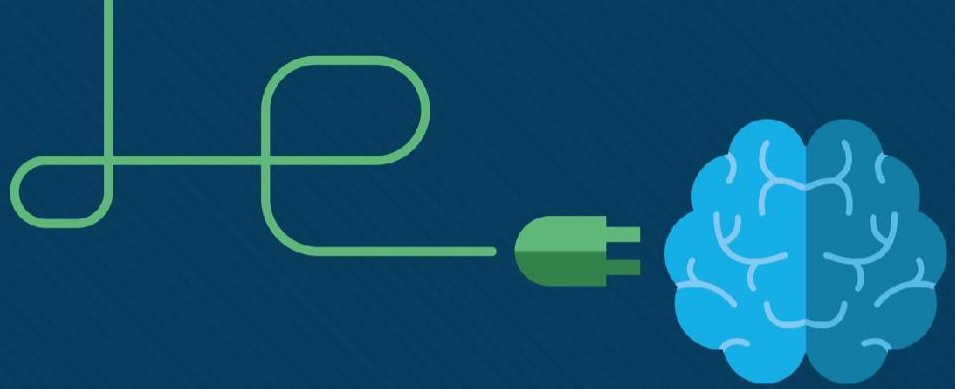
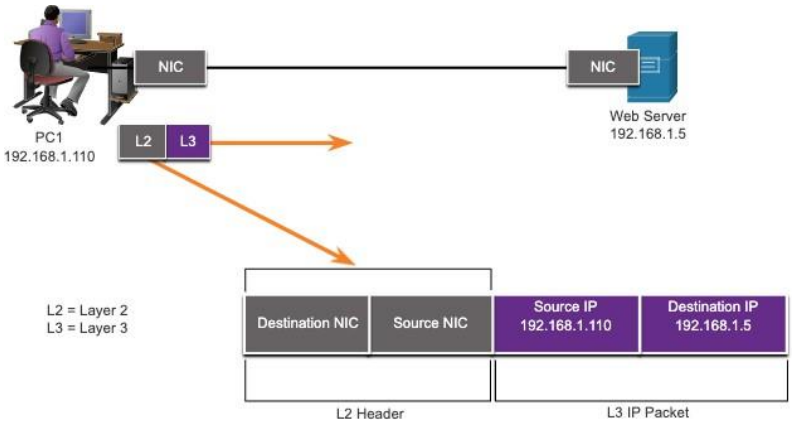


Module 6: Data Link Layer

Introduction to Networks v7.0
(ITN)

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.



The Frame

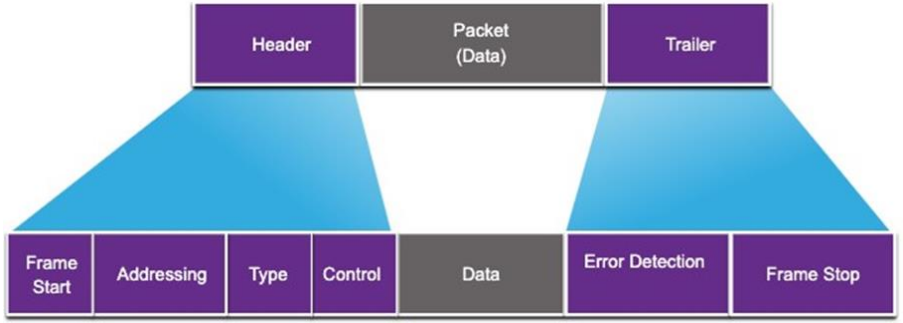
A frame is a sequence of bits of an agreed length.

Each network technology creates its own 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.



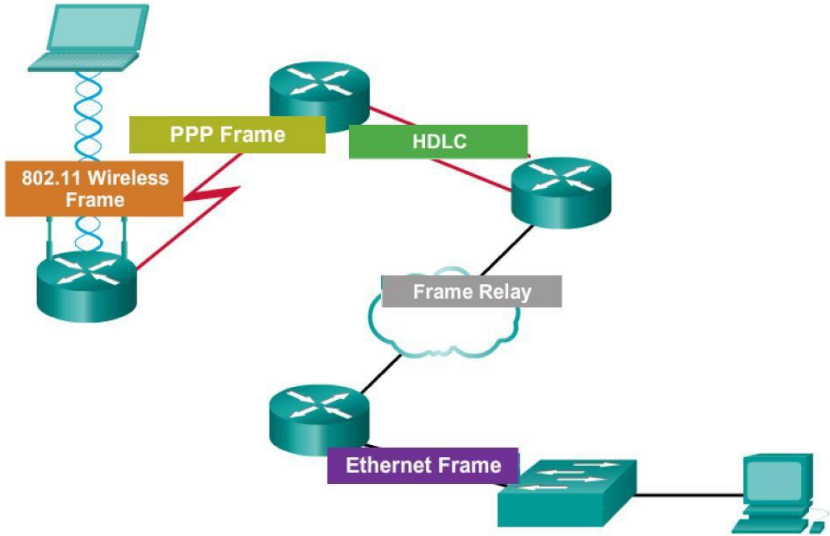
The Frame

Packets exchanged between networks may consists many data link layers and media transitions.

Each network defines its own L2 frame

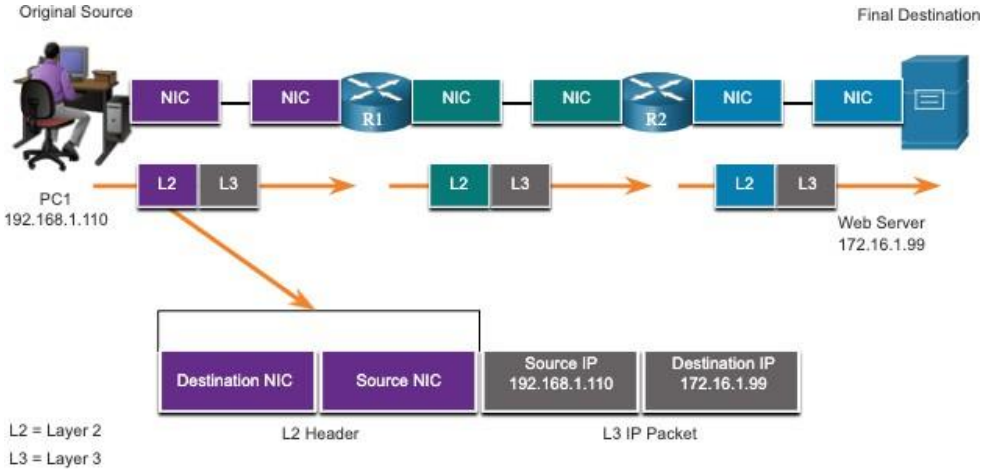
Each router performs four basic Layer 2 functions:

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



Data Link Layer Addresses

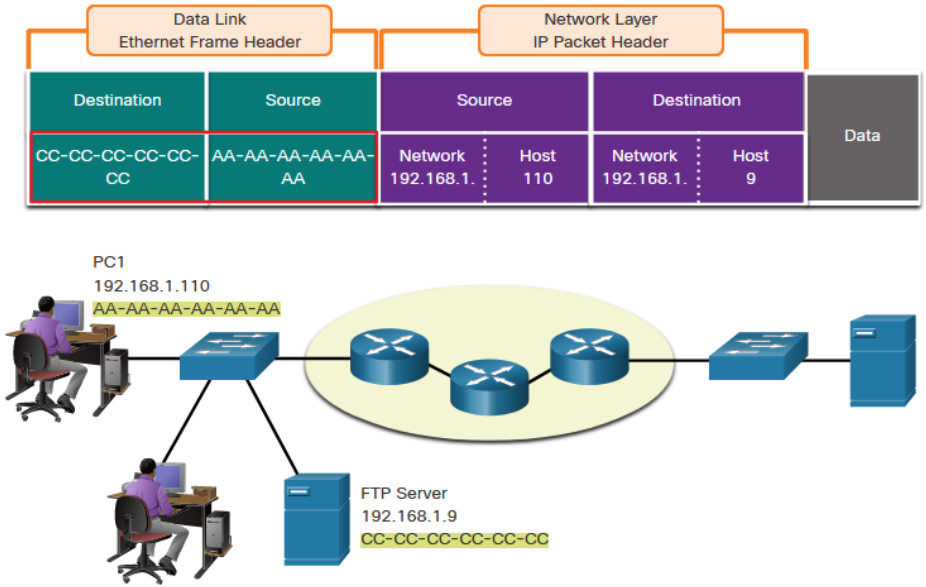
- Also referred to as a physical address.
- Used only for local delivery – each network has its own addresses
- Updated by each device that forwards the frame.



Role of the Data Link Layer Addresses: Same IP Network

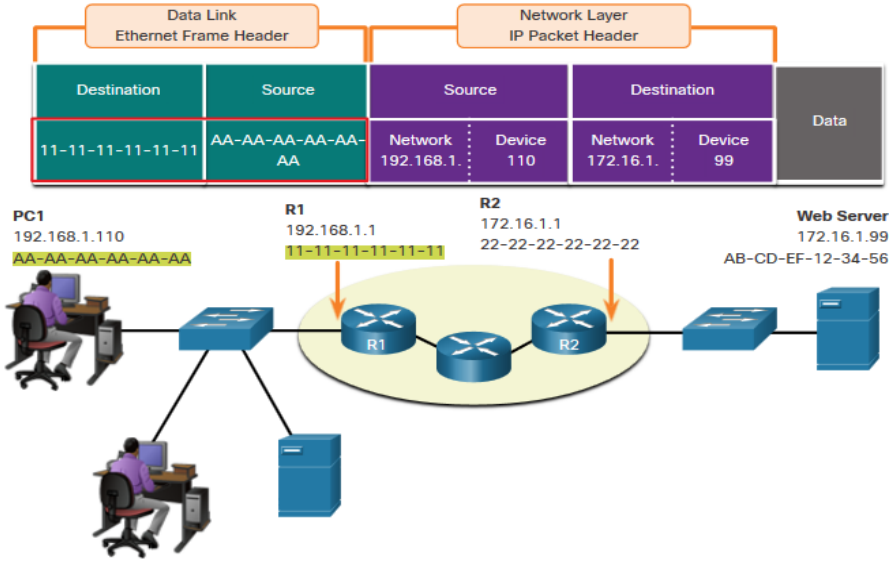
When devices are on the same network the data link frame will use the actual physical address of the NIC.

- The source address is the sender's address, and the destination address is the recipient's address.

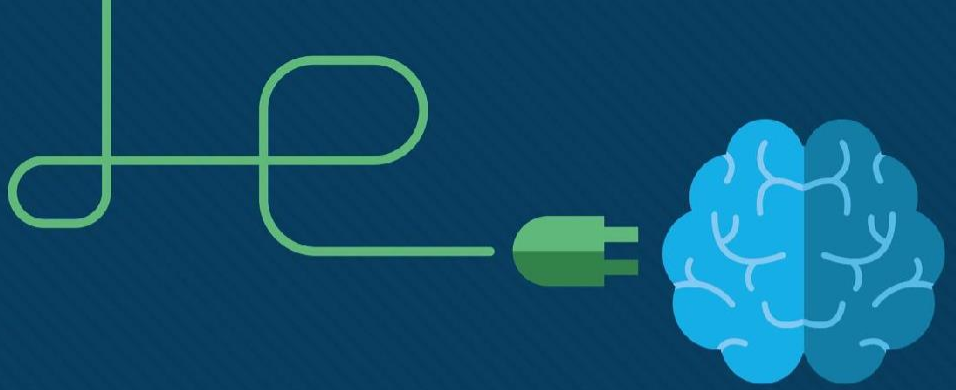


Role of the Data Link Layer Addresses: Different IP Networks

- The data link addressing is local addressing so it will have a source and destination for each link.
- The MAC addressing for the first segment is:
  - Source – AA-AA-AA-AA-AA-AA (PC1) Sends the frame.
  - Destination – 11-11-11-11-11-11 (R1) Receives the frame.
- The MAC addressing for the last segment is:
  - Source – 22-22-22-22-22-22- (Router R2) Sends the frame.
  - Destination – AB-CD-EF-12-34-56 (Web Server) Receives the frame.



Note: While the L2 local addressing will change from link to link or hop to hop, the L3 addressing remains the same.

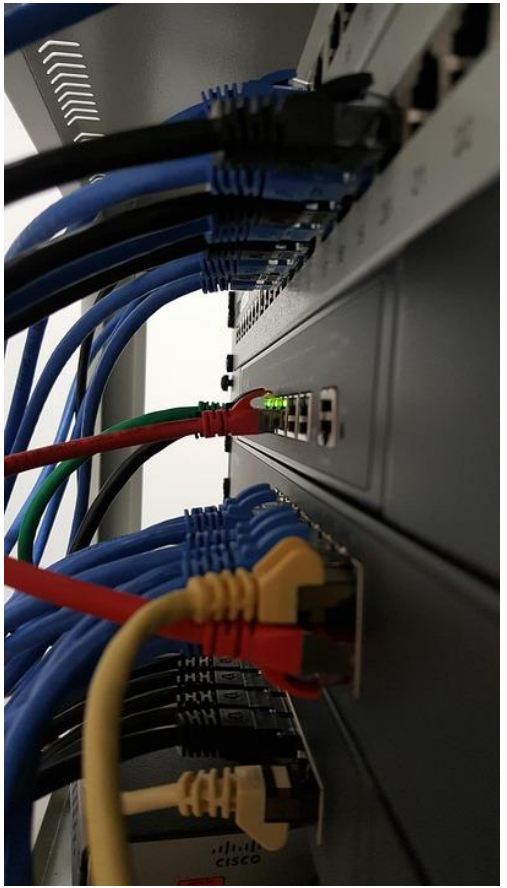


Module 7: Ethernet Switching

Introduction to Networks v7.0
(ITN)

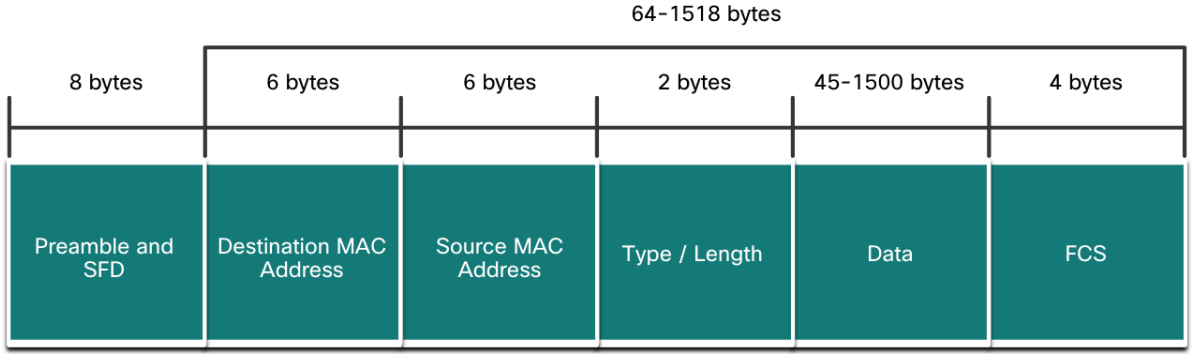
Ethernet

- One of the most widely used LAN technologies
- Operates in the data link layer and the physical layer
- Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps



Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame”
- Frames with more than 1500 bytes of data are considered “jumbo” frames”.
- If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame.
- Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



Ethernet MAC Addresses

An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.

- On each devises must be unique mac-address
- Mac-address is fixed part of the network interface card and usually cannot be change.

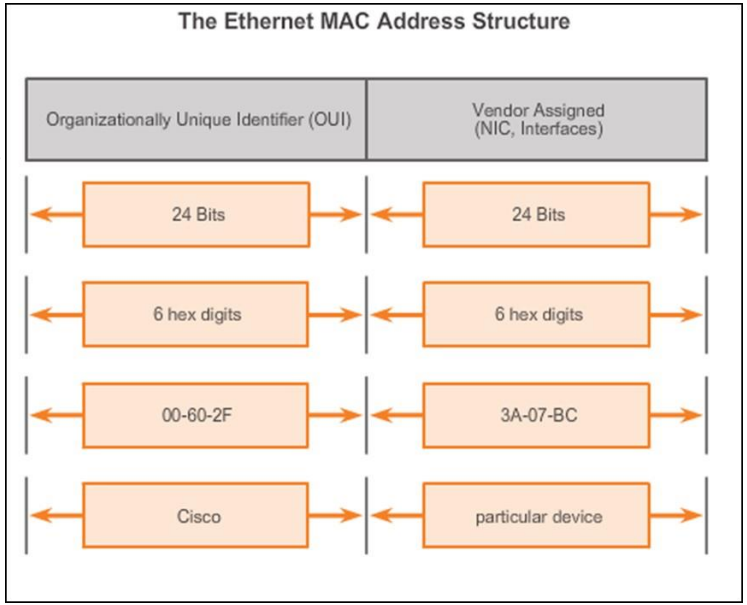
IEEE requires a vendor to follow these rules:

- Must use that vendor's assigned OUI as the first 3 bytes.
- All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0009.7C31.1969
   Link-local IPv6 Address.........: FE80::209:7CFF:FE31:1969
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.6.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.6.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............:
00-01-00-01-40-07-79-75-00-09-7C-31-19-69
   DNS Servers.....................: ::
                                     192.168.6.1
```

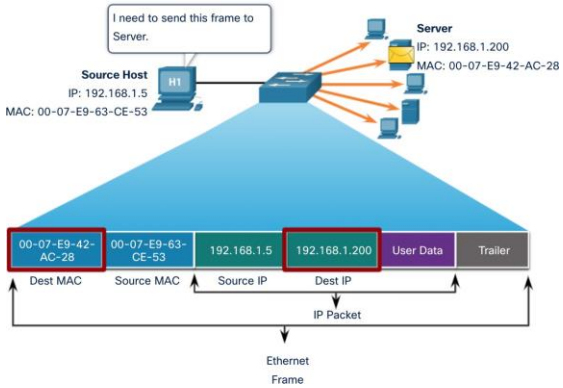


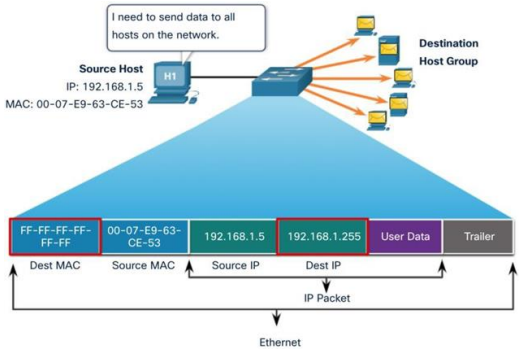
Different MAC Address

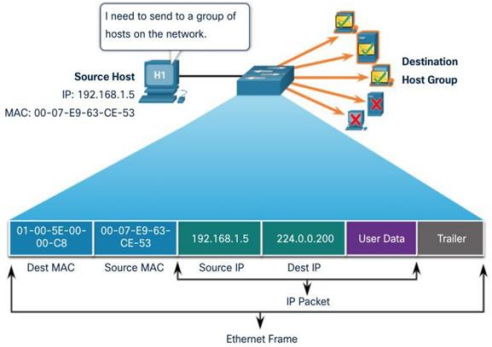
In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- 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.

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



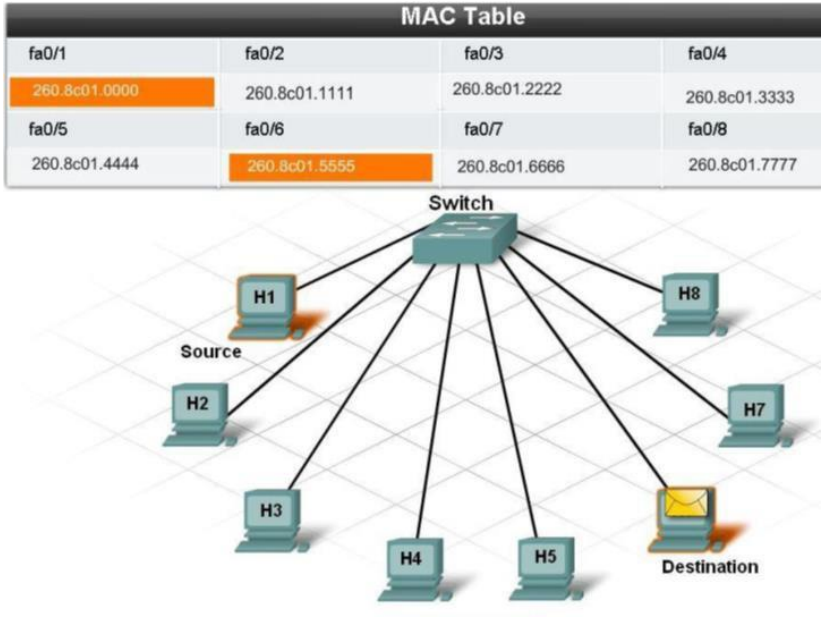




Switch Fundamentals

Switch Fundamentals

- A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions.
- It is completely unaware of the protocol being carried in the data portion of the frame. So, it is must not to know anything about IP addresses of the source and destination
- The switch makes its forwarding decisions based on the Layer 2 Ethernet MAC addresses.
- An Ethernet switch examines its MAC address table to make a forwarding decision for each frame.
- When a switch is turned on, the MAC address table is empty



- PC1 wants to communicate with PC6 and sends a frame to the switch.
- The switch reads the source and destination addresses of the frame
- The switch compares the destination address of the frame to the MAC address table and notice that the destination MAC address is found on port 6
- The switch sends the frame to the port 6 and to the PC6

Learning

- 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.*

Forwarding

- 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.*

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.