1. Data Link Layer (Layer 2)

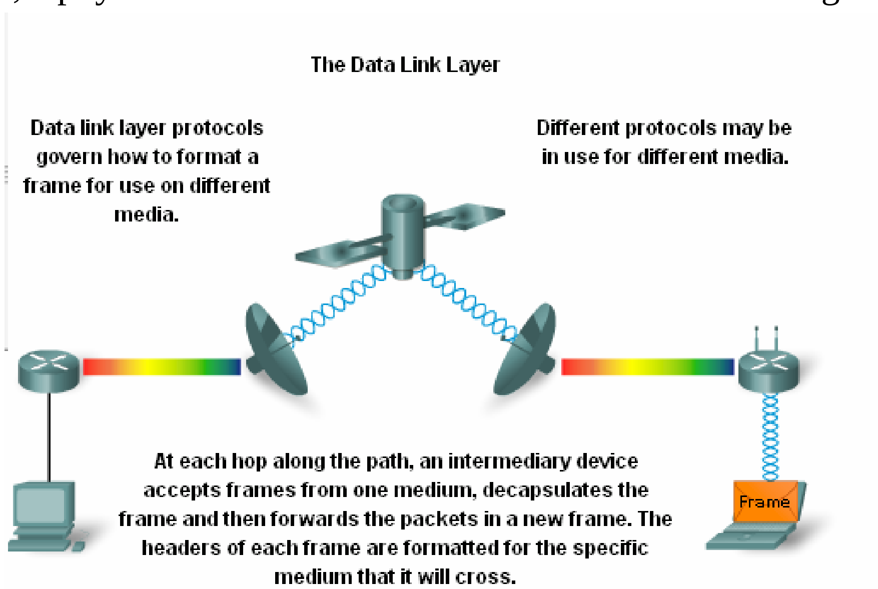
The Data Link layer provides a means for exchanging data over a common local media.

The Data Link layer performs two basic services:

- Allows the upper layers to access the media using techniques such as framing.
- Controls how data is placed onto the media and is received from the media using techniques such as media access control and error detection.

The Data Link layer is responsible for the exchange of frames between nodes over the media of a physical network.

- It is important to understand the meaning of the words medium and media within the context of this chapter. Here, these words refer to the material that actually carries the signals representing the transmitted data. Media is the physical copper cable, optical fiber, or atmosphere through which the signals travel. In this chapter media does not refer to content programming such as audio, animation, television, and video as used when referring to digital content and multimedia.
- A physical network is different from a logical network. Logical networks are defined at the Network layer by the arrangement of the hierarchical addressing scheme. Physical networks represent the interconnection of devices on a common media. Sometimes, a physical network is also referred to as a network segment.



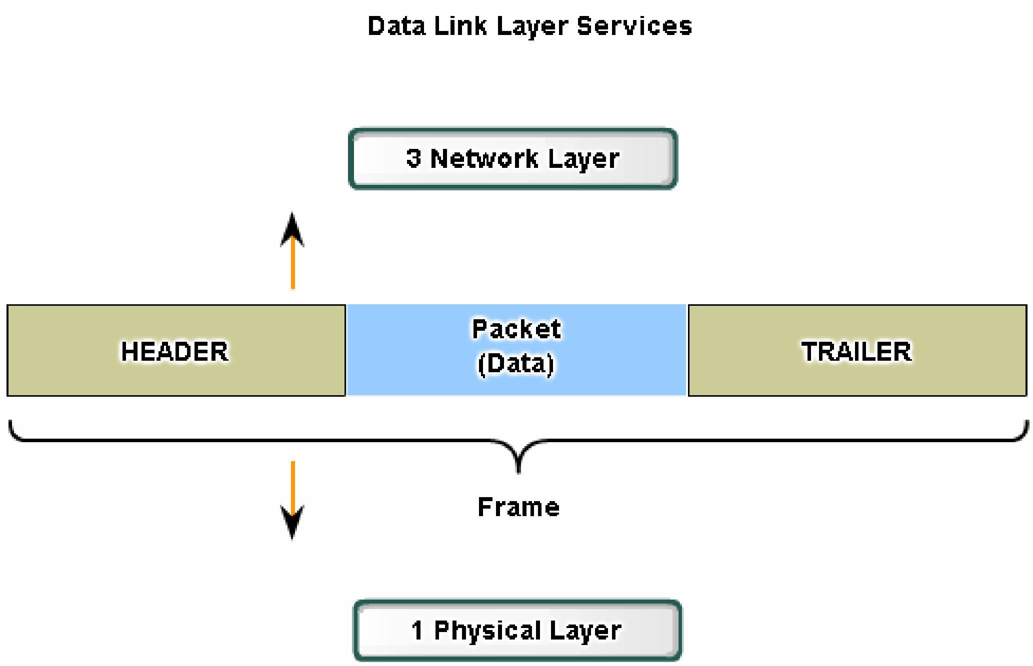
The description of a frame is a key element of each Data Link layer protocol. Data Link layer protocols require control information to enable the protocols to function. Control information may tell:

- Which nodes are in communication with each other
- When communication between individual nodes begins and when it ends
- Which errors occurred while the nodes communicated
- Which nodes will communicate next

The Data Link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer to create a frame.

the Data Link layer frame includes:

- Data - The packet from the Network layer
- Header - Contains control information, such addressing, and is located at the beginning of the PDU
- Trailer - Contains control information added to the end of the PDU

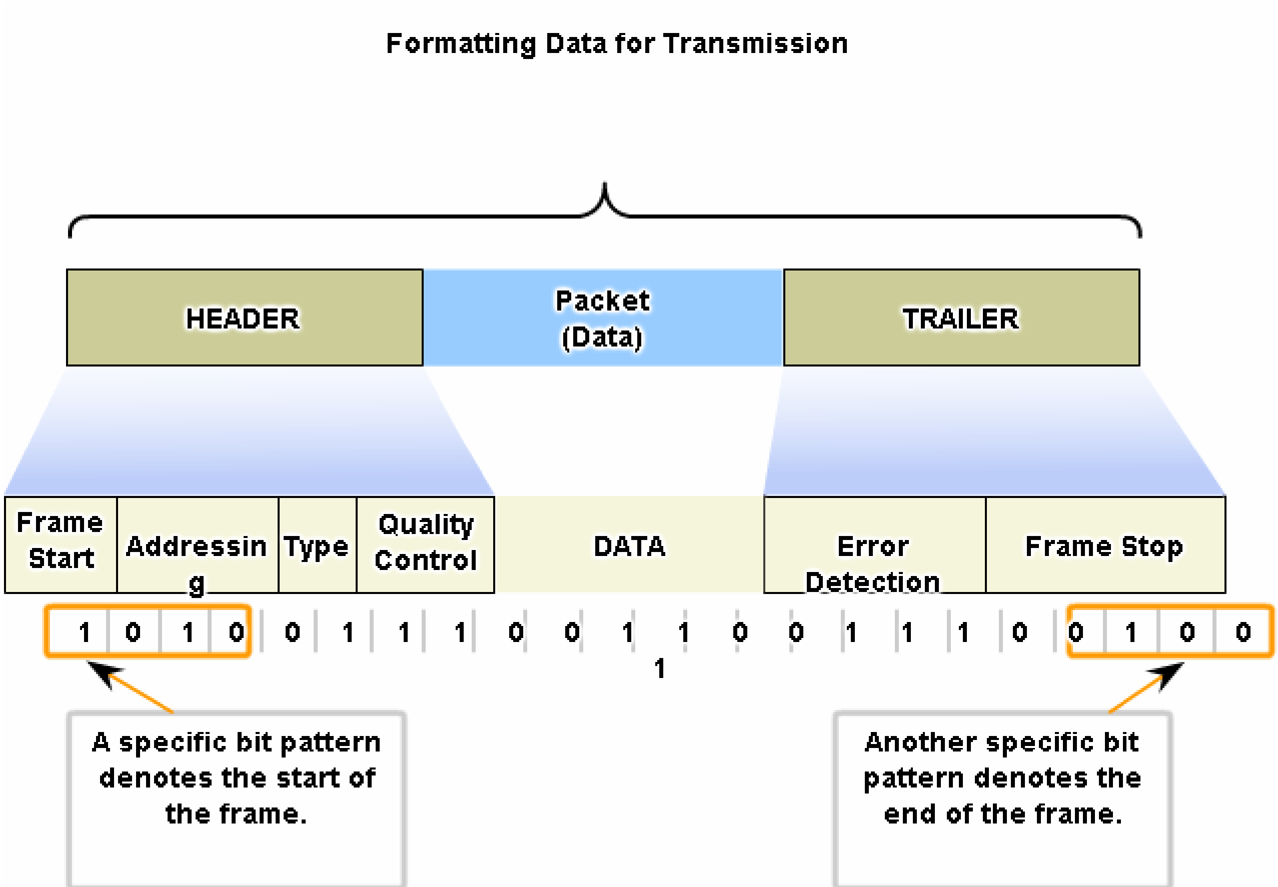


Typical field types include:

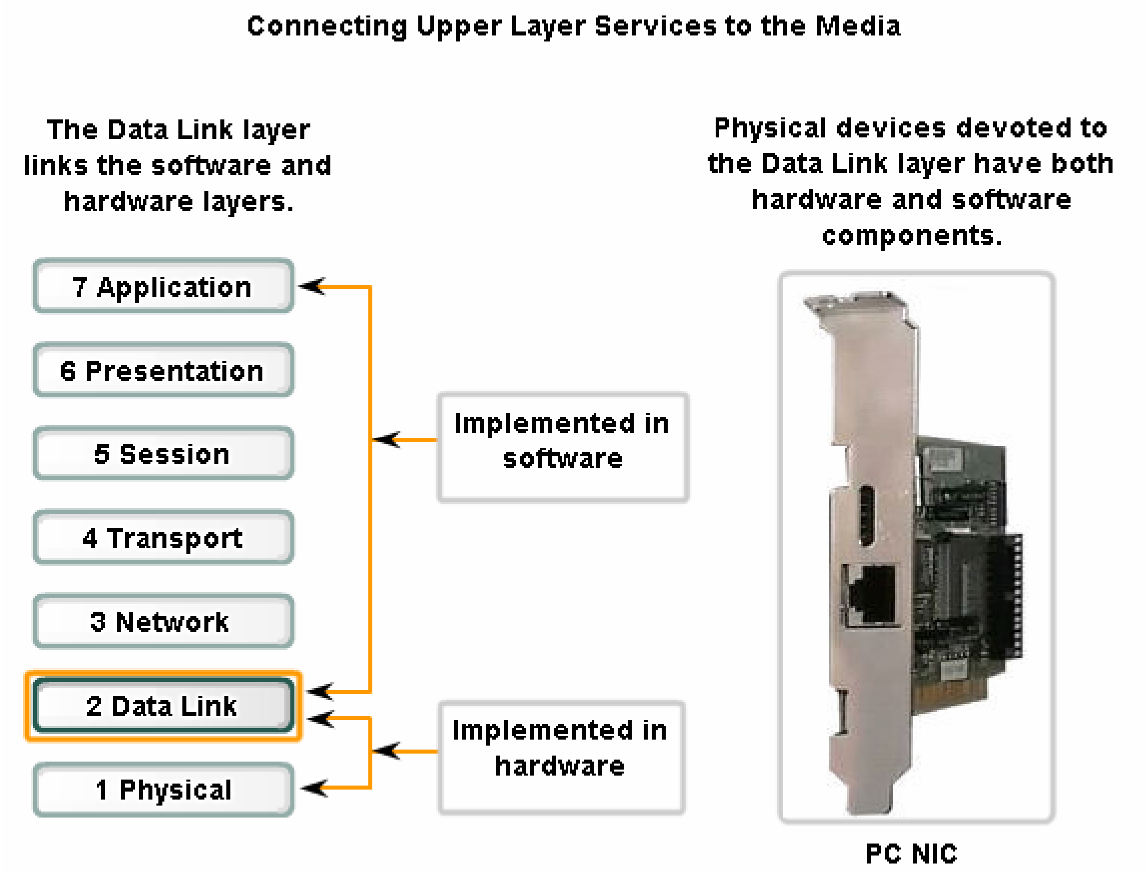
- Start and stop indicator fields - The beginning and end limits of the frame
- Naming or addressing fields
- Type field - The type of PDU contained in the frame
- Quality - control fields

• A data field -The frame payload (Network layer packet)

Fields at the end of the frame form the trailer. These fields are used for error detection and mark the end of the frame.



In many cases, the Data Link layer is embodied as a physical entity, such as an Ethernet network interface card (NIC), which inserts into the system bus of a computer and makes the connection between running software processes on the computer and physical media. The NIC is not solely a physical entity, however. Software associated with the NIC enables the NIC to perform its intermediary functions of preparing data for transmission and encoding the data as signals to be sent on the associated media.



2- Data Link Sublayers

To support a wide variety of network functions, the Data Link layer is often divided into two sublayers: an upper sublayer and an lower sublayer.

The upper sublayer defines the software processes that provide services to the Network layer protocols.

The lower sublayer defines the media access processes performed by the hardware.

Separating the Data Link layer into sublayers allows for one type of frame defined by the upper layer to access different types of media defined by the lower layer. Such is the case in many LAN technologies, including Ethernet.

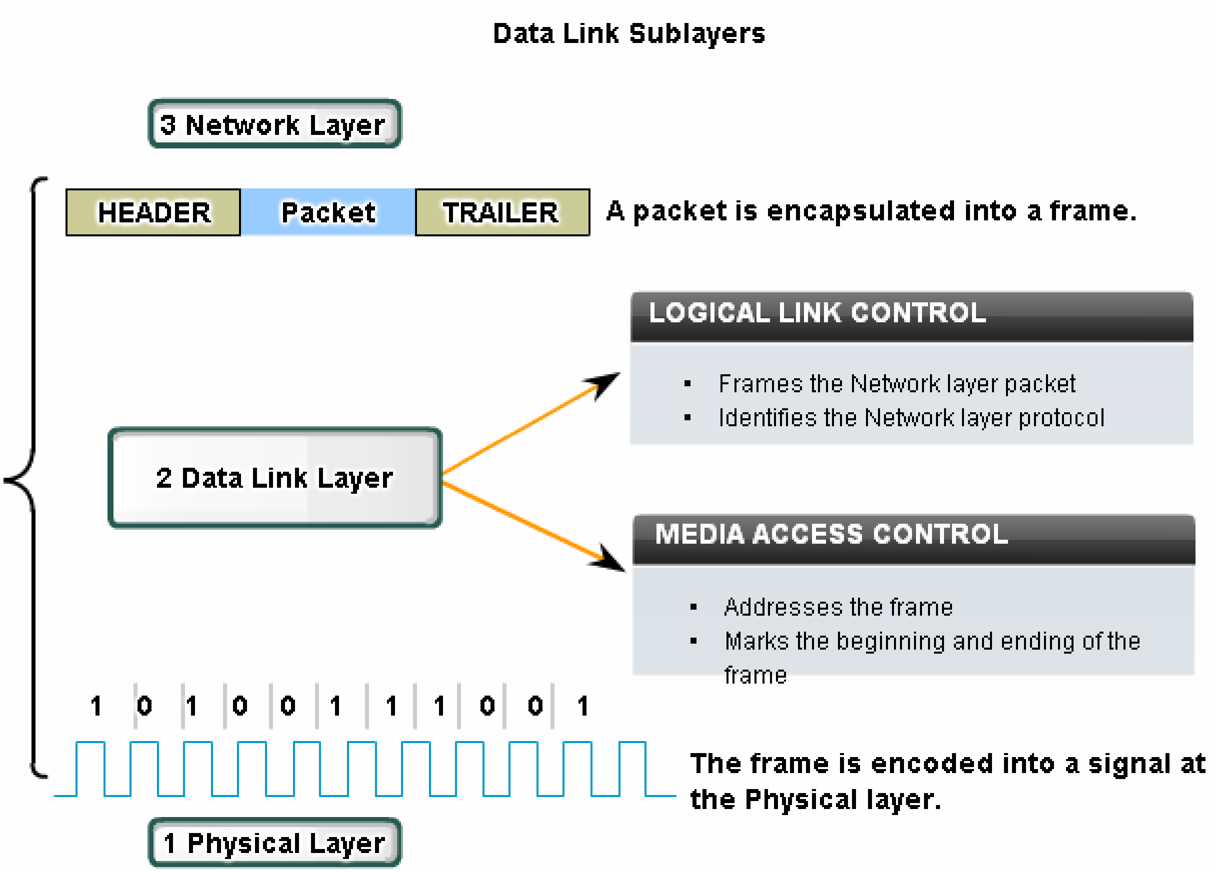
The two common LAN sublayers are:

2-1 Logical Link Control 802.2

Responsible for identifying Network layer protocols and then encapsulating them. An LLC header tells the Data Link layer what to do with a packet once a frame is received. Logical Link Control (LLC) places information in the frame that identifies which Network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IP and IPX, to utilize the same network interface and media.

2-2 Media Access Control 802.3

Defines how packets are placed on the media. Contention media access is "first come/first served" access where everyone shares the same bandwidth. Media Access Control (MAC) provides Data Link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of Data Link layer protocol in use.



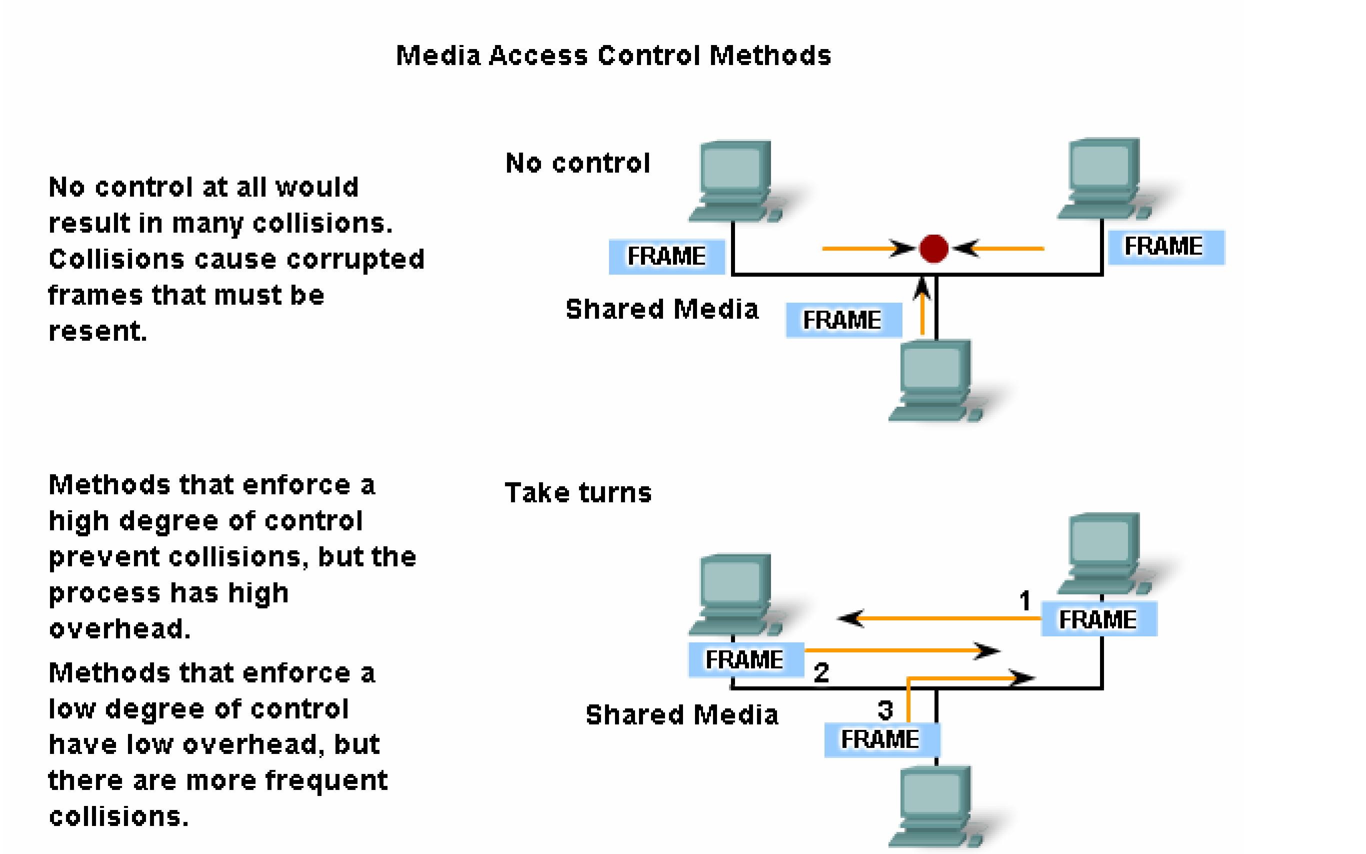
Regulating the placement of data frames onto the media is known as media access control. Among the different implementations of the Data Link layer protocols, there are different methods of controlling access to the media. These media access control techniques define if and how the nodes share the media.

there are different ways to regulate the placing of frames onto the media. The protocols at the Data Link layer define the rules for access to different media. Some media access control methods use highly-controlled processes to ensure that frames are safely placed on the media. These methods are defined by sophisticated protocols, which require mechanisms that introduce overhead onto the network.

The method of media access control used depends on:

• Media sharing - If and how the nodes share the media

• Topology - How the connection between the nodes appears to the Data Link layer.



Some network topologies share a common medium with multiple nodes. At any one time, there may be a number of devices attempting to send and receive data using the network media. There are rules that govern how these devices share the media.

There are two basic media access control methods for shared media:

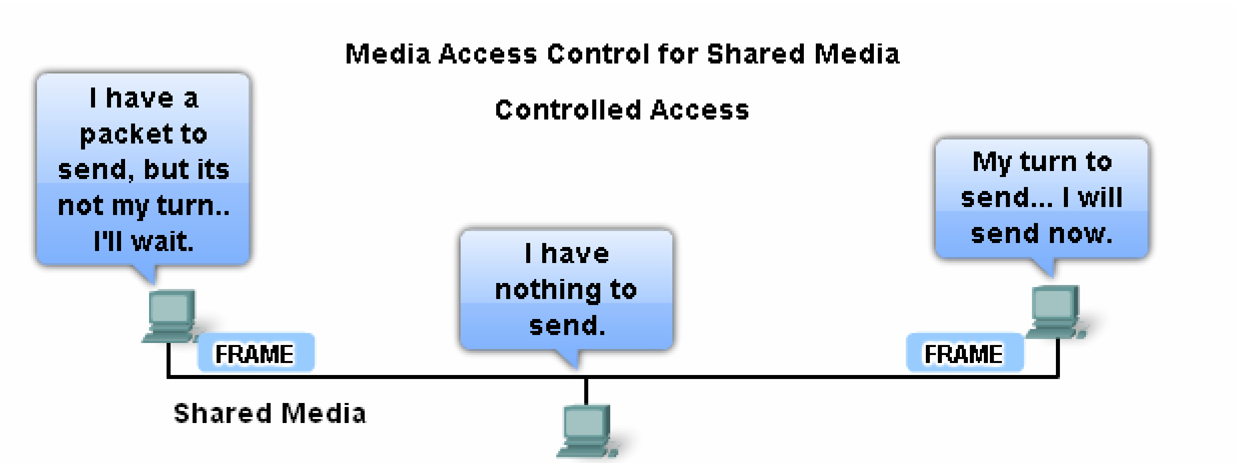
• Controlled - Each node has its own time to use the medium

• Contention-based - All nodes compete for the use of the medium.

* Media Access Control Protocols for Shared Media

1. Controlled Access for Shared Media:

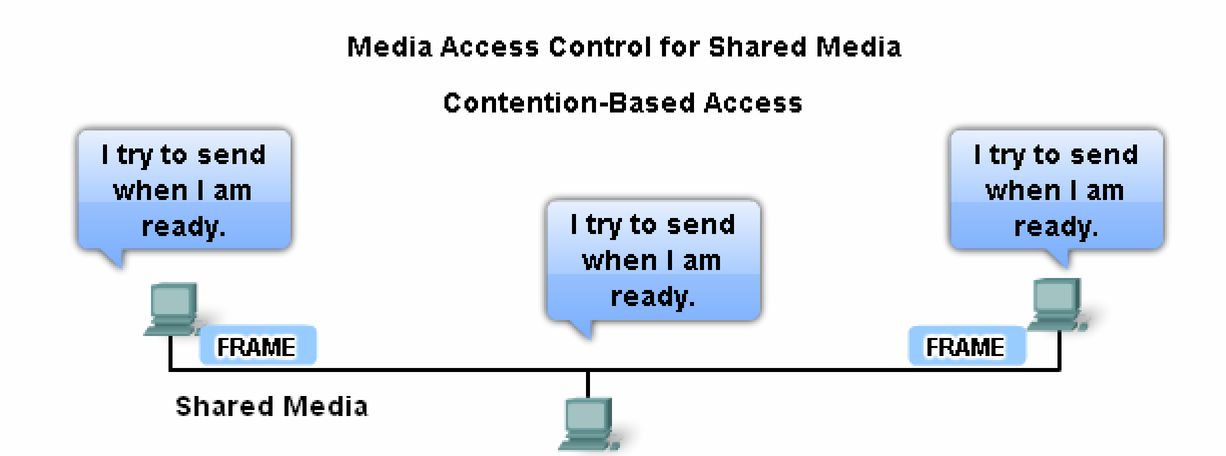
When using the controlled access method, network devices take turns, in sequence, to access the medium. This method is also known as scheduled access or deterministic. If device does not need to access the medium, the opportunity to use the medium passes the next device in line. When one device places a frame on the media, no other device can do so until the frame has arrived at the destination and has been processed by the destination.



Method	Characteristics	Example
Controlled Access	• Only one station transmits at a time • Devices wishing to transmit must wait their turn • No collisions • Some deterministic networks use token passing	• Token Ring • FDDI

2. Contention Based for shared Media

Also referred to as non-deterministic, contention-based methods allow any device to try to access the medium whenever it has data to send. To prevent complete chaos on the media, these methods use a Carrier Sense Multiple Access (CSMA) process to first detect if the media is carrying a signal. If a carrier signal on the media from another node is detected, it means that another device is transmitting. When the device attempting to transmit sees that the media is busy, it will wait and try again after a short time period. If no carrier signal is detected, the device transmits its data. Ethernet and wireless networks use contention-based media access control. It is possible that the CSMA process will fail and two devices will transmit at the same time. This is called a data collision. If this occurs, the data sent by both devices will be corrupted and will need to be resent. Contention-based media access control methods do not have the overhead of controlled access methods. A mechanism for tracking whose turn it is to access the media is not required. However, the contention-based systems do not scale well under heavy media use. As use and the number of nodes increases, the probability of successful media access without a collision decreases. Additionally, The recovery mechanisms required to correct errors due to these collisions further diminishes the throughput.



Method	Characteristics	Example
Contention Based Access	• Stations can transmit at any time • Collisions exist • Mechanisms exist to resolve contention: • CSMA/CD for Ethernet networks • CSMA/CA for 802.11 wireless networks	• Ethernet • Wireless

2.1 CSMA/Collision Detection

In CSMA/Collision Detection (CSMA/CD), the device monitors the media for the presence of a data signal. If a data signal is absent, indicating that the media is free, the device transmits the data. If signals are then detected that show another device was transmitting at the same time, all devices stop sending and try again later. Traditional forms of Ethernet use this method.

2.2 CSMA/Collision Avoidance

In CSMA/Collision Avoidance (CSMA/CA), the device examines the media for the presence of a data signal. If the media is free, the device sends a notification across the media of its intent to use it. The device then sends the data. This method is used by 802.11 wireless networking technologies.

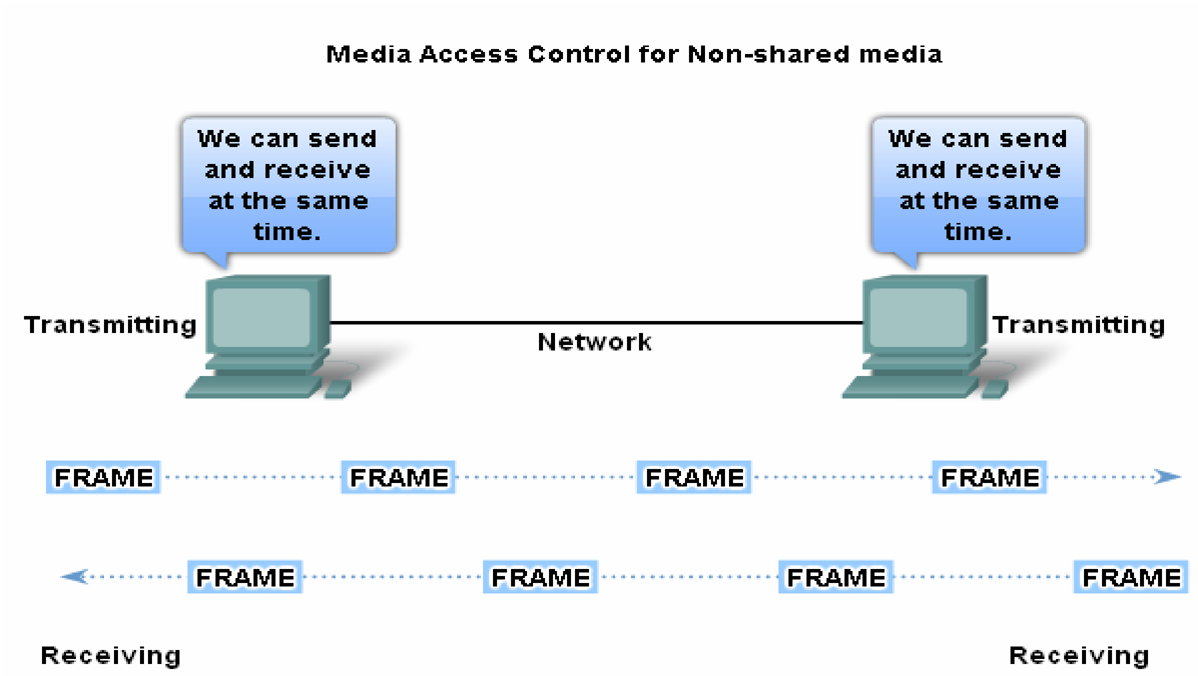
** Media Access Control Protocols for Non-Shared Media

Media access control protocols for non-shared media require little or no control before placing frames onto the media. These protocols have simpler rules and procedures for media access control. Such is the case for point-to-point topologies. In point-to-point topologies, the media interconnects just two nods. In this arrangement, the nodes do not have to share the media with other hosts or determine if a
frame is destined for that node. Therefore, Data Link layer protocols have little to do for controlling non-shared media access.

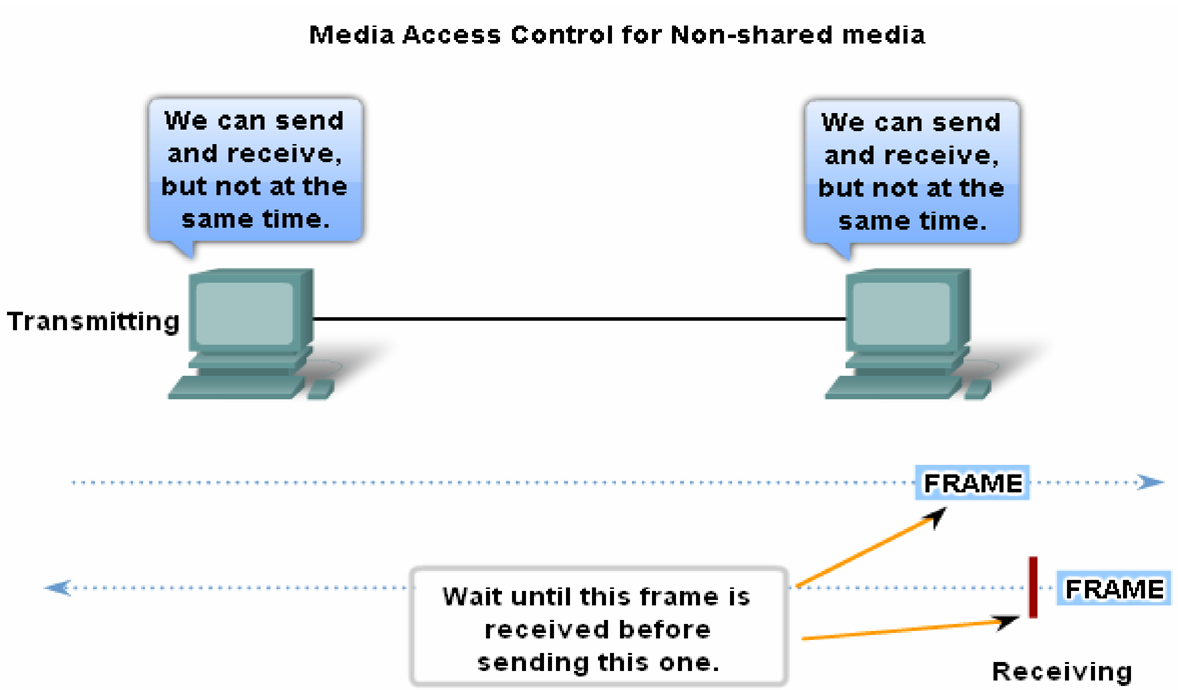
Full Duplex and Half Duplex

In point-to-point connections, the Data Link layer has to consider whether the communication is half-duplex or full-duplex.

1- Full-Duplex. In Full-duplex communication, both devices can transmit and receive on the media at the same time. The Data Link layer assumes that the media is available for transmission for both nodes at any time. Therefore, there is no media arbitration necessary in the Data Link layer.



2- Half-duplex communication means that the devices can both transmit and receive on the media but cannot do so simultaneously. Ethernet has established arbitration rules for resolving conflicts arising from instances when more than one station attempts to transmit at the same time.



Ethernet at the Data Link Layer

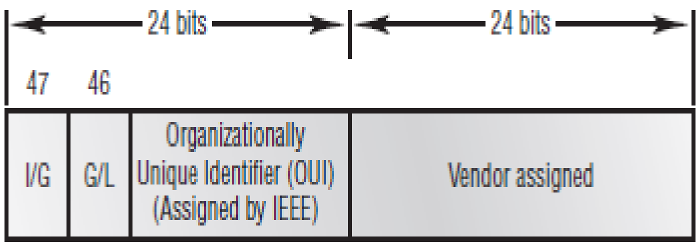
Ethernet at the Data Link layer is responsible for Ethernet addressing, commonly referred to as hardware addressing or MAC addressing. Ethernet is also responsible for framing packets received from the Network layer and preparing them for transmission on the local network through the Ethernet contention media access method.

Ethernet Addressing

Here's where we get into how Ethernet addressing works. It uses the *Media Access Control (MAC) address* burned into each and every Ethernet network interface card (NIC). The MAC, or hardware, address is a 48-bit (6-byte) address written in a hexadecimal format.

Figure 1.19 shows the 48-bit MAC addresses and how the bits are divided.

FIGURE 1.19 Ethernet addressing using MAC addresses



The *organizationally unique identifier (OUI)* is assigned by the IEEE to an organization. It's composed of 24 bits, or 3 bytes. The organization, in turn, assigns a globally administered address (24 bits, or 3 bytes) that is unique (supposedly, again—no guarantees) to each and every adapter it manufactures.

Ethernet Protocol

A Common Data Link Layer Protocol for LANs

Frame

Field name	**Preamble**	**Destination**	**Source**	**Type**	**Data**	**Frame Check Sequence**
Size	**8 bytes**	**6 bytes**	**6 bytes**	**2 bytes**	**46 - 1500 bytes**	**4 bytes**

Preamble - used for synchronization; also contains a delimiter to mark the end of the timing information.

Destination Address - 48 bit MAC address for the destination node.

Source Address - 48 bit MAC address for the source node.

Type - value to indicate which upper layer protocol will receive the data after the Ethernet process is complete.

Data or payload - this is the PDU, typically an IPv4 packet, that is to be transported over the media.

Frame Check Sequence (FCS) - A value used to check for damaged frames.