I. DATA LINK LAYER

1. Introduction

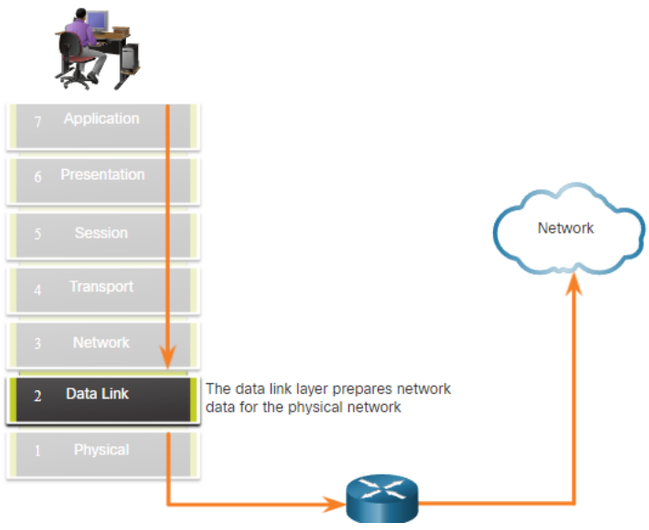
Why should I take this module?
Every network has physical components and media connecting the components. Different types of media need different information about the data in order to accept it and move it across the physical network. Think of it this way: A well-hit golf ball moves through the air fast and far. It can also move through water but not as fast or as far unless it is helped by a more forceful hit. This is because the golf ball is traveling through a different medium; water instead of air.

Data must have help to move it across different media. The data link layer provides this help. As you might have guessed, this help differs based on a number of factors. This module gives you an overview of these factors, how they affect data, and the protocols designed to ensure successful delivery. Let's get started!

2. Purpose of the Data Link Layer

The Data Link Layer
The data link layer of the OSI model (Layer 2), as shown in the figure, prepares network data for the physical network. The data link layer is responsible for network interface card (NIC) to network interface card communications. The data link layer does the following:

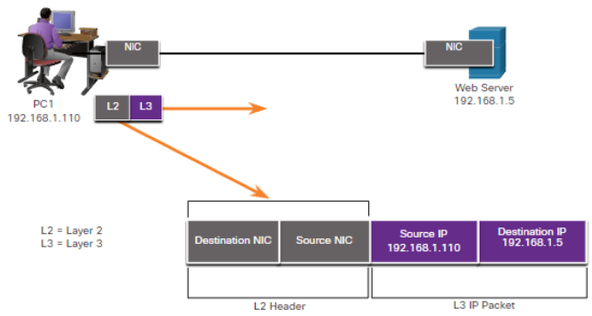
- Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
- Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
- Controls how data is placed and received on the media.
- Exchanges frames between endpoints over the network media.
- Receives encapsulated data, usually Layer 3 packets, and directs them to the proper upper-layer protocol.
- Performs error detection and rejects any corrupt frame.



In computer networks, a node is a device that can receive, create, store, or forward data along a communications path. A node can be either an end device such as a laptop or mobile phone, or an intermediary device such as an Ethernet switch.

Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. Additionally, every time a new network technology or medium was developed IP, would have to adapt.

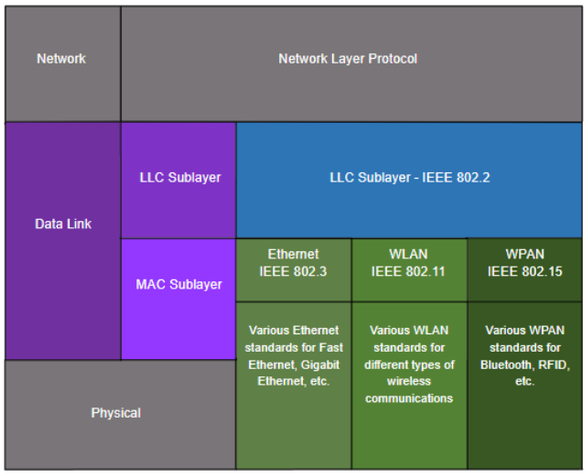
The figure displays an example of how the data link layer adds Layer 2 Ethernet destination and source NIC information to a Layer 3 packet. It would then convert this information to a format supported by the physical layer (i.e., Layer 1).



IEEE 802 LAN/MAN Data Link Sublayers
IEEE 802 LAN/MAN standards are specific to Ethernet LANs, wireless LANs (WLAN), wireless personal area networks (WPAN) and other types of local and metropolitan area networks. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers:

- **Logical Link Control (LLC)** - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It 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 IPv4 and IPv6, to use the same network interface and media.
- **Media Access Control (MAC)** – Implements this sublayer (IEEE 802.3, 802.11, or 802.15) in hardware. It is responsible for data encapsulation and media access control. It provides data link layer addressing and it is integrated with various physical layer technologies.

The figure shows the two sublayers (LLC and MAC) of the data link layer.



The LLC sublayer takes the network protocol data, which is typically an IPv4 or IPv6 packet, and adds Layer 2 control information to help deliver the packet to the destination node.

The MAC sublayer controls the NIC and other hardware that is responsible for sending and receiving data on the wired or wireless LAN/MAN medium.

The MAC sublayer provides data encapsulation:

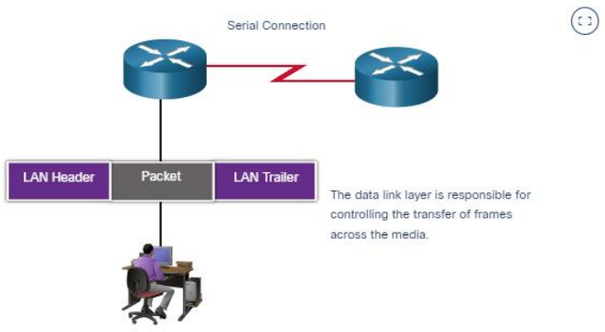
- **Frame delimiting** - The framing process provides important delimiters to identify fields within a frame. These delimiting bits provide synchronization between the transmitting and receiving nodes.
- **Addressing** - Provides source and destination addressing for transporting the Layer 2 frame between devices on the same shared medium.
- **Error detection** - Includes a trailer used to detect transmission errors.

The MAC sublayer also provides media access control, allowing multiple devices to communicate over a shared (half-duplex) medium. Full-duplex communications do not require access control.

Providing Access to Media
Each network environment that packets encounter as they travel from a local host to a remote host can have different characteristics. For example, an Ethernet LAN usually consists of many hosts contending for access on the network medium. The MAC sublayer resolves this. With serial links the access method may only consist of a direct connection between only two devices, usually two routers. Therefore, they do not require the techniques employed by the IEEE 802 MAC sublayer.
Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. In any given exchange of network layer packets, there may be numerous data link layers and media transitions.
At each hop along the path, a router performs the following Layer 2 functions:

1. Accepts a frame from a medium
2. De-encapsulates the frame
3. Re-encapsulates the packet into a new frame
4. Forwards the new frame appropriate to the medium of that segment of the physical network

Press play to view the animation. The router in the figure has an Ethernet interface to connect to the LAN and a serial interface to connect to the WAN. As the router processes frames, it will use data link layer services to receive the frame from one medium, de-encapsulate it to the Layer 3 PDU, re-encapsulate the PDU into a new frame, and place the frame on the medium of the next link of the network.



Data Link Layer Standards
Data link layer protocols are generally not defined by Request for Comments (RFCs), unlike the protocols of the upper layers of the TCP/IP suite. The Internet Engineering Task Force (IETF) maintains the functional protocols and services for the TCP/IP protocol suite in the upper layers, but they do not define the functions and operation of the TCP/IP network access layer.
Engineering organizations that define open standards and protocols that apply to the network access layer (i.e., the OSI physical and data link layers) include the following:
Institute of Electrical and Electronics Engineers (IEEE)
International Telecommunication Union (ITU)
International Organization for Standardization (ISO)
American National Standards Institute (ANSI)
The logos for these organizations are shown in the figure.
Engineering Organization Logos

3. Topologies

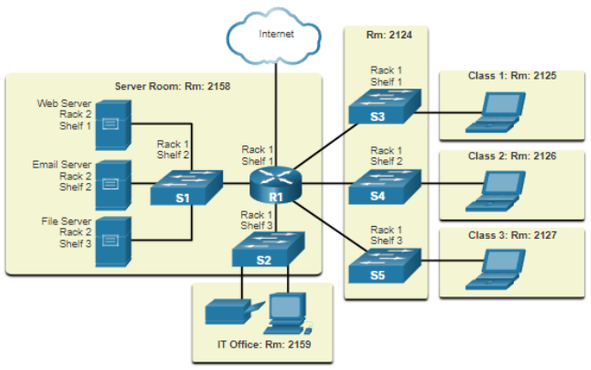
Physical and Logical Topologies
As you learned in the previous topic, the data link layer prepares network data for the physical network. It must know the logical topology of a network in order to be able to determine what is needed to transfer frames from one device to another. This topic explains the ways in which the data link layer works with different logical network topologies.
The topology of a network is the arrangement, or the relationship, of the network devices and the interconnections between them.
There are two types of topologies used when describing LAN and WAN networks:

- **Physical topology** – Identifies the physical connections and how end devices and intermediary devices (i.e, routers, switches, and wireless access points) are interconnected. The topology may also include specific device location such as room number and location on the equipment rack. Physical topologies are usually point-to-point or star.
- **Logical topology** - Refers to the way a network transfers frames from one node to the next. This topology identifies virtual connections using device interfaces and Layer 3 IP addressing schemes.

The data link layer "sees" the logical topology of a network when controlling data access to the media. It is the logical topology that influences the type of network framing and media access control used.
The figure displays a sample **physical** topology for a small sample network.
The physical network topology shows six rooms, each highlighted in a light-yellow box, with various networking devices and cabling. On the left side is the server room labeled room 2158. It contains a router labeled R1 mounted on rack 1 shelf 1 with six cable connections. A cable at the top connects to a cloud labeled Internet. A cable to the left connects to a switch labeled S1 mounted on rack 1 shelf 2. S1 is connected to three servers: a web server mounted on rack 2 shelf 1, an email server mounted on rack 2 shelf 2, and a file server mounted on rack 2 shelf 3. A cable connected to the bottom of R1 connects to a switch labeled S2 mounted on rack 1 shelf 3. S2 has two connections leading to a printer and a PC in the IT office labeled room 2159. R1 has three cables to the right connected to three switches located in room 2124. The top switch is labeled S3 and mounted on rack 1 shelf 1. The middle switch is labeled S4 and mounted on rack 1 shelf 2. The bottom switch is

labeled S5 and mounted on rack 1 shelf 3. S3 has a cable on the left connected to a laptop in a room labeled class 1 room 2125. S4 has a cable on the left connected to a laptop in a room labeled class 2 room 2126. S5 has a cable on the left connected to a laptop in a room labeled class 3 room 2127.

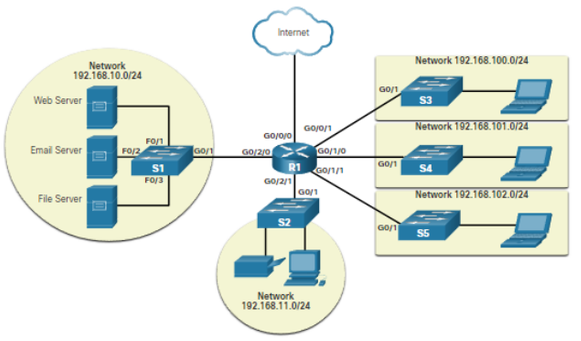
Physical Topology



The next figure displays a sample **logical** topology for the same network.

The logical network topology shows devices, port labels, and the network addressing scheme. In the middle of the picture is a router labeled R1. A port labeled G0/0/0 connects to a cloud at the top labeled Internet. A port labeled G0/2/0 connects at the left to a switch labeled S1 at port G0/1. S1 is connected to three servers. S1 and the servers are highlighted in a light yellow circle with the network 192.168.10.0/24 written at the top. Port F0/1 on S1 connects to a web server. Port F0/2 on S1 connects to an email server. Port F0/3 on S1 connects to a file server. Port G0/0/1 on R1 connects at the bottom to a switch labeled S2. S2 connects to a printer and a PC, all of which are highlighted in a light yellow circle with the network 192.168.11.0/24 written on the bottom. At the right of R1 are three additional connections, each connecting to a switch at port G0/1 which is then connected to a laptop at port F0/1. Each switch and laptop are highlighted in yellow and the network address shown. Port G0/0/1 of R1 connects at the top to a switch labeled S3 on network 192.168.100.0. Port G0/1/0 of R1 connects in the middle to a switch labeled S4 on network 192.169.101.0. Port G0/1/1 on R1 connects at the bottom to a switch labeled S5 on network 192.168.102.0. R1 connects to the Internet on interface G0/0/0.

Logical Topology



WAN Topologies

The figures illustrate how WANs are commonly interconnected using three common physical WAN topologies.

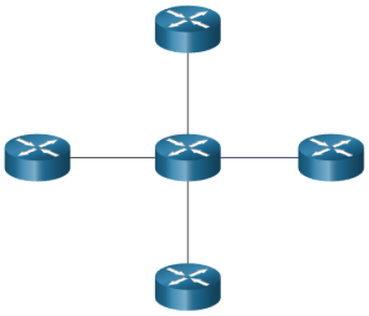
Point-to-Point

This is the simplest and most common WAN topology. It consists of a permanent link between two endpoints.

A hybrid is a variation or combination of any topologies. For example, a partial mesh is a hybrid topology in which some, but not all, end devices are interconnected.

Hub and Spoke

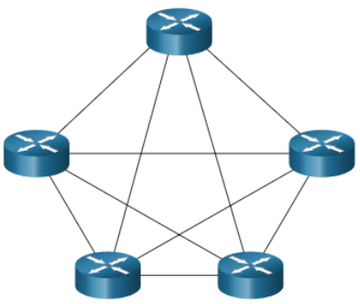
This is a WAN version of the star topology in which a central site interconnects branch sites through the use of point-to-point links. Branch sites cannot exchange data with other branch sites without going through the central site.



A hybrid is a variation or combination of any topologies. For example, a partial mesh is a hybrid topology in which some, but not all, end devices are interconnected.

Mesh

This topology provides high availability but requires that every end system is interconnected to every other system. Therefore, the administrative and physical costs can be significant. Each link is essentially a point-to-point link to the other node.



A hybrid is a variation or combination of any topologies. For example, a partial mesh is a hybrid topology in which some, but not all, end devices are interconnected.

Point-to-Point WAN Topology

Physical point-to-point topologies directly connect two nodes, as shown in the figure. In this arrangement, two nodes do not have to share the media with other hosts. Additionally, when using a serial communications protocol such as Point-to-Point Protocol (PPP), a node does not have to make any determination about whether an incoming frame is destined for it or another node. Therefore, the logical data link protocols can be very simple, as all frames on the media can only travel to or from the two nodes. The node places the frames on the media at one end and those frames are taken from the media by the node at the other end of the point-to-point circuit.

Point-to-point topologies are limited to two nodes.

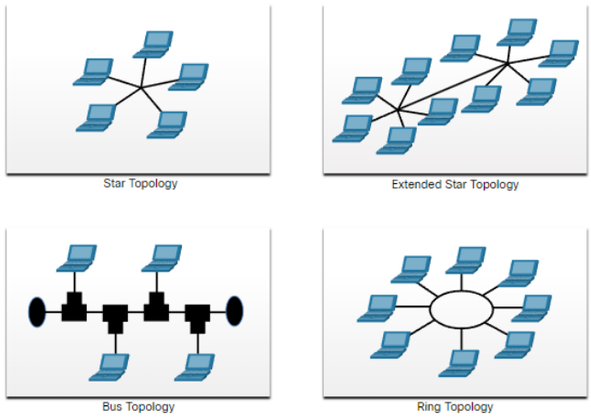
Note: A point-to-point connection over Ethernet requires the device to determine if the incoming frame is destined for this node.
A source and destination node may be indirectly connected to each other over some geographical distance using multiple intermediary devices. However, the use of physical devices in the network does not affect the logical topology, as illustrated in the figure. In the figure, adding intermediary physical connections may not change the logical topology. The logical point-to-point connection is the same.

LAN Topologies
In multiaccess LANs, end devices (i.e., nodes) are interconnected using star or extended star topologies, as shown in the figure. In this type of topology, end devices are connected to a central intermediary device, in this case, an Ethernet switch. An **extended star** extends this topology by interconnecting multiple Ethernet switches. The star and extended topologies are easy to install, very scalable (easy to add and remove end devices), and easy to troubleshoot. Early star topologies interconnected end devices using Ethernet hubs.
At times there may be only two devices connected on the Ethernet LAN. An example is two interconnected routers. This would be an example of Ethernet used on a point-to-point topology.
Legacy LAN Topologies
Early Ethernet and legacy Token Ring LAN technologies included two other types of topologies:

- **Bus** - All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Legacy Ethernet networks were often bus topologies using coax cables because it was inexpensive and easy to set up.
- **Ring** - End systems are connected to their respective neighbor forming a ring. The ring does not need to be terminated, unlike in the bus topology. Legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks used ring topologies.

The figures illustrate how end devices are interconnected on LANs. It is common for a straight line in networking graphics to represent an Ethernet LAN including a simple star and an extended star. comparison of four physical topologies: star, extended star, bus, and ring

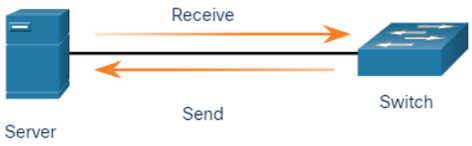
Physical Topologies



Half and Full Duplex Communication
Understanding duplex communication is important when discussing LAN topologies because it refers to the direction of data transmission between two devices. There are two common modes of duplex.

Half-duplex communication
Both devices can transmit and receive on the media but cannot do so simultaneously. WLANs and legacy bus topologies with Ethernet hubs use the half-duplex mode. Half-duplex allows only one device to send or receive at a time on the shared medium. Click play in the figure to see the animation showing half-duplex communication.

Full-duplex communication
Both devices can simultaneously transmit and receive on the shared media. The data link layer assumes that the media is available for transmission for both nodes at any time. Ethernet switches operate in full-duplex mode by default, but they can operate in half-duplex if connecting to a device such as an Ethernet hub. Click play in the figure to see the animation showing full-duplex communication.



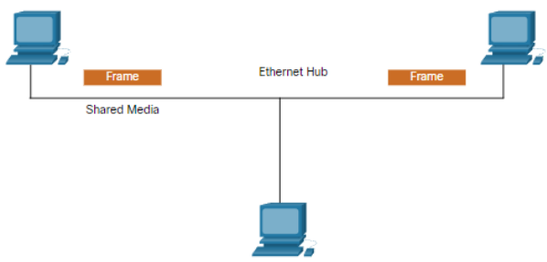
In summary, half-duplex communications restrict the exchange of data to one direction at a time. Full-duplex allows the sending and receiving of data to happen simultaneously.
It is important that two interconnected interfaces, such as a host NIC and an interface on an Ethernet switch, operate using the same duplex mode. Otherwise, there will be a duplex mismatch creating inefficiency and latency on the link.

Access Control Methods
Ethernet LANs and WLANs are examples of multiaccess networks. A multiaccess network is a network that can have two or more end devices attempting to access the network simultaneously.
Some multiaccess networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media:

- Contention-based access
- Controlled access

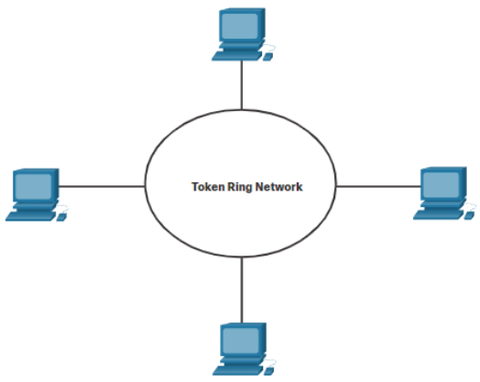
Contention-based access
In contention-based multiaccess networks, all nodes are operating in half-duplex, competing for the use of the medium. However, only one device can send at a time. Therefore, there is a process if more than one device transmits at the same time. Examples of contention-based access methods include the following:

- Carrier sense multiple access with collision detection (CSMA/CD) used on legacy bus-topology Ethernet LANs
- Carrier sense multiple access with collision avoidance (CSMA/CA) used on Wireless LANs



Controlled access
In a controlled-based multiaccess network, each node has its own time to use the medium. These deterministic types of legacy networks are inefficient because a device must wait its turn to access the medium. Examples of multiaccess networks that use controlled access include the following:

- Legacy Token Ring
- Legacy ARCNET



Each node must wait for its turn to access the network medium.

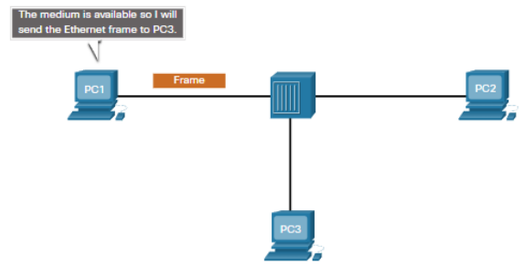
Note: Today, Ethernet networks operate in full-duplex and do not require an access method.

Contention-Based Access - CSMA/CD
Examples of contention-based access networks include the following:

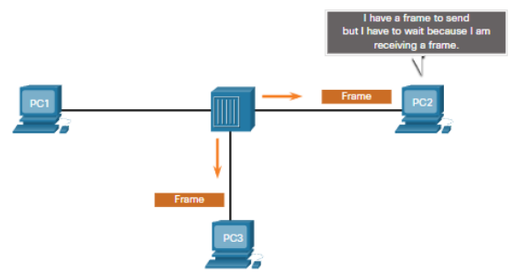
- Wireless LAN (uses CSMA/CA)
- Legacy bus-topology Ethernet LAN (uses CSMA/CD)
- Legacy Ethernet LAN using a hub (uses CSMA/CD)

These networks operate in half-duplex mode, meaning only one device can send or receive at a time. This requires a process to govern when a device can send and what happens when multiple devices send at the same time.
If two devices transmit at the same time, a collision will occur. For legacy Ethernet LANs, both devices will detect the collision on the network. This is the collision detection (CD) portion of CSMA/CD. The NIC compares data transmitted with data received, or by recognizing that the signal amplitude is higher than normal on the media. The data sent by both devices will be corrupted and will need to be resent.

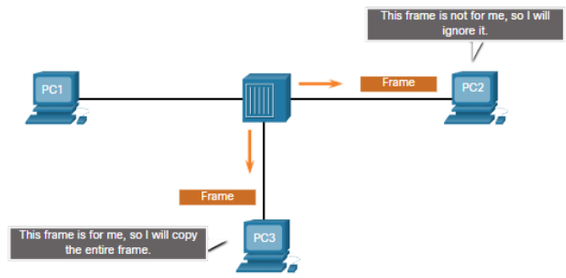
PC1 Sends a Frame
PC1 has an Ethernet frame to send to PC3. The PC1 NIC needs to determine if any device is transmitting on the medium. If it does not detect a carrier signal (in other words, it is not receiving transmissions from another device), it will assume the network is available to send. The PC1 NIC sends the Ethernet Frame when the medium is available, as shown in the figure.



The Hub Receives the Frame
The Ethernet hub receives and sends the frame. An Ethernet hub is also known as a multiport repeater. Any bits received on an incoming port are regenerated and sent out all other ports, as shown in the figure.
If another device, such as PC2, wants to transmit, but is currently receiving a frame, it must wait until the channel is clear, as shown in the figure.

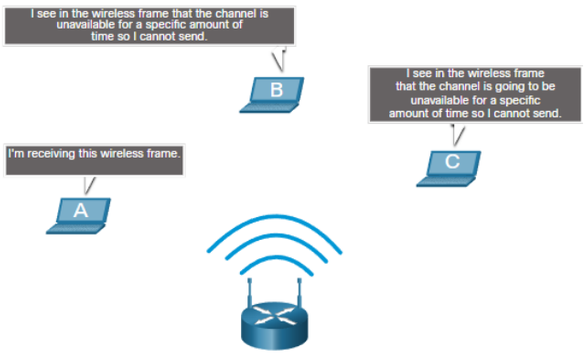


The Hub Sends the Frame
All devices attached to the hub will receive the frame. However, because the frame has a destination data link address for PC3, only that device will accept and copy in the entire frame. All other device NICs will ignore the frame, as shown in the figure.



Contention-Based Access - CSMA/CA
Another form of CSMA used by IEEE 802.11 WLANs is carrier sense multiple access/collision avoidance (CSMA/CA).
CMSA/CA uses a method similar to CSMA/CD to detect if the media is clear. CMSA/CA uses additional techniques. In wireless environments it may not be possible for a device to detect a collision. CMSA/CA does not detect collisions but attempts to avoid them by waiting before transmitting. Each device that transmits includes the time duration that it needs for the transmission. All other wireless devices receive this

information and know how long the medium will be unavailable.
In the figure, if host A is receiving a wireless frame from the access point, hosts B, and C will also see the frame and how long the medium will be unavailable.



After a wireless device sends an 802.11 frame, the receiver returns an acknowledgment so that the sender knows the frame arrived.
Whether it is an Ethernet LAN using hubs, or a WLAN, contention-based systems do not scale well under heavy media use.
Note: Ethernet LANs using switches do not use a contention-based system because the switch and the host NIC operate in full-duplex mode.

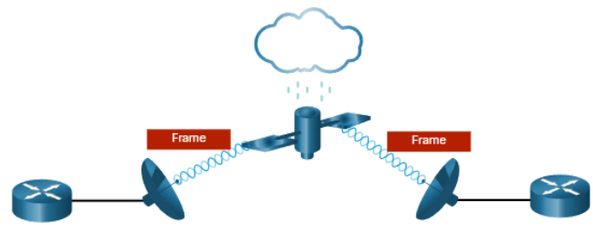
4. Data Link Frame

The Frame

This topic discusses in detail what happens to the data link frame as it moves through a network. The information appended to a frame is determined by the protocol being used.
The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame.
The data link protocol is responsible for NIC-to-NIC communications within the same network. Although there are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts:

- Header
- Data
- Trailer

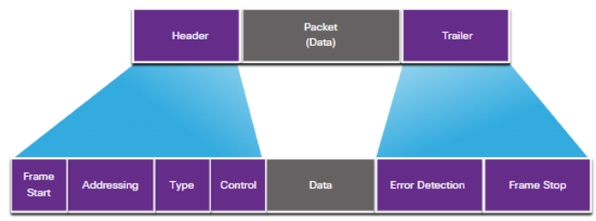
Unlike other encapsulation protocols, the data link layer appends information in the form of a trailer at the end of the frame.
All data link layer protocols encapsulate the data within the data field of the frame. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol.
There is no one frame structure that meets the needs of all data transportation across all types of media.
Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. For example, a WLAN frame must include procedures for collision avoidance and therefore requires additional control information when compared to an Ethernet frame.
As shown in the figure, in a fragile environment, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.



Greater effort is needed to ensure delivery. This means higher overhead and slower transmission rates.

Frame Fields

Framing breaks the stream into decipherable groupings, with control information inserted in the header and trailer as values in different fields. This format gives the physical signals a structure that are by recognized by nodes and decoded into packets at the destination.
The generic frame fields are shown in the figure. Not all protocols include all these fields. The standards for a specific data link protocol define the actual frame format.



Frame fields include the following:

- **Frame start and stop indicator flags** - Used to identify the beginning and end limits of the frame.
- **Addressing** - Indicates the source and destination nodes on the media.
- **Type** - Identifies the Layer 3 protocol in the data field.
- **Control** - Identifies special flow control services such as quality of service (QoS). QoS gives forwarding priority to certain types of messages. For example, voice over IP (VoIP) frames normally receive priority because they are sensitive to delay.
- **Data** - Contains the frame payload (i.e., packet header, segment header, and the data).
- **Error Detection** - Included after the data to form the trailer.

Data link layer protocols add a trailer to the end of each frame. In a process called error detection, the trailer determines if the frame arrived without error. It places a logical or mathematical summary of the bits that comprise the frame in the trailer. The data link layer adds error detection because the signals on the media could be subject to interference, distortion, or loss that would substantially change the bit values that those signals represent.
A transmitting node creates a logical summary of the contents of the frame, known as the cyclic redundancy check (CRC) value. This value is placed in the frame check sequence (FCS) field to represent the contents of the frame. In the Ethernet trailer, the FCS provides a method for the receiving node to determine whether the frame experienced transmission errors.

Layer 2 Addresses

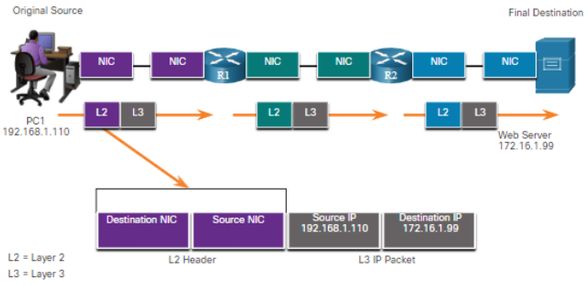
The data link layer provides the addressing used in transporting a frame across a shared local media. Device addresses at this layer are referred to as physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. It is typically at the beginning of the frame, so the NIC can quickly determine if it matches its own Layer 2 address before accepting the rest of the frame. The frame header may also contain the source address of the frame.

Unlike Layer 3 logical addresses, which are hierarchical, physical addresses do not indicate on what network the device is located. Rather, the physical address is unique to the specific device. A device will still function with

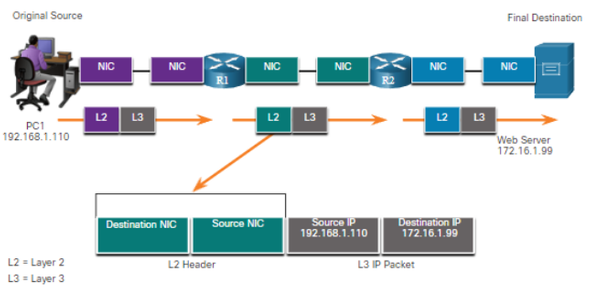
the same Layer 2 physical address even if the device moves to another network or subnet. Therefore, Layer 2 addresses are only used to connect devices within the same shared media, on the same IP network.

The figures illustrate the function of the Layer 2 and Layer 3 addresses. As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame. Each data link frame contains the source data link address of the NIC sending the frame, and the destination data link address of the NIC receiving the frame.

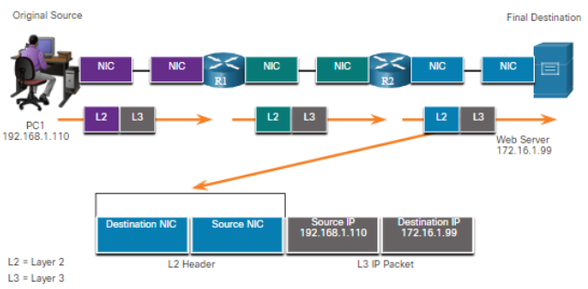
Host-to-Router
The source host encapsulates the Layer 3 IP packet in a Layer 2 frame. In the frame header, the host adds its Layer 2 address as the source and the Layer 2 address for R1 as the destination.



Router-to-Router
R1 encapsulates the Layer 3 IP packet in a new Layer 2 frame. In the frame header, R1 adds its Layer 2 address as the source and the Layer 2 address for R2 as the destination.



Router-to-Host
R2 encapsulates the Layer 3 IP packet in a new Layer 2 frame. In the frame header, R2 adds its Layer 2 address as the source and the Layer 2 address for the server as the destination.



The data link layer address is only used for local delivery. Addresses at this layer have no meaning beyond the local network. Compare this to Layer 3, where addresses in the packet header are carried from the source host to the destination host, regardless of the number of network hops along the route.
If the data must pass onto another network segment, an intermediary device, such as a router, is necessary. The router must accept the frame based on the physical address and de-encapsulate the frame in order to examine the hierarchical address, which is the IP address. Using the IP address, the router can determine the network location of the destination device and the best path to reach it. When it knows where to forward the packet, the router then creates a new frame for the packet, and the new frame is sent on to the next network segment toward its final destination.

LAN and WAN Frames
Ethernet protocols are used by wired LANs. Wireless communications fall under WLAN (IEEE 802.11) protocols. These protocols were designed for multiaccess networks.

WANs traditionally used other types of protocols for various types of point-to-point, hub-spoke, and full-mesh topologies. Some of the common WAN protocols over the years have included:

- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- X.25

These Layer 2 protocols are now being replaced in the WAN by Ethernet.

In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media.

Each protocol performs media access control for specified Layer 2 logical topologies. This means that a number of different network devices can act as nodes that operate at the data link layer when implementing these protocols. These devices include the NICs on computers as well as the interfaces on routers and Layer 2 switches.

The Layer 2 protocol that is used for a particular network topology is determined by the technology used to implement that topology. The technology used is determined by the size of the network, in terms of the number of hosts and the geographic scope, and the services to be provided over the network.

A LAN typically uses a high bandwidth technology capable of supporting large numbers of hosts. The relatively small geographic area of a LAN (a single building or a multi-building campus) and its high density of users make this technology cost-effective.

However, using a high bandwidth technology is usually not cost-effective for WANs that cover large geographic areas (cities or multiple cities, for example). The cost of the long-distance physical links and the technology used to carry the signals over those distances typically results in lower bandwidth capacity.

The difference in bandwidth normally results in the use of different protocols for LANs and WANs.
Data link layer protocols include:

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

II. ETHERNET SWITCHING

1. Introduction

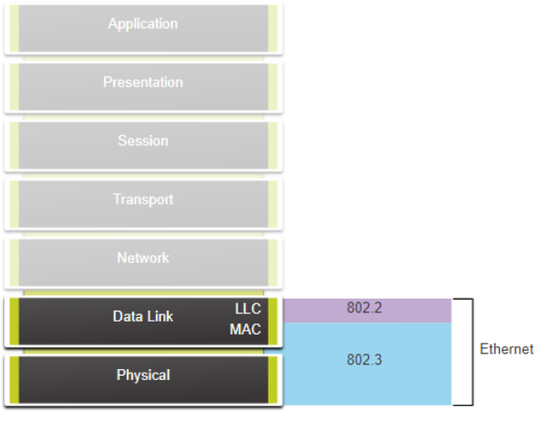
If you are planning to become a network administrator or a network architect, you will definitely need to know about Ethernet and Ethernet switching. The two most prominent LAN technologies in use today are Ethernet and WLAN. Ethernet supports bandwidths of up to 100 Gbps, which explains its popularity. This module contains a lab using Wireshark in which you can look at Ethernet frames and another lab where you view network device MAC addresses. There are also some instructional videos to help you better understand Ethernet. By the time you have finished this module, you too could create a switched network that uses Ethernet!

2. Ethernet Frames

Ethernet Encapsulation
This module starts with a discussion of Ethernet technology including an explanation of MAC sublayer and the Ethernet frame fields.
Ethernet is one of two LAN technologies used today, with the other being wireless LANs (WLANs). Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.
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 supports data bandwidths of the following:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

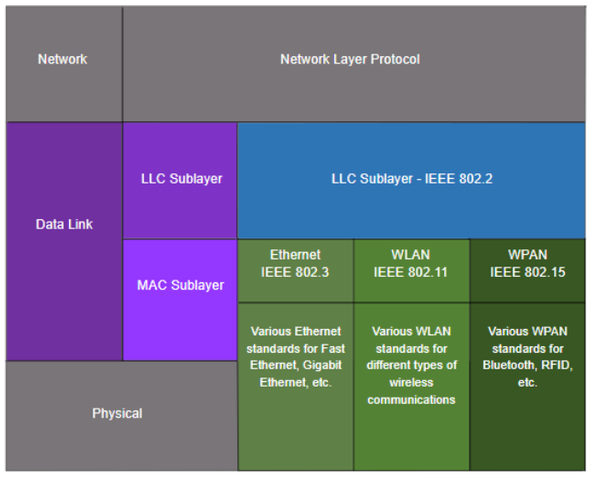
As shown in the figure, Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
Ethernet and the OSI Model



Ethernet is defined by data link layer and physical layer protocols.

Data Link Sublayers
IEEE 802 LAN/MAN protocols, including Ethernet, use the following two separate sublayers of the data link layer to operate. They are the Logical Link Control (LLC) and the Media Access Control (MAC), as shown in the figure.
Recall that LLC and MAC have the following roles in the data link layer:

- **LLC Sublayer -** This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It 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 IPv4 and IPv6, to use the same network interface and media.
- **MAC Sublayer -** This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware and is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies.

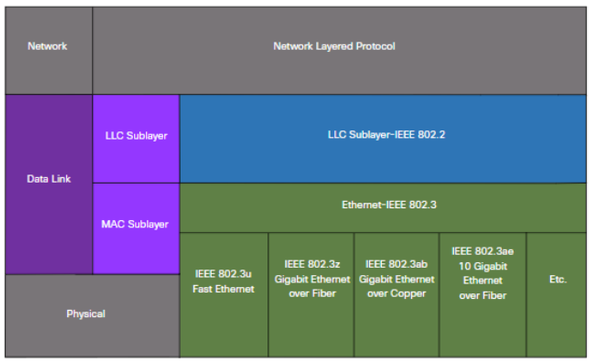


MAC Sublayer
The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation
IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame** - This is the internal structure of the Ethernet frame.
- **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.
- **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Accessing the Media
As shown in the figure, the IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.
The diagram is showing various Ethernet standards in the MAC sublayer. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the IEEE 802.2 LLC sublayer. Next is the Ethernet IEEE 802.3 MAC sublayer. Below that are five columns with various Ethernet standards and media types that span the lower part of the MAC sublayer and the entire OSI physical layer. From left to right the columns are: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet over Fiber; IEEE 802.ab Gigabit Ethernet over Copper; IEEE 802.3ae 10 Gigabit Ethernet over Fiber; and Etc.
Ethernet Standards in the MAC Sublayer



Recall that 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) This ensures that only one device is transmitting at a time. CSMA/CD allows multiple devices to share the same half-duplex medium, detecting a collision when more than one device attempts to transmit simultaneously. It also provides a back-off algorithm for retransmission.
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 expected maximum is 1518 bytes. This includes all bytes from the destination MAC address field through the frame check sequence (FCS) field. The preamble field is not included when describing the size of the frame.

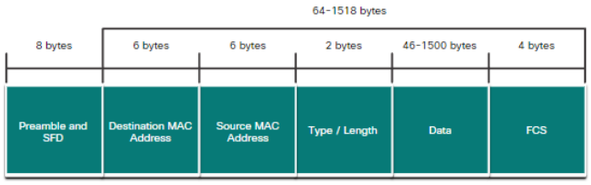
Note: The frame size may be larger if additional requirements are included, such as VLAN tagging. VLAN tagging is beyond the scope of this course.

Any frame less than 64 bytes in length is considered a "collision fragment" or "runt frame" and is automatically discarded by receiving stations. 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.

The figure shows each field in the Ethernet frame. Refer to the table for more information about the function of each field.

The diagram shows the fields of an Ethernet frame. From left to right the fields and their length are: Preamble and SFD, 8 bytes; destination MAC address, 6 bytes; source MAC address, 6 bytes; type / length, 2 bytes; data, 46 - 1500 bytes; and F C S, 4 bytes. Excluding the first field, the total number of bytes in the remaining fields is between 64 – 1518 bytes.
Ethernet Frame Fields



Field	Description
Preamble and Start Frame Delimiter Fields	The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (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. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.
Destination MAC Address Field	This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. Can be a unicast, multicast or broadcast address.
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. Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP. **Note**: You may also see this field referred to as EtherType, Type, or Length.
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. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.
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). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

3. Ethernet MAC Address

MAC Address and Hexadecimal

In networking, IPv4 addresses are represented using the decimal base ten number system and the binary base 2 number system. IPv6 addresses and Ethernet addresses are represented using the hexadecimal base sixteen number system. To understand hexadecimal, you must first be very familiar with binary and decimal.

The hexadecimal numbering system uses the numbers 0 to 9 and the letters A to F.

An Ethernet MAC address consists of a 48-bit binary value. Hexadecimal is used to identify an Ethernet address because a single hexadecimal digit represents four binary bits. Therefore, a 48-bit Ethernet MAC address can be expressed using only 12 hexadecimal values.
The figure compares the equivalent decimal and hexadecimal values for binary 0000 to 1111.
The figure is three columns showing the decimal and hexadecimal equivalents of select 4-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 16 rows below the header.

Decimal and Binary Equivalents of 0 to F Hexadecimal

Decimal	Binary	Hexadecimal
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

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, as shown in the next figure.
The figure is three columns showing the decimal and hexadecimal equivalents of select 8-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 18 rows below the header.

Selected Decimal, Binary, and Hexadecimal Equivalents

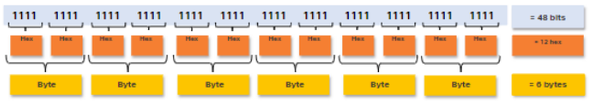
Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example, in the table, the binary value 0000 1010 is shown 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).
You may have to convert between decimal and hexadecimal values. If such conversions are required, convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as appropriate.

Ethernet MAC Address

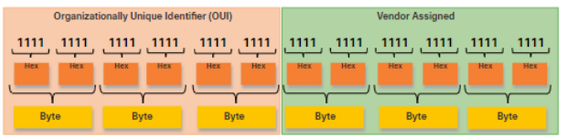
In an Ethernet LAN, every network device is connected to the same, shared media. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model.
An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in the figure. 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). When a vendor assigns a MAC address to a device or Ethernet interface, the vendor must do as follows:

- Use its assigned OUI as the first 6 hexadecimal digits.
- Assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value, as shown in the figure.



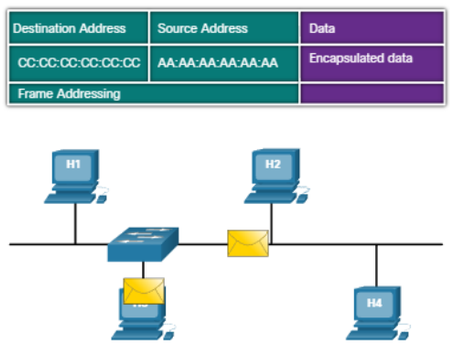
For example, assume that Cisco needs to assign a unique MAC address to a new device. The IEEE has assigned Cisco a OUI of **00-60-2F**. Cisco would then configure the device with a unique vendor code such as **3A-07-BC**. Therefore, the Ethernet MAC address of that device would be **00-60-2F-3A-07-BC.**
It is the responsibility of the vendor to ensure that none of its devices be assigned the same MAC address. However, it is possible for duplicate MAC addresses to exist because of mistakes made during manufacturing, mistakes made in some virtual machine implementation methods, or modifications made using one of several software tools. In any case, it will be necessary to modify the MAC address with a new NIC or make modifications via software.

Frame Processing

Sometimes the MAC address is referred to as a burned-in address (BIA) because the address is hard coded into read-only memory (ROM) on the NIC. This means that the address is encoded into the ROM chip permanently.
Note: On modern PC operating systems and NICs, it is possible to change the MAC address in software. This is useful when attempting to gain access to a network that filters based on BIA. Consequently, filtering or controlling traffic based on the MAC address is no longer as secure.

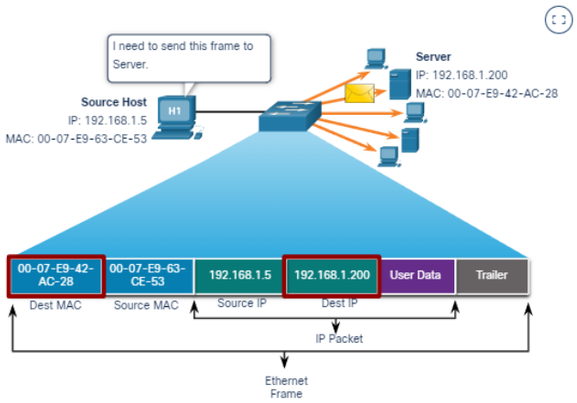
When the computer boots up, the NIC copies its MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network, the Ethernet header includes these:

- **Source MAC address** - This is the MAC address of the source device NIC.
- **Destination MAC address** - This is the MAC address of the destination device NIC.



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.
Click Play in the animation to view how a unicast frame is processed. In this example the destination MAC address and the destination IP address are both unicast.

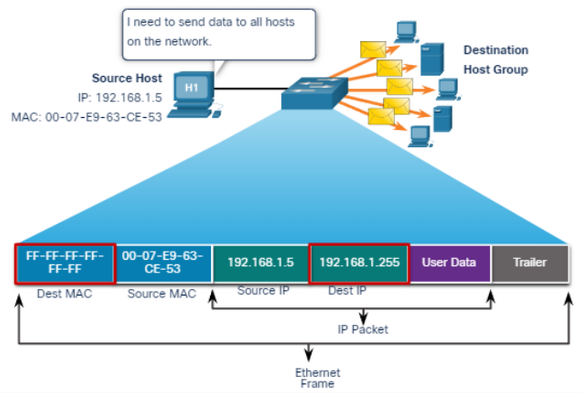


In the example shown in the animation, a host with IPv4 address 192.168.1.5 (source) requests a web page from the server at IPv4 unicast address 192.168.1.200. For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.
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.
Click Play in the animation to view how a broadcast frame is processed. In this example the destination MAC address and destination IP address are both broadcasts.



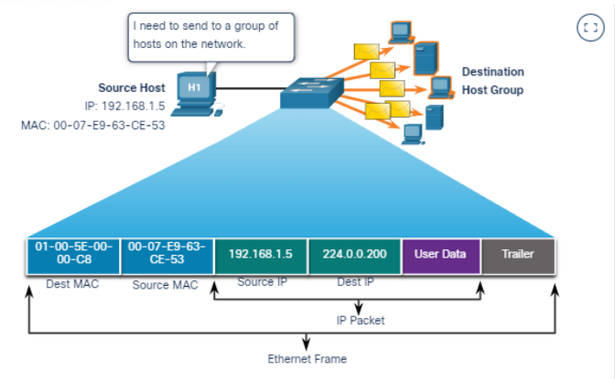
As shown in the animation, the source host sends an IPv4 broadcast packet to all devices on its network. The IPv4 destination address is a broadcast address, 192.168.1.255. When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
DHCP for IPv4 is an example of a protocol that uses Ethernet and IPv4 broadcast addresses.
However, not all Ethernet broadcasts carry an IPv4 broadcast packet. For example, ARP Requests do not use IPv4, but the ARP message is sent as an Ethernet broadcast.

Multicast MAC Address
An Ethernet multicast frame is received and processed by a group of devices on the Ethernet LAN that belong to the same multicast group. The features of an Ethernet multicast are as follows:

- 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) and Link Layer Discovery Protocol (LLDP).
- 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.

If the encapsulated data is an IP multicast packet, the devices that belong to a multicast group are assigned a multicast group IP address. The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of

IPv6 multicast addresses begins with ff00::/8. 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 to deliver frames on a local network. The multicast MAC address is associated with, and uses addressing information from, the IPv4 or IPv6 multicast address.
Click Play in the animation to view how a multicast frame is processed. In this example, the destination MAC address and destination IP address are both multicasts.

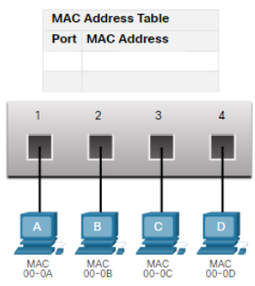


Routing protocols and other network protocols use multicast addressing. Applications such as video and imaging software may also use multicast addressing, although multicast applications are not as common.

4. The MAC Address Table

Switch Fundamentals

Now that you know all about Ethernet MAC addresses, it is time to talk about how a switch uses these addresses to forward (or discard) frames to other devices on a network. If a switch just forwarded every frame it received out all ports, your network would be so congested that it would probably come to a complete halt.
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. In the figure, the four-port switch was just powered on. The table shows the MAC Address Table which has not yet learned the MAC addresses for the four attached PCs.
Note: MAC addresses are shortened throughout this topic for demonstration purposes.



The switch MAC address table is empty.

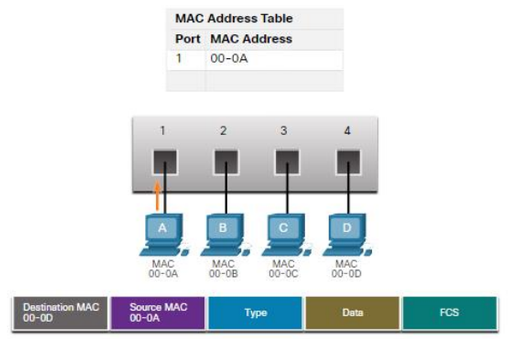
Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table. While the term CAM table is fairly common, for the purposes of this course, we will refer to it as a MAC address table.

Switch Learning and Forwarding

The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.

Examine the Source MAC Address

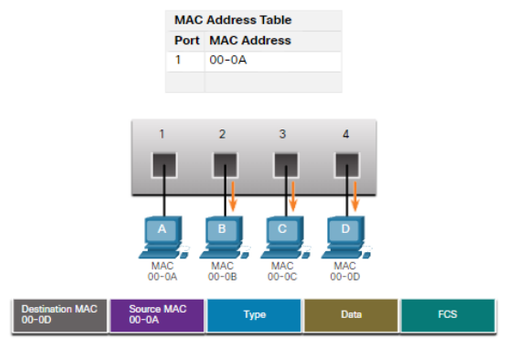
Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the port number where the frame entered the switch. If the source MAC address does not exist, it is added to the table along with the incoming port number. If the source MAC address does exist, the switch updates the refresh timer for that entry in the table. By default, most Ethernet switches keep an entry in the table for 5 minutes.
In the figure for example, PC-A is sending an Ethernet frame to PC-D. The table shows the switch adds the MAC address for PC-A to the MAC Address Table.
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.



1. PC-A sends an Ethernet frame.
2. The switch adds the port number and MAC address for PC-A to the MAC Address Table.

Find the Destination MAC Address

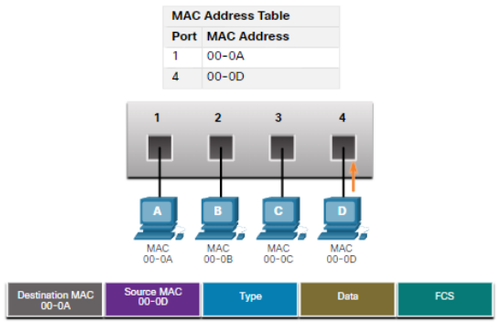
If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, it will forward the frame out the specified port. If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.
As shown in the figure, the switch does not have the destination MAC address in its table for PC-D, so it sends the frame out all ports except port 1.
Note: If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.



1. The destination MAC address is not in the table.
2. The switch forwards the frame out all other ports.

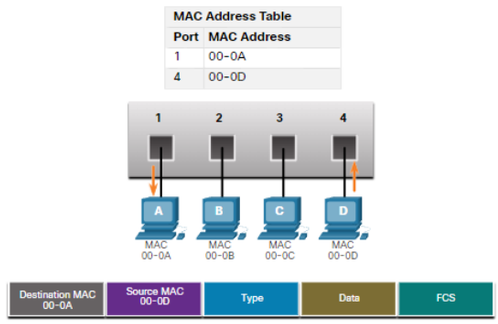
Filtering Frames
As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.

PC-D to Switch
In the figure, PC-D is replying back to PC-A. The switch sees the MAC address of PC-D in the incoming frame on port 4. The switch then puts the MAC address of PC-D into the MAC Address Table associated with port 4.



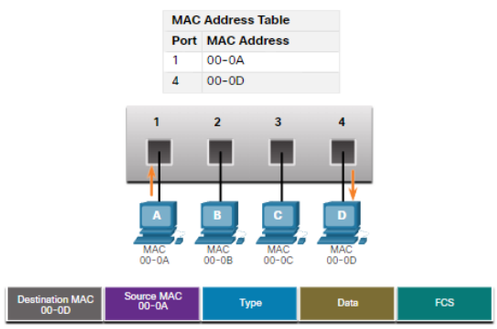
The switch adds the port number and MAC address for PC-D to its MAC address table.

Switch to PC-A
Next, because the switch has destination MAC address for PC-A in the MAC Address Table, it will send the frame only out port 1, as shown in the figure.



1. The switch has a MAC address entry for the destination.
2. The switch filters the frame, sending it only out port 1.

PC-A to Switch to PC-D
Next, PC-A sends another frame to PC-D, as shown in the figure. The MAC address table already contains the MAC address for PC-A; therefore, the five-minute refresh timer for that entry is reset. Next, because the switch table contains the destination MAC address for PC-D, it sends the frame only out port 4.



1. The switch receives another frame from PC-A and refreshes the timer for the MAC address entry for port 1.
2. The switch has a recent entry for the destination MAC address and filters the frame, forwarding it only out port 4.

MAC Address Tables on Connected Switches
A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.

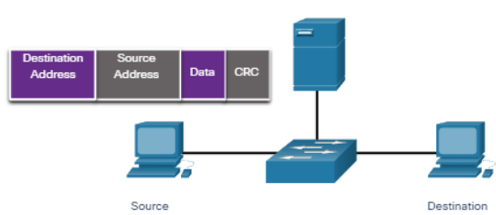
Sending the Frame to the Default Gateway
When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the default gateway, the router.
Click Play in the figure to view a demonstration of how PC-A communicates with its default gateway.
Note: In the video, the IP packet that is sent from PC-A to a destination on a remote network has a source IP address of PC-A and a destination IP address of the remote host. The returning IP packet will have the source IP address of remote host and the destination IP address will be that of PC-A.

5. Switching Speeds and Forwarding Methods

Frame Forwarding Methods on Cisco Switches
As you learned in the previous topic, switches use their MAC address tables to determine which port to use to forward frames. With Cisco switches, there are actually two frame forwarding methods and there are good reasons to use one instead of the other, depending on the situation.
Switches use one of the following forwarding methods for switching data between network ports:

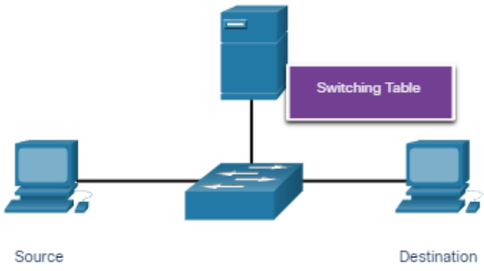
- **Store-and-forward switching** - This frame forwarding method receives the entire frame and computes the CRC. CRC uses a mathematical formula, based on the number of bits (1s) in the frame, to determine whether the received frame has an error. If the CRC is valid, the switch looks up the destination 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.
Click Play in the animation for a demonstration of the store-and-forward process.



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 destination MAC address is located in the first 6 bytes of the frame following the preamble. The switch looks up the destination MAC address in its switching

table, determines the outgoing interface port, and forwards the frame onto its destination through the designated switch port. The switch does not perform any error checking on the frame.
Click Play in the animation for a demonstration of the cut-through switching process.



There are two variants of cut-through switching:

- **Fast-forward switching** - Fast-forward switching offers the lowest level of latency. Fast-forward switching immediately forwards 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. This occurs infrequently, and the destination NIC discards the faulty packet upon receipt. In fast-forward mode, latency is measured from the first bit received to the first bit transmitted. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching** - In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes. Fragment-free switching tries to enhance fast-forward switching by performing a small error check on the first 64 bytes of the frame to ensure that a collision has not occurred before forwarding the frame. Fragment-free switching is 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.

Some switches are configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, and then they automatically change to store-and-forward. When the error rate falls below the threshold, the port automatically changes back to cut-through switching.

Memory Buffering on Switches
An Ethernet switch may use a buffering technique to store frames before forwarding them. Buffering may also be used when the destination port is busy because of congestion. The switch stores the frame until it can be transmitted.
As shown in the table, there are two methods of memory buffering
Memory Buffering Methods

Method	Description
Port-based memory	• Frames are stored in queues that are linked to specific incoming and outgoing ports. • A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted. • It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. • This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	• 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. • 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.

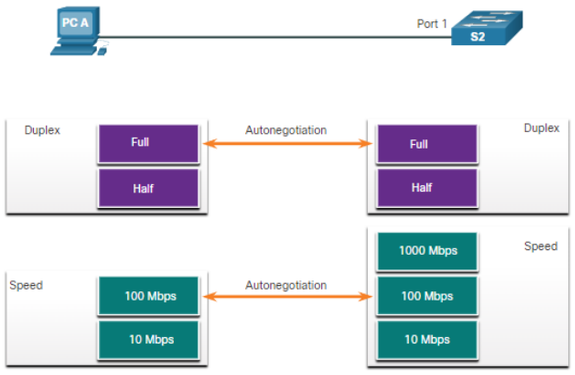
Shared memory buffering also results in the ability to store larger frames with potentially fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports such as when connecting a server to a 10 Gbps switch port and PCs to 1 Gbps ports.

Duplex and Speed Settings
Two of the most basic settings on a switch are the bandwidth (sometimes referred to as “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, such as a computer or another switch.
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.

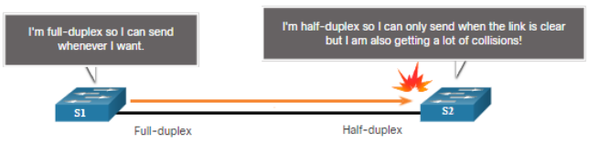
Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth.

In the figure, the Ethernet NIC for PC-A can operate in full-duplex or half-duplex, and in 10 Mbps or 100 Mbps.



PC-A is connected to switch S2 on port 1, which can operate in full-duplex or half-duplex, and in 10 Mbps, 100 Mbps or 1000 Mbps (1 Gbps). If both devices are using autonegotiation, the operating mode will be full-duplex and 100 Mbps.

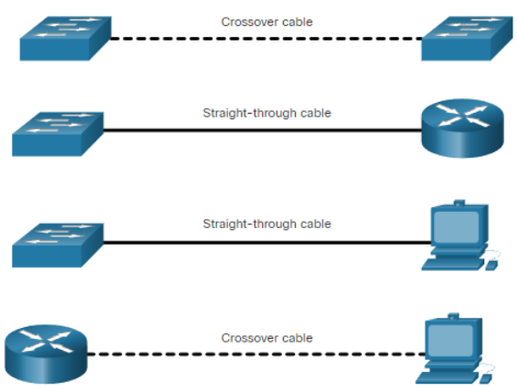
Note: Most Cisco switches and Ethernet NICs default to autonegotiation for speed and duplex. Gigabit Ethernet ports only operate in full-duplex.
Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex, as shown in the figure.



S2 will continually experience collisions because S1 keeps sending frames any time it has something to send.

Duplex mismatch occurs 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.

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.
For example, the figure identifies the correct cable type required to interconnect switch-to-switch, switch-to-router, switch-to-host, or router-to-host devices. A crossover cable is used when connecting like devices, and a straight-through cable is used for connecting unlike 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. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.
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.