UNIT 2
LINK LAYER

DLC SERVICES

The data link control (DLC) deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast. Data link control functions include

- framing and
- flow and
- error control.

Framing

The data-link layer needs to pack bits into frames, so that each frame is distinguishable from another.

Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame Size

Frames can be of **fixed or variable** size. In **fixed-size framing**, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

In **variable-size framing**, we need a way to define the end of one frame and the beginning of the next. Historically, two approaches were used for this purpose:

- a character-oriented approach and
- a bit-oriented approach.

Character-Oriented Framing

In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits, are also multiples of 8 bits.

To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

Any character used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix this problem, a byte-stuffing strategy was added to character-oriented framing.

In **byte stuffing** (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape

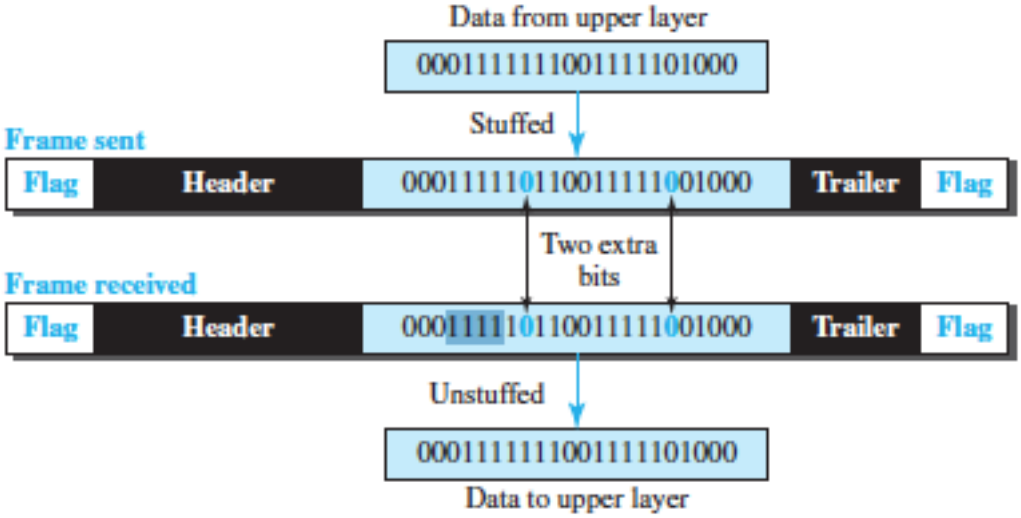
character (ESC) and has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.

Bit-Oriented Framing

In bit-oriented framing, the data section of a frame is a sequence of bits. However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame.

If the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame. We do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing.

In **bit stuffing**, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver.



Flow Control

If the receiving rate is less than the transmission rate, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.

An acknowledgment (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received an earlier frame

If the sender does not receive an acknowledgment after a reasonable amount of time, then it retransmits the original frame. This is known as timeout.

The strategy of using acknowledgments and timeouts to implement reliable delivery is called automatic repeat request (ARQ).

The ARQ mechanism available:
o Stop and Wait ARQ
o Sliding Window
Go Back N ARQ
Selective Repeat ARQ

Error Control

- The data link layer adds reliability to the physical layer by adding a trailer to detect and retransmit damaged/lost frames and to recognize duplicate frames.
- Since electromagnetic signals are susceptible to error, a frame is susceptible to error. The error needs first to be detected. Types of Error Detection – Two Dimensional Parity, Internet Checksum, Cyclic Redundancy Check (CRC)
- After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node. Types of Error Correction – Hamming Code
- Bit errors are introduced into frames because of electrical interference or thermal noise. This interference can change the shape of the signal
- The two types of error are single-bit error and burst error. Single-bit error means that only 1 bit of a given data unit is changed. The term burst error means that 2 or more bits in the data unit have changed.

ADDRESS RESOLUTION PROTOCOL

- A host or a router to send a IP datagram, needs to know both the logical and physical address of the receiver.

- The IP address is obtained from DNS (host) or from its routing table (router). The physical address of the receiver is needed to pass through the physical network.

- The address resolution protocol (ARP) enables to know the physical address of a node when the logical address is known.

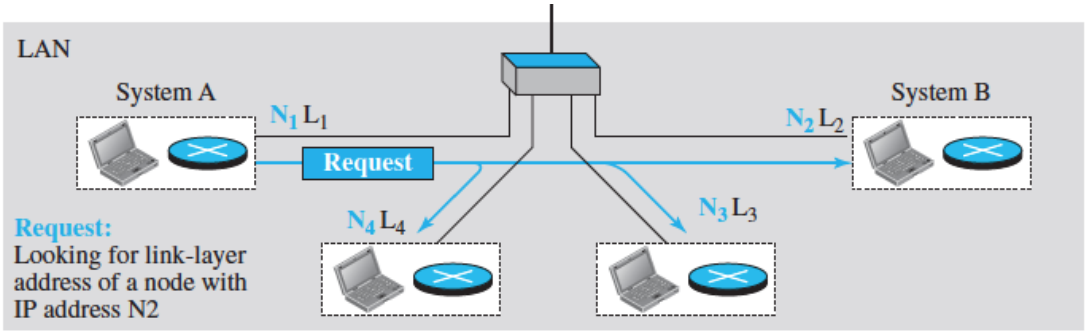
- ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

- ARP enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.

ARP Working Mechanism

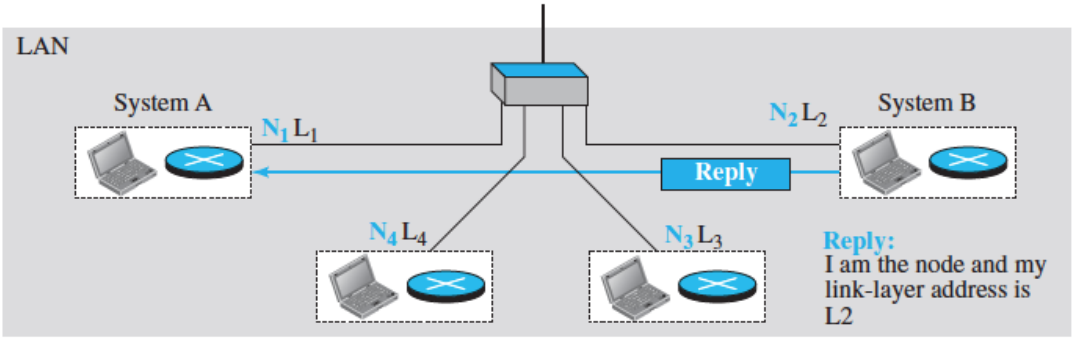
- Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet.
- An ARP request packet is created with value for operation field as 1.
- The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver.

- Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address.
- The target physical address field is unknown and is filled with 0s (broadcast).

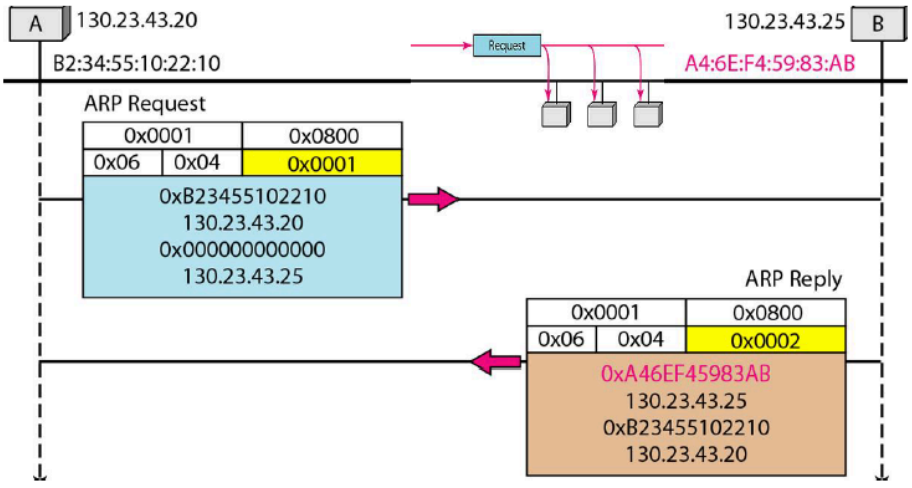


a. ARP request is broadcast

- Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The target node constructs an ARP reply packet with value of 2 for operation.
- The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.

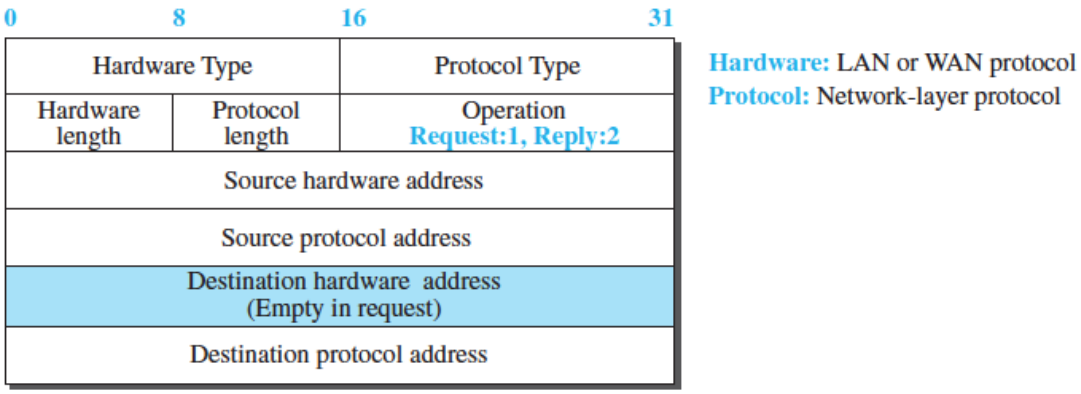


b. ARP reply is unicast



Packet Format of ARP

- Hardware type - defines the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. Ethernet has value 1.
- Protocol type - specifies the protocol value. ARP can be used with any higher-level protocol. For IPv4 the value is 0x0800.
- Hardware length - specifies length of the physical address in bytes. For Ethernet, the value is 6
- Protocol length - specifies length of the logical address in bytes. For IPv4 protocol, the value is 4
- Operation - defines the type of packet. It is either ARP request (1) or ARP reply (2).
- Sender hardware address - a variable-length field contains physical address of the sender.
- Sender protocol address - a variable-length field contains logical address of the sender.
- Target hardware address - a variable-length field contains physical address of the target.
- Target protocol address - a variable-length field contains logical address of the target.



DLC PROTOCOLS

Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:

- Simple,
- Stop-and-Wait,
- Go-Back-N, and
- Selective-Repeat

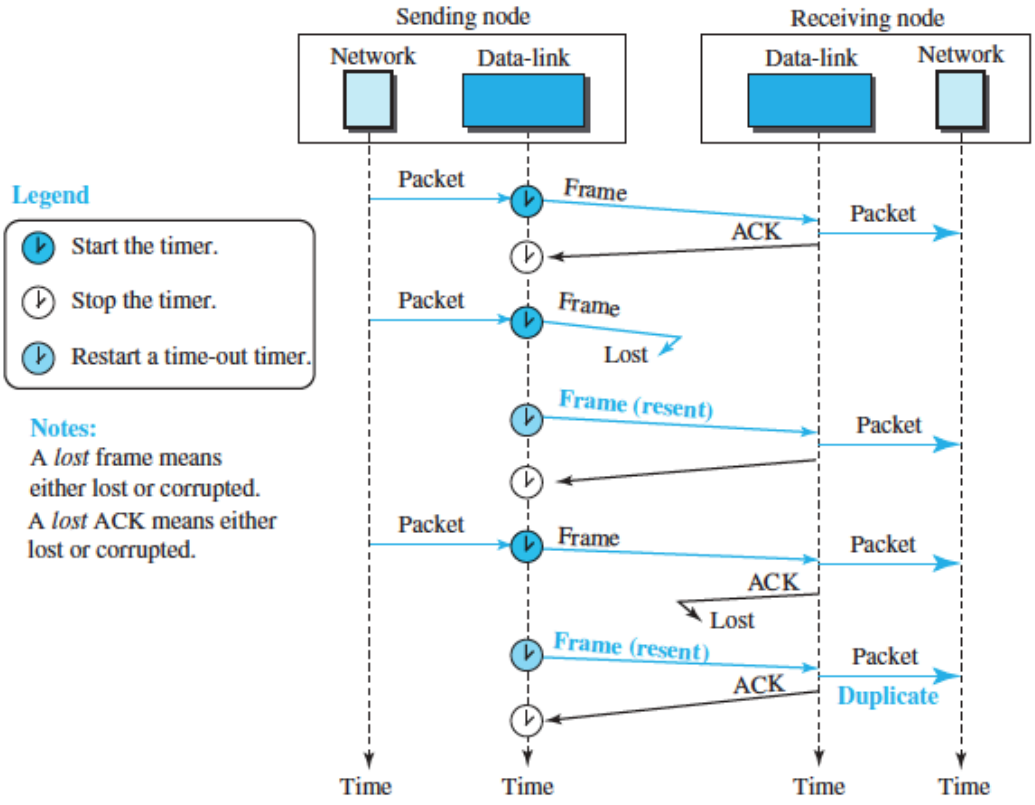
Simple Protocol

- Our first protocol is a simple protocol with neither flow nor error control.
- We assume that the receiver can immediately handle any frame it receives. In other words, the receiver can never be overwhelmed with incoming frames.
- The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.

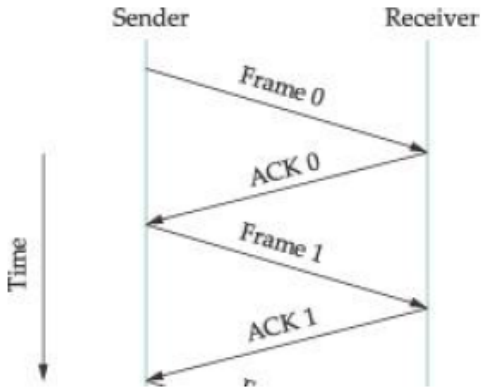
- The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.
- The data-link layers of the sender and receiver provide transmission services for their network layers.

Stop-and-Wait Protocol

- The sender keeps a copy of the frame and then transmits it.
- The sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive before the sender times out and retransmits the frame.
- In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- To detect corrupted frames, we need to add a CRC to each data frame.
- Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame.
- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives.
- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.

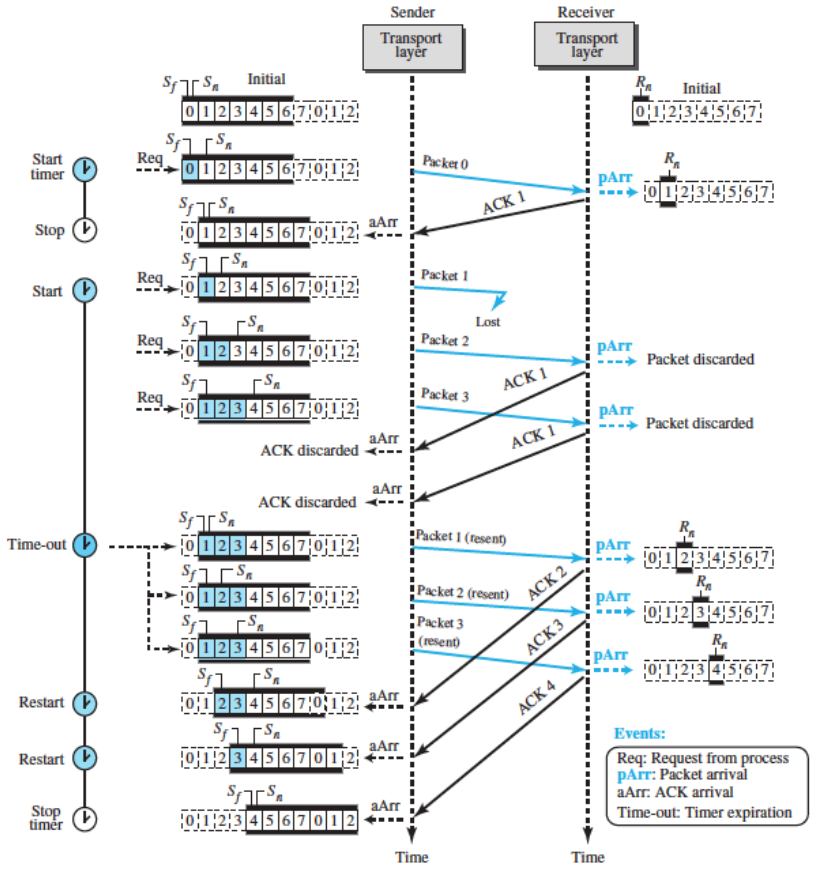


- To address duplicate frames, the header for a stop-and-wait protocol includes a 1-bit sequence number (0 or 1)



Go Back N ARQ

- Several frames are sent before receiving acknowledgment. No. of frames that can be sent depends on the size of send window.
- Only one timer is used. When the timer for the first outstanding frame expires, all outstanding frames are resent.
- An acknowledgment number in this protocol is cumulative and defines the sequence number of the next packet expected. For example, if the acknowledgment number (ackNo) is 7, it means all packets with sequence number up to 6 have arrived, safe and sound, and the receiver is expecting the packet with sequence number 7.



Send Window

- The send window is an imaginary box covering the sequence numbers of the data packets that can be in transit or can be sent.
- In each window position, some of these sequence numbers define the packets that have been sent; others define those that can be sent. The maximum size of the window is 2m − 1,

Receive Window

- The receive window makes sure that the correct data packets are received and that the correct acknowledgments are sent. In Go-Back-N, the size of the receive window is always 1.
- The receiver is always looking for the arrival of a specific packet. Any packet arriving out of order is discarded and needs to be resent.

Disadvantage

- Each time a single packet is lost or corrupted, the sender resends all outstanding packets, even though some of these packets may have been received safe and sound but out of order.
- If the network layer is losing many packets because of congestion in the network, the resending of all of these outstanding packets makes the congestion worse, and eventually more packets are lost. This has an avalanche effect that may result in the total collapse of the network.

Selective Repeat ARQ

- Only the damaged/lost frame is resent. This is done by increasing the complexity at the receivers end.

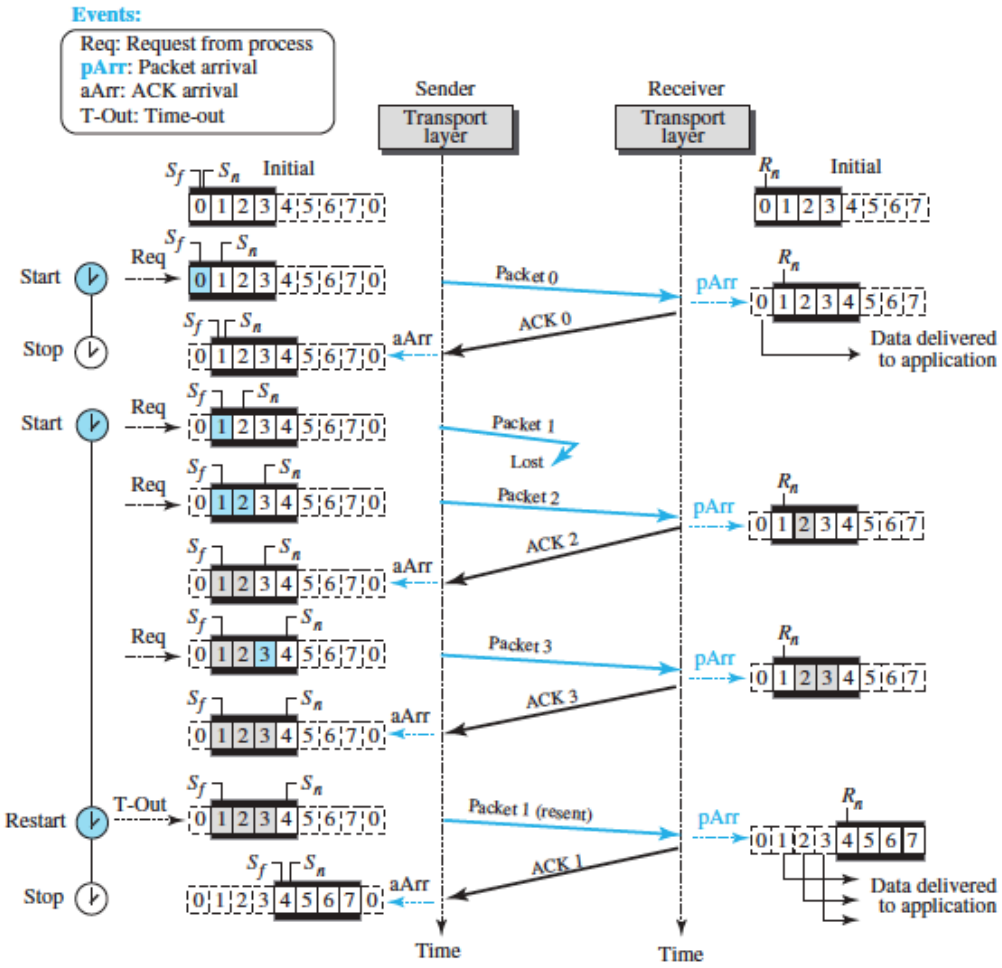
- The Selective-Repeat protocol also uses two windows: a send window and a receive window. However, there are differences between the windows in this protocol and the ones in Go-Back-N .

- First, the maximum size of the send window is much smaller; it is 2m−1 . Second, the receive window is the same size as the send window.

- The Selective-Repeat protocol allows as many packets as the size of the receive window to arrive out of order and be kept until there is a set of consecutive packets to be delivered to the application layer.

- Theoretically, Selective-Repeat uses one timer for each outstanding packet. When a timer expires, only the corresponding packet is resent.

- In SR, an ackNo defines the sequence number of a single packet that is received safe and sound; there is no feedback for any other



HDLC

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the Stop-and-Wait protocol.

Configurations and Transfer Modes

HDLC provides two common transfer modes that can be used in different configurations:

- Normal response mode (NRM) and
- Asynchronous balanced mode (ABM).

In normal response mode (NRM), the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond.

In ABM, the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers).

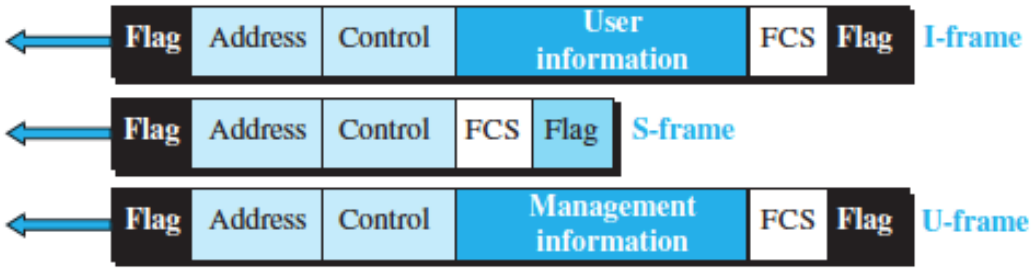
Framing

To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames:

- information frames (I-frames),
- supervisory frames (S-frames), and
- unnumbered frames (U-frames).

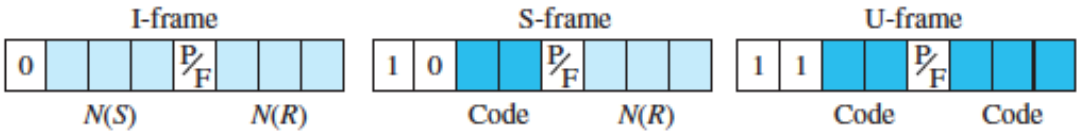
Each type of frame serves as an envelope for the transmission of a different type of message.

- I-frames are used to data-link user data and control information relating to user data (piggybacking).
- S-frames are used only to transport control information.
- U-frames are reserved for system management. Information carried by U-frames is intended for managing the link itself. Each frame in HDLC may contain up to six fields



- Flag field. This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- Address field. This field contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary station creates the frame, it contains a from address. The address field can be one byte or several bytes long, depending on the needs of the network.
- Control field. The control field is one or two bytes used for flow and error control.
- Information field. The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- FCS field. The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

Control Fields



Control Field for I-Frames

- I-frames are designed to carry user data from the network layer. In addition, they can include flow- and error-control information (piggybacking).
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N (S), define the sequence number of the frame.

- The last 3 bits, called N (R), correspond to the acknowledgment number when piggybacking is used.
- The P/F field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final. It means poll when the frame is sent by a primary station to a secondary.
- It means final when the frame is sent by a secondary to a primary

Control Field for S-Frames

- Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- S-frames do not have information fields. If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- The last 3 bits, called N (R), correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK)
- The 2 bits called code are used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described Receive ready (RR), Receive not ready (RNR), Reject (REJ), Selective reject (SREJ).

- Receive ready (RR). If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value of the N(R) field defines the acknowledgment number.

- Receive not ready (RNR). If the value of the code subfield is 10, it is an RNR Sframe. This kind of frame is an RR frame with additional functions. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. The value of N (R) is the acknowledgment number.

- Reject (REJ). If the value of the code subfield is 01, it is an REJ S-frame. This is a NAK frame, indicating last frame is lost or damaged. The value of N (R) is the negative acknowledgment number.

- Selective reject (SREJ). If the value of the code subfield is 11, it is an SREJ Sframe. This is a NAK frame used in Selective Repeat ARQ. The value of N (R) is the negative acknowledgment number.

Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.
- Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data.
- U-frame codes are divided into two sections: a 2-bit prefix before the P/ F bit and a 3-bit suffix after the P/F bit.
- Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

POINT-TO-POINT PROTOCOL (PPP)

One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP).

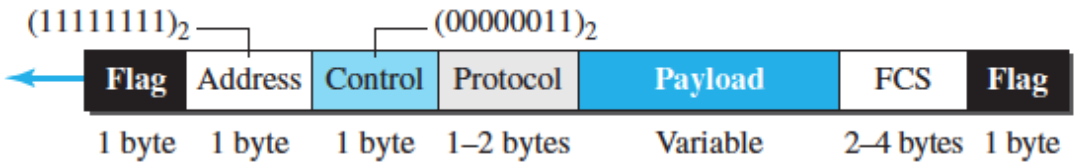
Services Provided by PPP
PPP defines the format of the frame to be exchanged between devices.

It also defines how two devices can negotiate the establishment of the link and the exchange of data.

Authentication is also provided in the protocol, but it is optional. The new version of PPP, called Multilink PPP, provides connections over multiple links.

One interesting feature of PPP is that it provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

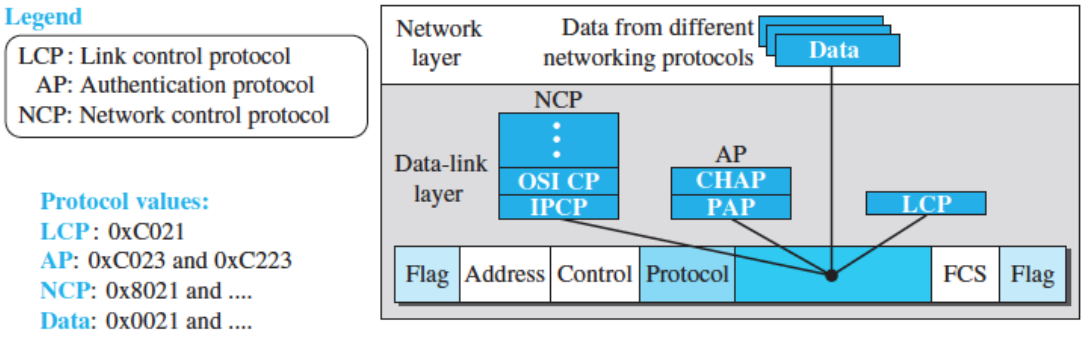
Framing
PPP uses a character-oriented (or byte-oriented) frame.
Frame Format



- Address - The address field in this protocol is a constant value and set to 11111111 (broadcast address).
- Control - This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC).
- Protocol - The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.
- Payload field - This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation.
- FCS. The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

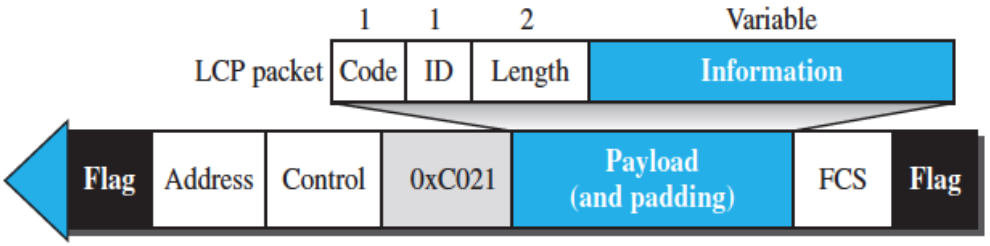
Multiplexing
Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate the parties involved, and carry the network-layer data. Three sets of protocols are defined to make PPP powerful: the

- Link Control Protocol (LCP),
- two Authentication Protocols (APs), and
- several Network Control Protocols (NCPs).



Link Control Protocol

The Link Control Protocol (LCP) is responsible for establishing, maintaining, configuring, and terminating links. It also provides negotiation mechanisms to set options between the two endpoints.



The code field defines the type of LCP packet. There are 11 types of packets.

- There are three categories of packets. The first category, comprising the first four packet types, is used for link configuration during the establish phase.
- The second category, comprising packet types 5 and 6, is used for link termination during the termination phase.
- The last five packets are used for link monitoring and debugging.

Authentication Protocols

Authentication plays a very important role in PPP because PPP is designed for use over dial-up links where verification of user identity is necessary.

Authentication means validating the identity of a user who needs to access a set of resources.

PPP has created two protocols for authentication:

- Password Authentication Protocol and
- Challenge Handshake Authentication Protocol.

PAP

The **Password Authentication Protocol (PAP)** is a simple authentication procedure with a two-step process:

a. The user who wants to access a system sends an authentication identification (usually the user name) and a password.

b. The system checks the validity of the identification and password and either accepts or denies connection.

When a PPP frame is carrying any PAP packets, the value of the protocol field is 0xC023.

The three PAP packets are

- authenticate-request - used by the user to send the user name and password
- authenticate-ack - used by the system to allow access
- authenticate-nak - used by the system to deny access

CHAP

The Challenge Handshake Authentication Protocol (CHAP) is a three-way handshaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.

a. The system sends the user a challenge packet containing a challenge value, usually a few bytes.

b. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

c. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

CHAP is more secure than PAP, especially if the system continuously changes the challenge value.

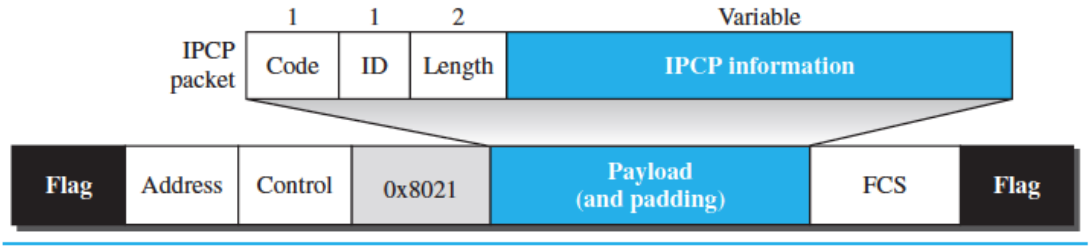
Network Control Protocols

PPP is a multiple-network-layer protocol.

IPCP

One NCP protocol is the **Internet Protocol Control Protocol (IPCP**). This protocol configures the link used to carry IP packets in the Internet.

IPCP defines seven packets, distinguished by their code value



Other Protocols

There are other NCP protocols for other network-layer protocols. The OSI Network Layer Control Protocol has a protocol field value of 8023; the Xerox NS IDP Control Protocol has a protocol field value of 8025; and so on.

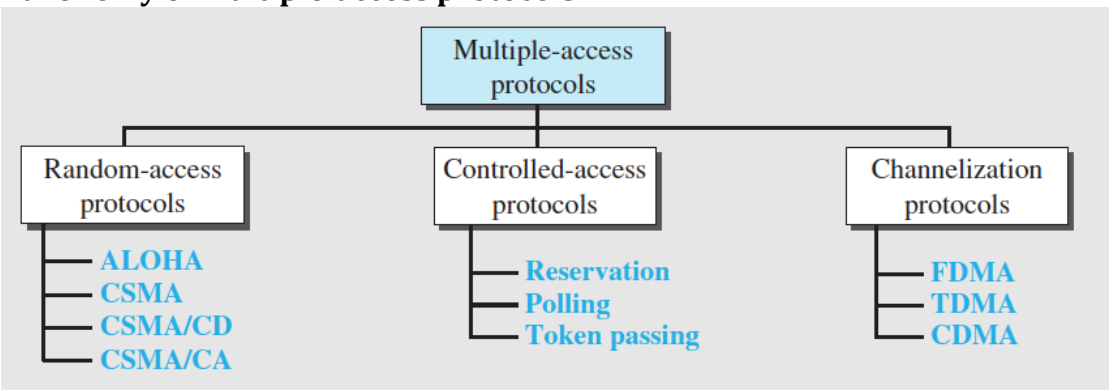
MEDIA ACCESS CONTROL

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.

At any one time, there may be a number of devices attempting to send and receive data using the network media.

When two or more nodes are sending data at the same time, data may be unusable due to collision. There are rules that govern how these devices share the media to solve the collision problem.

Taxonomy of multiple-access protocols



RANDOM ACCESS PROTOCOLS

- In random-access or contention methods, no station is superior to another station and none is assigned control over another.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This decision depends on the state of the medium (idle or busy)

Protocols

1. ALOHA
2. Carrier Sense Multiple Access (CSMA)
3. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
4. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

1. ALOHA

- This is the earliest random access method, was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Types

- Pure ALOHA
- Slotted ALOHA

Pure ALOHA

- The original ALOHA protocol is called pure ALOHA. The idea is that each station sends a frame whenever it has a frame to send (multiple access).
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.
- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.
- The randomness will help avoid more collisions. We call this time the backoff time T_B

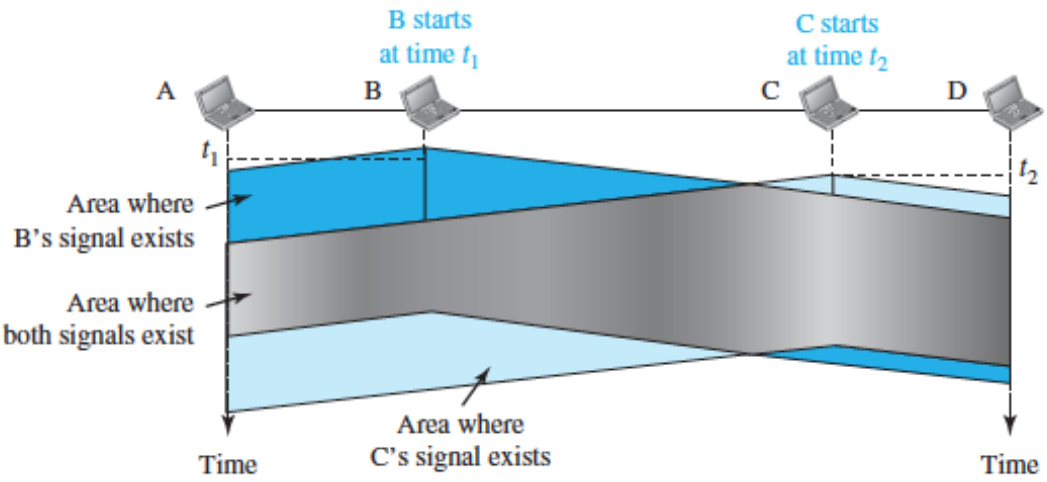
Slotted ALOHA

- In slotted ALOHA we divide the time into slots of seconds and force the station to send only at the beginning of the time slot.
- Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.
- This means that the station which started at the beginning of this slot has already finished sending its frame

2. Carrier sense multiple access (CSMA)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- CSMA requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.”
- CSMA can reduce the possibility of collision, but it cannot eliminate.
- The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it.

- In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.



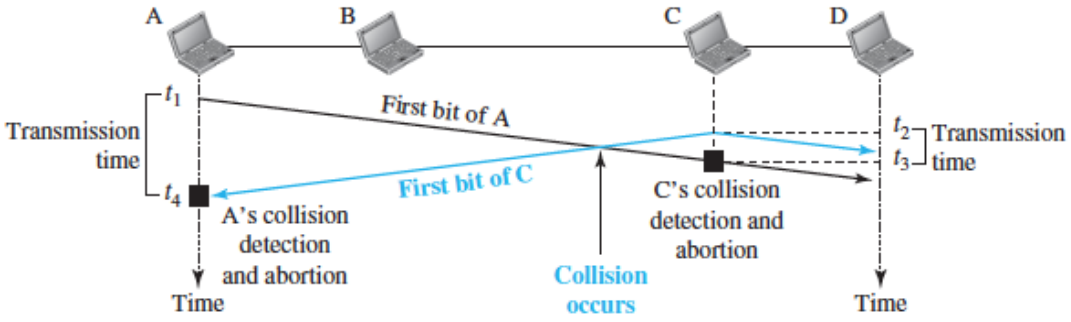
Persistence Methods
What should a station do if the channel is busy?
What should a station do if the channel is idle?

Three methods have been devised to answer these questions: the

- **1-persistent method** - If the station finds the line idle, it sends its frame immediately (with probability 1). Highest chance of collision because two or more stations may find the line idle and send their frames immediately
- **the nonpersistent method** - a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. It reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- **the p-persistent method** - The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. After the station finds the line idle it follows these steps:
- 1. With probability p , the station sends its frame.
  2. With probability q = 1 − p , the station waits for the beginning of the next time slot and checks the line again

3. Carrier sense multiple access with collision detection (CSMA/CD)

- The CSMA method does not specify the procedure following a collision.
- CSMA/CD augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished.
- If, however, there is a collision, the frame is sent again



4. Carrier sense multiple access with collision Avoidance (CSMA/CA)
CSMA/CA was invented for wireless networks.
Collisions are avoided through the use of CSMA/CA's three strategies:

- the interframe space,
- the contention window, and
- Acknowledgments

Interframe Space (IFS) - First, collisions are avoided by deferring transmission even if the channel is found idle.
When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.

Contention Window - The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.

Acknowledgment. With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame

CONTROLLED ACCESS PROTOCOLS
In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

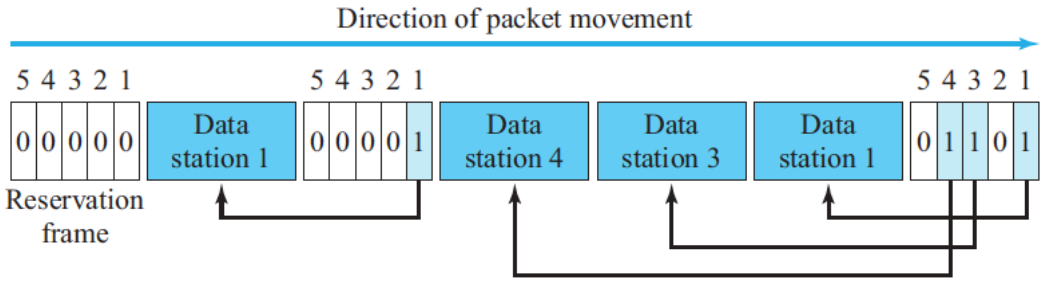
Types

1. Reservation
2. Polling
3. Token Passing

1. Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

- If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.
- Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot.
- The stations that have made reservations can send their data frames after the reservation frame.

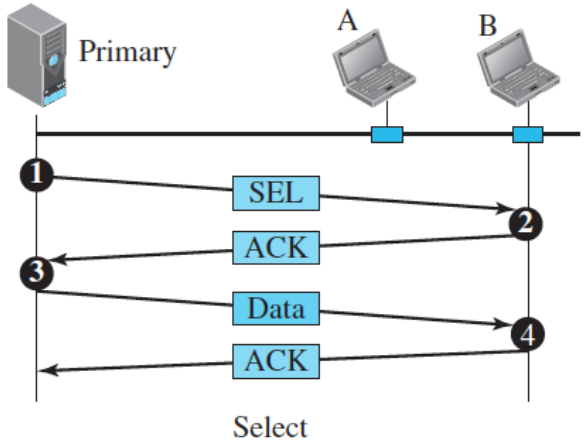


2. Polling

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations .
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.
- The primary device controls the link; the secondary devices follow its instructions.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.
- The primary device, therefore, is always the initiator of a session
- This method uses poll and select functions to prevent collisions. However, the drawback is if the primary station fails, the system goes down.

Select Function

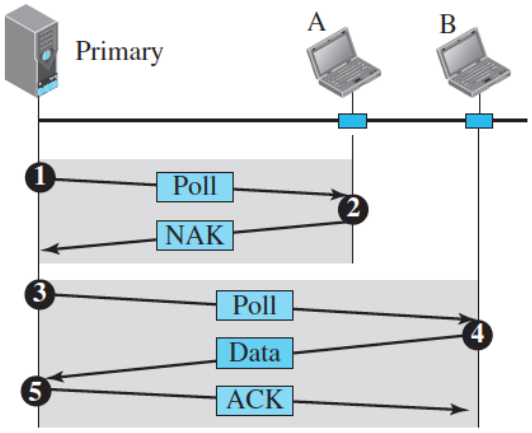
- The select function is used whenever the primary device has something to send. If primary station has something to send, it sends data.
- What it does not know, however, is whether the target device is prepared to receive.



- So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status.
- Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Poll

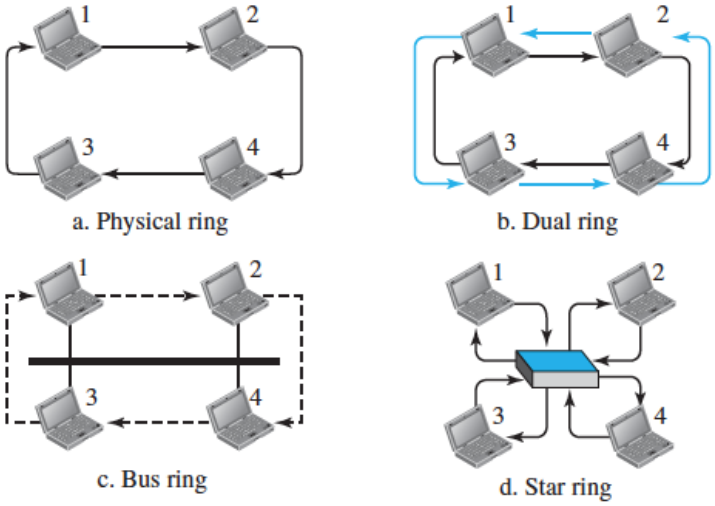
- The poll function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send.
- When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame) if it does.
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send.
- When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.



Poll

3. Token Passing

- In the token-passing method, the stations in a network are organized in a logical ring In other words, for each station, there is a predecessor and a successor.
- The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.
- In this method, a special packet called a token circulates through the ring.
- The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor.
- It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.



CHANNELIZATION PROTOCOLS

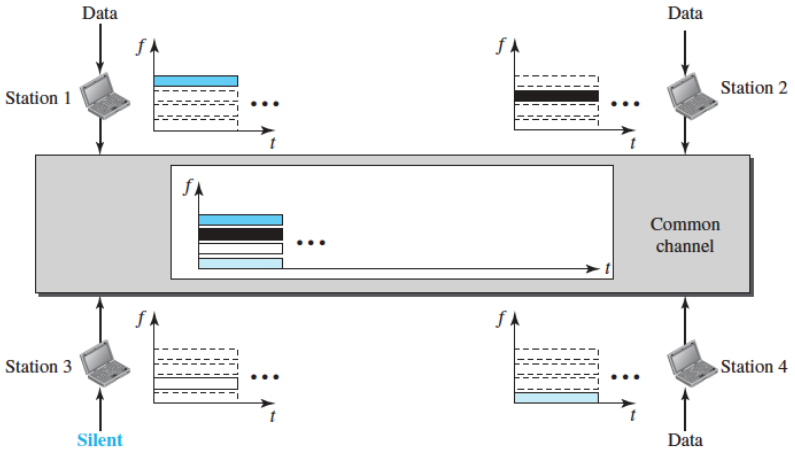
Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.

Types

1. Frequency Division Multiple Access (FDMA)
2. Time division multiple access (TDMA)
3. Code division multiple access (CDMA)

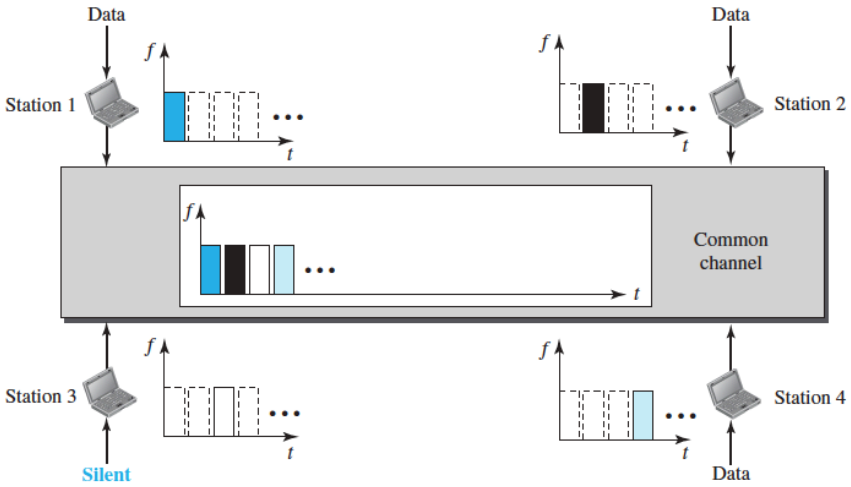
1. Frequency Division Multiple Access (FDMA)

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a bandpass filter to confine the transmitter frequencies.
- To prevent station interferences, the allocated bands are separated from one another by small guard bands.



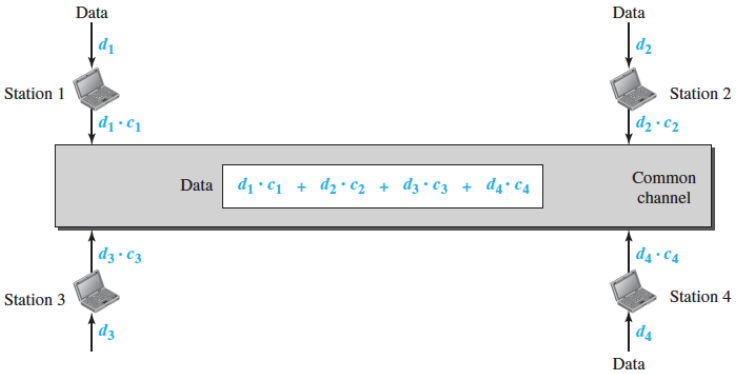
2. Time-division multiple access

- In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data.
- Each station transmits its data in its assigned time slot.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot.
- Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.



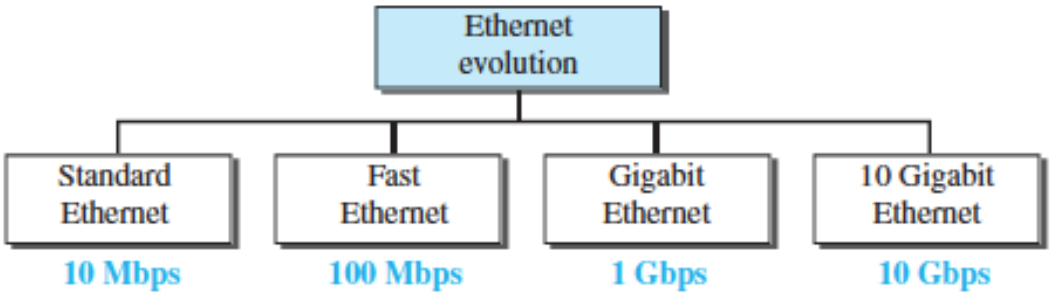
3. Code-division multiple access (CDMA)

- CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link. It differs from TDMA in that all stations can send data simultaneously.
- CDMA simply means communication with different codes.
- For example, in a large room with many people, two people can talk privately in English if nobody else understands English.
- Another two people can talk in Chinese if they are the only ones who understand Chinese, and so on.
- CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips. The codes are called orthogonal sequences.



Wired LAN – Ethernet – IEEE802.3

- In the 1980s and 1990s several different types of LANs were used. All of these LANs used a media-access method to solve the problem of sharing the media.
- The Ethernet used the CSMA/CD approach. The Token Ring, Token Bus, and FDDI (Fiber Distribution Data Interface) used the token-passing approach.
- The Ethernet LAN was developed in the 1970s by **Robert Metcalfe and David Boggs**.
- Digital Equipment and Intel Corporation joined Xerox to define a 10-Mbps Ethernet standard in 1978. It then formed the basis for **IEEE standard 802.3**
- Since then, it has gone through four generations: **Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps)**
- Terabit Ethernet or TbE has also evolved recently with speed over 100 Gbps. 400 Gigabit Ethernet (400G, 400GbE) and 200 Gigabit Ethernet (200G, 200GbE).



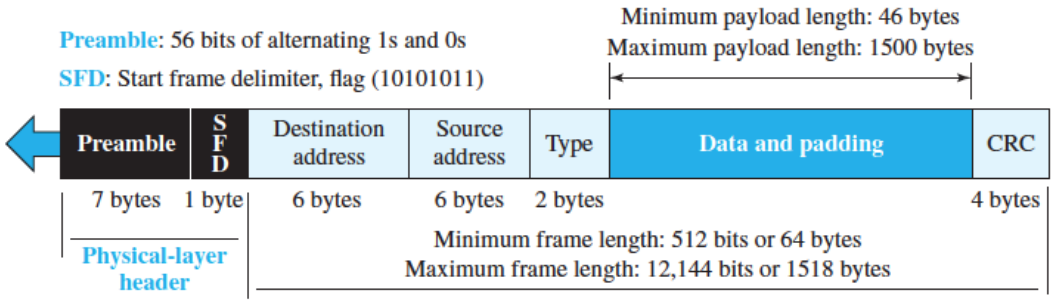
Characteristics of Ethernet

- Ethernet is limited to supporting a maximum of 1024 hosts.
- Ethernet has a total reach of only 2500 m (with the use of repeaters)
- Ethernets works best under lightly loaded conditions (less than 30%).
- Easy to administer and maintain
- Ethernet uses Manchester Encoding to transmit on physical links
- Connectionless and Unreliable
    - No connection establishment
    - Frames may be dropped or lost during transmission
    - No acknowledgement
    - Corrupted frame may be dropped silently

Frame Format

Frame Length

An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes.
The maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

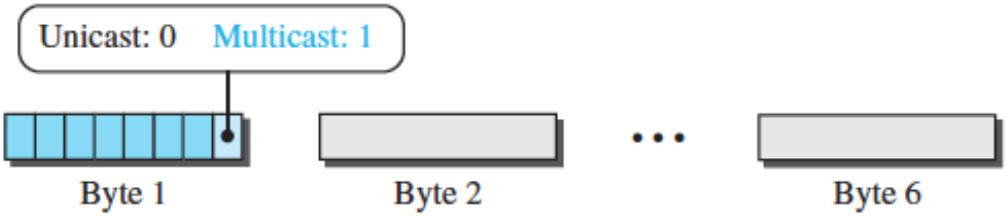


- **Preamble** - This field contains 7 bytes (56 bits) alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.
- **Start frame delimiter (SFD)** - This field (1 byte: 10101011) signals the beginning of the frame.
- **Destination address (DA)** - This field is six bytes (48 bits) and contains the linklayer address of the destination station or stations to receive the packet.
- **Source address (SA)** - This field is also six bytes and contains the link-layer address of the sender of the packet.
- **Type** - This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on.
- **Data** - This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **CRC** - The last field contains error detection information, in this case a CRC-32

Address Format

Each station on an Ethernet network has its own network interface card (NIC).
The Ethernet address is **6 bytes (48 bits)**, normally written in hexadecimal notation, with a colon between the bytes.
Ethernet MAC address - **4A:30:10:21:10:1A**

- Unicast - If the least significant bit of the first byte in a destination address is 0, the address is unicast;
- Multicast - If the least significant bit of the first byte in a destination address is 0, the address is multicast.
- Broadcast - A broadcast destination address is forty-eight 1s (All one's)



Example

a. 4A:30:10:21:10:1A - Unicast
b. 47:20:1B:2E:08:EE - Multicast
c. FF:FF:FF:FF:FF:FF – Broadcast

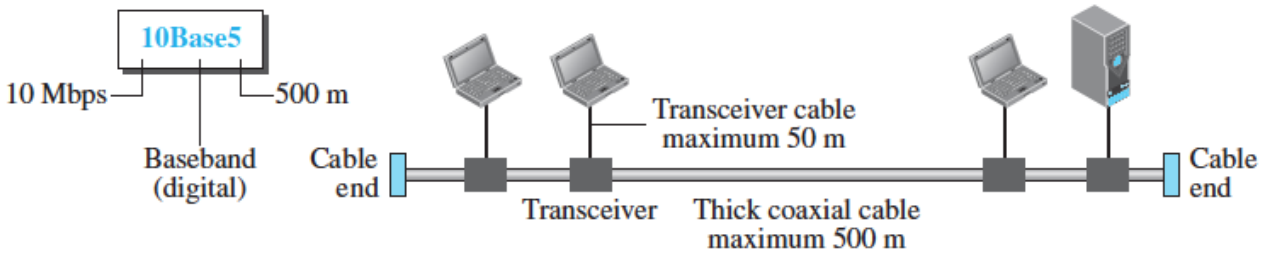
Implementation

The implementations of Standard Ethernet are 10Base5, 10Base2, 10Base-T & 10Base-F

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

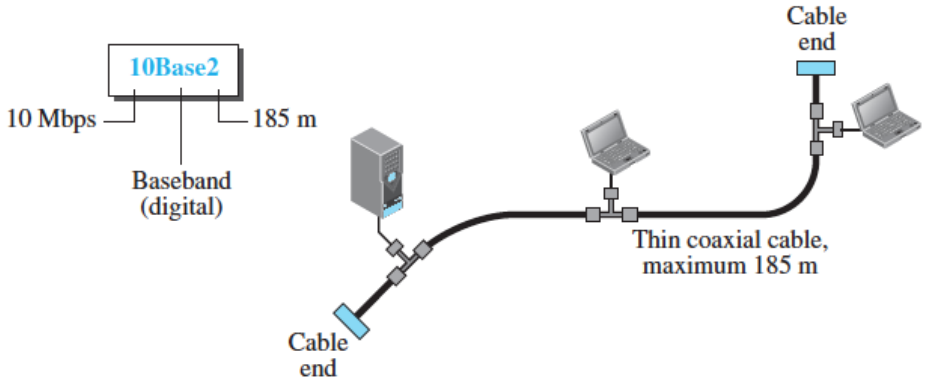
10Base5: Thick Ethernet

- The first implementation is called 10Base5, thick Ethernet, or Thicknet.
- Thick Ethernet uses bus topology with an external transceiver connected via a tap to a thick coaxial cable.
- The transceiver is responsible for transmitting, receiving, and detecting collisions.
- Collision occurs only in the coaxial cable.
- The maximum length of the cable must not exceed 500m.



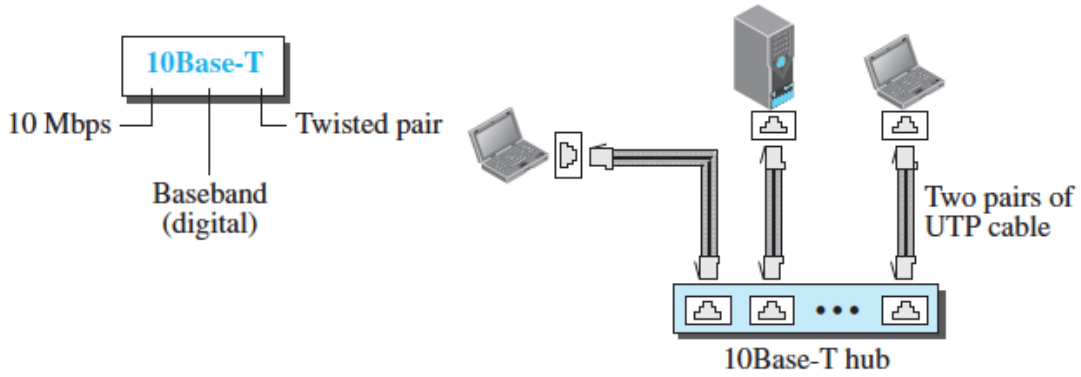
10Base2: Thin Ethernet

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet.
- 10Base2 also uses a bus topology, but the cable is much thinner and more flexible
- The transceiver is part of the network interface card (NIC).
- Thin coaxial cable is less expensive and easy installation than thick ethernet
- The length of each segment should not exceed 185m.



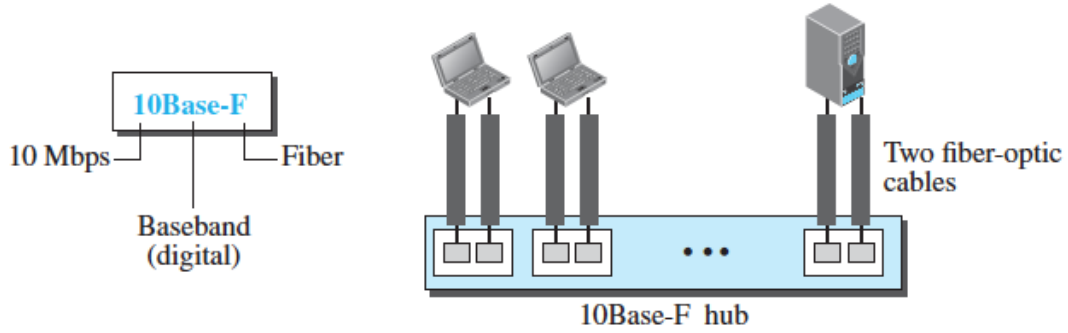
10Base-T: Twisted-Pair Ethernet

- The third implementation is called 10Base-T or twisted-pair Ethernet.
- 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable
- The maximum length of the twisted cable is 100m
- Any collision happens in the hub only.



10Base-F: Fiber Ethernet

- Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F.
- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.
- Maximum Length is 2000m



Access Method

Ethernet follows Carrier Sense Multiple Access with Collision Detect (CSMA/CD)
Transmitter Algorithm

Ethernet is said to be a 1-persistent protocol. When the adaptor has a frame to send:

- If line is idle, it transmits the frame immediately.
- If line is busy, it waits for the line to go idle and then transmits immediately.

It is possible for two (or more) adaptors to begin transmitting at the same time.

- In such case, the frames collide
- They transmit a 32-bit jamming sequence and then stop the transmission.
- Retransmits after a back-off procedure

1. FAST ETHERNET

In the 1990s, some LAN technologies with transmission rates higher than 10 Mbps, such as FDDI and Fiber Channel, appeared on the market.

Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet.

The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format

Access Method

- With CSMA/CD use a passive hub and star topology but make the maximum size of the network 250 meters.
- With link-layer switch with a buffer to store frames and a full-duplex connection to each host to make the transmission medium private for each host. In this case, there is no need for CSMA/CD

Autonegotiation - New Feature

Autonegotiation allows two devices to negotiate the mode or data rate of operation.

It was designed particularly to allow incompatible devices to connect to one another.

Topology

Fast Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.

Encoding and Cabling

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

2. GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps).

The IEEE committee calls it the **Standard 802.3z.**

The goals of the Gigabit Ethernet were to upgrade the data rate to 1 Gbps, but keep the address length, the frame format, and the maximum and minimum frame length the same. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.

2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Support autonegotiation as defined in Fast Ethernet.

MAC Sublayer

- A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate of 1 Gbps, this was no longer possible.
- Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and fullduplex.
- Almost all implementations of Gigabit Ethernet follow the full-duplex approach, so we mostly ignore the half-duplex mode
- In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation in the cable.
- In full-duplex mode, there is a central switch connected to all computers or other switches. In this mode, for each input port, each switch has buffers in which data are stored until they are transmitted
- This means that CSMA/CD is not used.

Topology

Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.

Implementation and Encoding

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

3. 10 GIGABIT ETHERNET

The IEEE committee created 10 Gigabit Ethernet and called it IEEE Standard **802.3ae.**

The goals of the 10 Gigabit Ethernet design can be summarized as upgrading the data rate to 10 Gbps, keeping the same frame size and format, and allowing the interconnection of LANs, MANs, and WAN possible.

This data rate is possible only with fiber-optic technology at this time. The standard defines two types of physical layers: LAN PHY and WAN PHY.

The first is designed to support existing LANs; the second actually defines a WAN with links connected through SONET OC-192.

Implementation
10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet.

Four implementations are the most common: 10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4.

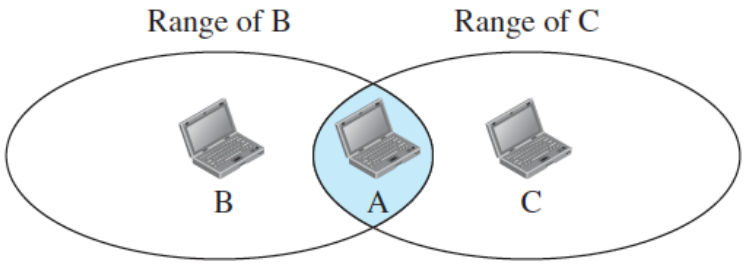
Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

Wireless LAN – IEEE 802.11

CSMA/CD does not work with Wireless Because

1. To detect a collision, a host needs to send and receive at the same time in Full Duplex Mode. Wireless hosts do not have enough power to do so. They can only send or receive at one time.
2. Because of the hidden station problem, in which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.
3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

To avoid these problems CSMA/CA was invented.



a. Stations B and C are not in each other's range.

IEEE 802.11 PROJECT
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called wireless Ethernet.

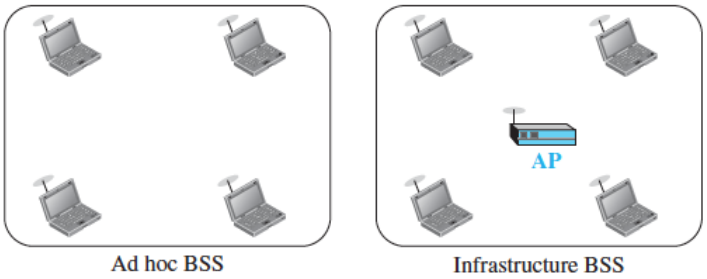
Architecture
The standard defines two kinds of services:

- the basic service set (BSS) and
- the extended service set (ESS).

Basic Service Set

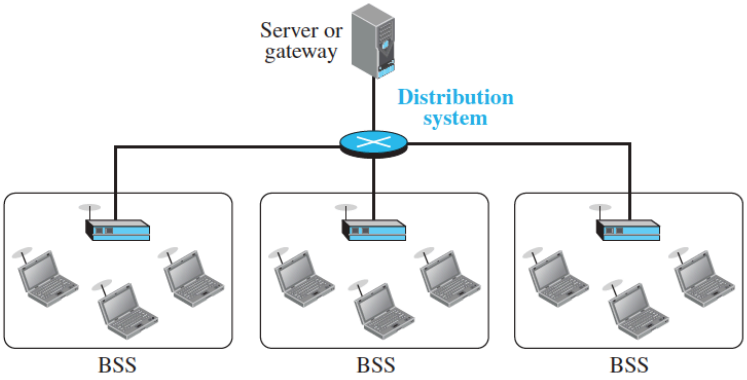
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point.

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs.
- It is called an ad hoc architecture . In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS.
- A BSS with an AP is sometimes referred to as an infrastructure BSS .



Extended Service Set

- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network. The distribution system connects the APs in the BSSs



Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

- no-transition - A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS
- BSS-transition - A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- ESS-transition mobility - A station with ESS-transition mobility can move from one ESS to another.

MAC Sublayer

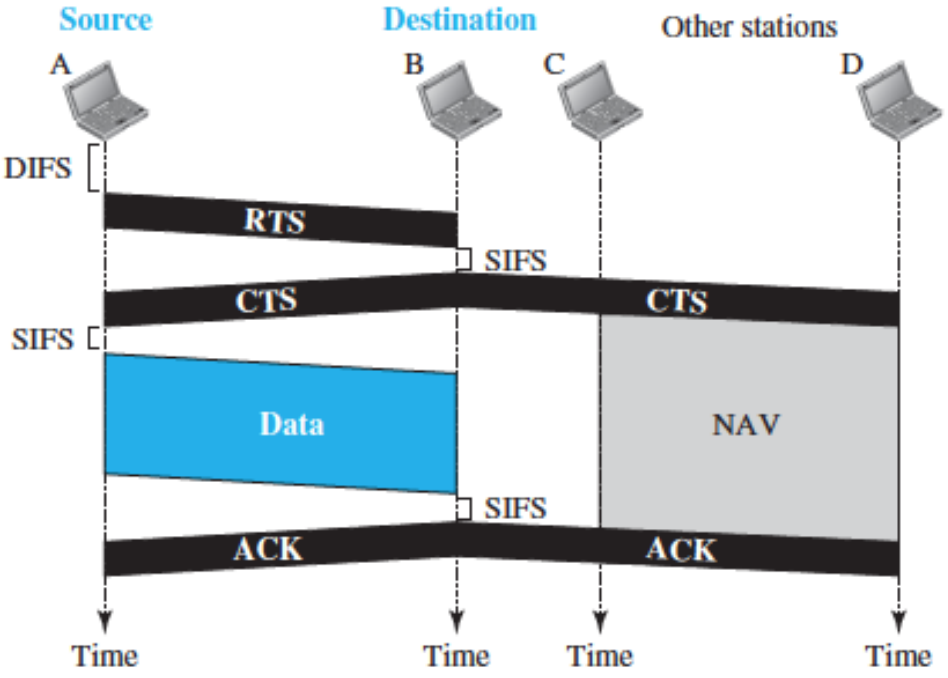
IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

Distributed Coordination Function

DCF uses CSMA/CA as the access method.

Frame Exchange Time Line

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
    a. The channel uses a persistence strategy with backoff until the channel is idle.
    b. After the station is found to be idle, the station waits for a period of time called the **distributed interframe space (DIFS);** then the station sends a control frame called the **request to send (RTS)** .
2. After receiving the RTS and waiting a period of time called the **short interframe space (SIFS)**, the destination station sends a control frame, called the **clear to send (CTS),** to the source station. This control frame indicates that the destination station is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.



Network allocation vector (NAV)
It is a timer that shows how much time must pass before other stations are allowed to check the channel for idleness.

Point Coordination Function (PCF)
The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network.

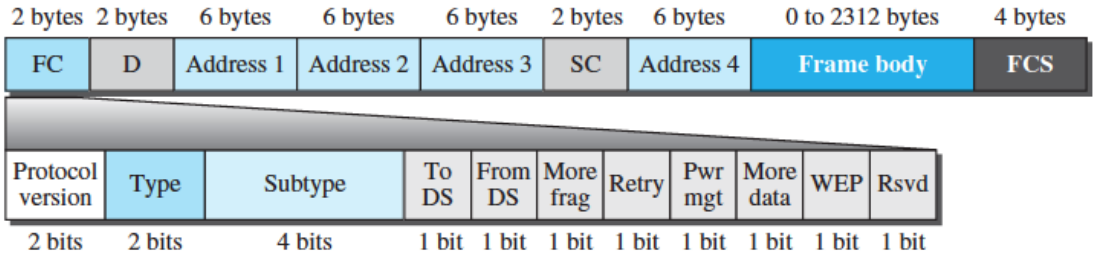
Active Scanning
The technique for selecting an AP is called active scanning as follows:

- The node sends a Probe frame.
- All APs within reach reply with a Probe Response frame.

- The node selects one of the access points and sends that AP an Association Request frame.
- The AP replies with an Association Response frame

Passive Scanning
APs also periodically send a Beacon frame that advertises its features such as transmission rate. This is known as passive scanning

Frame Format



Frame control (FC). The FC field is 2 bytes long and defines the type of frame and some control information.

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

D - This field defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

Addresses - There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields.

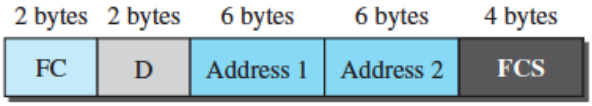
- When one node is sending directly to another, both the **DS bits are 0**, Addr1 identifies the target node, and Addr2 identifies the source node
- When both **DS bits are set to 1**, the message went from a node onto the distribution system, and then from the distribution system to another node.
- Addr1 identifies the ultimate destination, Addr2 identifies the immediate sender, Addr3 identifies the intermediate destination and Addr4 identifies the original source

- Sequence control - This field, often called the SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.
- Frame body - This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.
- FCS - The FCS field is 4 bytes long and contains a CRC-32 error-detection sequence.

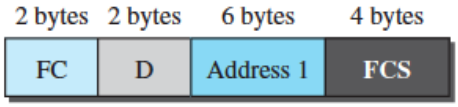
Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:

- **Management frames** - initial communication between stations and AP. Ex probe, probe response etc.
- **Control frames** - used for accessing the channel and acknowledging frames. Ex – RTS, CTS, ACK
- **Data frames** - used for carrying data and control information



RTS

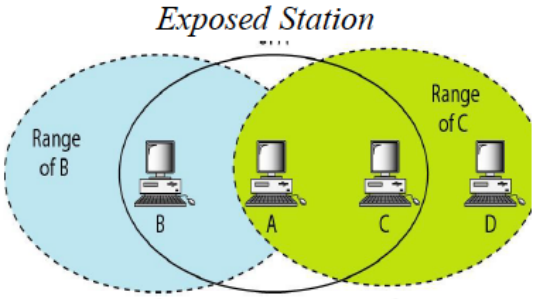


CTS or ACK

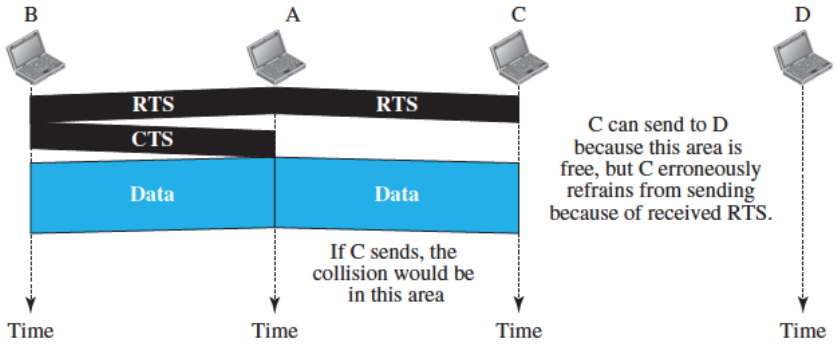
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Exposed Station Problem

- A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending.
- In other words, C is too conservative and wastes the capacity of the channel.



C is exposed to transmission from A to B



Physical Layer

802.11 was designed to run over three different physical media namely FHSS, DSSS and infrared. The data rate for spread spectrum currently is 11 Mbps.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

IEEE 802.11 FHSS

- IEEE 802.11 FHSS uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.400–4.835 GHz ISM band.
- The band is divided into 79 subbands of 1 MHz (and some guard bands).
- A pseudorandom number generator selects the hopping sequence.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps.

IEEE 802.11 DSSS

- IEEE 802.11 DSSS uses the direct-sequence spread spectrum (DSSS)
- DSSS uses the 2.400–4.835 GHz ISM band.
- The modulation technique in this specification is PSK at 1 Mbaud/s.
- The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps

IEEE 802.11 Infrared

- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm.
- The modulation technique is called pulse position modulation (PPM).
- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.

- The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

IEEE 802.11a OFDM

- IEEE 802.11a OFDM describes the orthogonal frequency-division multiplexing (OFDM) method for signal generation in a 5.725–5.850 GHz ISM band.
- The band is divided into 52 subbands, with 48 subbands for sending 48 groups of bits at a time and 4 subbands for control information.
- OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

IEEE 802.11b DSSS

- IEEE 802.11b DSSS describes the high-rate direct-sequence spread spectrum (HRDSSS) method for signal generation in the 2.400–4.835 GHz ISM band.
- HR-DSSS is similar to DSSS except for the encoding method, which is called **complementary code keying** (CCK). CCK encodes 4 or 8 bits to one CCK symbol.
- To be backward compatible with DSSS, HR-DSSS defines four data rates: 1, 2, 5.5, and 11 Mbps.
- The first two use the same modulation techniques as DSSS.
- The 5.5-Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.
- The 11-Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

IEEE 802.11g

- This new specification defines forward error correction and OFDM using the 2.400– 4.835 GHz ISM band. The modulation technique achieves a 22- or 54-Mbps data rate.
- It is backward-compatible with 802.11b, but the modulation technique is OFDM.
-

IEEE 802.11n

- An upgrade to the 802.11 project is called 802.11n (the next generation of wireless LAN).
- The goal is to increase the throughput of 802.11 wireless LANs.
- The new standard emphasizes not only the higher bit rate but also eliminating some unnecessary
- overhead.
- The standard uses what is called MIMO (multiple-input multiple-output antenna) to overcome the noise problem in wireless LANs.
- Some implementations of this project have reached up to 600 Mbps data rate.

BLUETOOTH – IEEE 802.15

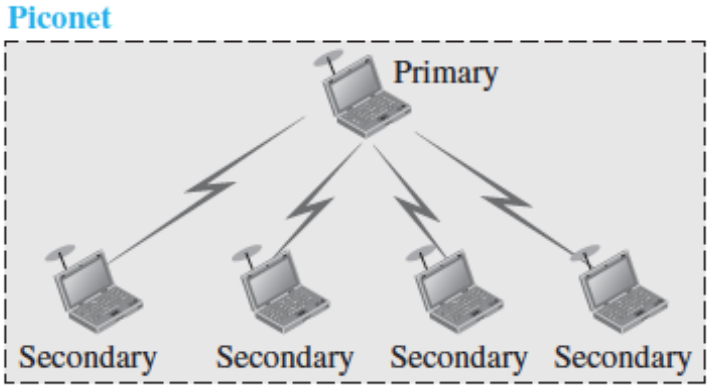
- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; i.e. infrastructure-less the devices, sometimes called gadgets, find each other and make a network called a piconet.
- Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English.
- Today, Bluetooth technology is the implementation of a protocol defined by the **IEEE 802.15** standard.
- The standard defines a **wireless personal-area network (WPAN)** operable in an area the size of a room or a hall.

Architecture

- Bluetooth defines two types of networks: piconet and scatternet

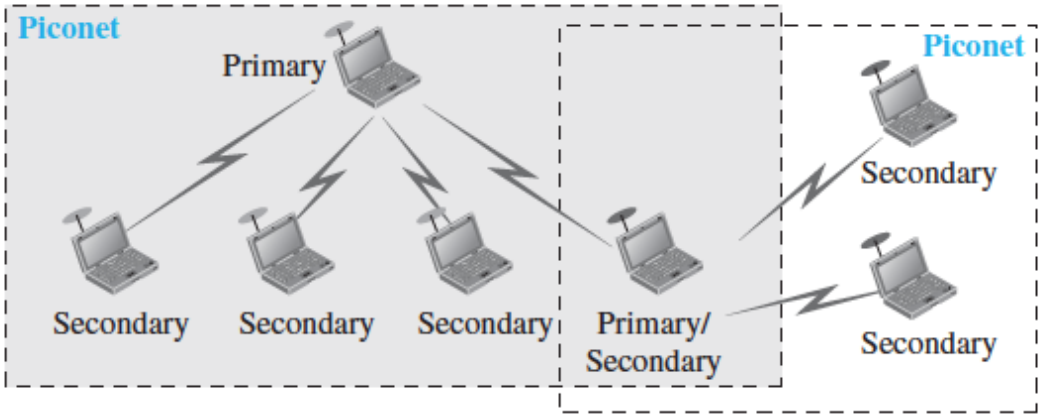
Piconet

- A Bluetooth network is called a piconet, or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- Note that a piconet can have only one primary station.
- The communication between the primary and secondary stations can be one-to-one or one-to-many



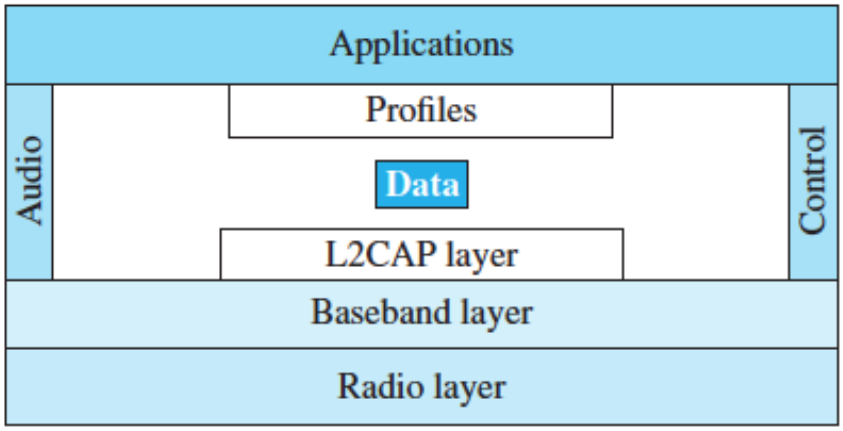
Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets



Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet.



L2CAP

- The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.
- It is used for data exchange on an ACL link; SCO channels do not use L2CAP.
- The L2CAP has specific functions: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Frame format

- The 16-bit length field defines the size of the data, in bytes, coming from the upper layers.
- Data can be up to 65,535 bytes.
- The channel ID (CID) defines a unique identifier for the virtual channel created at this level

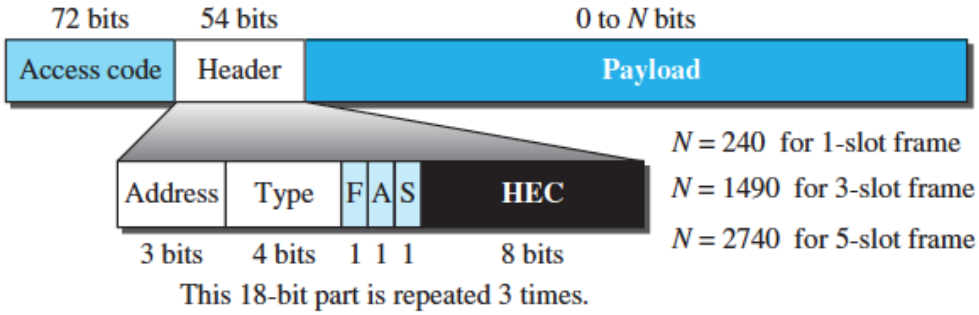
Baseband Layer

- The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- The access method is TDMA.
- The baseband layer establishes the Bluetooth piconet. The piconet is formed when two Bluetooth devices connect.
- The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 μ s.

TDMA

- Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA). TDD-TDMA is a kind of half-duplex communication.
- **Single-Secondary Communication** - If the piconet has only one secondary, the TDMA operation is very simple.
- **Multiple-Secondary Communication** The process is a little more involved if there is more than one secondary in the piconet.

Frame Format



- Access code - This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.
- Header - This 54-bit field is a repeated 18-bit pattern. Address represents address of devices upto 7 address for 7 devices. 0 for broadcast. Type – Represents type of data. F- Flowcontrol. 1 indicated buffer full.
- A – Ack, S – Sequence number, HEC – Error Control. (Header Error Check.)
- Payload - This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

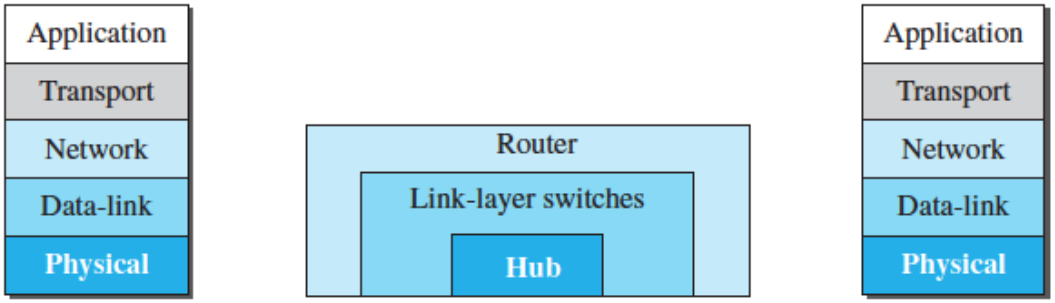
- **Band** - Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- **FHSS** - Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other network.
- **Modulation** - To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering

Connecting Devices

There are three kinds of connecting devices:

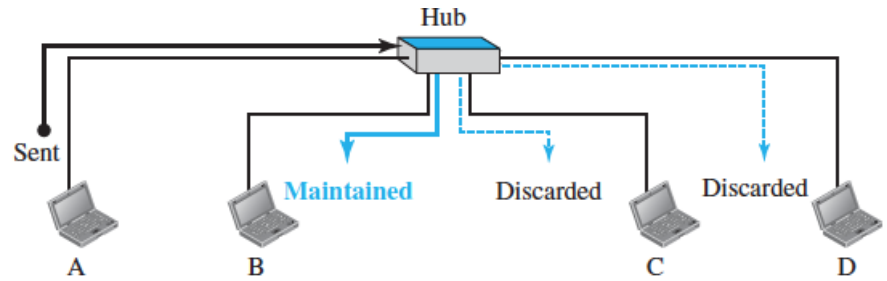
- Hubs,
- Link-layer switches, and
- Routers.

Hubs today operate in the first layer of the Internet model.
Link-layer switches operate in the first two layers.
Routers operate in the first three layers



HUB

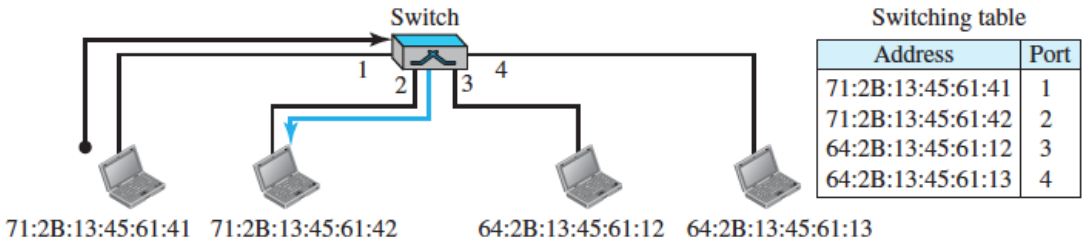
- A hub is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern.
- The repeater then sends the refreshed signal.
- Ethernet LANs use star topology. In a star topology, a repeater is a multiport device, often called a hub, that can be used to serve as the connecting point and at the same time function as a repeater.
- Hub does not have filtering capability it simply forwards packets on all outgoing ports.



Link Layer Switch

- A link-layer switch (or switch) operates in both the physical and the data-link layers.
- As a physical-layer device, it regenerates the signal it receives.
- As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

- A link-layer switch has filtering capability. It can check the destination address of a frame and can decide from which outgoing port the frame should be sent.



Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

Static Switches

The earliest switches had switching tables that were static. The system administrator would manually enter each table entry during switch setup.

Transparent Switches

- A transparent switch is a switch in which the stations are completely unaware of the switch's existence. Transparent switches uses dynamic tables.
- To make a table dynamic, we need a switch that gradually learns from the frames' movements. To do this, the switch inspects both the destination and the source addresses in each frame that passes through the switch.

Learning

- When station A sends a frame to station D, the switch does not have an entry for either D or A. The frame goes out from all three ports; the frame floods the network.
- However, by looking at the source address, the switch learns that station A must be connected to port 1. This means that frames destined for A, in the future, must be sent out through port 1. The switch adds this entry to its table. The table has its first entry now.

Gradual building of table

Address	Port

a. Original

Address	Port
71:2B:13:45:61:41	1

b. After A sends a frame to D

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

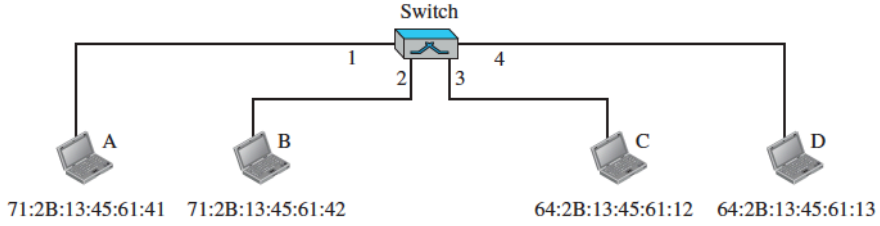
c. After D sends a frame to B

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

d. After B sends a frame to A

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. After C sends a frame to D



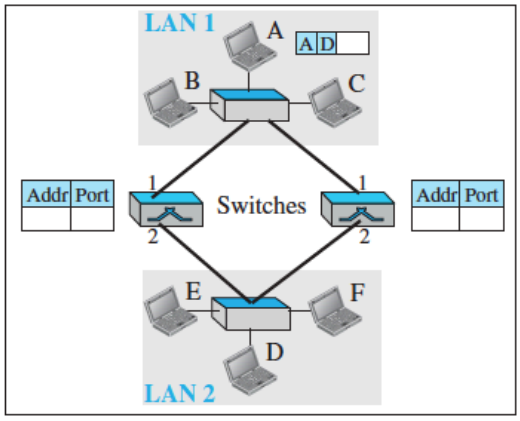
- When station D sends a frame to station B, the switch has no entry for B, so it floods the network again. However, it adds one more entry to the table related to station D.
- The learning process continues until the table has information about every port.

Disadvantage of Switches

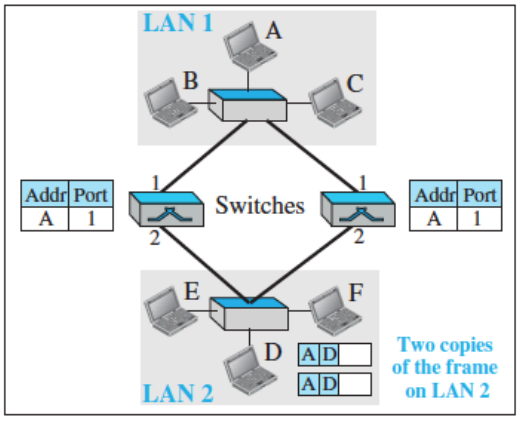
Looping Problem

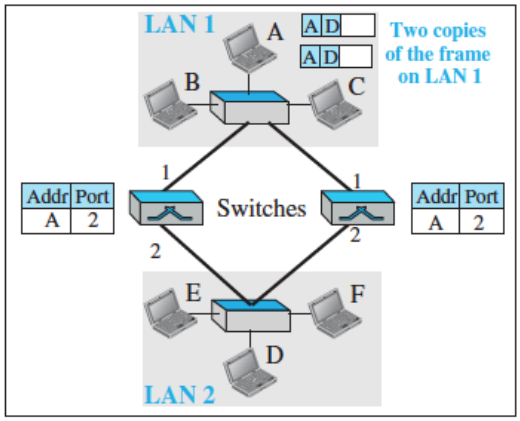
Transparent switches work fine as long as there are no redundant switches in the system. Systems administrators, however, like to have redundant switches (more than one switch between a pair of LANs) to make the system more reliable. If a switch fails, another switch takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable.

a. Station A sends a frame to station D

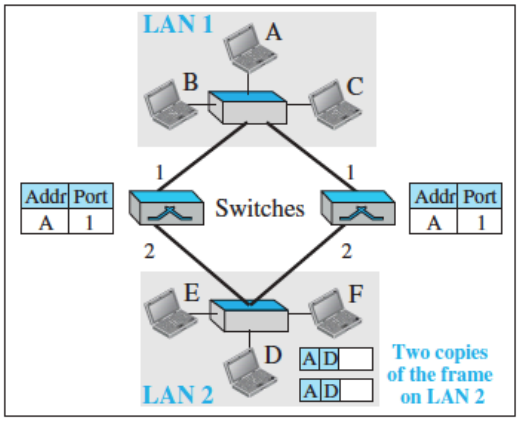


b. Both switches forward the frame





c. Both switches forward the frame



c. Both switches forward the frame

Solving Looping Problem

Spanning Tree Algorithm

- Extended LAN can be represented as a graph that can contain loops
- Spanning tree creates a sub-graph that has no loops, i.e., each LAN can be reached from any other LAN through one path only.
- Each switch decides the ports over which it is willing to forward frames.
- Some ports are removed, reducing the extended LAN to an acyclic graph.

Root Switch

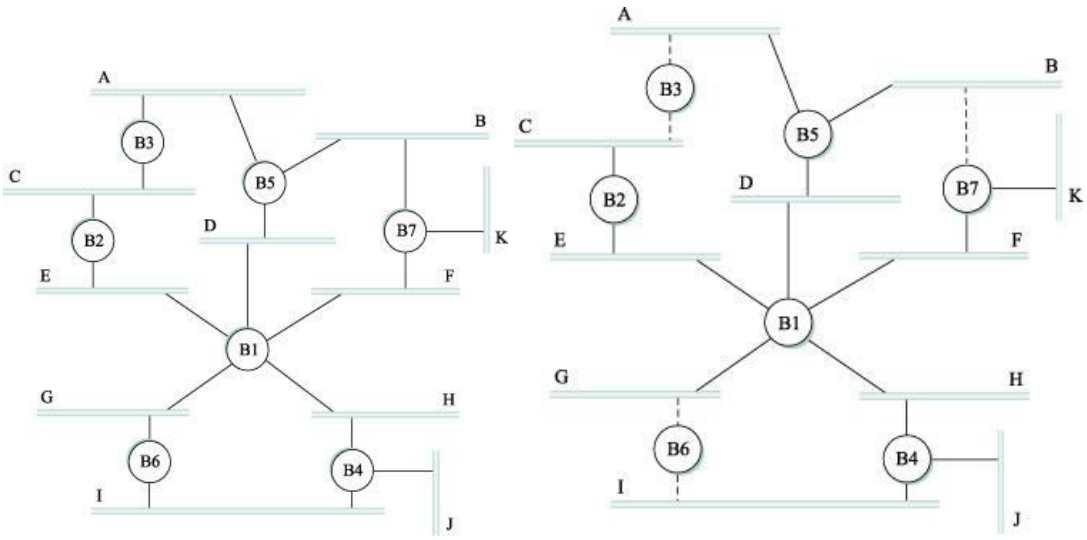
- Each Switch has a unique identifier.
- Each Switch broadcasts its ID.
- The Switch with the smallest ID is selected as the root bridge.
- The root Switch always floods the frames.

Designated Switch

- Each switch computes the shortest path to the root and notes the port on this path
- All the switch connected to a given LAN elect a single designated bridge
- Each LAN's designated switch is the one that is closest to the root
- If two or more switch are equally close to the root, then smallest switch identifier wins
- The designated switch will be responsible for forwarding frames to the root switch

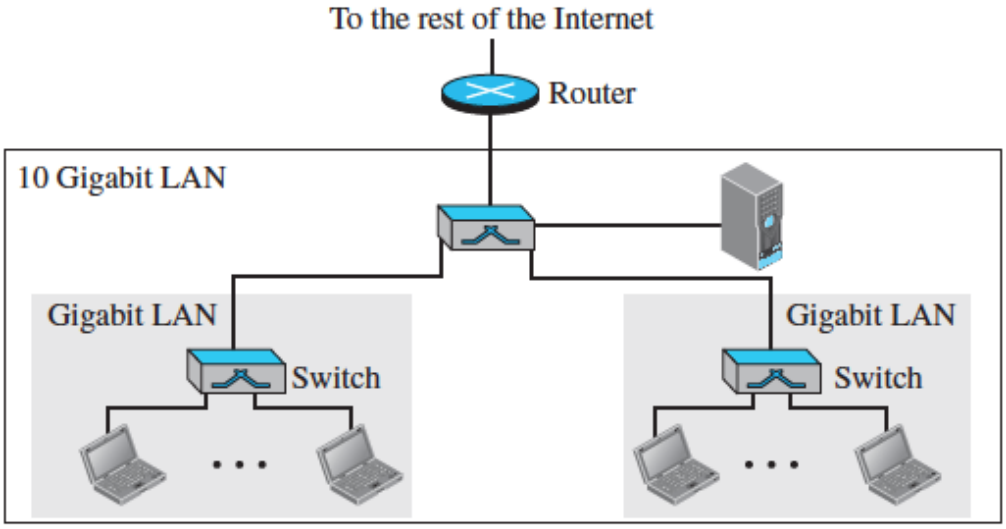
Control Frames

It contains:
o the id of the bridge that is sending the message
o the id for what the sending bridge believes to be the root bridge
o the distance (in hops) from sending bridge to the root bridge



Router

- A router is a three-layer device; it operates in the physical, data-link, and network layers.
- As a physical-layer device, it regenerates the signal it receives.
- As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet.
- As a network-layer device, a router checks the network-layer addresses.
- A router can connect networks. In other words, a router is an internetworking device; it connects independent networks to form an internetwork.
- According to this definition, two networks connected by a router become an internetwork or an internet.


To the rest of the Internet
Router
10 Gigabit LAN
Gigabit LAN
Switch
Gigabit LAN
Switch