UNIT II

DATA-LINK LAYER & MEDIA ACCESS

1 INTRODUCTION TO DATA LINK LAYER

The Internet is a combination of networks attached together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these networks as shown in Figure 2.1. Communication at the data-link layer is made up of five separate logical connections between the data-link layers in the path.

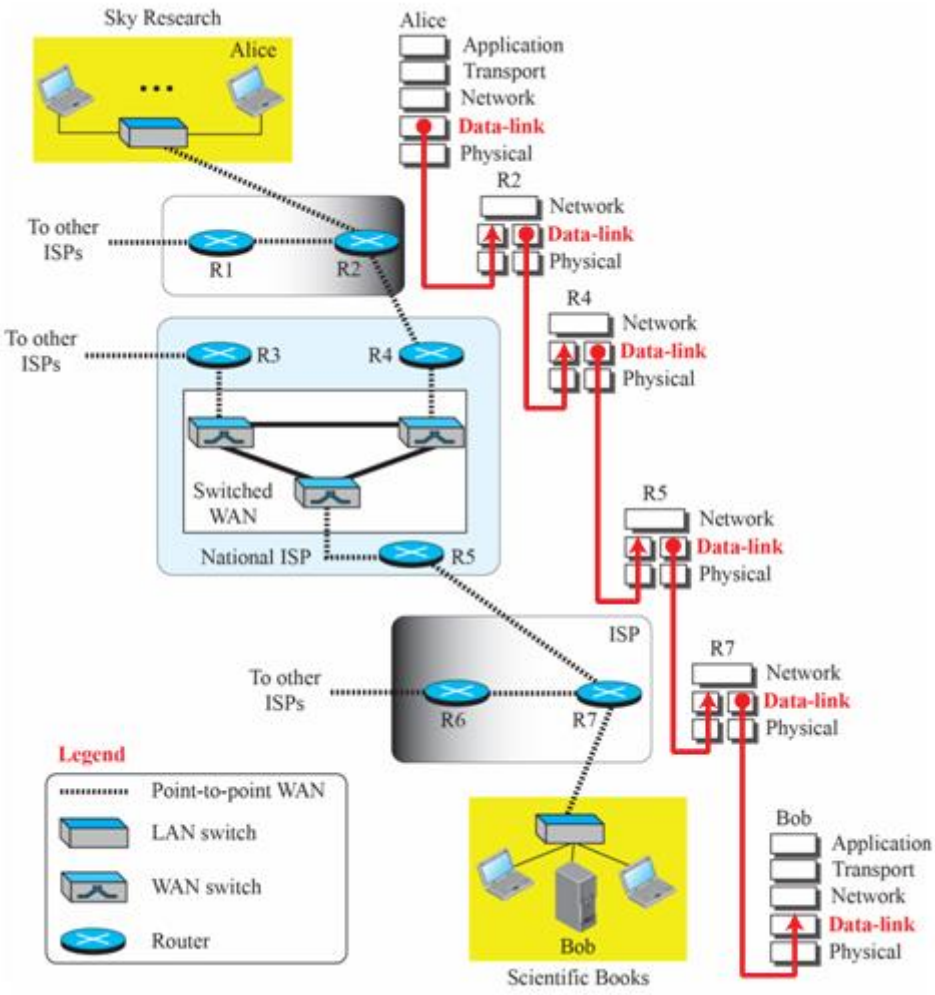


Figure 2.1 Communication at the data-link layer

The data-link layer at Alice's computer communicates with the data-link layer at router R2. The data-link layer at router R2 communicates with the data-link layer at router R4, and so on. Finally, the data-link layer at router R7 communicates with the data-link layer at Bob's computer. ***Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router.***

The reason is that Alice's destination, Bob's computers are each connected to a single network, but each router takes an input from one network and sends output to another network. Nodes and Links Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. Theses LANs and WANs are

connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

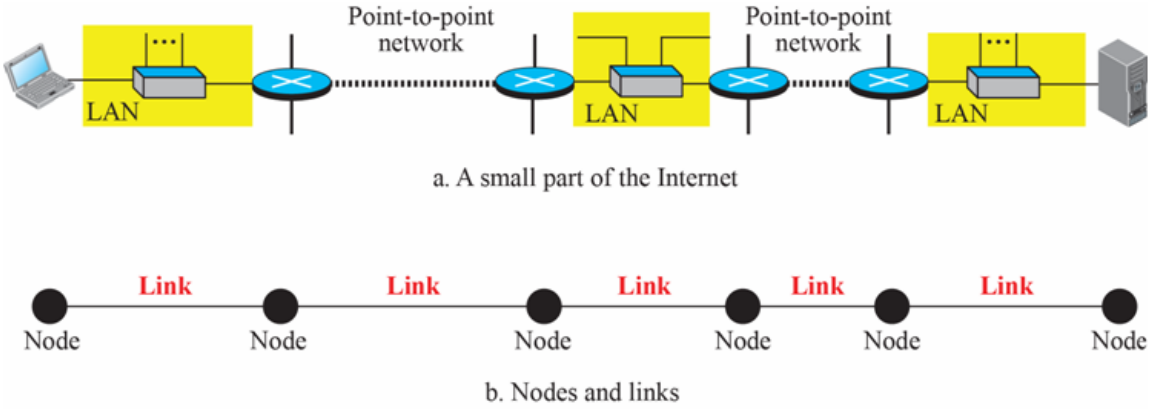


Figure 2.2 Nodes and Links

In figure 2.2, the first node is the source host and the last node is the destination host. The other four nodes are four routers. The first, the third, and the fifth links represent the three LANs. The second and the fourth links represent the two WANs.

1.1 Services

The data-link layer is located between the physical and the network layers. The data-link layer provides services to the network layer and it receives services from the physical layer. The duty of the data-link layer is node-to-node delivery. When a packet is traveling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path. In order to this job, the data-link layer of the node needs to encapsulate the datagram received from the network in a frame, and the data-link layer of the receiving node needs to decapsulates the datagram from the frame.

The data-link layer of the source host needs only to encapsulate, the data-link layer of the destination host needs to decapsulate, but each ***intermediate node needs to both encapsulate and decapsulate.*** Figure 2.3 shows the encapsulation and decapsulation at the data-link layer. In figure 2.3, only one router is there between the source and destination. The datagram received by the data-link layer of the source host is encapsulated in a frame. The frame is logically transported from the source host to the router. The frame is decapsulated at the data-link layer of the router and encapsulated at another frame. The new frame is logically transported from the router to the destination host.

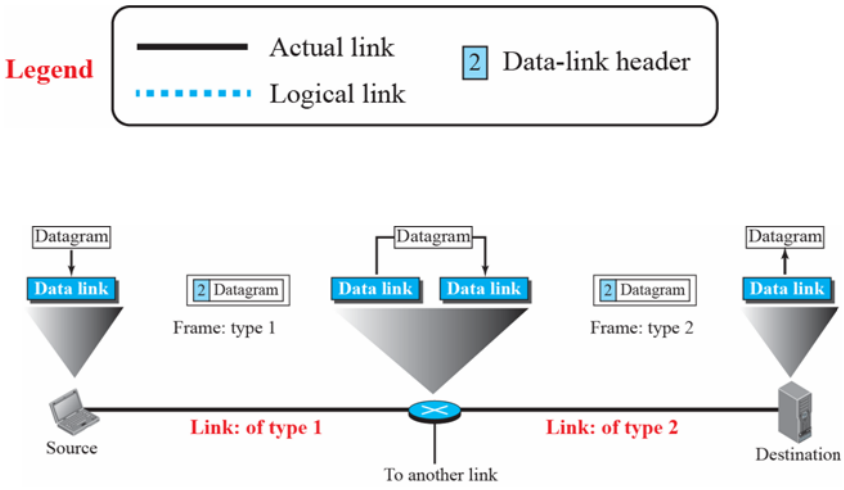


Figure 2.3 Encapsulation and decapsulation at the data-link layer

Services provided by a data-link layer

i. Framing

The data-link layer at each node needs to encapsulate the datagram in a frame before sending it to the next node. The node also needs to decapsulate datagram from the frame received on the logical channel. Different data-link layers have different formats for framing. ***A packet at the data-link layer is normally called a frame.***

ii. Flow Control

The sending data-link layer at the end of a link is a producer of frames and the receiving data-link layer at the other end of a link is a consumer. If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed (processed). ***Due to limited buffer size at the receiving side, the receiving data-link layer may drop the frames if its buffer is full otherwise the receiving data-link layer may send a feedback to the sending data-link layer to ask it to stop or slow down.*** Different data-link-layer protocols use different strategies for flow control.

iii. Error Control

At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media. At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame. Since electromagnetic signals are susceptible to error, a frame is susceptible to error. Hence, the error needs to be detected and either corrected at the receiver node or discarded and retransmitted by the sending node.

iv. Congestion Control

A link may be congested with frames, which may result in frame loss. Most data-link-layer protocols do not directly use a congestion control to alleviate congestion. In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature.

1.2 Two Categories of Links

When two nodes are physically connected by a transmission medium such as cable or air, the data-link layer controls how the medium is used. A data-link layer may use the whole capacity of the medium or only part of the capacity of the link (Point-to-point link or a broadcast link).

- In a point-to-point link, the link dedicated to the two devices.
- In a broadcast link, the link is shared between several chat.

1.3 Two Sublayers

The data-link layer can be divided into two sublayers: ***data link control (DLC) and media access control (MAC).***

- The data link control sublayer deals with all issues common to both point-to-point and broadcast links.
- The media access control sub-layer deals only with issues specific to broadcast links.

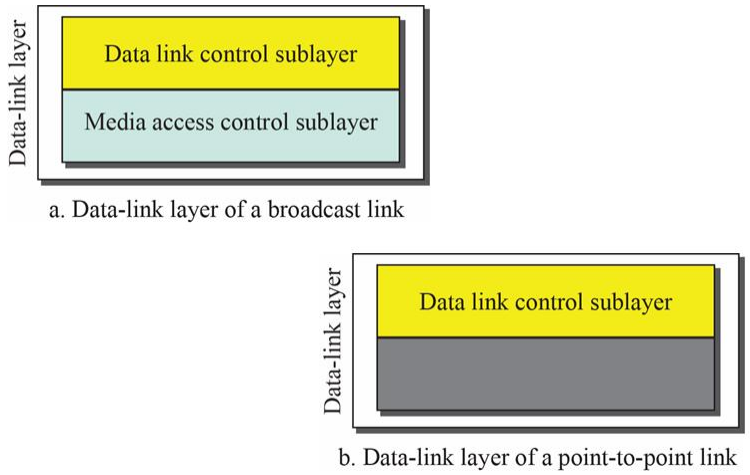


Figure 2.4 Two sublayers of a data-link layer

2 LINK-LAYER ADDRESSING

In the Internet, the source and destination IP addresses define the two ends but cannot define which links the datagram should pass through. The IP addresses in a datagram should not be changed. When the destination IP address in a datagram changes the packet never reaches its destination. If the source IP address in a datagram changes the router can never communicate with the source if a response needs to be sent back or an error needs to be reported back to the source. His issue can be solved by using the link-layer addresses of the two nodes.

A link-layer address is called a physical address or a MAC address. When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header. These two addresses are changed every time the frame moves from one link to another.

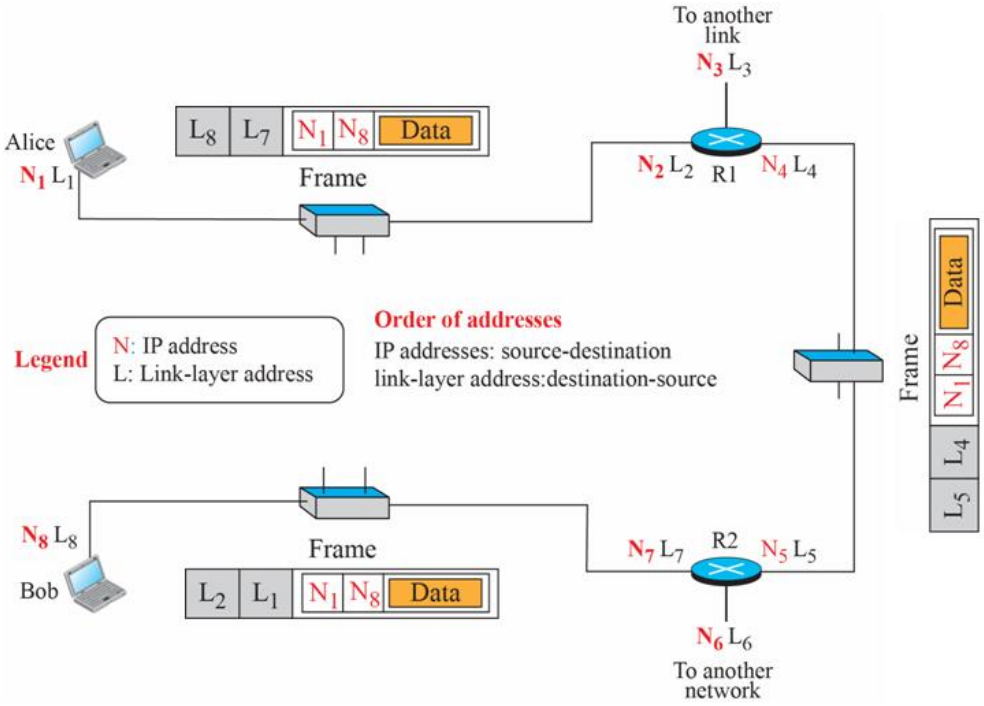


Figure 2.5 IP addresses and link-layer addresses in a small internet

In figure 2.5, we have three links, two routers and two hosts namely Alice (source) and Bob (destination). For each host, we have two addresses called the IP addresses (N) and the link-layer addresses (L). A router may have many pairs of addresses based on the number of links connected to that particular router.

In figure 2.5, each link consist a frame. Each frame carries the same datagram with the same source and destination addresses (Ni and N8), but the link-layer addresses of the frame change from link to link. In link 1, the link-layer addresses are L1 and L2. In link 2, they are L4 and L5. In link 3, they are L7 and L8. Here, the IP addresses and the link layer addresses are not in the same order. For IP addresses, the source address comes before the destination address. For the link-layer address, the destination address comes before the source.

2.1 Types of Addresses

Link-layer protocols define three types of addresses namely unicast, multicast, and broadcast.

i. **Unicast Address:** Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

ii. **Multicast Address:** Multicasting means one-to-many communication.

iii. **Broadcast Address**: Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

2.2 Address Resolution Protocol (ARP)

Anytime a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node. The source host knows the IP address of the default router. Each router except the last one in

the path gets the IP address of the next router by using its for-warding table. The last router knows the IP address of the destination host.

Without using the link-layer address of the next node, the IP address of the next node is not helpful in moving a frame through a link. The ARP protocol is one of the auxiliary protocols, which accepts an IP address from the IP protocol and maps the address to the corresponding link-layer address then passes it to the data-link layer.

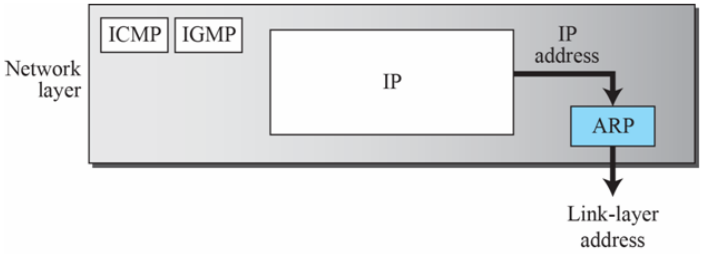


Figure 2.6 Position of ARP in TCP/IP protocol suite

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. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because, the sender doesn't know the link layer address of the receiver. The query is broadcast over the link using the link-layer broadcast address.

2.3 ADDRESS TRANSLATION WITH ARP

ARP Request

Argon broadcasts an ARP request to all stations on the network: **"What is the hardware address of Router137?"**

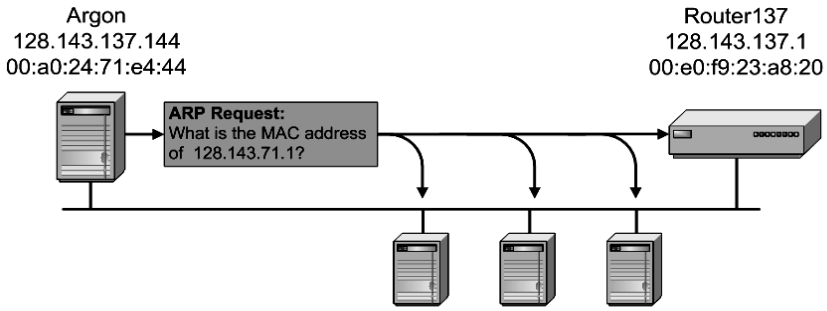


Figure 2.7 ARP Request

ARP Reply

Router 137 responds with an ARP Reply which contains the hardware address.

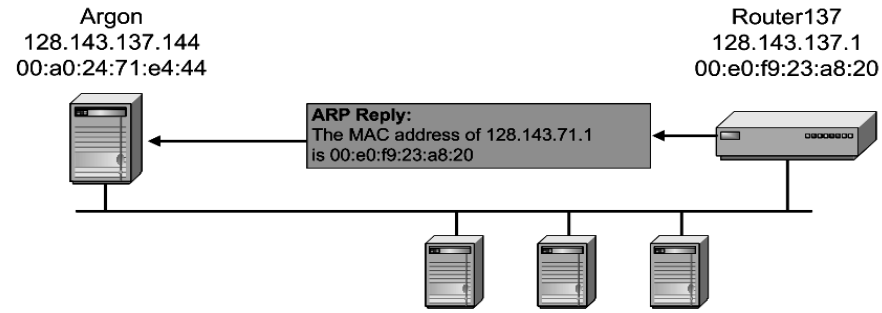


Figure 2.8 ARP Reply

2.4 ARP PACKET FORMAT

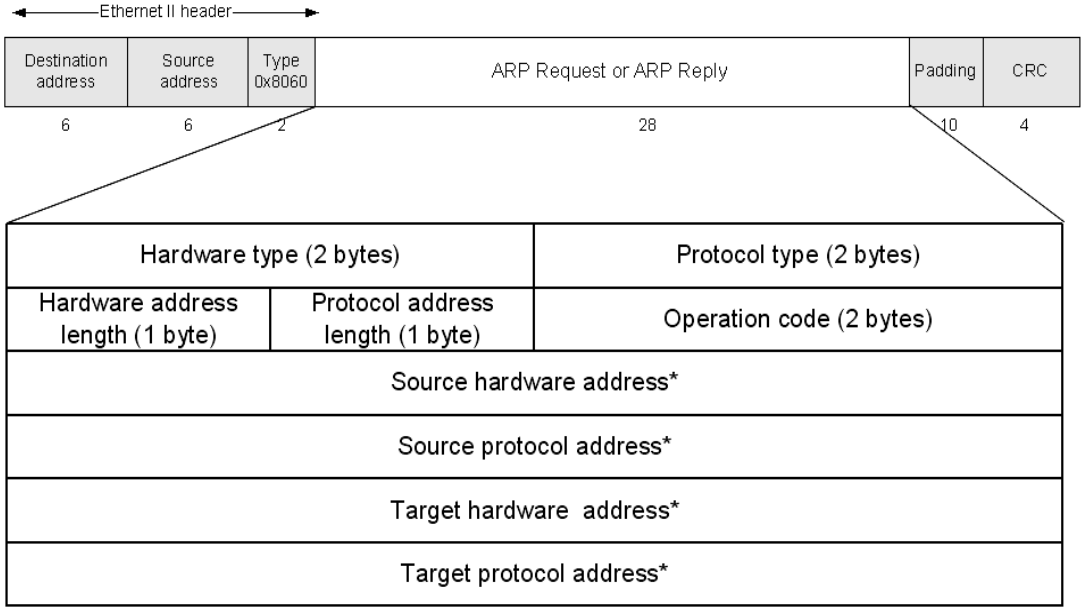


Figure 2.9 ARP Packet Format

The above figure 2.9 shows the packet format of ARP. It contains the following fields.

i. Hardware type
   - This is a 16-bit field defining the type of the network on which ARP is running.
   - Each LAN has been assigned an integer based on its type.
   - For example, Ethernet is given type 1.
   - ARP can be used on any physical network.

ii. Protocol type
   - This is a 16-bit field defining the protocol.
   - For example, the value of this field for the IPv4 protocol is 080016, ARP can be used with any higher-level protocol.

iii. Hardware length
   - This is an 8-bit field defining the length of the physical address in bytes.
   - For example, for Ethernet the value is 6.

iv. Protocol length
   - This is an 8-bit field defining the length of the logical address in bytes.
   - For example, for the IPv4 protocol the value is 4.

v. Operation
   - This is a 16-bit field defining the type of packet.
   - Two packet types are defined: ARP request (1) and ARP reply (2).

vi. Sender hardware address
   - This is a variable-length field defining the physical address of the sender.

- For example, for Ethernet this field is 6 bytes long.

vii. Sender protocol address

- This is a variable-length field defining the logical (for example, IP) address of the sender.
- For the IP protocol, this field is 4 bytes long.

viii. Target hardware address

- This is a variable-length field defining the physical address of the target.
- For an ARP request message, this field is all 0s' because the sender does not know the physical address of the target.

ix. Target protocol address

- Defining the logical address of the target.

Example

(i) ARP Request from Argon:

Source hardware address: 00:a0:24:71:e4:44

Source protocol address: 128.143.137.144

Target hardware address: 00:00:00:00:00:00

Target protocol address: 128.143.137.1

(ii) ARP Reply from Router137:

Source hardware address: 00:e0:f9:23:a8:20

Source protocol address: 128.143.137.1

Target hardware address: 00:a0:24:71:e4:44

Target protocol address: 128.143.137.144

There are four types of ARP messages that may be sent by the ARP protocol. These are identified by four values in the operation field of an ARP message. The types of messages are;

i. ARP request
ii. ARP reply
iii. RARP request
iv. RARP reply

2.6 ARP Cache

Since sending an ARP request/reply for each IP datagram is inefficient, hosts maintain a cache (ARP Cache) of current entries. The entries expire after 20 minutes. Contents of the ARP Cache:

(128.143.71.37) at 00:10:4B:C5:D1:15 [ether] on eth0

(128.143.71.36) at 00:B0:D0:E1:17:D5 [ether] on eth0

(128.143.71.35) at 00:B0:D0: DE: 70:E6 [ether] on eth0

(128.143.136.90) at 00:05:3C:06:27:35 [ether] on eth1

(128.143.71.34) at 00:B0:D0:E1:17: DB [ether] on eth0

(128.143.71.33) at 00:B0:D0:E1:17: DF [ether] on eth0

Vulnerabilities of ARP

i. Since ARP does not authenticate requests or replies, ARP Requests and Replies can be forged

ii. ARP is stateless: ARP Replies can be sent without a corresponding ARP Request

iii. According to the ARP protocol specification, a node receiving an ARP packet (Request or Reply) must update its local ARP cache with the information in the source fields, if the receiving node already has an entry for the IP address of the source in its ARP cache. (This applies for ARP Request packets and for ARP Reply packets)

Proxy ARP

Host or router responds to ARP Request that arrives from one of its connected networks for a host that is on another of its connected networks.

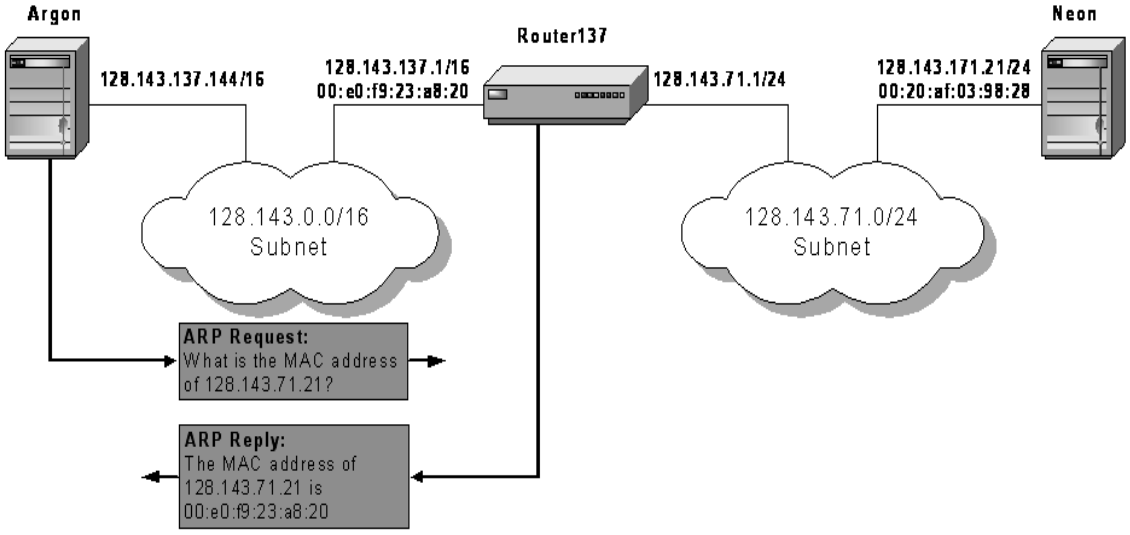


Figure 2.10 Proxy ARP

3. OVERVIEW OF DATA LINK CONTROL

The two main functions of the data link layer are data link control and media access control. The data link control deals with the design and procedures for communication between two adjacent nodes (node-to-node communication). The second function of the data link layer is media access control, or how to share the link.

Data link control functions include framing, flow and error control, and software implemented protocols that provide smooth and reliable transmission of frames between nodes. To implement data link control, we need protocols. Protocol is a set of rules that need to be implemented in software and run by the two nodes involved in data exchange at the data link layer.

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing.

3.1FRAMING

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, or from other messages to other destinations, 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. Frames can be of fixed or variable size.

i. Fixed-Size Framing

In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells. ATM (Asynchronous Transfer Mode) is a connection oriented, high-speed network technology that is used in both LAN and WAN over optical fiber and operates up to gigabit speed.

ii. Variable-Size Framing

In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Two approaches were used for this purpose: ***a character-oriented approach and a bit oriented approach.***

Character-Oriented Protocols

In a character-oriented protocol, 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 or error correction redundant bits, are also multiples of 8 bits.

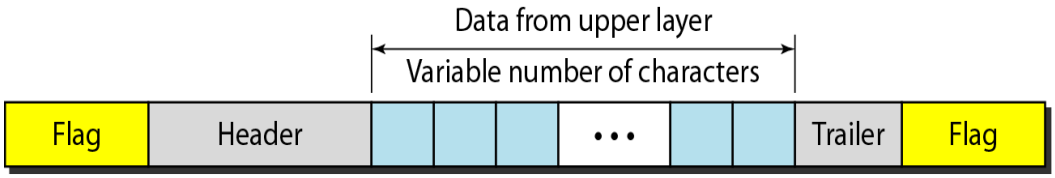


Figure 2.11 A frame in a character-oriented protocol

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. Figure 2.11 shows the format of a frame in a character-oriented protocol

Bit-Oriented Protocols

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. 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, as shown in Figure 2.12.

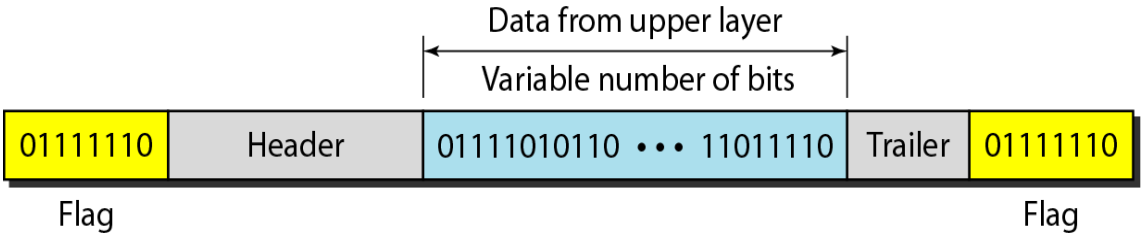


Figure 2.12A frame in a bit-oriented protocol

3.2 FLOW AND ERROR CONTROL

The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as ***data link control.*** Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment. Each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Error control is both error detection and error correction. It allows the receiver to tell the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. Error control in the data link layer is based on automatic repeat request (ARQ), which is the retransmission of data.

4. PROTOCOLS USED FOR FLOW CONTROL

All the protocols are unidirectional. The data frames travel from one node, called the sender, to another node, called the receiver. Special frames, called acknowledgment (ACK) and negative acknowledgment (NAK) can flow in the opposite direction.

In bidirectional data flow – the protocol includes the control information such as ACKs and NAKs with the data frames. This technique is called piggybacking.

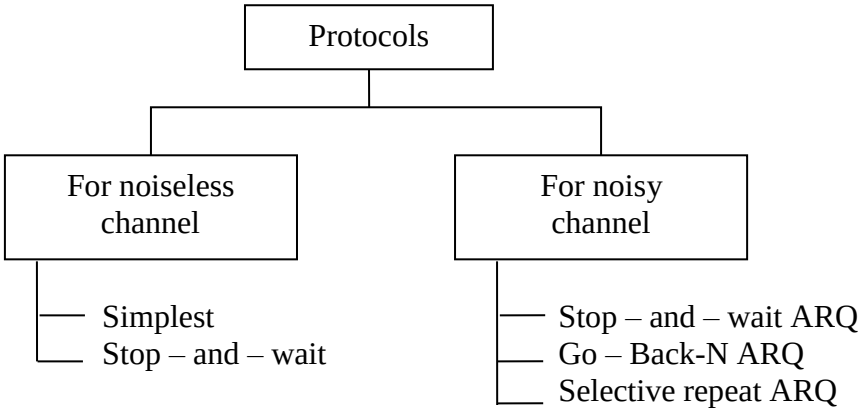


Figure 2.13 ***Taxonomy of protocols used for flow control***

Noiseless Channels

An ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel. The first is a protocol that does not use flow control; the second is the one that does.

4.1 Simplest Protocol

It is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver. The receiver can immediately handle any frame it receives with in a processing time. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately. Here the receiver can never be overwhelmed with incoming frames.

Design

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer. The data link layers of the sender and receiver provide transmission services for their network layers. The data link layers use the services provided by their physical layers (such as signaling, multiplexing, and so on) for the physical transmission of bits.

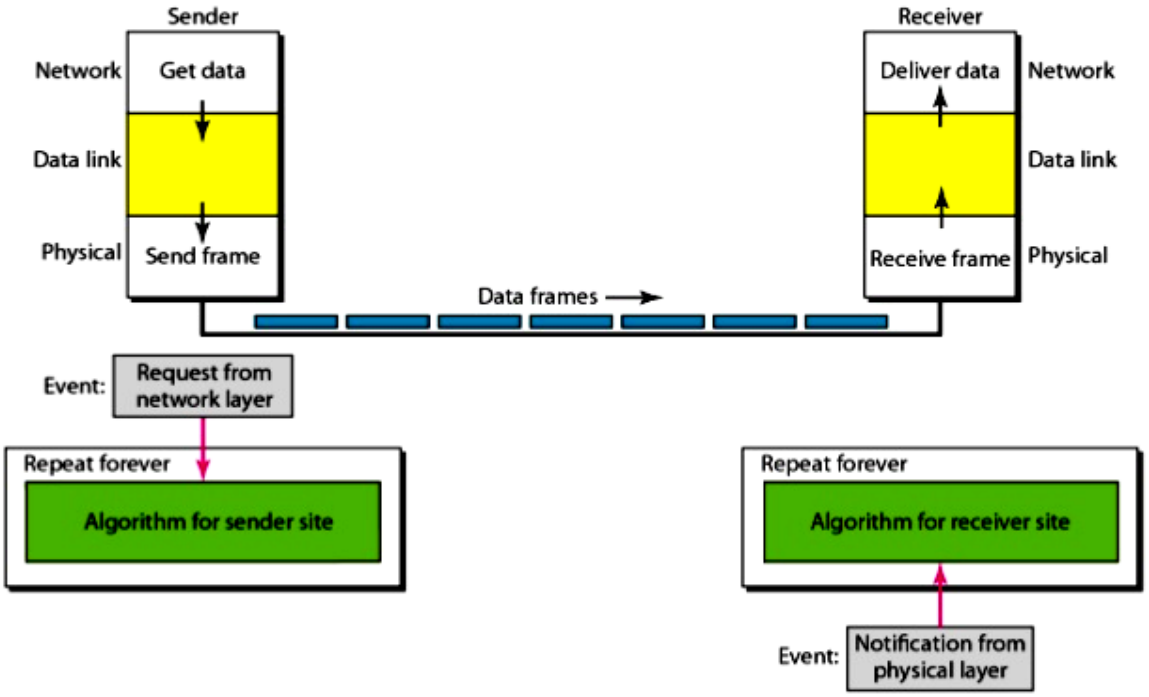


Figure 2.14 Simplest Protocol Design

The procedure used by both data link layers

The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives. The procedure / event of a protocol are as follows;

i. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer.

ii. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives.

Both procedures are constantly running because they do not know when the corresponding events will occur.

Sender-site algorithm for the simplest protocol

```
1   while (true)                          //Repeat forever
2   {
3     WaitForEven( )I                     // Sleep until an event occurs
4     If(Event(RequestToSend>>// There is a packet to send
5     {
6        GetData( )i
7        MakeFrame( )i
8       sendFrame( )i                     // Send the frame
9     }
10  }
```

Where,

i. GetData( ) - takes a data packet from the network layer.

ii. MakeFrame( ) - adds a header and delimiter flags to the data packet to make a frame.

iii. SendFrame( ) - delivers the frame to the physical layer for transmission.

Receiver-site algorithm for the simplest protocol

```
1   While(true)                           // Repeat forever
2   {
3     waitForEvent( ) I                   II Sleep until an event occur
4     if (Event(ArrivalNotification>>II Data frame arrived
5     {
6        ReceiverFrame( ) i
7        ExtractData( )i
8        DeliverData( ) I                 // Deliver data to network layer
9     }
10  }
```

Flow diagram

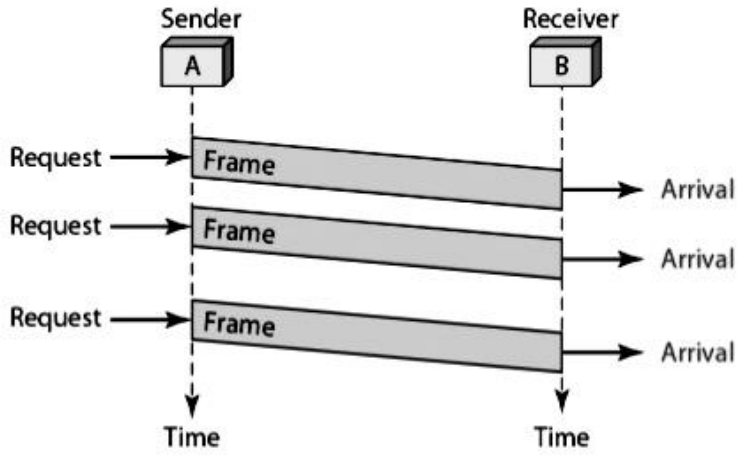


Figure 2.15 Simplest Protocol – Flow diagram

4.2 Stop-and-Wait Protocol

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. The receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames, we need to tell the sender to slow down. There must be a feedback from the receiver to the sender. In the Stop-and-Wait Protocol sender sends one frame, stops until it receives confirmation from the receiver and then sends the next frame.

In Stop-and-Wait Protocol

i. Data frames will follow the unidirectional communication.

ii. ACK frames (simple tokens of acknowledgment) can travel from the other direction.

Design

At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. We therefore need a half-duplex link.

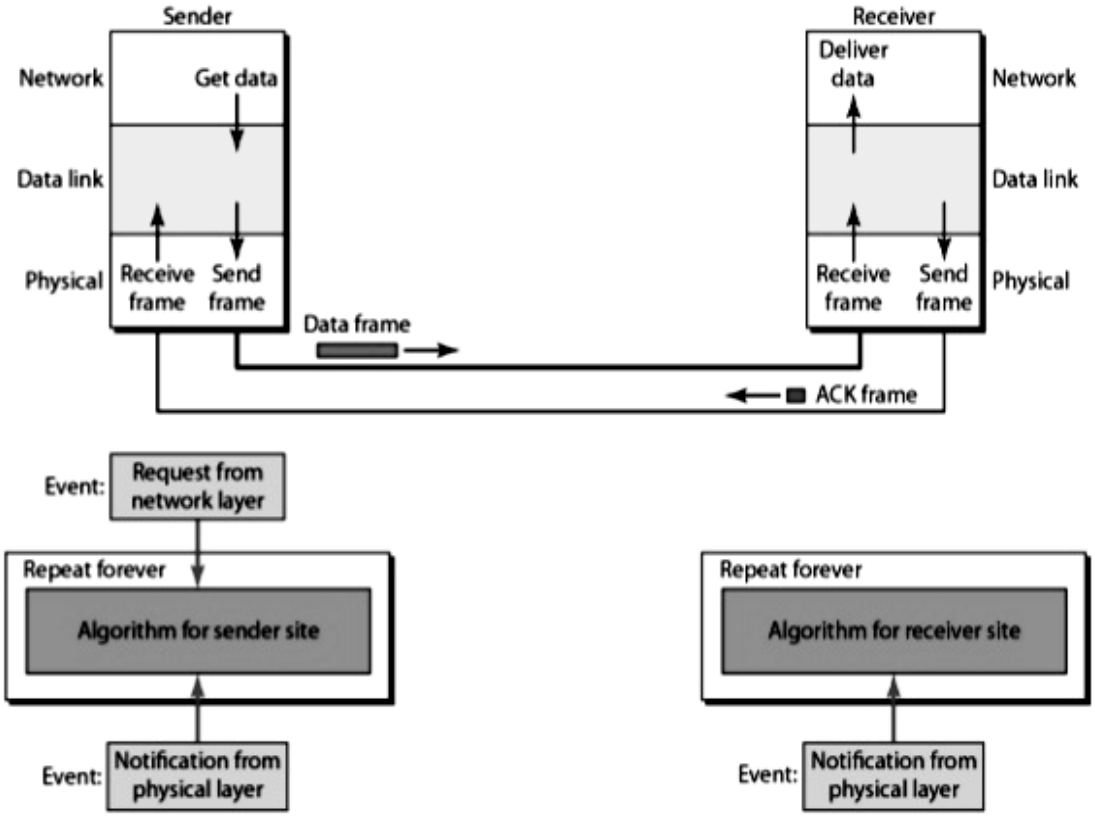


Figure 2.16 Design of Stop-and- Wait Protocol

Sender-site algorithm for Stop-and- Wait Protocol

```
while (true)                                   II Repeat forever
canSend = true                                 II Allow the first frame to go
{
  waitForEvent ( )i                            II Sleep until an event occurs
  if (Event(RequestToSend) AND canSend)
```

```
  {
     GetData( )i
     MakeFrame ( );
     SendFrame ( )i                    I/Send the data frame
     canSend = false;                  I / cannot send until ACK arrives
}
waitForEvent ( )i                      II Sleep until an event occurs
if(Event(Arrival Notification)         / I An ACK has arrived
   {
     ReceiverFrame( )i                 I / Receive the ACK frame
     cansend = true;
   }
}
```

Receiver-site algorithm for Stop-and-Wait Protocol

```
while (true)                           II Repeat forever
{
  waitForEvent ( )i                    II Sleep until an event occurs
  if(Event(Arrival Notification)       II Data frame arrives
  {
      ReceiverFrame( }i                I / Receive the ACK frame
      ExtractData( }i
      Deliver(data};                   / I Deliver data to network layer
      SendFrame( );                    II Send an ACK frame
   }
}
```

Data flow diagram for Stop and wait Protocol

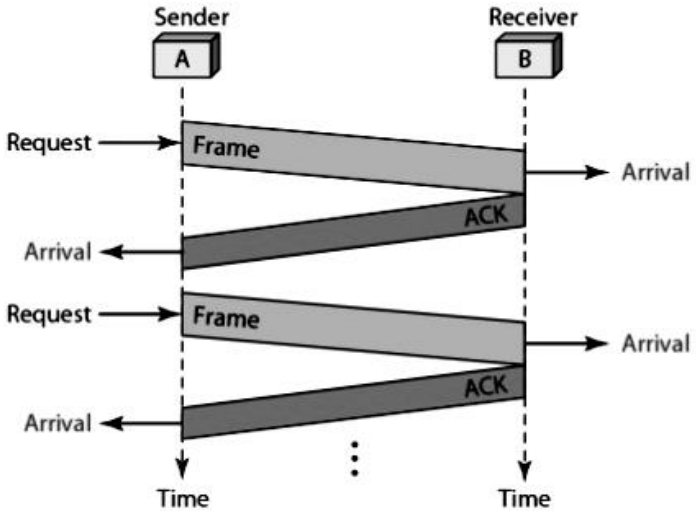


Figure 2.17 Flow diagram for Stop-and- Wait Protocol

NOISY CHANNELS

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. We discuss three protocols in this section that use error control.

4.3 Stop-and-Wait Automatic Repeat Request

The Stop-and-Wait Automatic Repeat Request protocol adds a simple error control mechanism. To detect and correct the corrupted frames - need to add redundancy bits to our data frame. When the frame arrives at the receiver site - it is checked and if it is corrupted, it is silently discarded. The detection of errors is manifested by the silence of the receiver. To number the frames - handle the corrupted frames, duplicate, or a frame out of order.

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires before receiving the ACK. In Stop-and-Wait ARQ - we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic. In Stop-and-Wait ARQ - the acknowledgment number always announces in modulo-2 arithmetic, the sequence number of the next frame expected.

Flow diagram for Stop-and-Wait ARQ

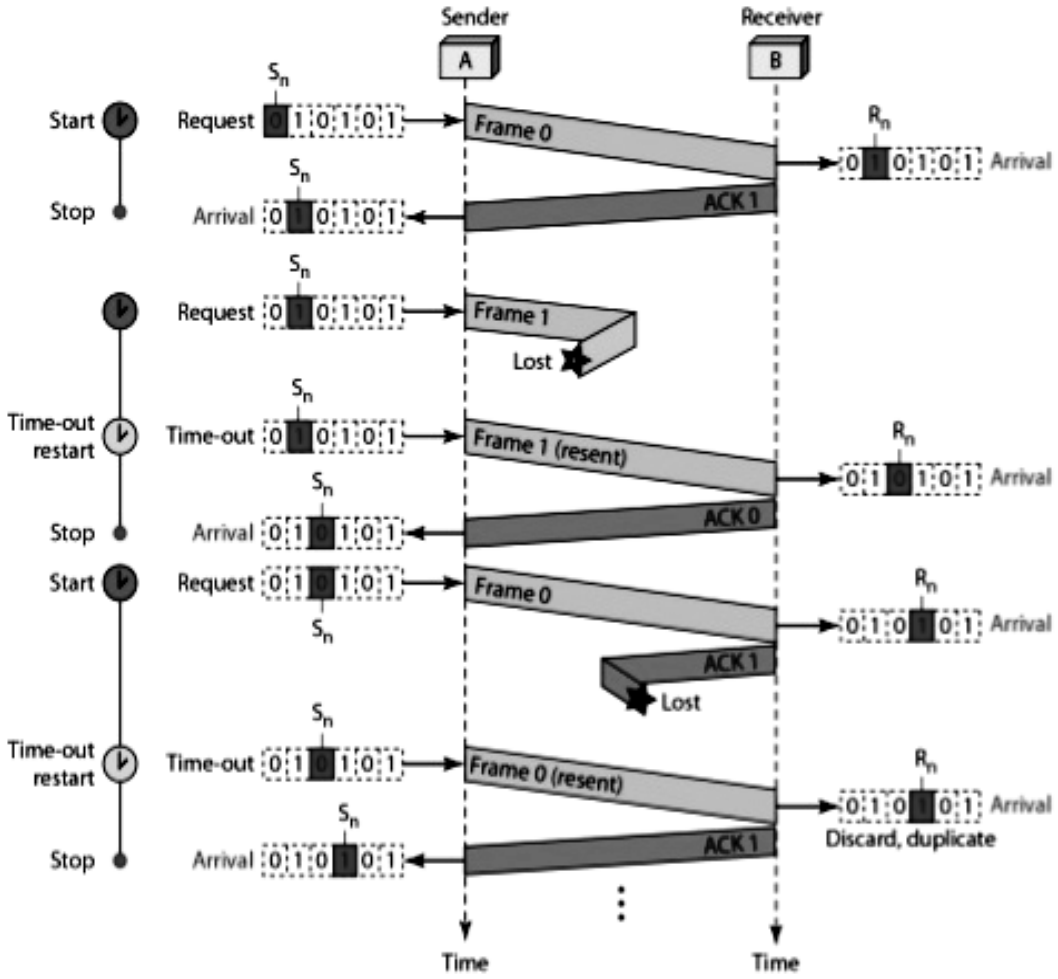


Figure 2.18 Flow diagram for Stop-and- Wait ARQ

Efficiency

The Stop-and-Wait ARQ discussed in the previous section is very inefficient if our channel is thick and long. By thick, we mean that our channel has a large and width; by long, we mean the round-trip delay is long.

4.4 Go-Back-N Automatic Repeat Request

To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition by the sender while waiting for acknowledgment (to keep the channel busy). The first is called Go-Back-N ARQ – In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive. In the Go-Back-N Protocol, the sequence numbers are modulo 2^m where m is the size of the sequence number field in bits. So the sequence numbers are 0, 1,2,3,4,5,6, 7,8,9, 10, 11, 12, 13, 14, 15,0, 1,2,3,4,5,6,7,8,9,10, 11, ...

Control Variables

- Sender has 3 variables: S, S_F, and S_L
- S holds the sequence number of recently sent frame
- S_F holds the sequence number of the first frame
- S_L holds the sequence number of the last frame
- Receiver only has the one variable, R that holds the sequence number of the frame it expects to receive.

❖ If the seq. no. is the same as the value of R, the frame is accepted, otherwise rejected.

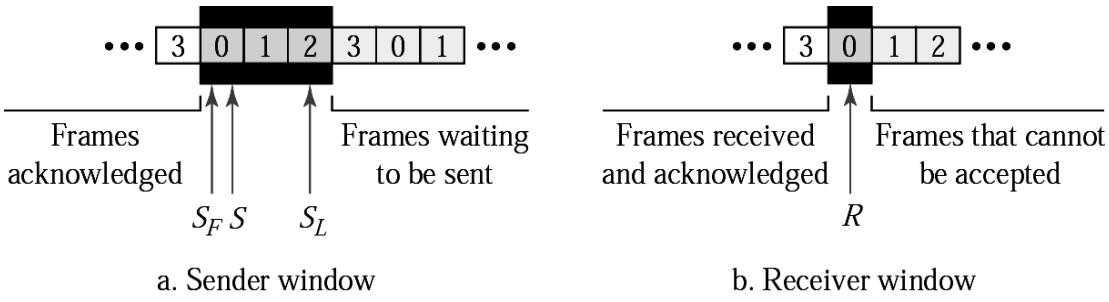


Figure 2.19 Go-Back-N ARQ

Normal operation of Go-Back-N ARQ

The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.

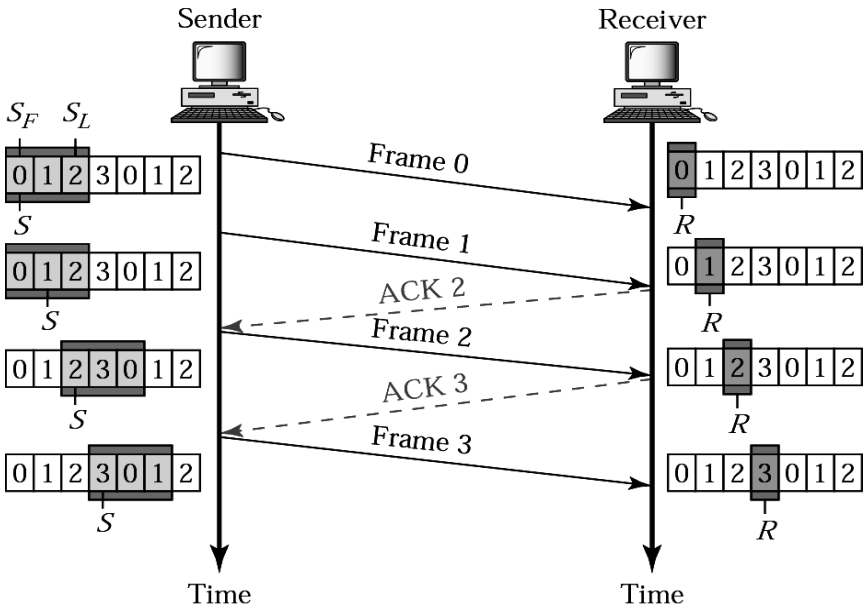


Figure 2.20 Normal operation of Go-Back-N ARQ

Go-Back-N ARQ - Lost frame

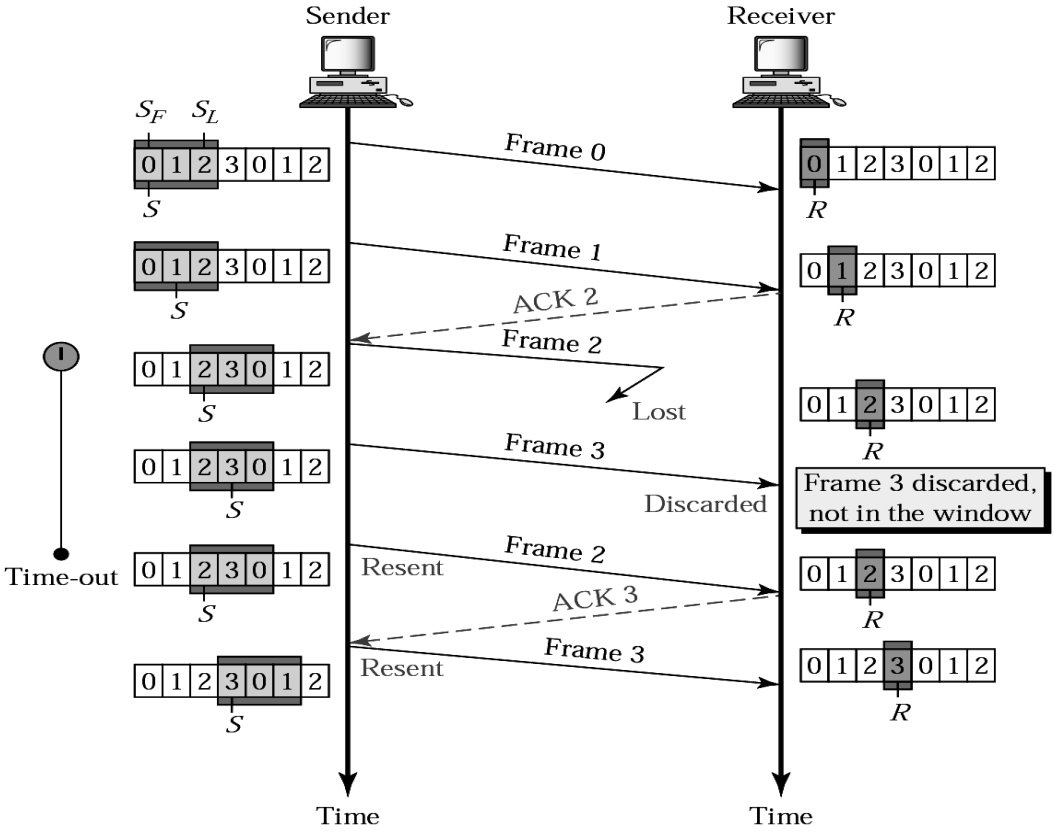


Figure 2.21 Go-Back-N ARQ- Lost frame

Consider a situation that if frame 2 is lost and the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window). After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (Go back to 2)

4.5 Selective Repeat ARQ

Sender and receiver windows

Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded. However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission. In Selective Repeat ARQ, only the damaged frame is resent. It may give more bandwidth efficiency but more complex processing at receiver site. It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.

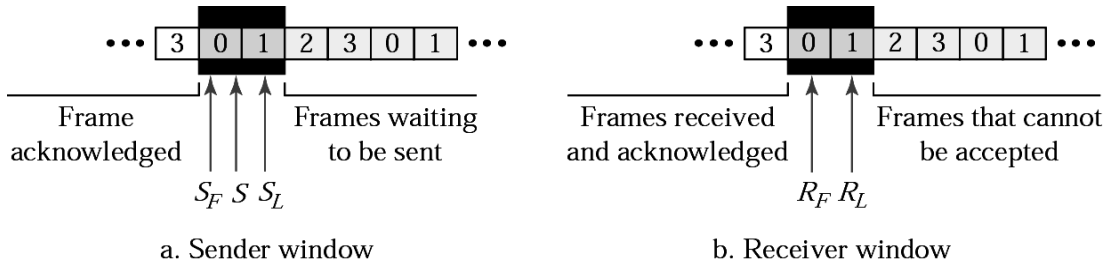


Figure 2.22 Selective Repeat ARQ

Selective Repeat ARQ- Lost frame

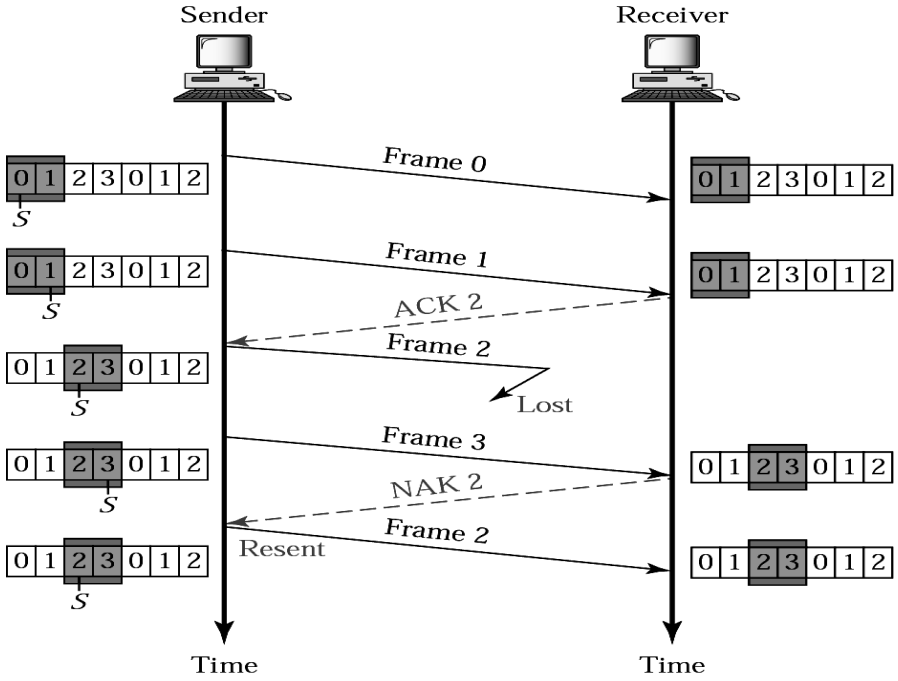


Figure 2.23 Selective Repeat ARQ- Lost frames

Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same thing will be followed for frame 3. Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

Selective Repeat ARQ - Sender window size

Size of the sender and receiver windows must be at most one-half of 2^m. If m = 2, window size should be $2^m/2 = 2$. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an error.

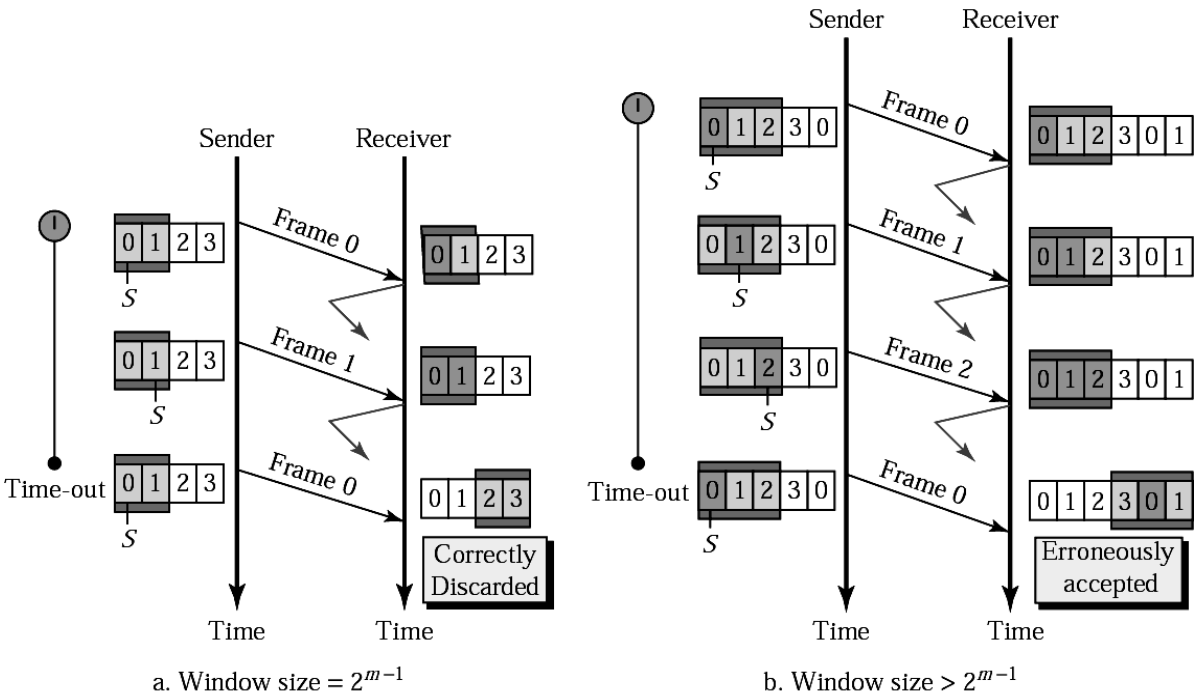


Figure 2.24 Selective Repeat ARQ – Sender window

5. HIGH-LEVEL DATA LINK CONTROL (HDLC)

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the ARQ mechanisms. The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. In 1979, the ISO made HDLC the standard as a Bit-oriented control protocol. The HDLC provides a transparent transmission service at the data link layer of the OSI. The users of the HDLC service provide PDUs which are encapsulated to form data link layer frames. These frames are ***separated by HDLC "flags" and are modified by "zero bit insertion" to guarantee transparency.***

Each piece of data is encapsulated in an HDLC frame by adding a trailer and a header. The header contains an HDLC address and an HDLC control field. The trailer is found at the end of the frame, and contains a (CRC) which detects any errors which may occur during transmission. The frames are separated by HDLC flag sequences which are transmitted between each frame and whenever there is no data to be transmitted. HDLC provides two common transfer modes that can be used in different configurations: ***normal response mode (NRM) and asynchronous balanced mode (ABM).***

i. Normal response mode (NRM)

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 and a secondary station can only respond. The NRM is used for both point-to-point and multiple-point links, as shown in Figure 2.25.

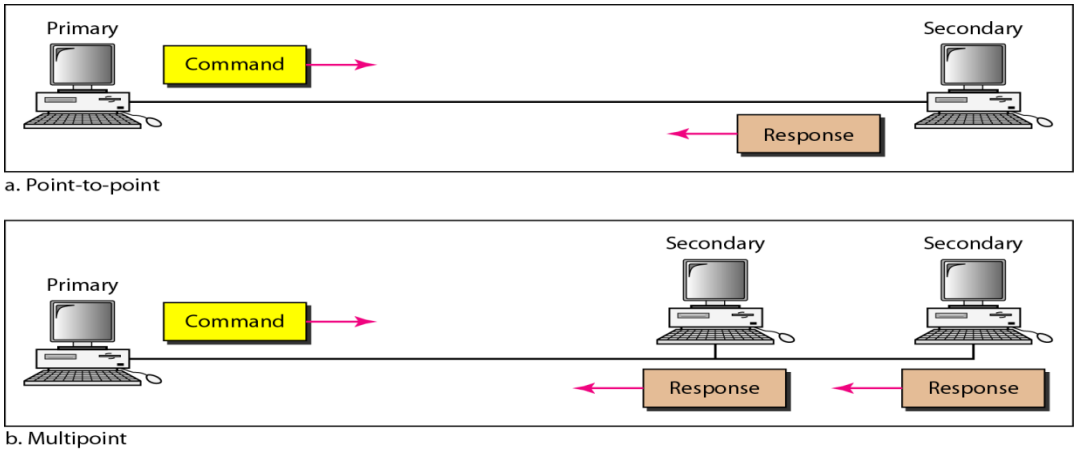


Figure 2.25 Normal response mode

ii. Asynchronous Balanced Mode

In asynchronous balanced mode (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), as shown in Figure 2.26. This is the common mode today.

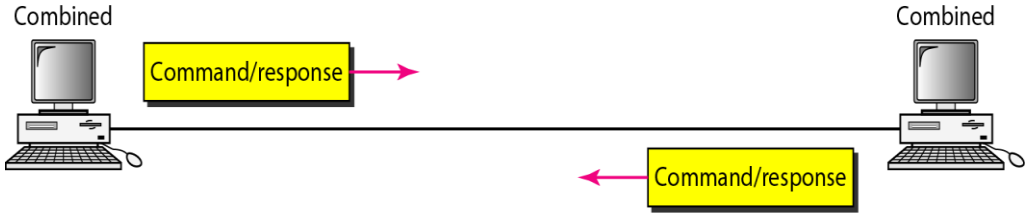


Figure 2.26 Asynchronous balanced mode

5.1 Frames

To provide the flexibility, HDLC defines three types of frames namely ***information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (V-frames)***. Each type of frame serves as an envelope for the transmission of a different type of message.

- I-frames are used to transport user data and control information relating to user data (piggybacking).
- S-frames are used only to transport control information.
- V-frames are reserved for system management. Information carried by V-frames is intended for managing the link itself.

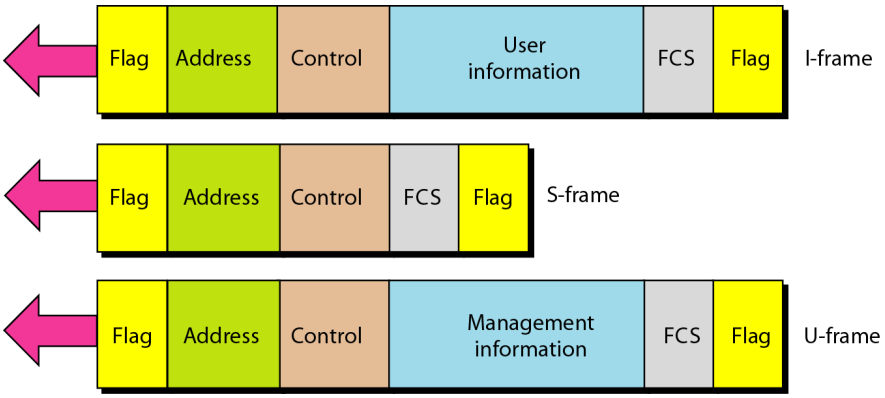


Figure 2.27 HDLC frames

Frame Format

Each frame in HDLC contain up to six fields, as shown in Figure 2.27.

(a) Beginning flag field
(b) An address field
(c) A control field
(d) An information field
(e) A frame check sequence (FCS) field
(f) An ending flag field.

In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

Fields and their use in different frame types

i. **Flag field:** The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver. The ending flag of one frame can be used as the beginning flag of the next frame.

ii. **Address field:** The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a ***to address***. If a secondary creates the frame, it contains *a* ***from address***. An address field can be 1 byte or several bytes long, depending on the needs of the network. One byte can identify up to 128 stations.

- If the address field is only 1 byte, the last bit is always a 1.

- If the address is more than 1 byte, all bytes but the last one will end with 0; only the last will end with 1.
- Ending each intermediate byte with 0 indicates to the receiver that there are more address bytes to come.

iii. **Control field:** The control field is a 1- or 2-byte segment of the frame used for flow and error control. The interpretation of bits in this field depends on the frame type.

iv. **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.

v. **FCS field:** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte ITU-T CRC.

5.1.1 Bit Stuffing

HDLC uses a process called **Bit Stuffing**. Bit stuffing is the process of adding one extra zero whenever there are 5 consecutive 1's in the data, so that the receiver doesn't mistake the data for a flag. Every time a sender wants to transmit a bit sequence having more than 6 consecutive 1's, it inserts 1 redundant 0 after the 5_{th} 1.

Exceptions

- When the **bit sequence** is really a **flag.**
- When **transmission** is being **aborted.**
- When the **channel** is being put into **idle.**

Example

A frame before bit stuffing

01111110 01111100 101101111 110010

After

011111010 011111000 101101111 1010010

How does the receiver identify a stuffed bit?

- Receiver reads incoming bits and counts 1's.
- When number of consecutive 1s after a zero is 5, it checks the next bit (7^{th} bit).
- If 7^{th} bit = zero→ receiver recognizes it as a stuffed bit, discard it and resets the counter.
- If the 7^{th} bit = 1→ then the receiver checks the 8^{th} bit; If the 8^{th} bit = 0, the sequence is recognized as a flag.

01111010 011111000 101101111 1010010

5.2 Control Field

The control field determines the type of frame and defines its functionality. Figure 2.28 shows the control field format for the different frame types.

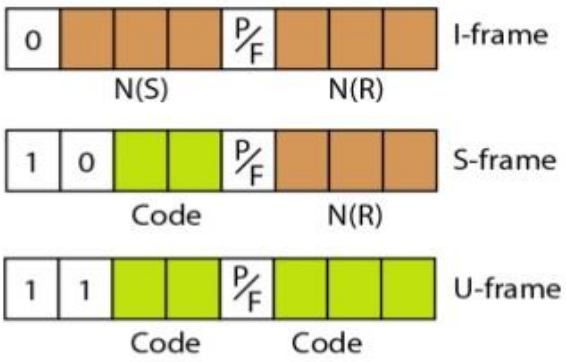


Figure 2.28 Control field format for the different frame types

Control Field forI-Frames

- I-frames are designed to carry user data from thenetwork-layer.
- In addition, they can include flow and error-control information(piggybacking).
- The subfields in the control fieldare:
    (i) The first bit defines thetype. If the first bit of the control field is 0, this means the frame is an I-frame.
    (ii) The next 3 bits N(S) define the sequence-number of the frame. With 3 bits, we can define a sequence-number between 0 and7.
    (iii) The last 3 bits N(R) correspond to the acknowledgment-number when piggybacking isused.
    (iv) The single bit between N(S) and N(R) is called the P/Fbit. The P/F field is a single bit with a dual purpose. It can mean poll or final.
        a) It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of thereceiver).
        b) It means final when the frame is sent by a secondary to a primary (when the address field contains the address of thesender).

Control Field forS-Frames

- Supervisory frames are used for flow and error-control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than anacknowledgment).
- S-frames do not have informationfields.
- The subfields in the control fieldare:
    (i) If the first 2 bits of the control field is 10, this means the frame is anS-frame.
    (ii) The last 3 bits N(R) corresponds to the acknowledgment-number (ACK) or negative acknowledgment-number (NAK).
    (iii) The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types ofS-frames:
        a) Receive Ready (RR) = 00

- This acknowledges the receipt of frame or group of frames.
- The value of N(R) is the acknowledgment-number.

b) Receive Not Ready (RNR) =10

- This is an RR frame with 1 additional function.
- It announces that the receiver is busy and cannot receive more frames.
- It acts as congestion control mechanism by asking the sender to slow down.
- The value of N(R) is the acknowledgment-number.

c) ReJect (REJ) =01

- It is a NAK frame used in Go-Back-N ARQ to improve the efficiency of the process.
- It informs the sender, before the sender time expires, that the last frame is lost or damaged.
- The value of N(R) is the negative acknowledgment-number.

d) Selective REJect (SREJ) =11

- This is a NAK frame used in Selective Repeat ARQ.
- The value of N(R) is the negative acknowledgment-number.

Control Field forU-Frames

- Unnumbered frames are used to exchange session management and control information between connecteddevices.
- U-frames contain an information field used for system management information, but not userdata.
- Much of the information carried by U-frames is contained in codes included in the controlfield.
- U-frame codes are divided into 2sections:
  i) A 2-bit prefix before the P/Fbit
  ii) A 3-bit suffix after the P/Fbit.
- Together, these two segments (5 bits) can be used to create up to 32 different types ofU-frames.

5.3 POINT-TO-POINT PROTOCOL(PPP)

- PPP is one of the most common protocols for point-to-pointaccess.
- Today, millions of Internet users who connect their home computers to the server of an ISP usePPP.

Framing

- PPP uses a character-oriented (or byte-oriented) frame as shown in figure 2.29.

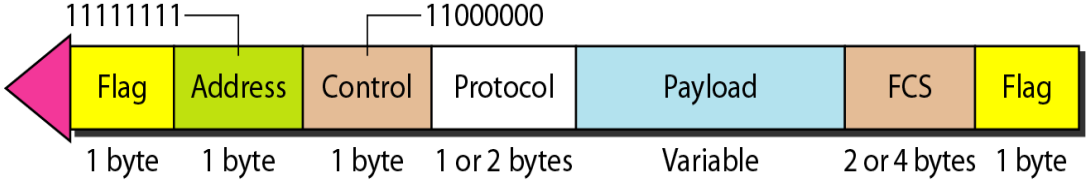


Figure 2.29 PPP *frame format*

Various fields of PPP frame

i. **Flag**
   - This field has a synchronization pattern01111110.
   - This field identifies both the beginning and the end of aframe.

ii. **Address**
   - This field is set to the constant value 11111111 (broadcastaddress).

iii. **Control**
   - This field is set to the constant value 00000011 (imitating unnumbered frames inHDLC).
   - PPP does not provide any flowcontrol.
   - Error control is also limited to errordetection.

iv. **Protocol**
   - This field defines what is being carried in the payloadfield.
   - Payload field carries either i) user data or ii) other controlinformation.
   - By default, size of this field = 2bytes.

v. **Payloadfield**
   - This field carries either i) user data or ii) other controlinformation.
   - By default, maximum size of this field = 1500bytes.
   - This field is byte-stuffed if the flag-byte pattern appears in thisfield.
   - Padding is needed if the payload-size is less than the maximumsize.

vi. **FCS**
   - This field is the PPP error-detectionfield.
   - This field can contain either a 2- or 4-byte standardCRC.

Byte Stuffing

Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of theframe. The escape byte is 01111101, which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not aflag. Obviously, the escape byte itself should be stuffed with another escapebyte.

TransitionPhases

- The transition diagram starts with the dead state as shown in figure2.30.

a) **Dead State**
   - In dead state, there is no active carrier and the line isquiet.

b) **Establish State**
   - When 1 of the 2 nodes starts communication, the connection goes into the establishstate.
   - In establish state, options are negotiated between the twoparties.

c) **AuthenticateState**
   - If the 2 parties agree that they need authentication, then the system needs to doauthentication; otherwise, the parties can simply start communication.

d) Open State

- Data transfer takes place in the openstate.

e) TerminateState

- When 1 of the endpoints wants to terminate connection, the system goes to terminatestate.

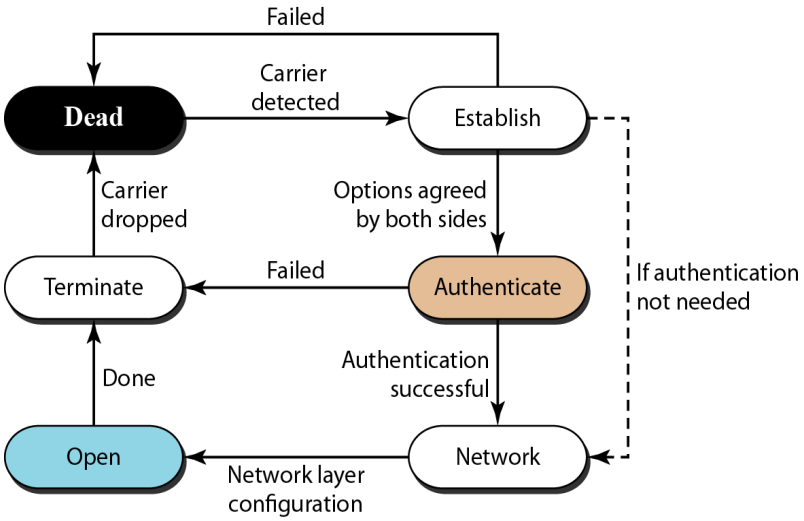


Figure 2.30 ***Transition phases***

6. MEDIA ACCESS CONTROL

The two main functions of the data link layer are data link control and media access control. The data link control deals with the design and procedures for communication between two adjacent nodes: node-to-node communication. The second function of the data link layer is media access control, or how to share the link.

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. The upper sub-layer of the DLL that is responsible for flow and error control is called the logical link control (LLC) layer. The lower sub-layer that is mostly responsible for multiple access resolution is called the media access control (MAC) layer. Many formal protocols have been devised to handle access to a shared links; we categorize them into three groups.

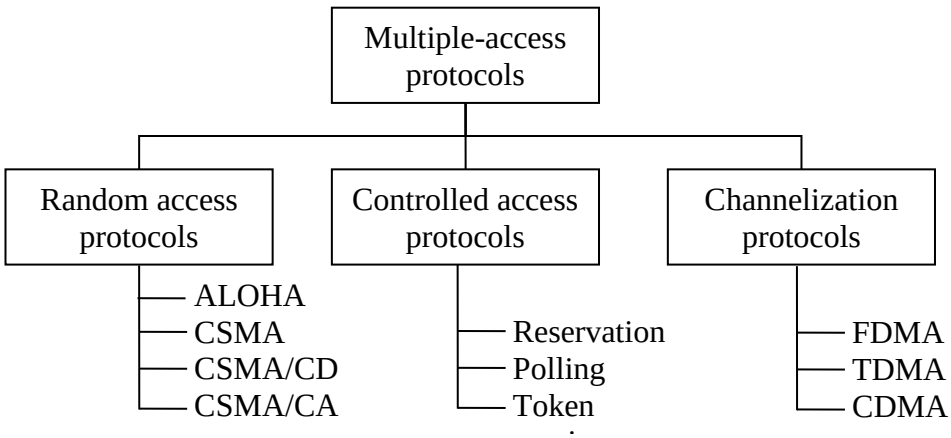


Figure 2.31 Taxonomy of multiple-access protocols

6.1 RANDOM ACCESS OR CONTENTION METHOD

In random access no station is superior to another station and none is assigned the control over another. 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). Two features of random access are;

i. There is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called **random access**.

ii. No rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called **contention methods**.

In a random access method, each station has the right to the medium without being controlled by any other station. If more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified. To avoid access conflict or to resolve it when it happens, each station follows a procedure that answers the following questions:

1) When can the station access the medium?
2) What can the station do if the medium is busy?
3) How can the station determine the success or failure of the transmission?
4) What can the station do if there is an access conflict?

The random access method using ALOHA protocol which used a very simple procedure called multiple access (MA). The method was improved with the addition of a procedure that forces the station to sense the medium before transmitting. This was called carrier sense multiple access. This method later evolved into two parallel methods:

i. Carriers sense multiple access with collision detection (CSMA/CD) : CSMA/CD tells the station what to do when a collision is detected

ii. Carrier sense multiple access with collision avoidance (CSMA/CA): CSMA/CA tries to avoid the collision.

ALOHA

ALOHA, the earliest random access method was designed for a radio (wireless) LAN, but it can be used on any shared medium. When the medium is shared between the stations, the data from the two stations collide and become garbled.

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. When the channel is shared, there is the possibility of collision between frames from different stations. Figure 2.32 shows an example of frame collisions in pure ALOHA.

There are four stations that contend with one another for access to the shared channel. The figure 2.32 shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. The pure ALOHA protocol relies on

acknowledgments from the receiver. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

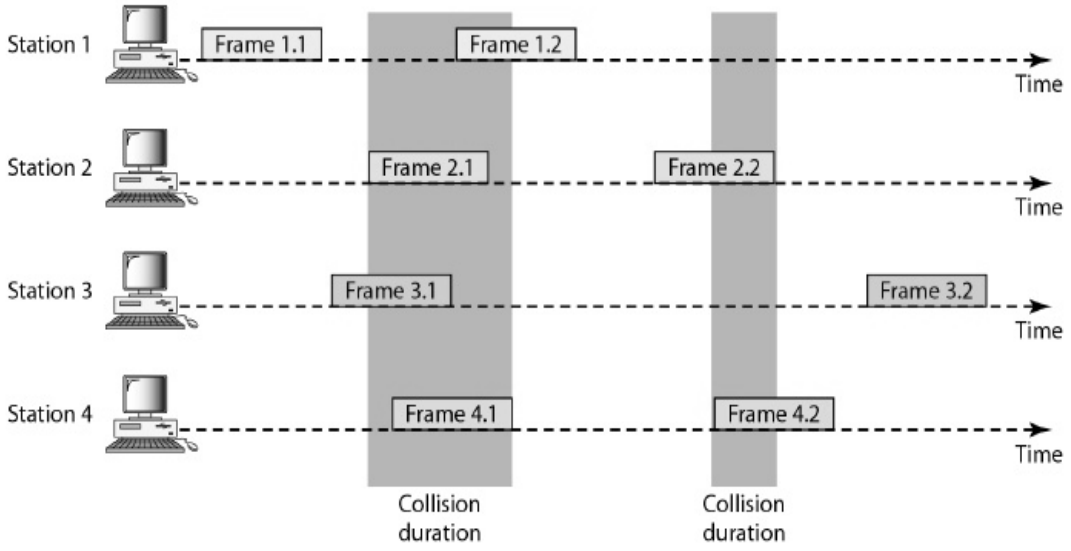


Figure 2.32 Frames in a pure ALOHA network

A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. 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 **back-off time TB.** Pure ALOHA has a 2nd method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later.

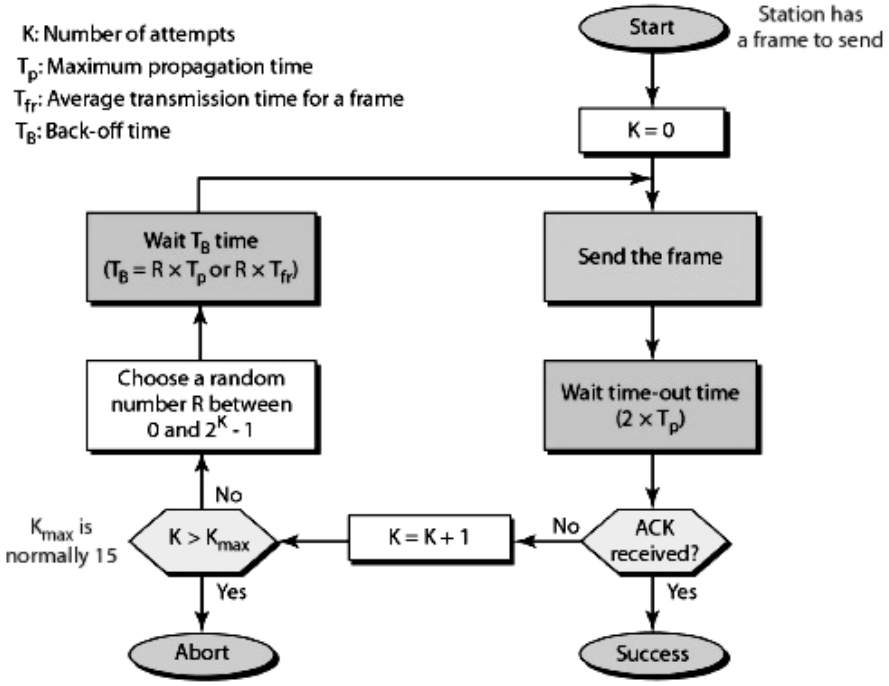


Figure 2.33 Procedure for pure ALOHA protocol

The length of time, the **vulnerable time,** in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking T_{fr}S to send. From figure 2.34, we see that the

vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

Pure ALOHA vulnerable time = 2 x T_{fr}

The throughput for pure ALOHA is

S =G x *e-2G.*

The maximum throughput

Smax =0.184 when G = (1/2)

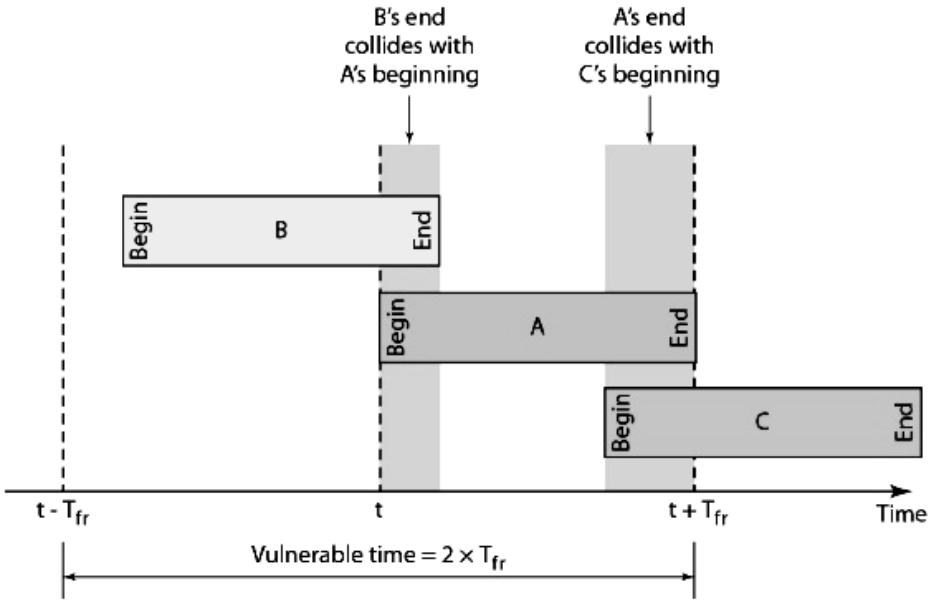


Figure 2.34 Vulnerable time for pure ALOHA protocol

Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 x Tfr .This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of T_{fr} s and force the station to send only at the beginning of the time slot. Figure 2.35 shows an example of frame collisions in slotted ALOHA.

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. The vulnerable time is now reduced to one-half, equal to Tfr.

Slotted ALOHA vulnerable time = Tfr

Throughput

It can be proved that the average number of successful transmissions for slotted ALOHA is,

S = G x e^{-G}

The maximum throughput Smax **is 0.368, when G = 1.**

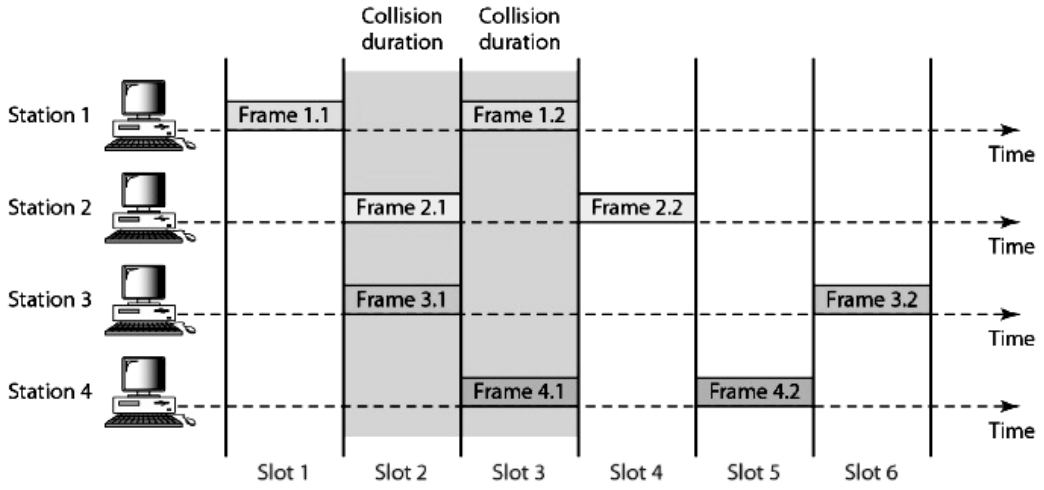


Figure 2.35 Frames in a slotted ALOHA network

Carrier Sense Multiple Access (CSMA)

CSMA is based on the principle "sense before transmit" or "listen before talk." CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is propagation delay (Stations are connected to a shared channel usually a dedicated medium). The possibility of collision still exists because of at time *t1* station B senses the medium and finds it idle, so it sends a frame.

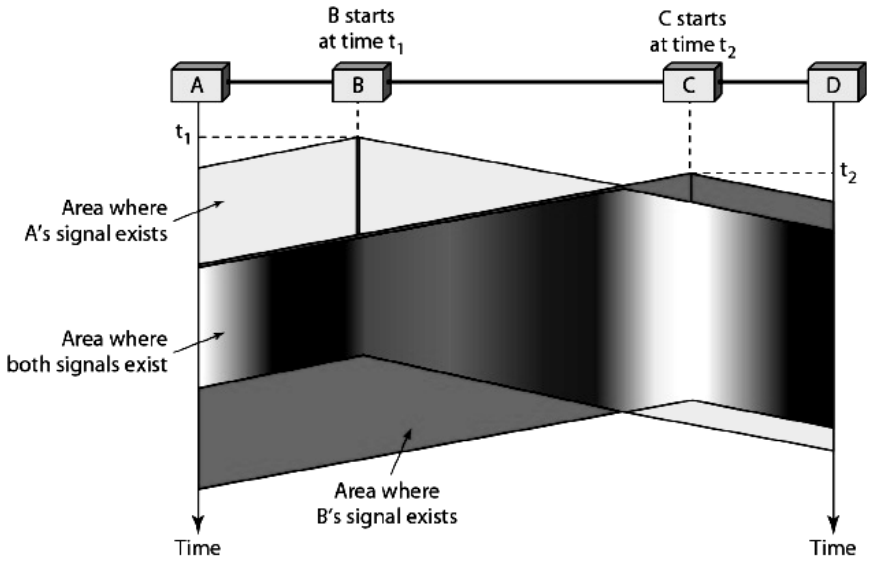


Figure 2.36 Space/time model of the collision in CSMA

At time t2 (t2> t1),station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. So station C also sends a frame. The two signals collide and both frames are destroyed.

Vulnerable Time

The vulnerable time for CSMA is the **propagation time Tp.** This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.

Persistence Methods

What should a station do if the channel is busy? What should a station do if the channel is idle? Three persistence methods have been devised to answer these questions:

i. 1-persistent method

ii. non-persistent method

iii. P-persistent method.

1-Persistent

In this method, after the station finds the line idle, it sends its frame immediately (with probability I). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

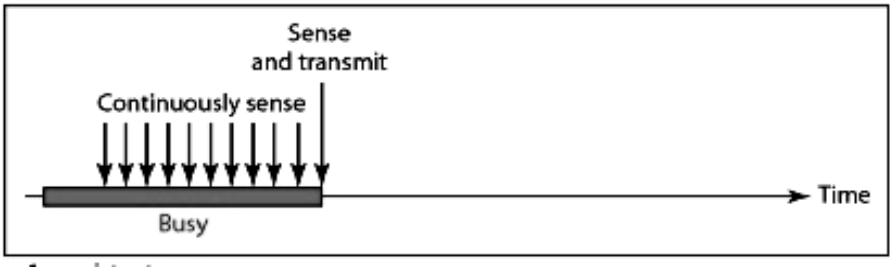


Figure 2.37 Behavior of 1-Persistence methods

Non-persistent

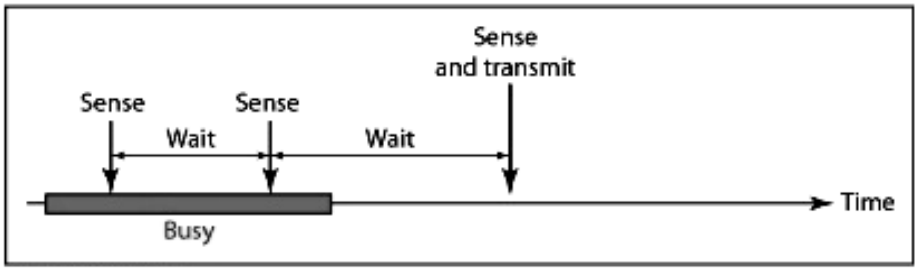


Figure 2.38Behavior of Non-Persistence methods

In this 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. The non-persistent approach reduces the chance of collision. This method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

The P-persistent method

Itis used if the channel has time slots with slot duration equal to or greater than the maximum propagation time. This approach reduces the chance of collision and improves efficiency. In this method, 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.
    a) If the line is idle, it goes to step 1.
    b) If the line is busy, it acts as though a collision has occurred and uses the back- off procedure.

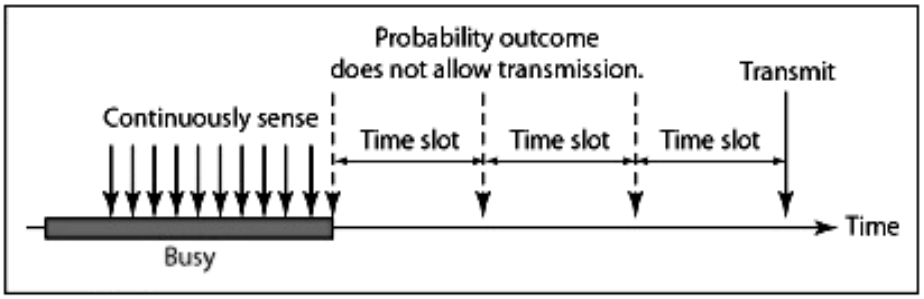


Figure 2.39 Behavior of P-Persistence methods

Flow diagram for three persistence methods

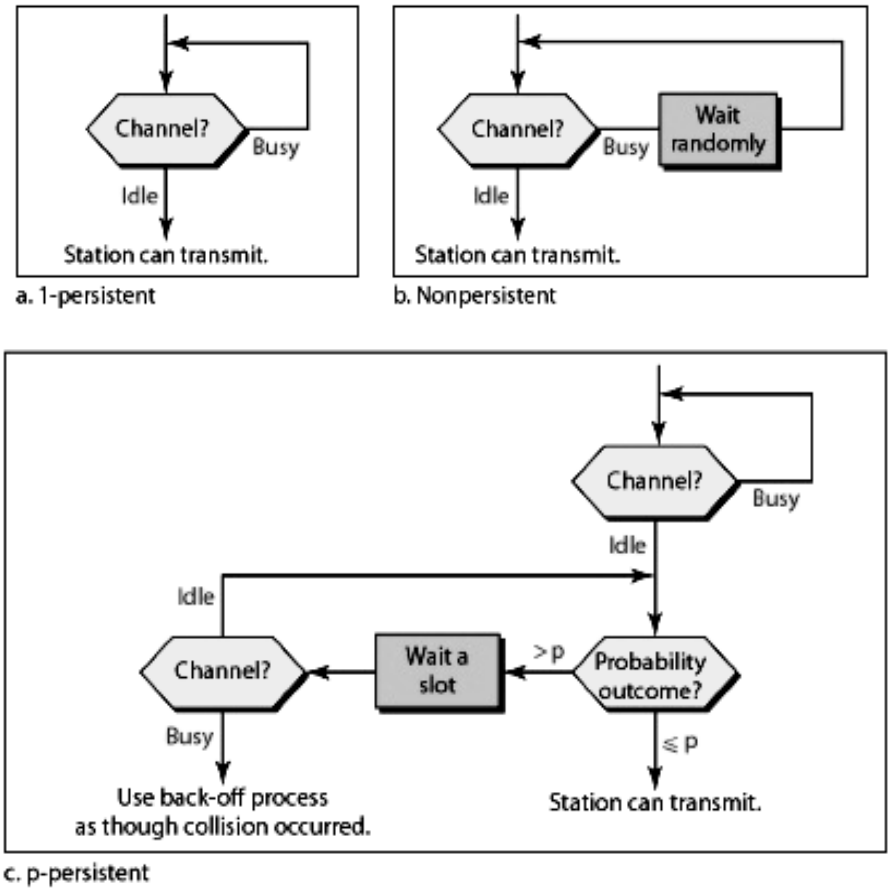


Figure 2.40 Flow diagram for three persistence methods

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

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.

Procedure

We need to sense the channel before we start sending the frame by using one of the persistence processes. Transmission and collision detection is a continuous process. We do not send the entire frame (bit by bit). By sending a short jamming signal, we can enforce the collision in case other stations have not yet sensed the collision.

Carrier sense multiple access with collision avoidance (CSMA/CA)

CSMA/CA was invented to avoid collisions on wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies:

i. The inter frame space (used to define the priority of a station)
ii. The contention window
iii. Acknowledgments

Interframe Space (IFS)

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. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station.

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. The station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data, and 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.

6.2 CONTROLLED ACCESS

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. Three popular controlled-access methods:

i. Reservation
ii. Polling
iii. Token passing

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. Figure 2.41 shows a situation with five stations and a five-mini slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

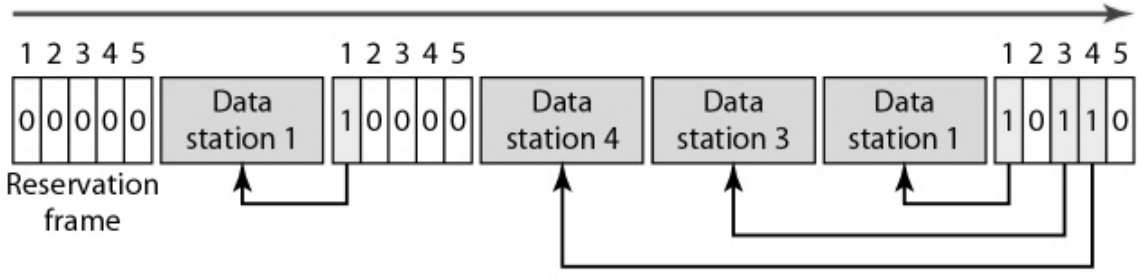


Figure 2.41 Reservation process in controlled access

Polling

Here 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. The primary device controls the link; the secondary devices follow its instructions. The primary device is always the initiator of a session. If the primary wants to receive data it asks the secondary if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

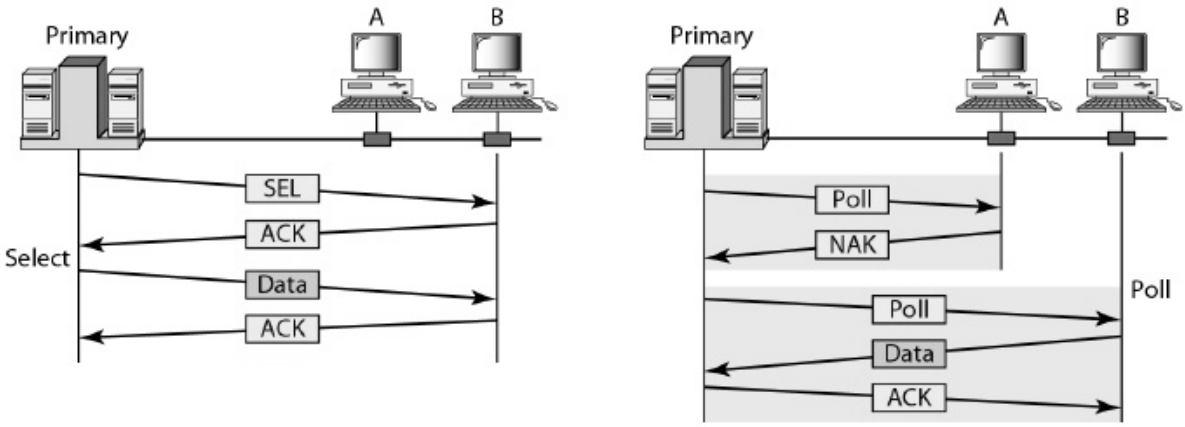


Figure 2.42 Polling in controlled access

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. For each station, there is a predecessor and a successor.

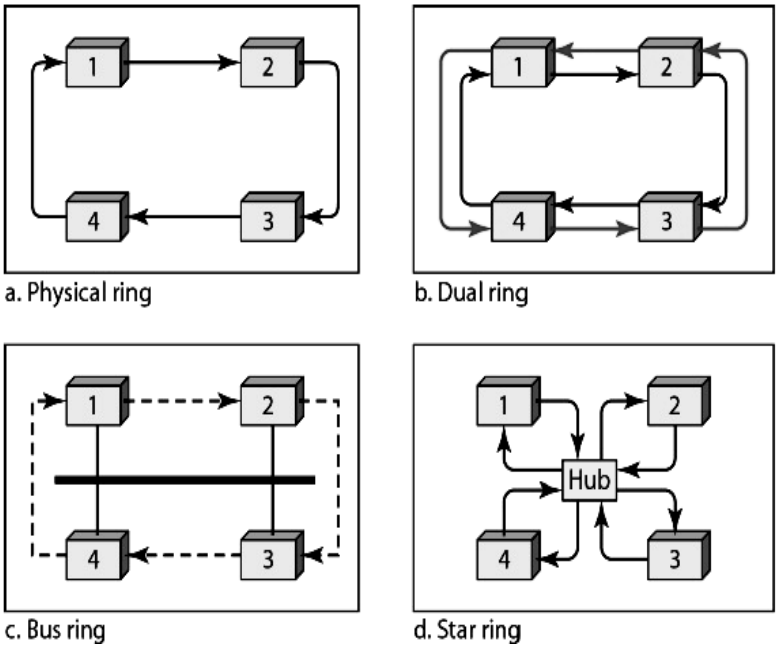


Figure 2.43 Token passing methods in controlled access

6.3 CHANNELIZATION

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. Three Channelization protocols are used. They are,

i. FDMA

ii. TDMA

iii. CDMA

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. Each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a band -pass filter to confine the transmitter frequencies.

To prevent station interferences, the allocated bands are separated from one another by small guard bands. FDMA specifies a predetermined frequency band for the entire period of communication (a continuous flow of data that may not be packetized).

Time-Division Multiple Access (TDMA)

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 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. This is difficult because of propagation delays introduced in the system if the stations are spread over a large area.

To compensate for the delays, we can insert guard times. Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.

Code-Division Multiple Access (CDMA)

CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link. It differs from TDMA because all stations can send data simultaneously; there is no timesharing. In CDMA, one channel carries all transmissions simultaneously.

7. ETHERNET (IEEE 802.3)

A LAN can be used as an isolated network to connect computers in an organization for sharing resources. Most of the LANs today are linked to a wide area network (WAN) or the Internet. The LAN market has seen several technologies such as,

i. Ethernet

ii. Token Ring

iii. Token Bus

iv. FDDI

v. ATM LAN.

The IEEE Standard Project 802 is designed to regulate the manufacturing and interconnectivity between different LANs.

7.1 IEEE STANDARDS

The IEEE 802 standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard. The relationship of the 802 Standard to the traditional OSI model is shown in figure 2.44. The IEEE has subdivided the data link layer into two sub layers:

i. Logical link control (LLC)
ii. Media access control (MAC).

The data link layer in the IEEE standard is divided into two sublayer. They are,

i. Logical Link Control (LLC)
ii. Media Access Control (MAC)

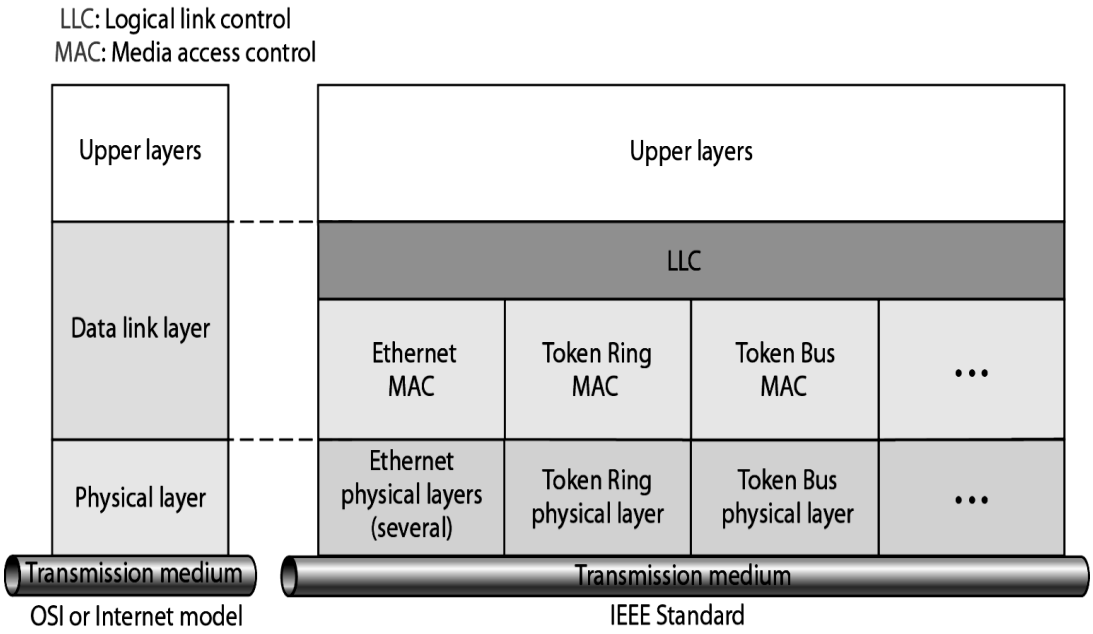


Figure 2.44 IEEE standard for LANs

Logical Link Control (LLC)

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into a sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer. The LLC provides a single data link control protocol for all IEEE LANs, but the MAC sublayer provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Media Access Control (MAC)

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs. A part of the framing function is also handled by the MAC layer. The MAC sublayer contains a number of distinct modules for defining the access method and the framing format specific to the corresponding

MAC Sublayer

In standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames the data received from the upper layer and passes them to the physical layer.

Frame Format

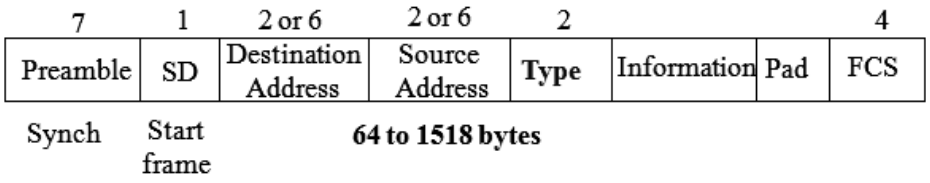


Figure 2.45 Frame Format

The Ethernet frame contains the following seven fields.

i. Preamble: 8 bytes with pattern 10101010 used to synchronize receiver, sender clock rates.

ii. SD: Eighth byte is used to indicate the start of frame (10101011)

iii. Addresses: The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet. The Source address (SA) field is also 6 bytes and contains the physical address of the sender of the packet.

iv. Type (DIX): Indicates the type of the Network layer protocol being carried in the payload field (IP, IP (0800), Novell IPX (8137) and AppleTalk (809B), ARP (0806))

v. Length: Number of bytes in the data field (Maximum 1500 bytes).

vi. CRC: Checked at receiver, if error is detected, the frame is discarded CRC-32.

vii. Data: Carries data encapsulated from the upper-layer protocols

viii. Pad: Zeros are added to the data field to make the minimum data length = 46 bytes

7.2 STANDARD ETHERNET

Ethernet data link layer protocol provides connectionless service to the network layer. (No handshaking between sending and receiving machine). It also provides an unreliable service to the network layer. Here the receiver doesn't send ACK or NAK to sender. This means that the stream of datagram's passed to network layer can have gaps (missing data).

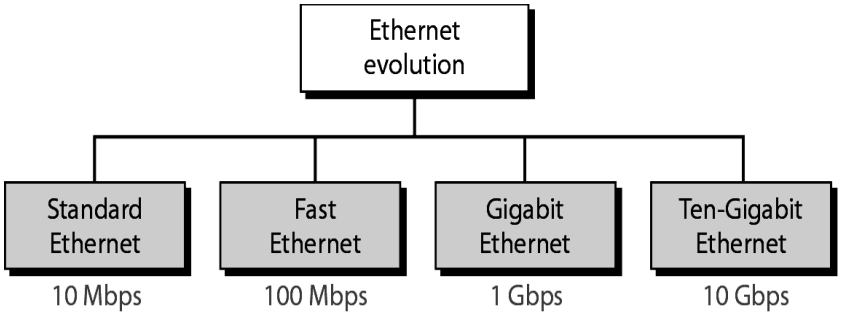
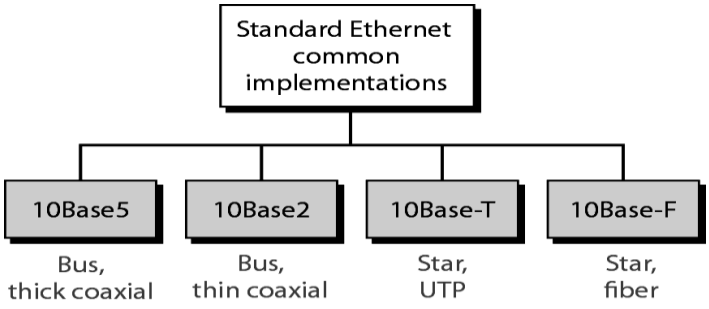


Figure 2.46 Ethernet evolution



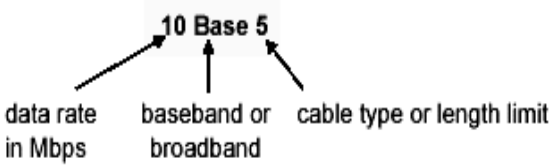


Figure 2.47Categories of traditional Ethernet

10BASE5

- Data transfer rate is10 Mbps.
- 500 meter segment length.
- Signal regeneration can be done with help of repeaters.
- Thick Coax is used as a transmission medium.

Advantages:

i. Low attenuation,
ii. Excellent noise immunity
iii. Superior mechanical strength

Disadvantages:

i. Bulky
ii. Difficult to pull
iii. Transceiver boxes are too expensive
iv. Wiring represented a significant part of total installed cost.

10BASE2 (Cheapernet)

- Data transfer rate is10 Mbps
- 185 meter segment length.
- Signal regeneration can be done with help of repeaters.
- Transceiver was integrated onto the adapter.
- Thin Coax is used as a transmission medium.

Advantages:

i. Easier to install
ii. Reduced hardware cost
iii. BNC connectors widely deployed (lower installation costs).

Disadvantages:

i. Attenuation is not good
ii. Could not support as many stations due to signal reflection caused by BNC Tee Connector.

10BaseT

- Uses twisted pair Cat3 cable.
- Star-wire topology.
- A hub functions as a repeater with additional functions.

Advantages:

i. Fewer cable problems

ii. Easier to troubleshoot than coax.

Disadvantages:

i. Cable length at most 100 meters.

1 BASE 5 (Star LAN)

- Data transfer rate is 1 Mbps
- 250 meter segment length.
- Signal regeneration can be done with help of repeaters.
- Transceiver integrated onto the adapter.
- Implemented with the help of star topology
- Two pairs of unshielded twisted pair cable are used as a transmission media.

Advantages:

i. It is easier to use installed wiring in the walls.

10BASE - T

- Most popularly used.
- Data transfer rate is 10 Mbps.
- 100 meter segment length.
- Signal regeneration can be done with help of repeaters.
- Transceiver is integrated onto adapter.
- Two pairs of UTP cable are used as a transmission media.
- Implemented with the help of star topology (Hub in the closet).

Advantages:

i. Could be done without pulling new wires.

ii. Each hub amplifies and restores incoming signal.

Hub Concept

It is used to separate transmit and receive pair of wires. The repeater in the hub retransmits the signal received on any input pair onto all output pairs. The hub emulates a broadcastchannel with collisions detected by receiving nodes.

7.3 CHANGES IN THE STANDARD

7.3.1 Bridged Ethernet

The first step in the Ethernet evolution was the division of a LAN by bridges. Bridges have two effects on an Ethernet LAN. They are,

i. Raise the bandwidth

ii. Separate collision domains.

Raising the Bandwidth

In an un-bridged Ethernet network, the total capacity (10 Mbps) is shared among all stations with a frame to send. The stations share the bandwidth of the network. For example, if two stations have a lot of

frames to send, they probably alternate in usage. When one station is sending, the other one refrains from sending.

A bridge divides the network into two or more networks. Bandwidth-wise, each network is independent. For example, a network with 12 stations is divided into two networks, each with 6 stations. Now each network has a capacity of 10 Mbps. The 10-Mbps capacity in each segment is now shared between 6 stations not 12 stations.

In a network with a heavy load, each station is offered 10/6 Mbps instead of 10/12 Mbps. If we use a four-port bridge, each station is now offered 10/3 Mbps, which is 4 times more than an un-bridged network.

Separating Collision Domains

In the bridged network, the collision domain becomes much smaller and the probability of collision is reduced tremendously.

7.3.2 Switched Ethernet

The basic idea behind the switched Ethernet is to overcome the drawbacks of Hub concept. The switch learns destination locations by remembering the ports of the associated source address in a table. The switch may not have to broadcast to all output ports. It may be able to send the frame only to the destination port. A big performance advantage of a switch over a hub is that, more than one frame transfer can go through it concurrently.

The advantage comes when the switched Ethernet backplane is able to repeat more than one frame in parallel (a separate backplane bus line for each node). The frame is relayed onto the required output port via the port's own backplane bus line. Under this scheme collisions are still possible when two concurrently arriving frames are destined for the same station. Each parallel transmission can take place at 10Mbps.

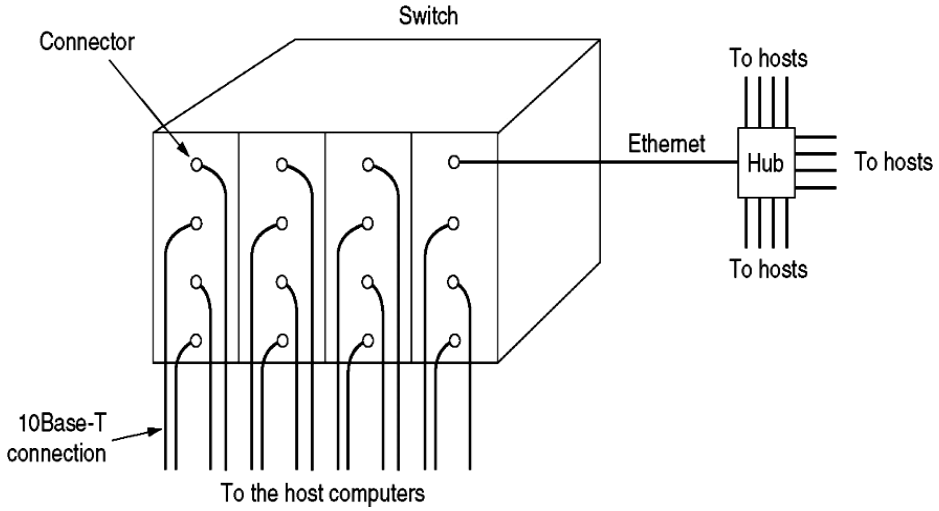


Figure 2.48 Example of switched Ethernet

7.3.3 Fast Ethernet

- Data transmission rate is 100 Mbps.
- Using the same frame format, media access, and collision detection rules as 10 Mbps Ethernet.
- It is possible to combine 10 Mbps Ethernet and Fast Ethernet on same network using a switch.
- Twisted pair (CAT 5) or fiber optic cable (no coax) can be used as a transmission media.

- Implemented with star-wire topology.

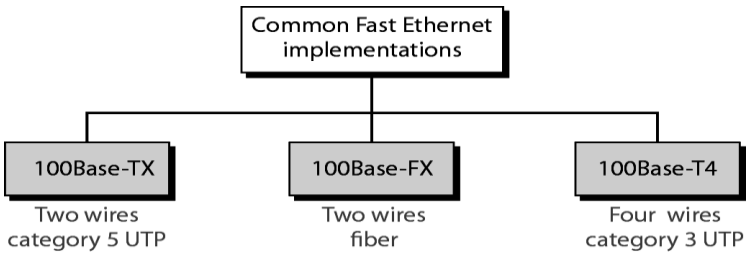


Figure 2.49 Fast Ethernet implementations

7.3.4 Gigabit Ethernet

- Data transmission rate is 1,000Mbps.
- Compatible with lower speeds.
- Uses standard framing and CSMA/CD algorithm.
- Distances are severely limited.
- Typically used for backbones and inter-router connectivity.
- Becoming cost competitive.
- Minimum frame length is 512 bytes
- Operates in full/half duplex modes mostly full duplex.
- 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.

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 pairs of STP	25m	Shielded twisted pair
1000Base-T	4 pairs of UTP	100m	Standard category 5 UTP

Table 2.1 Gigabit Ethernet implementations

10Gbps Ethernet

- Maximum link distances cover 300 m to 40 km.
- Operates only on full-duplex mode.
- No CSMA/CD.
- Uses optical fiber only.

7.4 EXPERIENCES WITH ETHERNET

i. Ethernets work best under light loads (Utilization over 30% is considered heavy).
ii. Network capacity is wasted by collisions
iii. Most networks are limited to about 200 hosts (Specification allows for up to 1024).
iv. Most networks are much shorter (5 to 10 microseconds RTT).
v. Transport level flow control helps reduce load (number of back to back packets)
vi. Ethernet is inexpensive, fast and easy to administer.

Ethernet Problems

- Ethernet's peak utilization is pretty low (like Aloha)
- Peak throughput worst with
    i. More hosts: More collisions needed to identify single sender.
    ii. Smaller packet sizes: More frequent arbitration.
    iii. Longer links: Collisions take longer to observe, more wasted bandwidth.
    iv. Efficiency is improved by avoiding these conditions.

Why dose Ethernet Win?

i. There are lots of LAN protocols
ii. Price
iii. Performance
iv. Availability
v. Ease of use
vi. Scalability

8. WIRELESS LAN

Wireless communication is one of the fastest-growing technologies because the demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas. IEEE 802.11 wireless LANs sometimes called wireless Ethernet. IEEE 802.11 operates on the physical and data link layers.

8.1 ARCHITECTURE

IEEE 802.11 defines two kinds of services. They are,

i. Basic service set (BSS)
ii. Extended service set (ESS).

Basic Service Set (BSS)

BSS - the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). 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 network.

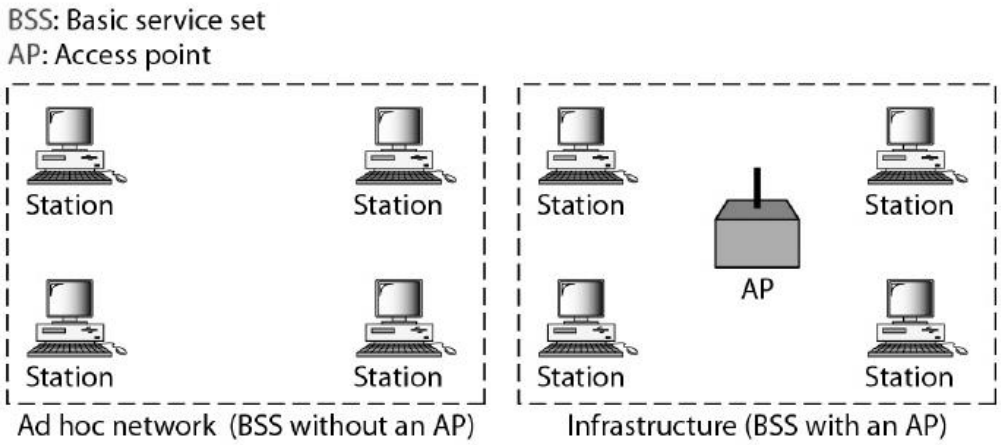


Figure 2.50 Architecture of IEEE 802.11 (BSS)

Extended Service Set (ESS)

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 usually a wired LAN such as an Ethernet. The distribution system connects the APs in the BSSs. The extended service set uses two types of stations. They are,

i. Mobile stations
ii. Stationary stations.

The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

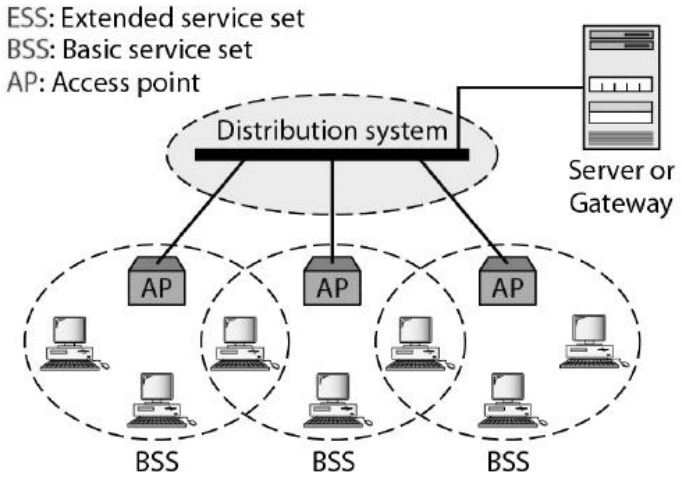


Figure 2.51 Architecture of IEEE 802.11 (ESS)

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs.

Station Types

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

i. No-transition mobility
ii. BSS-transition mobility
iii. ESS-transition mobility.

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

inside one ESS. A station with ESS-transition mobility can move from one ESS to another. However, IEEE 802.11 does not guarantee that communication is continuous during the move.

8.2 MAC SUBLAYER

IEEE 802.11 defines two types of MAC sub-layers. They are;

i. The distributed coordination function (DCF)

ii. The point coordination function (PCF).

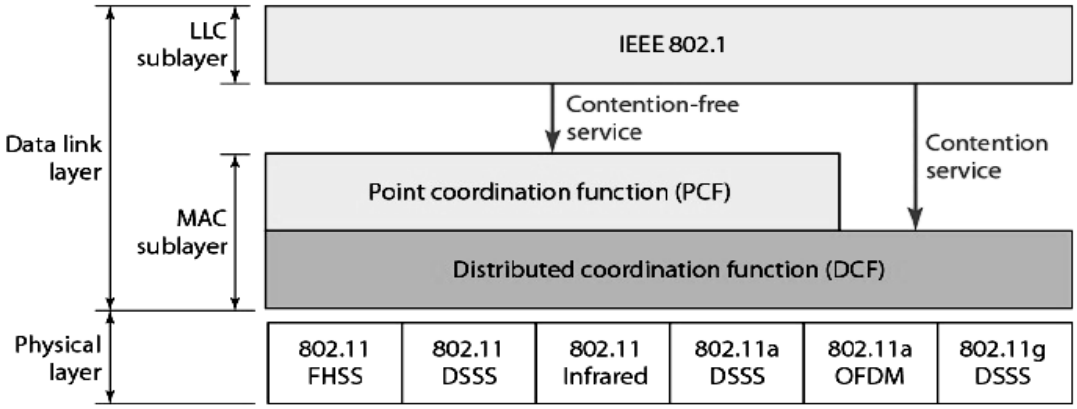


Figure 2.52 MAC layers in IEEE 802.11 standard

Distributed Coordination Function

One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method. Wireless LANs cannot implement CSMA/CD for the following three reasons:

i. For collision detection, a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.

ii. Collision may not be detected because of the hidden station problem.

iii. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Process Flowchart

The following figure 2.53 shows the process flowchart for CSMA/CA as used in wireless LANs. This includes the following steps;

i. 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 back-off 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).

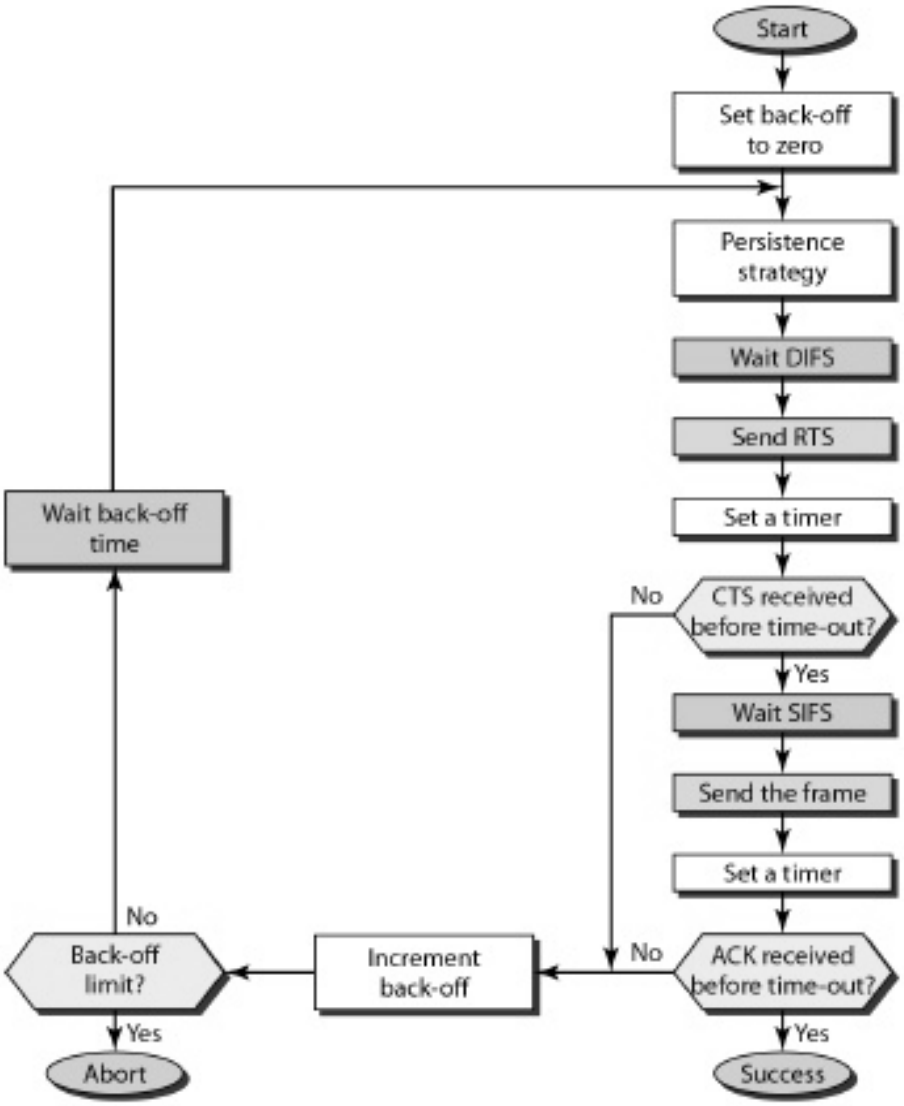


Figure 2.53 CSMA/CA flowchart

ii. 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.

iii. The source station sends data after waiting an amount of time equal to SIFS.

iv. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

Point Coordination Function (PCP)

The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

Frame Format

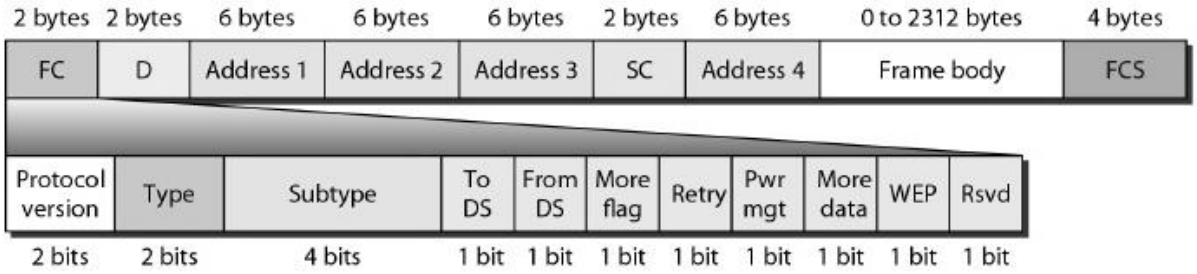


Figure 2.54 Frame format

The MAC layer frame consists of nine fields.

1. Frame control (FC) - The FC field is 2 bytes long and defines the type of frame and some control information.
2. D - In all frame types except one, this field defines the duration of the transmission. In the control frame - this field defines the ID of the frame.
3. 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.
4. Sequence control - This field defines the sequence number of the frame to be used in flow control.
5. 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.
6. FCS - The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

Below table describes the subfields of the Frame control (FC) field and the Values of subfields in control frames.

Subtype	Meaning
1011	Request to send (RTS)
1100	Clear to send (CTS)
1100	Acknowledgement (ACK)

Table 2.2 Values of subfields in control frames

Field	Explanation
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type
To DS	Defined later
From DS	Defined later
More flag	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

Table 2.3 Subfields of the Frame control (FC) field

Frame Types

IEEE 802.11 has the following three categories of frames.

i. Management frames
ii. Control frames
iii. Data frames

Management frames are used for the initial communication between stations and access points. Control frames are used for accessing the channel and acknowledging. Data frames are used for carrying data and control information.

8.3 ADDRESSING MECHANISM

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS. Each flag can be either 0 or 1, resulting in four different situations. The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags, as shown in below Table.

- Address 1 is always the address of the next device.
- Address 2 is always the address of the previous device.
- Address 3 is the address of the final destination station, if the address is not defined by address 1.
- Address 4 is the address of the original source station if it is not the same as address 2.

o DS	rom DS	ddress 1	ddress 2	ddress 3	ldress 4
		ation	e	D	
		ation	ng AP	e	
		ving AP	e	ation	
		ving AP	ng AP	ation	e

Table 2.4 Addresses

Four possible cases of addressing

Case 1: 00 In this case, *To DS* = 0 and *From DS* = 0.

This means that the frame is not going to a distribution system *(To DS* = 0) and is not coming from a distribution system *(From DS* =0). The frame is going from one station in a BSS to another without passing through the distribution system. The ACK frame should be sent to the original sender.

Case 2: 01 In this case, *To DS* = 0 and *From DS* = 1.

This means that the frame is coming from a distribution system *(From* DS = 1). The frame is coming from an AP and going to a station. The ACK should be sent to the AP. Note that address 3 contains the original sender of the frame (in another BSS).

Case 3: 10 In this case, *To DS* =1 and *From DS* =O.

This means that the frame is going to a distribution system *(To DS* = 1). The frame is going from a station to an AP. The ACK is sent to the original station. Note that address 3 contains the final destination of the frame (in another BSS).

Case 4:11 In this case, *To DS* =1 and *From DS* =1.

In this case the frame is going from one AP to another AP in a wireless distribution system. Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

8.4 PHYSICAL LAYER

All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges:902-928 MHz, 2.400-4.835 GHz, and 5.725-5.850 GHz. We discuss six specifications, as shown in Below Table.

IEEE	Technique	Band	Modulation	Rate (Mbps)
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	FSK	1 and 2
		Infrared	PPM	1 and 2
802.11 a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11 b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11 g	OFDM	2.4 GHz	Different	22 to 54

Table 2.5 Physical layers

IEEE 802.11 FHSS

- It uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.4 GHz ISM band.
- The band is divided into 79 sub-bands 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

- DSSS uses the direct sequence spread spectrum (DSSS) method.
- DSSS uses the 2.4-GHz ISM band.
- The modulation technique in this specification is PSK at 1 Mbaud/s.
- The system allows 1 or 2 bits/baud 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.lla – OFDM

- IEEE 802.Ila OFDM describes the orthogonal frequency-division multiplexing (OFDM) method for signal generation in a 5-GHz ISM band.
- OFDM is similar to FDM with one major difference: All the subbands are used by one source at a given time.
- 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.llb DSSS

- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS) method for signal generation in the 2.4-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.
- 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 using the OFDM with 2.4-GHz ISM band and forward error correction method.
- The modulation technique achieves a 22- or 54-Mbps data rate.

9. BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

The device sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is confusion.

9.1 ARCHITECTURE

Bluetooth defines two types of networks.

i. Piconet
ii. Scatternet.

Piconet

- A Bluetooth network is called a piconet, or a small net.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- It can have up to eight stations, one of which is called the master; the rest are called slaves.

- Maximum of seven slaves and only one master.

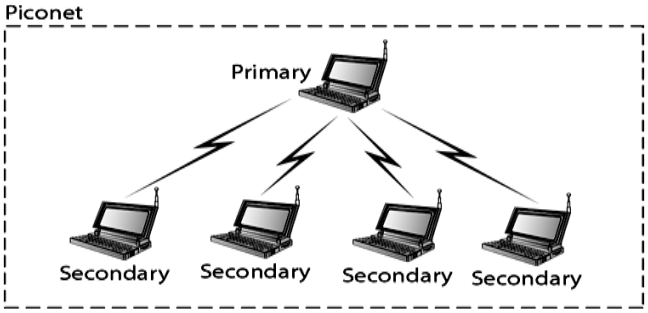


Figure 2.55 Piconet

- Slaves synchronize their clocks and hopping sequence with the master.
- But an additional eight slaves can stay in parked state, which means they can be synchronized with the master but cannot take part in communication until it is moved from the parked state.

Scatternet

- Piconets can be combined to form what is called a scatternet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliverthem to secondaries in the second piconet.
- A slave station in one piconet can become the master in another piconet.
- A Bluetooth device has a built-in short-range radio transmitter.

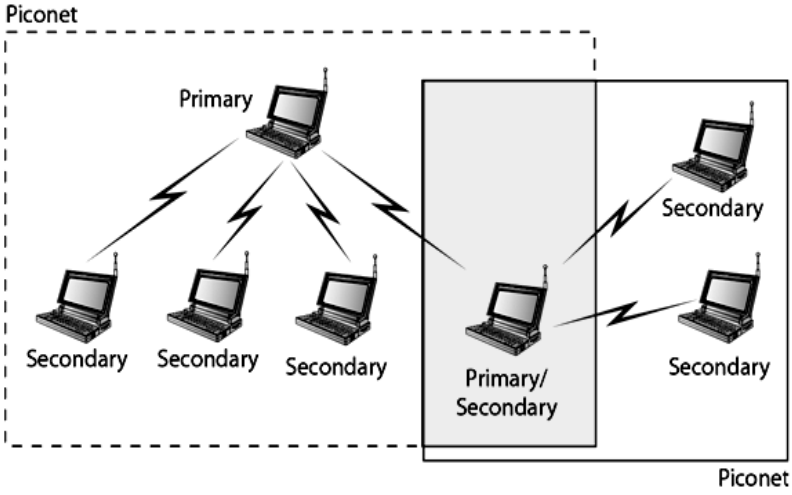


Figure2.56 Scatternet

9.2 BLUETOOTH LAYERS

Bluetooth uses several layers that do not exactly match those of the Internet model. Bluetooth devices are low-power and have a range 10 centimeters to 10 meters. Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

i. Radio Layer

- Roughly equivalent to physical layer of the Internet model. Physical links can be synchronous or asynchronous.
- Uses Frequency-hopping spread spectrum [Changing frequency of usage].
- Changes its modulation frequency 1600 times per second.

- Uses frequency shift keying (FSK) with Gaussian bandwidth filtering to transform bits to a signal.

ii. **Baseband layer**

- Roughly equivalent to MAC sublayer in LANs. Access is using Time Division (Time slots).
- Length of time slot = dwell time = 625 microsecond. So, during one frequency, a sender sends a frame to a slave, or a slave sends a frame to the master.
- Time division duplexing TDMA (TDD-TDMA) is a kind of half-duplex communication in which the slave and receiver send and receive data, but not at the same time (half-duplex).
- However, the communication for each direction uses different hops, like walkie-talkies.

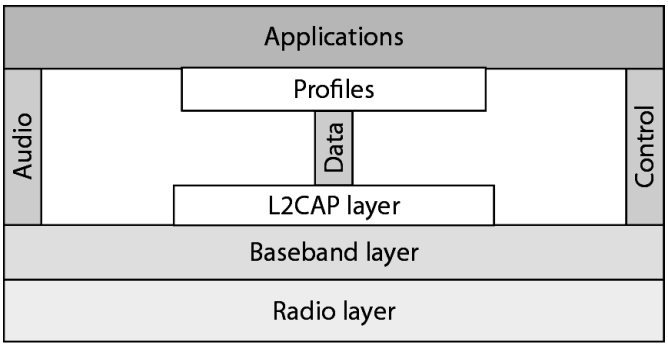


Figure 2.57 Blue tooth layers

9.2.1 Single-secondary communication

- Also called Single-slave communication
- If the piconet has only one secondary, the TDMA operation is very simple.
- The time is divided into slots of 625 micro seconds.

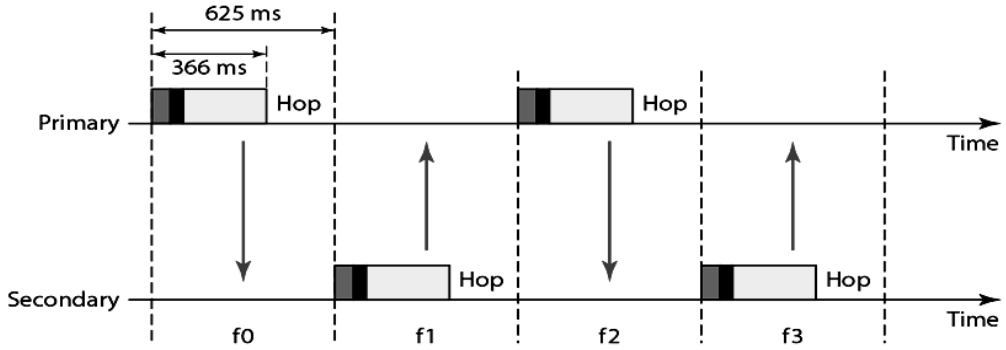


Figure 2.58 Single-secondary communications

- The primary uses even numbered slots (0, 2, 4 ...) and the secondary uses odd-numbered slots (1, 3, 5 ...).
- TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.
- In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives. The cycle is repeated.

9.3 MULTIPLE-SECONDARY COMMUNICATION

- Also called Multiple-slave communication (If there is more than one secondary in the piconet).

- ❖ Master uses even-numbered slots.
- ❖ Slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.
- ❖ The below figure 2.59 shows a multiple-secondary communication scenario.

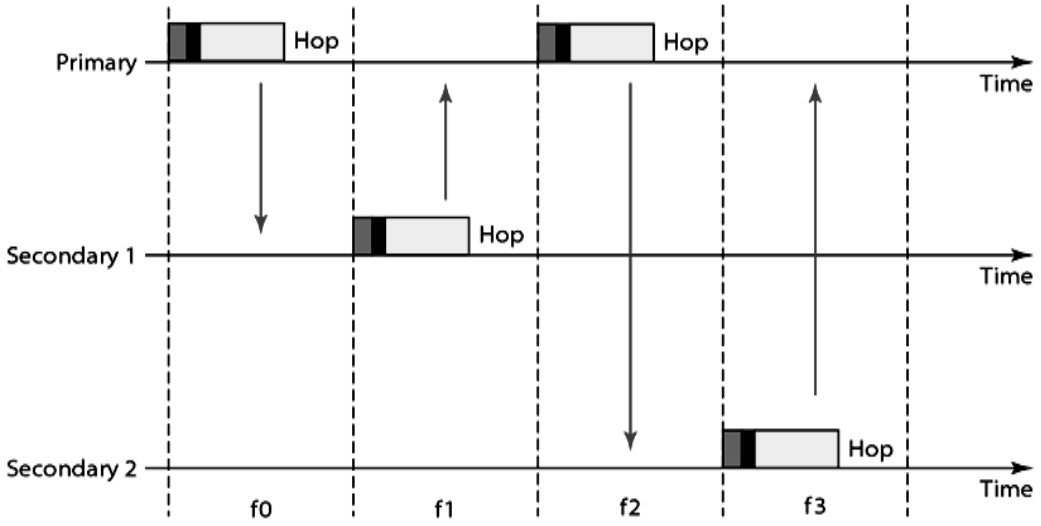


Figure 2.59 Multiple-secondary communications

Let us elaborate on the figure 2.59.

1) In slot 0, the primary sends a frame to secondary 1.
2) In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent.
3) In slot 2, the primary sends a frame to secondary 2.
4) In slot 3, only secondary 2 send a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent.
5) The cycle continues.
    - o We can say that this access method is similar to a poll/select operation with reservations.
    - o When the primary selects a secondary, it also polls it. The next time slot is reserved for the polled station to send its frame.
    - o If the polled secondary has no frame to send, the channel is silent.

9.4 PHYSICAL LINKS

Two types of links can be created between a primary and a secondary: SCQ links and ACL links. SCQ is used for real-time audio where avoiding delay is all-important. A secondary can create up to three SCQ links with the primary, sending digitized audio (PCM) at 64 kbps in each link.

i. Synchronous connection-oriented (SCQ)
    - Latency is important than integrity.
    - Transmission using slots.
    - No retransmission.

ii. Asynchronous connectionless link (ACL)
    - Integrity is important than latency.
    - Does like multiple-slave communication.

- Retransmission is done.

9.5 FRAME FORMAT

A frame in the baseband layer can be one of three types: one-slot, three-slot, or five-slot.

A slot, as we said before, is 625 micro seconds.

1) In a one-slot frame exchange, 259 micro seconds is needed for hopping and control mechanisms. The size of a one-slot frame is 366 (625 – 259) bits.
2) A three-slot frame occupies three slots. Since 259 micro seconds is used for hopping, the length of the frame is 3 x 625 - 259 = 1616 micro seconds or 1616 bits.
3) A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5 x 625 - 259 =2866 bits.

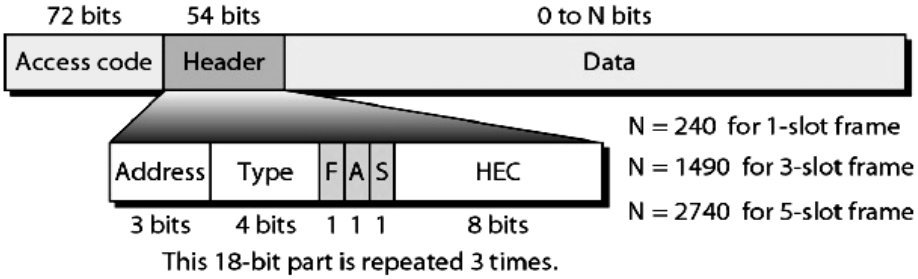


Figure 2.60 Format of the three frame types

The frame includes the following fields.

1) Access code: This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.
2) Header: This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
   i. Address: The 3-bit address subfield can define up to seven secondaries (l to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
   ii. Type: The 4-bit type subfield defines the type of data coming from the upper layers.
   iii. F: This 1-bit subfield is for flow control. If it is set to 1, it indicates that the device is unable to receive more frames (buffer is full).
   iv. A: This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.
   v. S: This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.
   vi. HEC: The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.
3) Payload: This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

9.6 L2CAP (Logical Link Control and Adaptation Protocol)

- Equivalent to LLC sublayer in LANs.

- Used for data exchange on ACL Link. SCQ channels do not use L2CAP.
- Frame format contains following three fields: Length, Channel ID, Data and Control.
- L2CAP can do Multiplexing, segmentation and Reassembly, QoS and group management.

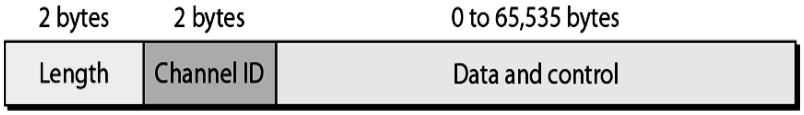


Figure 2.61 L2CAP data packet format