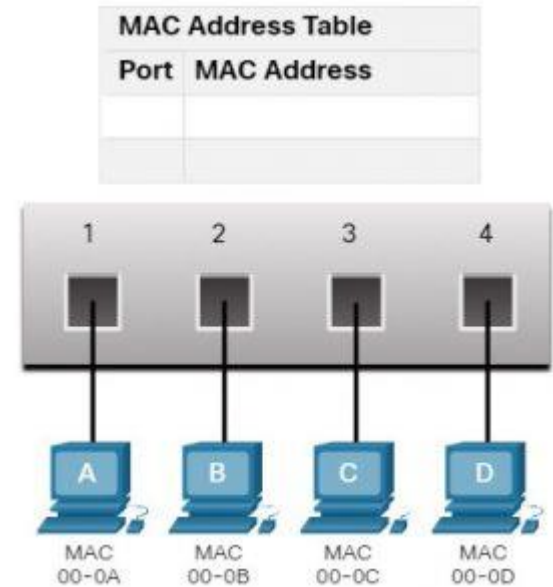


# The MAC Address Table

## 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 switch MAC address table is empty.

# The MAC Address Table

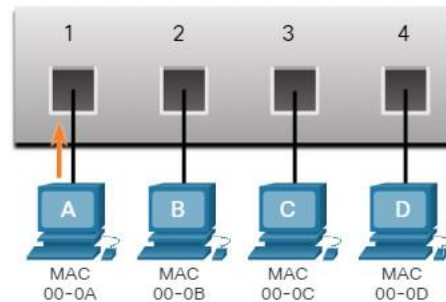
## Switch Learning and Forwarding

### 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.

MAC Address Table	
Port	MAC Address
1	00-0A



Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS
--------------------------	---------------------	------	------	-----

# The MAC Address Table

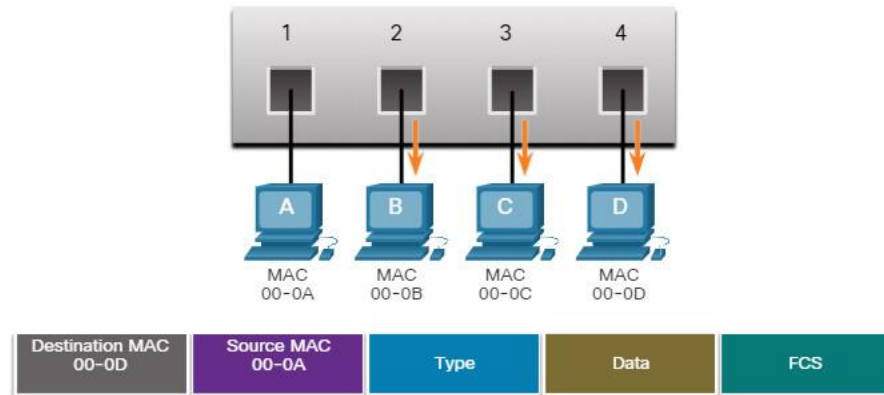
## Switch Learning and Forwarding (Contd.)

### 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.

MAC Address Table	
Port	MAC Address
1	00-0A



# The MAC Address Table

## 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.

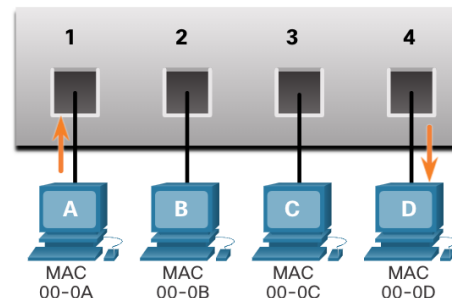
### Note:

**Frame Flooding:** When the switch receives a frame that is destined for a station address that it hasn't yet seen, the switch will send the frame out all of the ports other than the port on which it arrived. This process is called flooding or Frame Flooding.

**Learning:** In this state, the port does not yet forward frames, but it does learn source addresses from any frames received and adds them to the filtering database. The switch will **populate** the MAC address table with packets heard on the port (until the timer expires), before moving to the forwarding state.

**Frame Forwarding** :This is the operational state in which a port sends and receives station data.

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



Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS
--------------------------	---------------------	------	------	-----

# 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.

## Switch Speeds and Forwarding Methods

# 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.

# Switch Speeds and Forwarding Methods

## 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
<b>Port-based memory</b>	<ul style="list-style-type: none"><li>• Frames are stored in queues that are linked to specific incoming and outgoing ports.</li><li>• A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted.</li><li>• It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port.</li><li>• This delay occurs even if the other frames could be transmitted to open destination ports.</li></ul>
<b>Shared memory</b>	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>

- 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).



## Switch Speeds and Forwarding Methods

# 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.

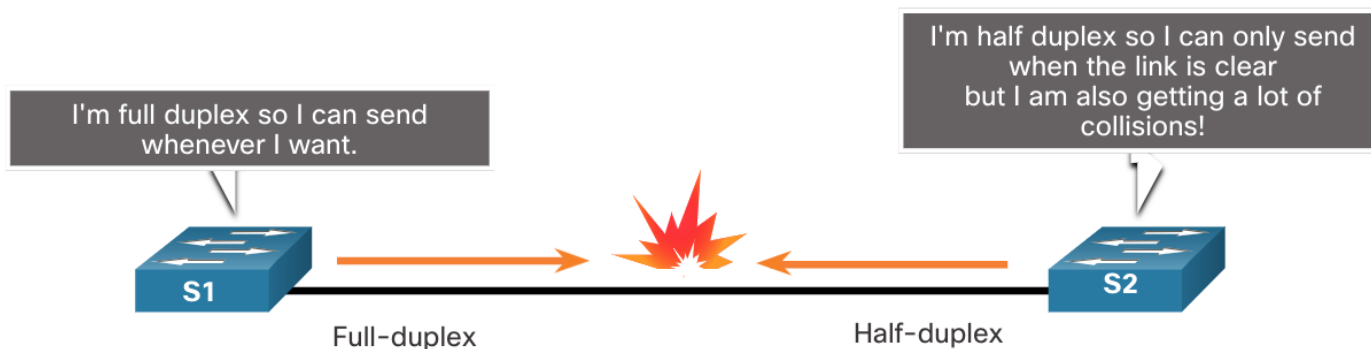
Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

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

# 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.



## 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.

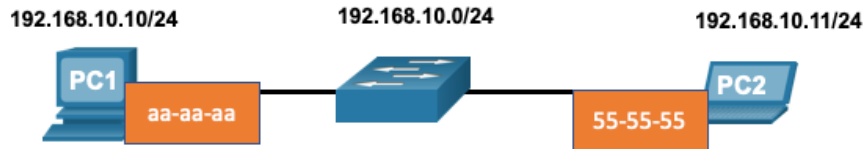
# MAC and IP

# Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.



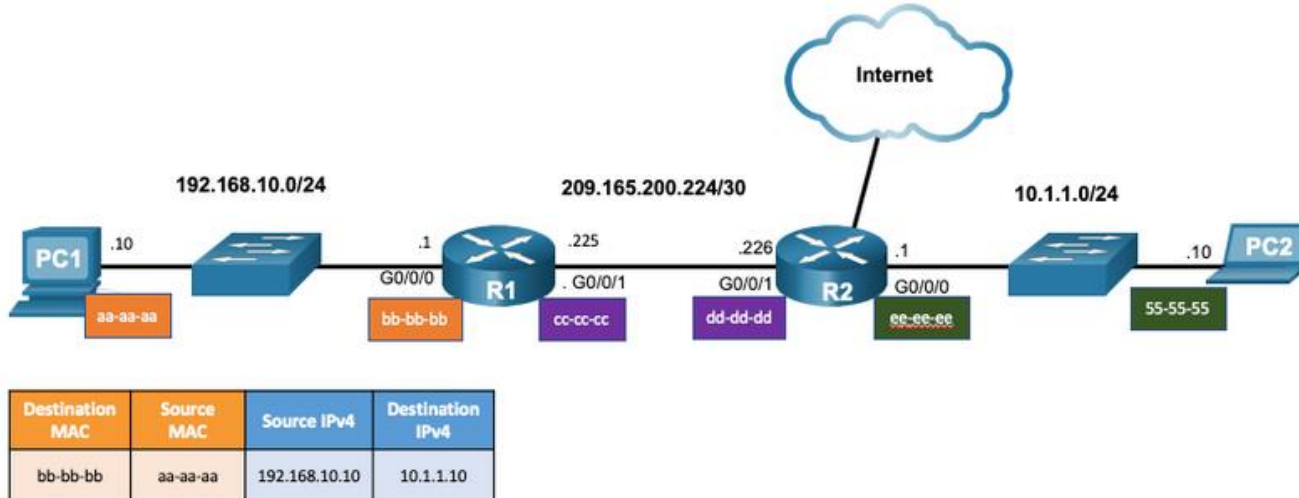
Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

# MAC and IP

## Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



# ARP

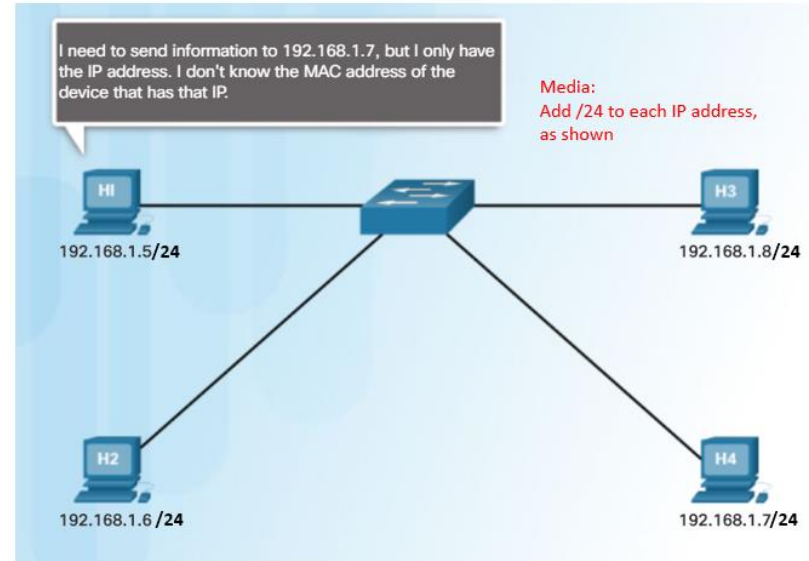
# ARP

## ARP Overview

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining an ARP table of IPv4 to MAC address mappings





# ARP

## ARP Functions

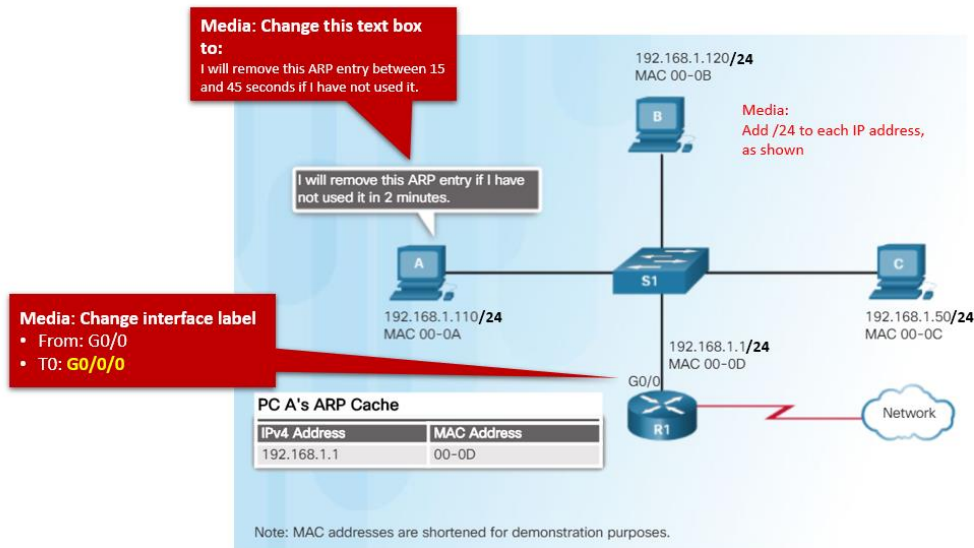
To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If there is no ARP table entry is found, then the device sends an ARP request.

# ARP

## Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer expires after a specified period of time.
- The duration of the ARP cache timer differs depending on the operating system.
- ARP table entries can also be removed manually by the administrator.



# ARP

## ARP Tables on Networking Devices

- The **show ip arp** command displays the ARP table on a Cisco router.
- The **arp -a** command displays the ARP table on a Windows 10 PC.

```
R1# show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.10.1	-	a0e0.af0d.e140	ARPA	GigabitEthernet0/0/0

```
C:\Users\PC> arp -a
```

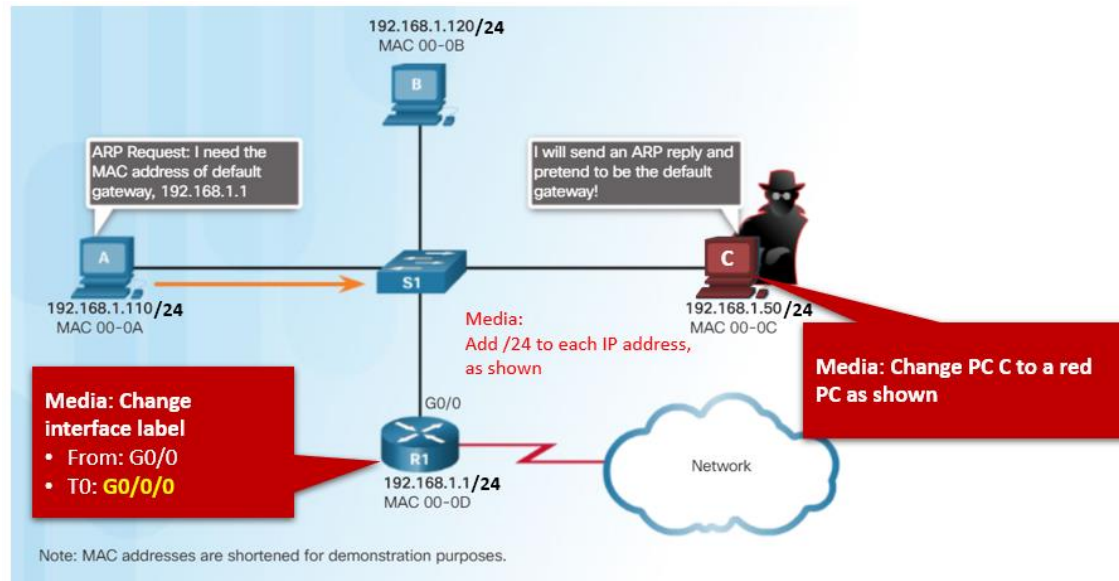
```
Interface: 192.168.1.124 --- 0x10
```

Internet Address	Physical Address	Type
192.168.1.1	c8-d7-19-cc-a0-86	dynamic
192.168.1.101	08-3e-0c-f5-f7-77	dynamic

# ARP

## ARP Issues – ARP Broadcasting and ARP Spoofing

- ARP requests are received and processed by every device on the local network.
- Excessive ARP broadcasts can cause some reduction in performance.
- ARP replies can be spoofed by a threat actor to perform an ARP poisoning attack.
- Enterprise level switches include mitigation technique known as Dynamic ARP Inspection (DAI) to protect against ARP attacks.



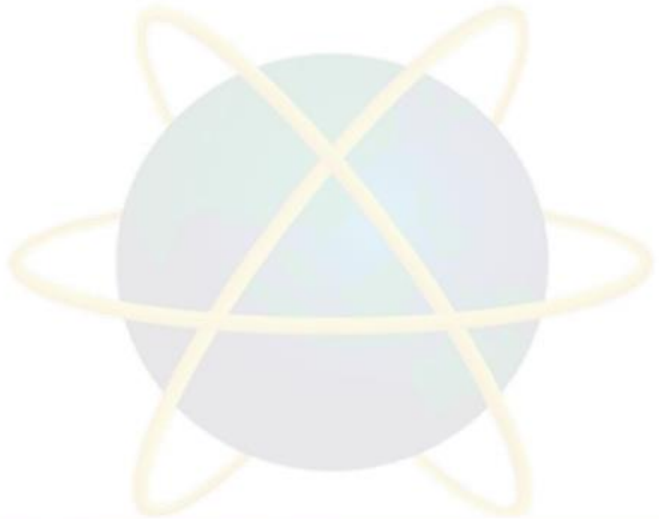
# Summary

# Summary of Main Teaching Points

- Explain how Data Link Layer supports communications across data networks.
- Compare media access control techniques and logical topologies used in networks.
- Explain the operation of Ethernet
- Explain how a Switch operates
- Explain how the address resolution protocol enables communication on a network.

# Question and Answer Session

## Q & A



## What We Will Cover Next:

# Configure Network Operating System





