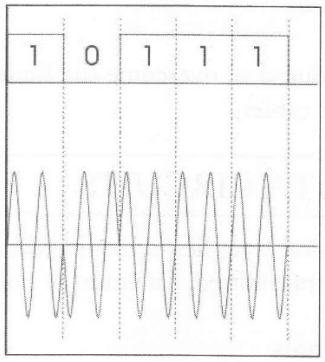


4.2.2 Analog Data to Digital Signal

The process is called digitization. Sampling frequency must be at least twice that of highest frequency present in the signal so that it may be fairly regenerated. Quantization - Max. And Min values of amplitude in the sample are noted. Depending on number of bits (say n) we use we divide the interval (min,max) into 2(^n) number of levels. The amplitude is then approximated to the nearest level by a 'n' bit integer. The digital signal thus consists of blocks of n bits. On reception the process is reversed to produce analog signal. But a lot of data can be lost if fewer bits are used or sampling frequency not so high.

Pulse Code Modulation (PCM): Here intervals are equally spaced. 8 bit PCB uses 256 different levels of amplitude. In non-linear encoding levels may be unequally spaced.

Delta Modulation (DM): Since successive samples do not differ very much we send the differences between previous and present sample. It requires fewer bits than in PCM.

4.3 BASEBAND AND BROADBAND TECHNOLOGIES

Baseband and Broadband transmissions are used to allocate the capacity of transmission media. In Baseband, the entire capacity of the mediumis devoted to one communication channel. Whereas Broadband allows two or more communication channels to share the bandwidth of the communications medium.

Baseband is the most commonly used mode of operation. For example Most LANs function in baseband mode. Baseband signaling can be processed with both analog and digital signals, although they have a great scope with broadband transmissions. Consider, for example, that the TV cable cominginto your house from an antenna or a cable provider is a broadband medium. The bandwidth of the cable is shared by many television signals as each signal is modulated using a separately assigned frequency. The television tune can be used to choose the channel that you want to watch by selecting its frequency.

This method of dividing bandwidth into frequency bands is called 'Frequency-division Multiplexing' (FDM). Another technique, called 'Time-division Multiplexing' (TDM), supports digital signals. FDM and works only with analog signals.

Baseband transmission uses digital signalling with Bi-directional transmission. It does not implement frequency-division multiplexing .Also its signal travels over short distances.

Broadband transmission Uses analog signaling with Unidirectional transmission. In broadband, Frequency-division multiplexing is possible. Also signal can travel over long distances before being attenuated.

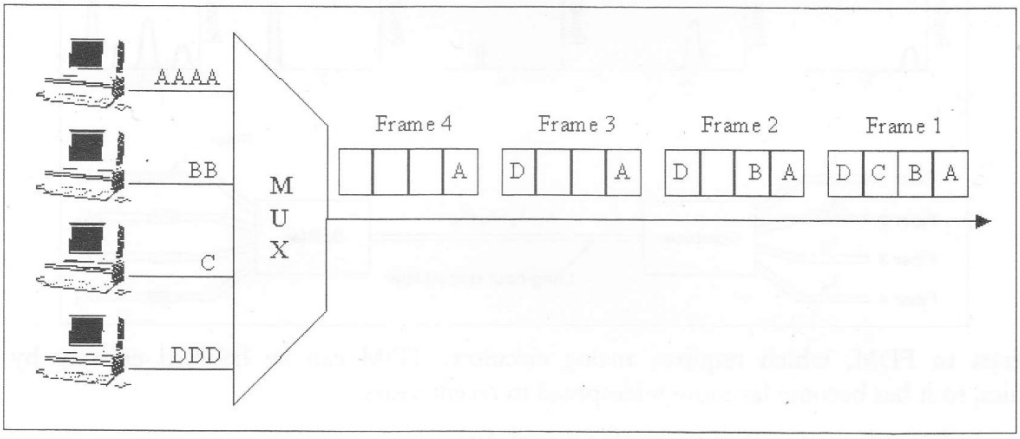
4.4 MULTIPLEXING

When two communicating nodes are connected through a media, it generally happens that bandwidth of media is several times greater than that of the communicating nodes. Transfer of a single signal at a time is both slow and expensive. The whole capacity of the link is not being utilized in this case. This link can be further exploited by sending several signals combined into one. This combining of signals into one is called multiplexing.

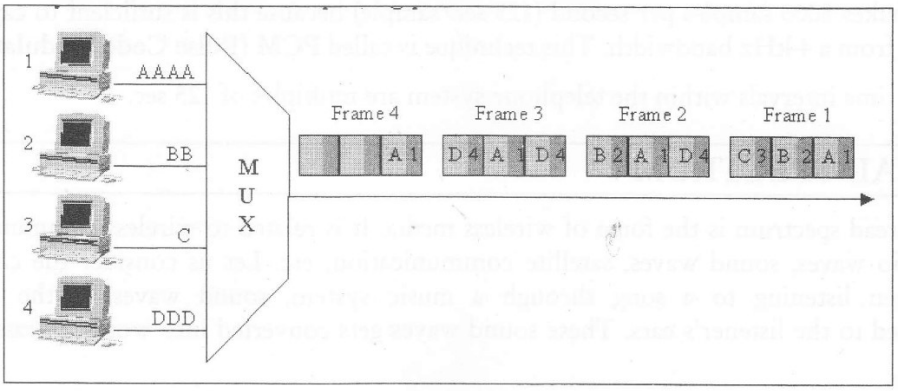
4.4.1 Time Division Multiplexing (TDM)

This is possible when data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted if each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

Synchronous TDM: Time slots are pre assigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle, or several turns per cycle, if it has a high data transfer rate, or may be once in a no. of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty. Synchronous TDM - multiplexing process in shown below:



Asynchronous TDM: In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission. Asynchronous TDM: multiplexing process is shown as following:



Physical channels are very valuable, so it is worthwhile to multiplex many logical channels over a single physical channel.

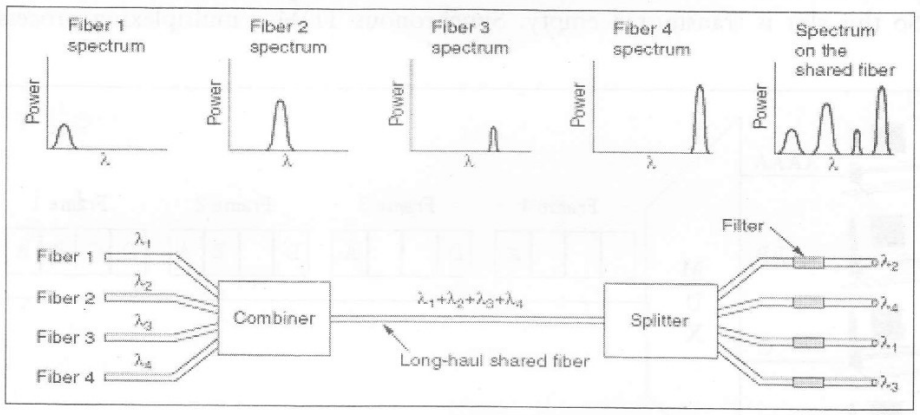
The users take turns (in round robin), each one periodically getting the entire bandwidth for a little burst of time.

An example: AM radio broadcasting system.

- The allocated spectrum is about 1 MHz (roughly 500 kHz - 1500 kHz).
- The allocated spectrum is divided into different portions, each for one station (FDM).
- Some stations may have two logical subchannels: music and advertising. These two alternate in time on the same frequency (TDM).

4.4.2 Wavelength Division Multiplexing

A simple way of achieving FDM on fibers is called WDM (Wavelength Division Multiplexing), as shown in Figure.



In contrast to FDM, which requires analog circuitry, TDM can be handled entirely by digital electronics, so it has become far more widespread in recent years.

TDM is mostly used in interoffice trunks for digital data.

Analog signals from the local loops can be digitized in the end office by a **codec** (coder-decoder), producing a 7- or 8- bit number.

The codec makes 8000 samples per second (125 sec/sample) because this is sufficient to capture all the information from a 4-kHz bandwidth. This technique is called **PCM (Pulse Code Modulation)**.

Virtually all time intervals within the telephone system are multiples of 125 sec.

4.5 SPREAD SPECTRUM

The term spread spectrum is the form of wireless media. It is related to wireless communication that includes radio waves, sound waves, satellite communication, etc. Let us consider the case of music system. When listening to a song through a music system, sound waves of the speaker are communicated to the listener's ears. These sound waves gets converted into words, phrases and tones

when they reach upon the eardrum of the listener. This process of conversion of the signals into human audition is termed as analog communication.

In general, spread spectrum is processed by some means of modulation. It involves narrow-band modulation schemes in which all of the power in a transmitted signal is confined to a very narrow portion of the frequency bandwidth. Amplitude Modulation (AM) is one example of a narrow-band modulation scheme in which two different voltage levels are used to represent 0 and 1, respectively.

A second popular form of modulation is Frequency Modulation (FM) in which two (or more) different tones are used. Spread spectrum is basically a set of modulation techniques.

There are three forms of spread spectrum modulation that are mentioned below:

- Direct Sequence
- Frequency Hopping,
- A third hybrid form of the two above which does exist in practice.

Direct Sequence is that form of spread spectrum in which a noise generator creates a high-speed noise code sequence. While direct sequence is a very popular form of spread spectrum transmission, there exists another method also. Another popular from of processing spread spectrum is Frequency Hopping.

Frequency Hopping is a form of spread spectrum in which spreading occurs by hopping from frequency to frequency over a wide band. The specific order in which the hopping takes place is determined by a hopping table which is generated with the help of a pseudo-random code sequence.

Check Your Progress

1. What is Modem?
2. What is Multiplexing?

4.6 LET US SUM UP

Long distance communication is done through modulation that includes amplitude modulation, frequency modulation and phase modulation. A modem (modulator-demodulator) is a device which accepts a serial stream of bits as input and produces a modulated signal as output (or vice versa). Leased analog data circuits involves moving data in the form of electromagnetic signals across a transmission medium. Data must be transformed to electromagnetic signals to get transmitted.

We have discussed baseband and broadband technologies that used to allocate the capacity of transmission media. Multiplexing includes FDM, TDM, and WDM which leads to combining of signals. Spread spectrum is the form of wireless media which is processed by some means of modulation that include AM modulation and FM modulation.

4.7 KEYWORDS

Modem: A device which accepts a serial stream of bits as input and produces a modulated signal as output (or vice versa).

Amplitude Shift Keying (ASK): A form of modulation, which represents digital data as variations in the amplitude of a carrier wave.

Frequency Shift Keying (FSK): The change in frequency defines different digits.

Phase Shift Keying (PSK): The phase of the carrier is discretely varied in relation either to a reference phase.

FDM: A number of signals can be transmitted at the same time.

TDM: Data transmission rate of the media is much higher than that of the data rate of the source.

4.8 QUESTIONS FOR DISCUSSION

1. Discuss the process of sending long signals through modulation. Also define the specific standards.
2. What is Spread Spectrum?
3. Discuss the process of converting digital data into analog data and vice versa.
4. Differentiate between Wavelength Division Multiplexing and Time Division Multiplexing.
5. Discuss Baseband and Broadband Technologies.
6. What is FDM? How is it used to multiplex many logical channels over a single physical channel?
7. What are the different standards that are used as error correction built into the modems?

Check Your Progress: Model Answers

1. A modem (modulator-demodulator) is a device which accepts a serial stream of bits as input and produces a modulated signal as output (or vice versa).
2. When two communicating nodes are connected through a media, it generally happens that bandwidth of media is several times greater than that of the communicating nodes. Transfer of a single signal at a time is both slow and expensive. This combining of signals into one is called multiplexing.

4.9 SUGGESTED READING

Anuranjan Misra, *Computer Networks*, Acme Learning Pvt. Ltd. Publications

UNIT III

LESSON

5

PACKET TRANSMISSION

CONTENTS

5.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Discuss frames in detail
- Know byte stuffing and bit stuffing
- Discuss types of error control
- Explain error detection mechanisms
- Discuss frame formats

5.1 INTRODUCTION

The Data Link Layer which is the second layer in the OSI model, above the Physical Layer, ensures that the error free data is transferred between the adjacent nodes in the network. It breaks the datagrams passed down by above layers and convert them into **frames or packets** ready for transfer. This is called Framing. It provides two main functionalities:

- Reliable data transfer service between two peer network layers.
- Flow Control mechanism which regulates the flow of frames such that data congestion is not there at slow receivers due to fast senders.

The data link layer receives a raw bit stream from the physical layer that may not be error free. To provide a reliable transfer of bit streams to the network layer the data link layer breaks the bit stream into frames. It then computes the checksum for each frame, which is transmitted with the frame. The destination host receives a frame and computes another checksum from its data to compare with the transmitted frame. This ensures the data link layer of the receiver to detect and correct frames. However, some of the checksum method does not provide correction.

Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is upto the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters. The four framing methods that are widely used, also known as frame identification methods, are discussed below.

5.2 FRAME IDENTIFICATION METHODS

1. Character count
2. Starting and ending characters, with character stuffing
3. Starting and ending flags, with bit stuffing
4. Physical layer coding violations

Character Count

This method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count,it knows how many characters follow, and hence where the end of the frame is. The disadvantage is that if the count is garbled by a transmission error, the destination will lose synchronization and will be unable to locate the start of the next frame. So, this method is rarely used.

Character Stuffing or Byte Stuffing

In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX.(where DLE is Data Link Escape, STX is Start of TeXt and ETX is End of TeXt.) This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization, it only has to look for DLE STX and DLE ETX characters. If however, binary data is being transmitted then there exists a possibility of the characters DLE STX and DLE ETX occurring in the data. Since this can interfere with the framing, a technique called character stuffing is

used. The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data. The receiver's data link layer removes this DLE before this data is given to the network layer. However character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

Bit Stuffing

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110 .

Physical Layer Coding Violations

The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

5.3 TRANSMISSION ERRORS

5.3.1 Error Control and Error Detection

It involves sequencing frames and sending control frames for acknowledgement. A noisy channel may cause flipping of bits, losing bits from a frame, introducing new bits in the frame, frames completely disappearing, etc during communication. For reliable communication, the destination host sends positive or negative acknowledgements accordingly to the source host within a specified time limit. The source host has a timeout to resend the frame again if it does not receive an acknowledgement in a given time period from destination host. Also, each outgoing frame is assigned a sequence number to prevent the destination host data link layer from passing the same frame more than once to the network layer. This entire affair is an integral part of data link layer design.

The bit stream transmitted by the physical layer is not guaranteed to be error free. The data link layer is responsible for error detection and correction. The most common error control method is to compute and append some form of a checksum to each outgoing frame at the sender's data link layer and to recompute the checksum and verify it with the received checksum at the receiver's side. If both of them match, then the frame is correctly received; else it is erroneous. The checksums may be of two types:

1. ***Error detecting:*** Receiver can only detect the error in the frame and inform the sender about it.
2. ***Error detecting and correcting:*** The receiver can not only detect the error but also correct it.

5.3.2 Probability, Mathematics and Error Detection

The error function also occurs in mathematics which is also known as Gauss error function. It is a special kind of function having sigmoid shape that occurs in statistics, probability, partial differential equations, etc.

5.3.3 Types of Error Control

Whenever an electromagnetic signal flows from one point to another, its is subject to unpredictable interference from heat, magnetism, and other forms of electricity. This interference can change the

shape or timing of the signal. If the signal is carrying encoded binary data, such changes can alter the meanings of the data. In a single-bit error, a O is changed to a 1 or a 0. In a burst error, multiple bits are changed. For example, a 0.01 second burst of impulse noise on a transmission with a data rate of 1200 bps might change all or some of 12 bits of information.

The types of error are follows:

1. ***Single-Bit-Error:*** The term single-bit error means that only bit of a given data unit (such as a byte, character, data unit, or packet) is changed from 1 to 0 or from 0 to 1. Single-bit errors are the least likely type of error in serial data transmission. To see why, imagine a sender sends data at 1 Mbps. This means that each bit lasts only 1/1,000,000 second, or 1 us. For a single-bit error to occur, the noise must have a duration of only 1 us, which is very rare; noise normally lasts much longer that this. However, a single-bit error can happen if we are sending data, using parallel transmission. For example, if eight wires is noisy, one bit can be corrupted in each byte. Think of parallel transmission inside a computer, between CPU and memory, for example.
2. ***Burst Error:*** The term **burst error** means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1. Figure 5.1 shows the effect of a burst error on a data unit. In this case, 0100010001000011 was sent, but 0101110101000011 was receiver. Note that a burst error does not necessarily mean that the errors occur in consecutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some of them have not been corrupted. Burst error is most likely to happen in a serial transmission. The duration of noise is normally longer than the duration of a bit, which means that when noise affects data, it effects a set of bits. The number of bits affected depends on the data rate and duration of noise. For example, if we are sending data at 1 Kbps, a noise of 1/100 seconds can affect 10 bits; if we are sending data at 1 Mbps, the same noise can affect 10,000 bits.

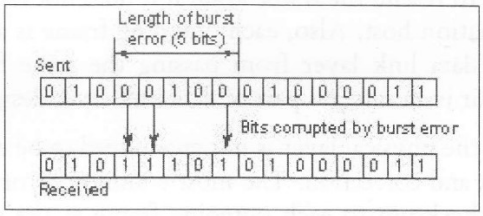


Figure 5.1: Burst Error of Length Five

5.4 FRAME FORMATS: BUILDING BLOCKS

Data link protocols regulate communication flow between various computers. A wide variety of computers and communication technologies are used to carry out useful tasks. These include mainframe computers, local area networks, workstations, personal computers, and proprietary and standards based networking platforms. All of these products are not interoperable and it is not easy to exchange data across different systems and applications. Therefore, standards were developed to ensure the interrelationship of many different standards adopted by various vendors. To establish a meaningful session, a certain sets of rules need to be adopted by vendors of networking device.

Some of the examples of data link protocol are High Level Data Link Control (HDLC) protocol and Point-to-Point Protocol (PPP). The discussion here of the simpler HDLC and PPP protocols will

explore many of the most important features of data link protocols. HDLC and PPP frame formats are discussed below:

5.4.1 High-level Data Link Control (HDLC)

HDLC procedure is standardized by ISO. This is suitable for high-speed transmission of large amounts of data, something the basic control procedure cannot provide. HDLC procedure has been standardized based on the SDLC. In addition to characters, bit strings of a desired length can also be transmitted through this procedure. The unit of data transmission is called a frame. With the basic control procedure, receipt of data is checked after multiple frames are sent for improved transmission efficiency. It also offers a form of advanced error control called CRC (Cyclic Redundancy Check).

The advantage of this procedure is that the sending equipment can send multiple blocks of data at one time for improved transmission efficiency. As the receiving equipment must inform the sending equipment how much data has been received, therefore, it is necessary to attach a sequence number to each piece of data.

The unit of data transmission is called a frame. The frame format of HDLC is depicted in Figure 5.2. Each frame has a 01111110 bit pattern, called a flag, at its beginning and end. That is, HDLC procedure uses a flag synchronous system.

(1) Bit order of transmission (Information Frame)

Flag	Address	Control	Information	FCS	Flag
F	A	C	I	FCS	F
0111110	8 Bits	8 Bits	N Bits	16 Bits	01111110

(2) Bit order of Transmission (Supervisory Frame)

Flag	Address	Control	FCS	Flag
F	A	C	FCS	F
0111110	8 Bits	8 Bits	16 Bits	01111110

Figure 5.2: HDLC Frame Format

In addition to these two flags, a frame consists of the following fields:

- *Address field:* This indicates the destination or source address of a frame.
- *Control fields:* This indicates the command or response addressed to remote equipment. The sequence number mentioned earlier is also included.
- *Information field:* This contains message.
- *FCS (Frame Check Sequence):* This is 16 bit sequence for error control.

The frame format given in (2) of Figure 5.2 is for response only and does not include any information field. As the control field holding control information and the information field holding information are clearly separated, any types of codes can be sent through the HDLC procedure. Also data sequence

numbers are included in the control field, consecutive data blocks (frame) can be sent without checking receipt of each data block.

The nice thing about standards is that you have so many to choose from. At the data link layer, we have the choices of IBM SDLC (Synchronous Data Link Control), ANSI ADCCP (Advanced Data Communication Control Procedure), ISO HDLC (High-level Data Link Control), CCITT LAP (Link Access Procedure), etc. If you do not like any of them, you can just wait for next year's model. All are bit-oriented and using bit stuffing. The frame is delimited with flag sequence 01111110. Address can be used to identify a terminal on multidrop lines or to distinguish commands from responses for point-to-point lines. Control is used for sequence numbers, acknowledgements, and others. Data can be arbitrarily long. Checksum uses CRC-CCITT. Three kinds of frames distinguished by the control field. The protocol uses a sliding window, with a 3-bit sequence number (Seq) and allows up to seven outstanding frames. Next contains a piggybacked ACK (the next frame expected).

Types of supervisory frames:

1. *Type 0:* an ACK frame (RECEIVE READY).
2. *Type 1:* an NAK frame (REJECT). The sender is required to retransmit all outstanding frames starting at Next.
3. *Type 2:* RECEIVE NOT READY. The sender is required to temporarily stop until other control frames arrive from the receiver.
4. *Type 3:* SELECTIVE REJECT. Retransmission of the frame specified.

Condition: the sender's window size must be half (or less) the sequence space size. Unnumbered frames are used for various control purposes (network management): disconnect a machine (DISC), reset sequence numbers (SNRM), report semantically wrong frames (FRMR), acknowledge control frames (UA), etc.

5.4.2 Point-to-Point Protocol (PPP)

PPP is for a dialup link from residential hosts. Hence, it is one of the most widely deployed data link protocols. The Point-to-Point Protocol is a data link layer protocol and operates over a point-to-point link that connects two communicating link-level peers at each end of the link. This link may be a serial dialup telephone line, a SONET/SDH link, an X.25 connection, an ISDN circuit, etc. The PPP frame comprises of the following fields:

- *Flag Field:* PPP frame begins and ends with a 1-byte flag field with a value of 01111110.
- *Address Field:* It has only one possible value as 11111111.
- *Control Field:* This field has one value as 00000011.
- *Protocol:* The protocol field indicates the upper layer protocol to which the received encapsulated data belongs. When a PPP frame is received, the PPP receiver will check the frame for correctness and then pass the encapsulated data. A 16-bit protocol codes is used by PPP.
- *Information:* This field contains the encapsulate packet that is forwarded by an upper layer protocol over the PPP link. The default maximum length of the information field is 1500 bytes.
- *Checksum:* The checksum field detects bit errors in a transmitted frame.

Figure 5.3 depicts a PPP data frame using HDLC like framing.

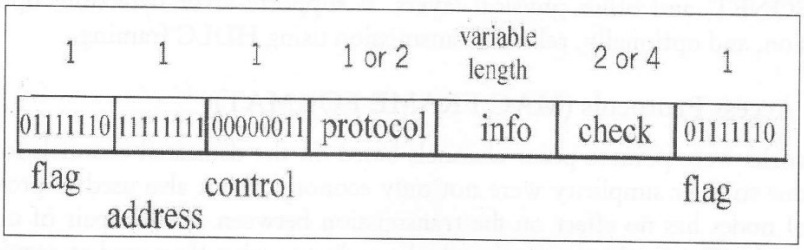


Figure 5.3: PPP Data Frame

PPP is an official Internet Standard protocol which provides three things:

(a) A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.

(b) A link control protocol for bringing lines up, testing them, negotiating options, and bringing them down again gracefully when they are no longer needed. This protocol is called **LCP** (Link Control Protocol).

(c) A way to negotiate network-layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different **NCP** (Network Control Protocol) for each network layer supported.

A typical scenario of a home user calling up an Internet service provider to make a home PC a temporary Internet host:

Physical connection setup phase:

(i) The PC calls the provider's router via a modem.

(ii) The router's modem answers the phone and establishes a physical connection.

Data link layer options negotiation phase: The PC sends the router a series of LCP packets in the payload field of one or more PPP frames. These packets and their responses select the PPP parameters to be used.

Network layer options negotiation phase: A series of NCP packets are sent to configure the network layer and to assign an IP address for the PC (if the PC wants to run a TCP/IP protocol stack).

Data communication phase: The PC sends and receives IP packets over the established connection.

Connection release phase:

(i) When the PC is finished, NCP is used to tear down the network layer connection and free up the IP address.

(ii) The LCP is used to shut down the data line layer connection.

The computer tells the modem to hang up the phone, releasing the physical connection. The phases that a line goes through when it is brought up, used, and taken down again. The PPP frame was chosen to closely resemble the HDLC frame.

In summary, PPP is a multiprotocol framing mechanism suitable for use over modems, HDLC bit-serial lines, SONET, and other physical layers. It supports error detection, option negotiation, header compression, and optionally, reliable transmission using HDLC framing.

5.4.3 Multiple Access Protocols (MAC FRAME FORMAT)

Traditional networks were point-to-point channels based on the dedicated channels for a pair of users. These channels due to their simplicity were not only economical but also used to provide transmission between a pair of nodes has no effect on the transmission between another pair of nodes even if they have a common node. The disadvantages of such channels were that they used to require fixed topology and enormous number of dedicated connections between a pair of channels thus imposing a challenge to design maintenance and cost effectiveness. Instead, broadcast channels began to use in which more than a single receiver can receive every transmitted message. The broadcast channels were good when a message is destined to a large number of destinations than a single or a very small number of destinations because it incurred wasteful processing results in all switches in which the message is not intended. The transmissions over a broadcast channel were also prone to interfere with another transmission.Thus, the transmission between a pair of nodes was no longer independent of other transmissions. To avoid such interference, a transmission control mechanism is required. Such transmission control mechanism known as multiple access protocol determines the access to shared channels in which allocation of shared resources are critical for desirable performance characteristics and proper operation of the network. These multiple access protocols are channel allocation schemes and they reside mostly in a specid layer called the Medium Access Control (MAC) layer within the data link layer of the OSI model.

Multiple Access Protocols Classification

There are numerous multiple access protocols. One of them is non-centralized multiple access protocols in which all hosts perform based on the same rules and no single host is allowed to coordinate the activities of the others. This also does not include polling type access protocols. Broadly, they are classified as conflict free and contention protocols.

- *Conflict Free Protocols:* They ensure successful transmission each time without interfering with another transmission. This further divided into static or dynamic conflict free protocols in which hosts communicate with channel allocation statically or dynamically.
- *Static Channel Allocation:* The channel resources in static conflict free schemes depend on time, frequency or mixed time-frequency. The channels are divided based on the frequency range (bandwidth) to a single host for a fraction of the time as in Time Division Multiple Access (TDMA) or giving a fraction of the frequency range to every host all of the time as in Frequency Division Multiple Access (FDMA) or providing every host a portion of the bandwidth for a fraction of the time as in Code Division Multiple Access (CDMA).
- *Dynamic Dhannel Allocation:* The dynamic channel allocation considers channel allocations based on demand so that optimum uses of channel may be ensured. The hosts who demand only little use of channel but keep the channel idle for most of the time within their allocated share in static allocation may leave the channel resources for more active hosts. It may further be classified into reservation and token passing scheme.
- *Reservation Scheme:* The hosts first announce their intent to transmit in the dynamic channel allocation by various reservation schemes and reserve their right to transmit before new hosts obtain a chance to announce their intent to transmit.

- *Token Passing Scheme:* A single token either in logical or physical form is circulated among the hosts for allowing the host to transmit who possesses the token so that interferences between transmissions of other hosts could b avoided.
- *Contention Schemes:* Unlike the conflict free schemes, a transmitting host is not guaranteed to be successful in contention schemes. The protocol must be embedded with some resolution processes to resolve conflicts when they happen so that all hosts could transmit successfully. The different resolution protocols build up the contention schemes. In contention schemes, idle hosts do not transmit and thus do not consume the channel resources.
- *Static Resolution:* It refers to the right of the first host to transmit when a conflict happens. It is also based on probability in which the transmission schedule for the interfering hosts is chosen from a fixed distribution that is independent of the actual number of interfering hosts. Examples are Aloha type protocols and the various versions of Carrier Sense Multiple Access (CSMA) protocols.
- *Dynamic Resolution:* It determines the highest priority or lowest priority to a packet based on the time of arrival in the system. The resolution can also be probabilistic. Some of the protocols based on this scheme are the multiplicity of the interfering packets and the exponential back-off scheme of the Ethernet.

5.5 ERROR DETECTION TECHNIQUES

One error detection mechanism that would satisfy these requirements would be to send every data unit twice. The receiving device would then be able to do a bit-for-bit comparison between the two versions of the data. Any discrepancy would indicate an error, and an appropriate correction mechanism could be set in place. This system would be completely accurate (the odds of errors being introduced into exactly the same bits in both sets of data are infinitesimally small), but it would also be insupportably slow. Not only would the transmission time double, but the time it takes to compare every unit bit by bit must be added. The concept of including extra information in the transmission solely for the purposes of comparison is a good one. But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called *redundancy* because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

Four types of redundancy checks are used in data communication: Vertical Redundancy Check (VRC) (also called parity check), Longitudinal Redundancy Check (LRC), Cyclical Redundancy Check (CRC), and checksum. The first three, VRC, LRC and CRC are normally implemented in the physical layer for use in the data link layer. The fourth, checksum, is used primarily by upper layers. These are the various error detection techniques which are describe in subsequent sections.

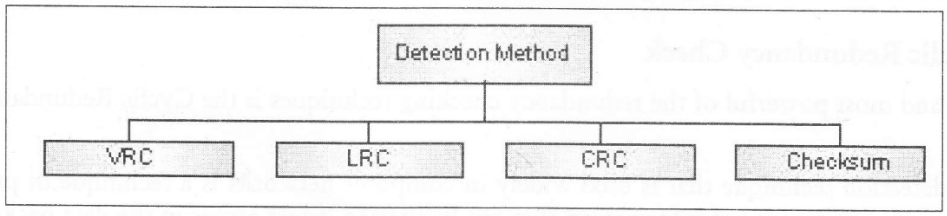


Figure 5.4: Detection Methods

5.5.1 Vertical Redundancy Check

The most common and least expensive mechanism for error detection is the Vertical Redundancy Check (VCR), often called a parity check. In this technique, a redundant bit, called a parity bit, is appended to every data unit so that the total number of bit is in the unit (including the parity bit) becomes even. number of bit is in the unit (including the parity bit) becomes even. Suppose we want to transmit the binary data unit 1100001. Adding together the number of 1s gives us 3, an odd number. Before transmitting, we pass the data unit through a parity generator. The parity generator counts the 1st and appends the parity bit (a 1 in this case) to the end. The total number of is now four, an even number. The section now transmits the entire expended unit across the network link. When it reaches its destination, the receiver puts all the eight bits through an even-parity checking function. If the receiver sees 11100001, it counts for 1st, an even number, and the data unit passes. But what if the data unit has been damaged in transit? What if, instead of 11100001, the receiver sees 11100101? The receiver known that an error has been introduced into the data somewhere and therefore rejects the whole unit. Note that for the sake of simplicity, we are discussing here even-parity checking, where the number of 1s should be an even number. Some system may use odd-parity checking, where the number of 1s should be odd. The principle is the same; the calculation is different.

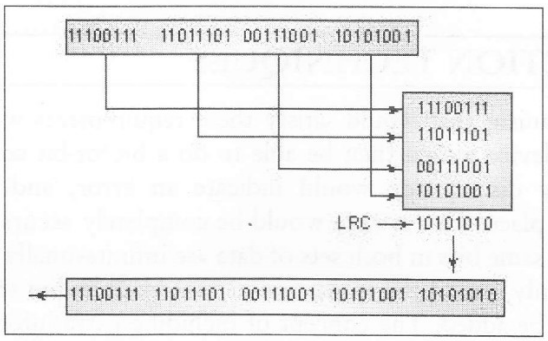


Figure 5.5: Original Data Plus LRC

5.5.2 Longitudinal Redundancy Check

In Longitudinal Redundancy Check (LRC), a block of bits is organized in a table (rows and columns). For example, instead of sending a block of 32 bits, we organize them in a table made of four rows and eight columns, as shown in figure. We then calculate the parity bit for each column and create a new row of eight bits, which are the parity bits for the whole block. Note that the first parity bit in the fifth row is calculated based on all first bits. The second parity bit is calculated based on all second bits, and so on. We then attach the eight parity bits to the send them to the receiver.

5.5.3 Cyclic Redundancy Check

The third and most powerful of the redundancy checking techniques is the Cyclic Redundancy Check (CRC).

An error detection technique that is used widely in computer networks is a technique of providing a data string added to packets of information that can be used to detect errors in the data packets. In the OSI or TCP/IP network models, CRC is added to a packet frame at the Data Link Layer. It is a method of checking for errors in data that has been transmitted on a communications link.

The data integrity of a received frame or packet is checked via a polynomial algorithm based on the content of the frame, and then matched with the result that is performed by the sender and included in a (most often 16-bit) field appended to the frame. Hence, CRC codes are also called as polynomial codes. It uses a dividend polynomial, which is initially preset to 0, and the 1s and 0s of the data stream become the coefficients of the dividend polynomial. The division uses subtraction modulo 2 (no carries), and the remainder is transmitted as the error check field. The receiving station compares the transmitted remainder with its own computed remainder, and an equal condition indicates that no error has occurred. The polynomial value depends on the protocol and code set being used.

While writing a data on disk or transmitting a data across a network, sometimes very minor error of 1 bit occurs, which however may prove hazardous. In this method an algorithm calculates the binary values in a packet or other block of data and stores the results with the data. When the data is retrieved from memory or received at the other end of a network, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error. However, a match does not necessarily mean the absence of errors, but only that the simple algorithm was not able to detect any.

For example, a data stream consisting of d bits can be represented as a sequence of k-bit integers. The k bit integers may be summed up and the result can be considered for the error detection bits. A destination host calculates the checksum over the received data and checks whether it matches the checksum carried in the received frame. This technique fails in case of reordering of the bytes, inserting or deleting zero-valued bytes and multiple errors that cancel each other out. We therefore need more advanced algorithm to take care of the above errors. One of these techniques is Cyclic Redundancy Check (CRC).

Unlike VRC and LRC, instead of adding bits together to achieve a desired parity, a sequence of redundant bits, called the CRC and CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be intact and is therefore accepted. A remainder indicated that the data unit has been damaged in transit and therefore must be rejected. The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor, the remainder is the CRC. To be valid, a CRC must have two qualities: it must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequency exactly divisible by the divisor. Both the theory and the application of CRC error detection are straightforward. The only complexity is a deriving the CRC. In order to clarify this process, we will start with an overview and add complexity as we go. Figure 5.6 below provides an outline of the three basic steps.

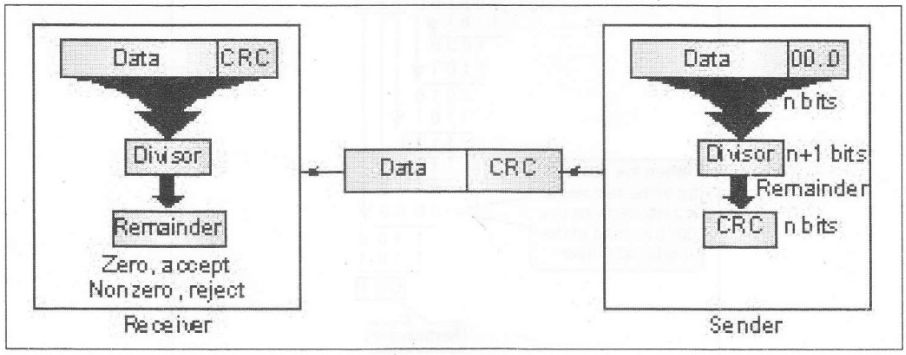


Figure 5.6

- First, a string of numbers is appended to the data unit. The number *n* is one less than the number of bits in the predetermined divisor, which is n + 1 bit.
- Second, the newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC.
- Third, the CRC of n bits derived in step 2 replaces the appended 0s at the end of the data unit. Note that the CRC may consist of all 0s. The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder. If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes. If the string has been changed in transist, the division yields a non-zero remainder and the data unit does not pass.

CRC Generator

A CRC generator used modulo-2 division, Figure 5.7 shows the process. In the first step, the four-bit divisor is subtracted from the first four bits of the dividend. Each bit of the divisor is subtracted from the corresponding bit of the dividend without disturbing the next higher bit. In our example, the divisor, 1101, is subtracted from the first four bits of the dividend, 1101. Yielding 1001. Yielding 100 (the leading 0 of the remainder is dropped off). The next unused bit from the dividend is then pulled down to make the number of bits in the remainder equal to the number of bits in the divisor. The next step, therfore, is 1000-1101, which yields 101, and so on. In this process, the divisor always begins with a 1; the divisor is subtracted from a portion of the previous dividend/remainder that is equal to it in length; the divisor can only be subtracted from a string of 0s, of the same length as the divisor, replaces the divisor in that step of the process. For string of 0s, of the same length as the divisor, replaces the divisor in that step of the process. For example, if the divisor is four bits long, it is replaced by four 0s. (Remember, we are dealing with bit patterns, not with quantitative values; 0000 is not the same as 0). This restriction means that, at any step, the leftmost subtraction will be either 0 - 0 or 1 - 1, both of which equal 0. So, after subtraction, the leftmost bit of the remainder. Note that only the first bit of the remainder is dropped- if the second bit is also 0. It is retained, and the dividend/remainder for the next step will begin with 0. This process repeats units the entire dividend has been used.

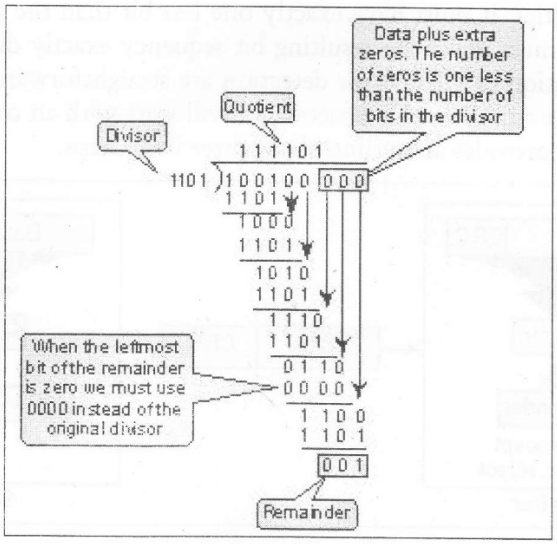


Figure 5.7: CRC Remainder

Check Your Progress

1. What is Byte stuffing?
2. What is CRC generator?

5.6 LET US SUM UP

Data link layer describes the techniques to access a shared communication channel and reliable data transmission. Its main tasks are framing, checksums, error detection and correction, acknowledgement, flow control, encapsulating packets from network layer to frames etc. There are many different types of link-level technologies that can be used to connect two nodes or machines. Examples of link-layer protocols are token ring, FDLC, and PPP. The data link layer provides unacknowledged connectionless service, acknowledged connectionless service and acknowledged connection-oriented service. Parity check is the simplest form of error detection method as the receiver needs to count only the number of 1's in the received data stream with additional parity bit. Checksum is a simple type of redundancy check used to detect errors in data. Cyclic Redundancy Check is used widely in computer networks, is a technique of providing a data string added to packets of information that can be used to detect errors in the data packets. Go Back N protocol needs buffer maintenance and therefore, is complicated to keep source and destination machines in synchronization. It is also considered the most inefficient because it retransmits all subsequent frames on the loss of a frame and thus incurs huge wastage of bandwidth. Selective Repeat is an improvement on Go Back N protocol and tries for more efficient use of bandwidth by reducing the number of retransmissions because it retransmits only one frame instead of the entire series. PPP and HDLC are widely used data link protocols.

5.7 KEYWORDS

Checksum: Error detecting scheme which overcomes the problem of two erroneous bits.

Cyclic Redundancy Check (CRC): An error detection technique that is used widely in computer networks is a technique of providing a data string added to packets of information that can be used to detect errors in the data packets.

Framing: It breaks the datagrams passed down by above layers and convert them into frames or packets ready for transfer.

LRC: A block of bits is organized in a table (rows and columns).

High-level Data Link Control (HDLC): It is suitable for high-speed transmission of large amounts of data, something the basic control procedure cannot provide.

Parity Checks: The parity bit is chosen that the number of 1 bits in the code word is either even(for even parity) or odd (for odd parity).

Point-to-Point Protocol (PPP): A data link layer protocol and operates over a point-to-point link that connects two communicating link-level peers at each end of the link.

5.8 QUESTIONS FOR DISCUSSION

1. What is Framing? Discuss Frame identification methods.
2. Discuss error control classification.
3. What is burst error? How is it different from single-bit error?
4. Explain how Cyclic Redundancy Check works while checking errors in data.
5. What are different data link protocols available? Why does PPP have become popular?
6. Explain MAC Frame format. Discuss its classification.

Check Your Progress: Model Answers

1. Each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX.(where DLE is Data Link Escape, STX is Start of TeXt and ETX is End of TeXt.)
2. The four-bit divisor is subtracted from the first four bits of the dividend. Each bit of the divisor is subtracted from the corresponding bit of the dividend without disturbing the next higher bit.

5.9 SUGGESTED READING

Anuranjan Misra, *Computer Networks*, Acme Learning Pvt Ltd Publications

Rajneesh Agrawal and Bhata Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill, Osborne Media

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

J.D. Spragins, *Telecommunications protocols and design*, Addison-Wesley, Reading MA

LESSON

6

LAN TECHNOLOGIES

CONTENTS

6.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Discuss LAN topologies
- Understand logical link layer
- Discuss ethernet technologies
- Know the working of CSMA/CD protocol
- Discuss IEEE 802.4 token bus with frame format
- Discuss IEEE 802.5 token ring with frame format

- Understand ATM concept
- Discuss broadcasting and multicasting

6.1 INTRODUCTION

Local Area Networks (LANs) are most often described as privately owned networks that offer reliable high speed communication channels optimized for connecting information processing equipment in a limited geographical area, namely, an office, building, complex of buildings, or campus.

A LAN is a form of local (limited-distance), shared packet network for computer communications. LANs interconnect computers and peripherals over a common medium in order that users might share access to host computers, databases, files, applications, and peripherals. They can also provide a connection to other networks either through a computer, which is attached to both networks, or through a dedicated device called a gateway. The main users of LANs include business organizations, research and development groups in science and engineering, industry, educational institutions. The electronic or paperless office concept is possible with LANs.

6.2 LAN TECHNOLOGIES

LANs offer raw bandwidth of 1 Mbps to 100 Mbps or more, although actual throughput often is much less. LANs are limited to a maximum distance of only a few miles or kilometres, although they may be extended through the use of bridges, routers, and other devices. Data is transmitted in packet format, with packet sizes ranging up to 1500 bytes and more. Mostly, IEEE develops LAN specifications, although ANSI and other standards bodies are also involved.

The shared medium for LANs includes most of the transmission media discussed previously. Although coaxial cable was the original medium and is still used widely in various configurations, twisted-pair has recently become the medium of choice in many environments. Fibre optic cable is used widely as a backbone technology. Wireless LANs generally are limited to special radio technologies, although infrared technology is used in certain applications. Microwave and infrared systems are used to connect LANs and LAN segments in a campus environment. Satellite is rarely used in any way, as propagation delay renders it generally unsatisfactory for interactive communications. Along with various technologies, we will also consider the associated hardware required to connect a computer to a network and the details of the transmitting and receiving packets.

IEEE Standards for Local Area Networks

IEEE 802 standards with its member standards deals with the Physical and Data Link layers as defined by OSI Reference Model. The relationship between the standard and other members of the IEEE 802 are given below:

- 802.1 - Introduction, Interface primitives, etc.
- 802.2 - Logical Link Control (LLC)
- 802.3 - CSMA/CD – Ethernet
- 802.4 Token Bus
- 802.5 Token Ring
- 802.6 Distributed Queue Dual Bus

The LAN technologies include types of LAN topologies, Ethernet, ATM (Asynchronous Transfer Mode), token ring, wireless and segmentation.

6.2.1 LAN Topologies

A network topology is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected. A network's topology is comparable to the blueprints of a new home in which components such as the electrical system, heating and air conditioning system, and plumbing are integrated into the overall design. Taken from the Greek work "Topos" meaning "Place," Topology, in relation to networking, describes the configuration of the network; including the location of the workstations and wiring connections. Basically it provides a definition of the components of a Local Area Network (LAN). A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance.

A network topology comprises of all sorts of physical, logical or virtual components put together in order to implement LAN. There are fundamentally three topologies, which are given below. All the others are combinations of these three fundamental topologies.

Bus Topology

The simplest and one of the most common of all topologies, Bus consists of a single cable, called a Backbone that connects all workstations on the network using a single line. All devices on network are attached to a single cable in a bus topology LAN, as shown in Figure 6.1. This provides only half-duplex operations between a station and a bus. The frame, which is transmitted from one node to another, contains only the address of the intended destination. If it gets lost, it cannot be retrieved. Moreover, bus topology provides broadcast kind of frames, which every node is capable of seeing. Therefore it lacks security.

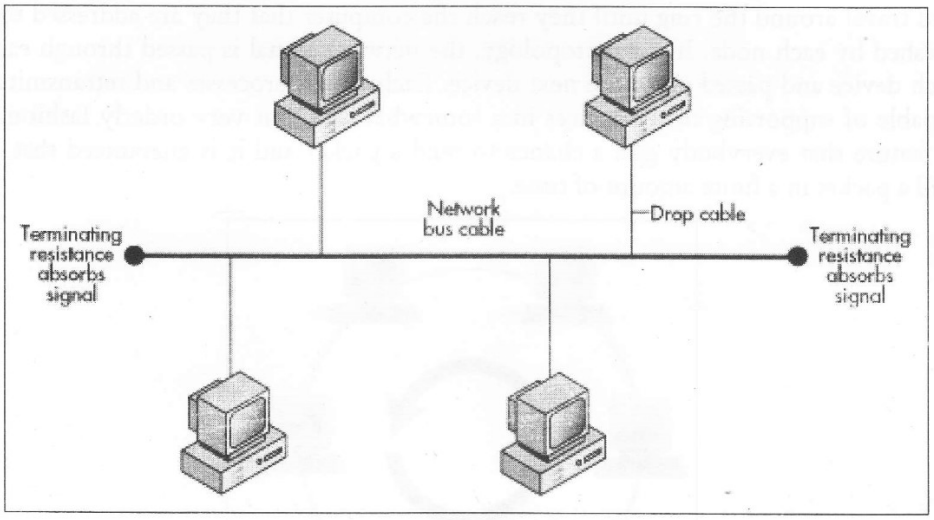


Figure 6.1: Bus topology LAN

All transmissions must pass through each of the connected devices to complete the desired request. Each workstation has its own individual signal that identifies it and allows for the requested data to be returned to the correct originator. In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code

with the message. Most Local Area Networks (LANs) are Bus Networks because the network will continue to function even if one computer is down. This topology works equally well for either peer to peer or client server.

The purpose of the terminators at either end of the network is to stop the signal being reflected back.

Advantages

1. Broadcasting and multicasting is much simpler
2. Network is redundant in the sense that failure of one node doesn't effect the network. The other part may still function properly
3. Least expensive since less amount of cabling is required and no network switches are required
4. Good for smaller networks not requiring higher speeds.

Disadvantages

1. Trouble shooting and error detection becomes a problem because, logically, all nodes are equal
2. Less secure because sniffing is easier
3. Limited in size and speed.

Ring Topology

Like bus topology, all the nodes or devices in the network are attached to the network on the same cable but in a circular fashion where the first nodes attach to the last node in cyclic mode in a ring topology LAN that is shown in Figure 6.2. It can use a single ring for half-duplex operations or dual-ring architecture for full-duplex operations.

All the nodes in a Ring Network are connected in a closed circle of cable. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. In a ring topology, the network signal is passed through each network card of each device and passed on to the next device. Each device processes and retransmits the signal, so it is capable of supporting many devices in a somewhat slow but very orderly fashion. There is a very nice feature that everybody gets a chance to send a packet and it is guaranteed that every node gets to send a packet in a finite amount of time.

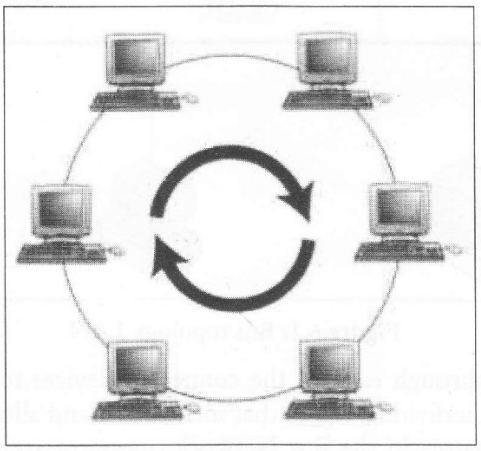


Figure 6.2: Ring Topology LAN

Advantages

1. Broadcasting and multicasting is simple since you just need to send out one message
2. Less expensive since less cable footage is required
3. It is guaranteed that each host will be able to transmit within a finite time interval
4. Very orderly network where every device has access to the token and the opportunity to transmit
5. Performs better than a star network under heavy network load.

Disadvantages

1. Failure of one node brings the whole network down
2. Error detection and network administration becomes difficult
3. Moves, adds and changes of devices can effect the network
4. It is slower than star topology under normal load.

Star Topology

Widely popular and most common is the star topology, which includes Ethernet, Fast Ethernet, and Gigabit Ethernet. Each node in a star topology connects to a dedicated link where the other end connects to a switch or hub. The distinguishing feature of star topology is that all nodes are joined at a single point, as shown in Figure 6.3. This single point is called a central node, hub, or switch, to which all other devices are attached directly, generally via UTP or STP. This topology is frequently used for networks in which control of the network is located in the central node. This method is optimal when the bulk of communication is between the central and outlying nodes. If traffic is high between outlying nodes, an undue switching burden is placed on the central node. All devices connected with a Star setup communicate through a central Hub by cable segments. Signals are transmitted and received through the Hub. It is the simplest and the oldest and all the telephone switches are based on this. In a star topology, each network device has a home run of cabling back to a network hub, giving each device a separate connection to the network. So, there can be multiple connections in parallel.

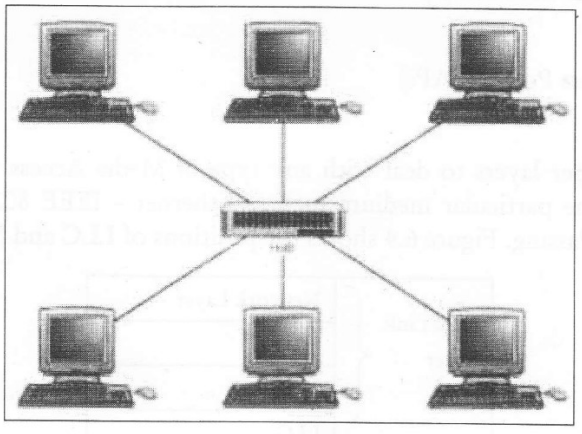


Figure 6.3: Star Topology

Transmission rates vary with AT&T's Star LAN operating at 1 to 10 Mbps, and both 100Base-T and 100VG-AnyLAN at 100 Mbps. The primary advantage of a star is that a disruptive or failed station can

be isolated; thereby eliminating any negative effect it may have on LAN performance. Additionally, each node has access to the full bandwidth of the LAN, at least in a LAN switch environment. The primary disadvantage is that a hub failure is catastrophic as all connectivity is provided through the central hub; its failure affects the entire LAN.

Advantages

1. Network administration and error detection is easier because problem is isolated to central node
2. Networks runs even if one host fails
3. Expansion becomes easier and scalability of the network increases
4. More suited for larger networks.

Disadvantages

1. Broadcasting and multicasting is not easy because some extra functionality needs to be provided to the central hub
2. If the central node fails, the whole network goes down; thus making the switch some kind of a bottleneck
3. Installation costs are high because each node needs to be connected to the central switch.

Note: Generally, BUS architecture is preferred over the other topologies - of course, this is a very subjective opinion and the final design depends on the requirements of the network more than anything else. Lately, most networks are shifting towards the STAR topology. Ideally we would like to design networks, which physically resemble the STAR topology, but behave like BUS or RING topology.

6.2.2 IEEE 802.2 LLC - Logical Link Control Layer

The Logical Link Control Layer (LLC) belongs to the upper portion of the Data Link Layer and defines Logical Link Control (LLC) for local area networks. The LLC sublayer performs the following basic functions:

- Managing the data-link communication by providing a uniform interface to the user of the data link service, usually the network layer
- Link Addressing
- Defining Service Access Points (SAPs)
- Sequencing.

The LLC enables the upper layers to deal with any type of Media Access Control sublayer (MAC), which is dependent on the particular medium such as Ethernet - IEEE 802.3 CSMA/CD or Token Ring IEEE 802.5 Token Passing. Figure 6.4 shows the positions of LLC and MAC.

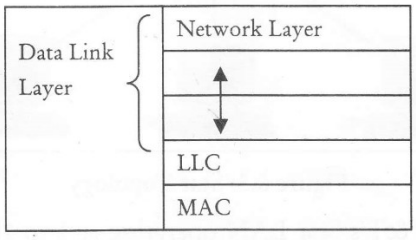


Figure 6.4: LLAC and MAC Sublayers

LLC Operation

IEEE 802.2 standard works on connectionless and connection-oriented modes.

- *Connectionless:* It is quite similar to the postal system with the assumption that once the data transmitted will be bound to reach to the destination. There is no acknowledgement from the destination to tell whether it arrived or not. This also does not guarantee regarding the order of the received frames as they have been transmitted.
- *Connection Oriented:* Like phone conversation, this service first creates a connection and gets acknowledgement of receipt of data from destination. If the data reaches damaged or lost the destination machine requests to retransmit the data. This is called Automatic Repeat Request (ARQ). This service provides sequence numbers to each frame of data transmitted and therefore ensures that the frames received are guaranteed to be in the order they have been sent and thus provides a reliable delivery.

LLC Header

IEEE 802.2 defines LLC header including a SNAP (Sub Network Access Protocol) header. Some protocols operate on top of 802.2 LLC, which facilitates both datagram and connection-oriented network services. The LLC header contains two additional eight-bit address fields known as service access points or SAPs to request SNAP service. Figure 6.5 illustrates the data field of the MAC layer Frame transmitting the LLC Protocol Data Unit (PDU).

DSAP	SSAP	Control	Information
8 Bits	8 Bits	8/16 bits	Number of bytes

Figure 6.5: LLC PDU Frame

6.2.3 IEEE 802.3 Ethernet Technologies

Among LAN standards, IEEE 802.3 Ethernet has become one of the most used LAN media. Its ample use and wide availability has made it one of the cheapest LAN media. Moreover, it can carry high-speed transmission. The evolution of Ethernet to such a widely accepted media may be traced back to late 1970s when the first Ethernet standard was created by Xerox. Around 1984, DIX (a consortium of Digital, Intel, and Xerox) and IEEE created standards for Ethernet which are popularly known as the IEEE 802.1. Subsequently, these groups segregated their work and worked as the Logical Link Control (LLC) Group focussing on end-to-end connectivity and came to be called the IEEE 802.2 Committee. Another group, called the Data Link and Medium Access Control (DLMAC) took the responsibility for developing medium access protocols. This group later formed committees for Ethernet (802.3), Token Bus (802.4), and Token Ring (802.5).

Ethernet is the least expensive high-speed LAN alternative. It transmits and receives data at a speed of 10 million bits per second. Data is transferred between wiring closets using either a heavy coaxial cable (thick net) or fibre optic cable. Thick net coaxial is still used for medium-long distances where medium levels of reliability are needed. Fibre goes a further distance and has greater reliability but a higher cost. To connect a number of workstations within the same room, a light duty coaxial cable called thin net is commonly used. These other media reflect an older view of workstation computers in a laboratory environment. Figure 6.6 shows the scheme of Ethernet where a sender transmits a modulated carrier wave that propagates from the sender toward both ends of the cable.

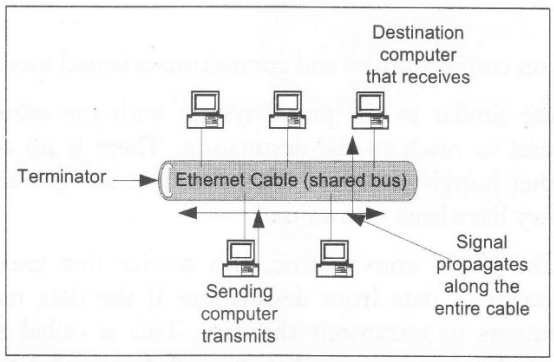


Figure 6.6: Signal Flow Across an Ethernet

Ethernet was first designed and installed by Xerox Corporation at its Palo Atto Research Center (PARC) in the mid 1970. In 1980 DEC Intel and Xerox came out with a joint specification, which has become the de facto standard. Ethernet from this period is often called DIX after its corporate sponsors Digital, Intel, and Xerox.

Collision and Broadcast Domains

Media access mechanism is a very important part of Ethernet technology and we will now understand collision and broadcast domains. Collision is nothing but the crashing of data when all devices or nodes on a single segment send data on the same physical wire. In case of a hub, all the nodes connected to the hub are in the same collision domain. We may recall that hub is basically a repeater that re-sends any signal it receives out of each one of its ports and this signal is accessible to all nodes connected to the same hub. This explains why any message or signal sent by any node is treated as broadcast signal and therefore all nodes on the same hub are in same broadcast domain.

Ethernet Frame

There are three basic elements, which makes an Ethernet. These are physical medium, a set of medium access control rules, and the Ethernet frame. Ethernet takes packets from upper-layer protocols, and places header and footer information around the data before it traverses the network. This process is called data encapsulation or framing. Ethernet frames travel at the Data Link layer of the OSI model and must be a minimum of 64 bytes and a maximum of 1518 bytes. Figure 6.7 shows an Ethernet IEEE 802.3 frame and an Ethernet frame.

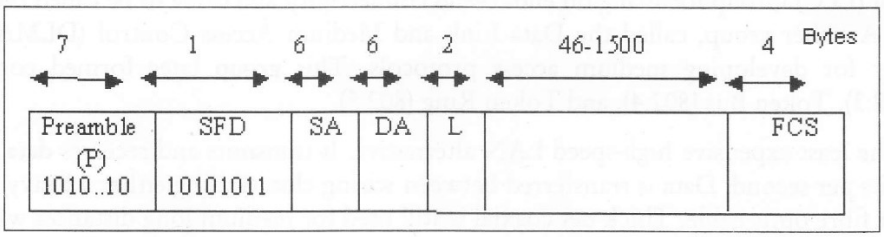


Figure 6.7: Frame format for IEEE 802.3

Below is a brief description of each field in an Ethernet IEEE 802.3 frame:

- ***Preamble (P):*** It is beginning of the frame and used to establish bit synchronization with the help of an alternating pattern of ones and zeros that is used by the receiver.

- *SFD (Start frame delimiter):* It lets the receiver know the beginning of the frame and contains one byte length.
- *Destination Address (DA) and Source Address (SA):* These are each six bytes long and are contained in hardware on the Ethernet interface card.
- *Type Field:* In Ethernet frames, this is the two-byte field after the source address. After Ethernet processing, the type field specifies the upper-layer protocol to receive the data.
- *Length Field:* It is a two-byte field following the source address. The length field indicates the number of bytes of data that follow this field and precede the frame check sequence field.
- *Data Field:* It is the place where the information to be transmitted is contained in the frame. It follows the type and length fields. After Physical-layer and Link-layer processes are complete, this data is sent to an upper-layer protocol. With Ethernet, the upper-layer protocol is identified in the type field. With IEEE 802.3, the upper-layer protocol must be defined within the data portion of the frame. If the data of the frame is not large enough to fill the frame to its minimum size of 64 bytes, padding bytes are inserted to ensure at least a 64-byte frame.
- *FCS (Frame Check Sequence) or CRC (Cyclic Redundancy Check) fields:* These are at the end of the frame. The frame check sequence recalculates the number of frames to make sure that none are missing or damaged. The CRC applies to all fields except the first, second, and last.

Ethernet Versions

The shared medium for LANs includes most of the transmission media discussed previously. Although coaxial cable was the original medium and is still used extensively in various configurations, twisted-pair has recently become the medium of choice in many environments. Fibre optic cable is used widely as a backbone technology. Wireless LANs generally are limited to special radio technologies, although infrared technology is used in certain applications. Microwave and infrared systems are used to connect LANs and LAN segments in a campus environment. Satellite rarely is used in any way, as propagation delay renders it generally unsatisfactory for interactive communications. In this chapter we will also consider the associated hardware required to connect a computer to a network and the details of the transmitting and receiving packets.

Implementation of LAN using Coaxial Cable

Coaxial cable was the first transmission medium employed in LANs. It is however expensive to acquire and costly to deploy and reconfigure but its performance characteristics are excellent. The advantages of coaxial cable include high bandwidth in the range of 500 MHz and more, better error performance, and lack of severe distance limitation. Additionally, security is high and durability is excellent. On the other hand, the costs of acquisition, deployment, and reconfiguration are high. The disadvantages of coaxial cable have been mitigated to a large extent through the development of new coaxial designs. The variations of coaxial designs are thick net and thin net. In the following sections both baseband and broadband versions of Ethernet/IEEE 802.3 are explained.

10Base5 (Thick Net/Yellow Ethernet)

This uses traditional thick baseband coaxial cable in bus topology to connect multiple computers as shown in Figure 6.8 This single transmission line is called a segment. A coaxial cable 10mm in diametre, known as a thick coaxial cable is used as a transmission line. A terminator is connected at

each end of the cable. Note that proper data communication cannot be assured if even one of these terminators is missing or not properly connected.

A transceiver is used to connect a coaxial cable and terminals. A transceiver cable also referred to as an AUI (Attachment Unit Interface) cable) is used to connect a transceiver and the NIC. The maximum length of this cable is 50 metres. Up to 100 transceivers can be connected to each segment. The minimum allowable distance between transceivers is 2.5 meters.

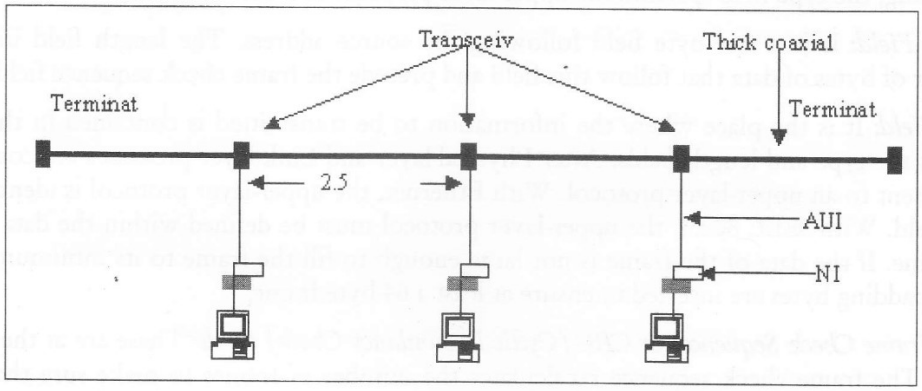


Figure 6.8: Hardware Configuration of 10Base5

10Base stands for 10Mbps and baseband transmission system. The 5 of 10Base5 signify a maximum of 500-metre segment length. The segment may be extended up to 1500 metres by using repeaters.

10Base2 (Thin Net/Black Ethernet)

This is also known as 10Base2, uses coaxial of thinner gauge of 5mm in diametre and bus topology as in the case of 10Base5 so that multiple computers can be connected to a single transmission line as shown in Figure 6.9). Primarily it was used in office environments. The thinner cable is less costly to acquire and deploy, although its performance is less in terms of transmission distance. Because of its cost it is sometimes called Cheapnet. 10Base2 signifies in the same manner as 10Bases5 except 2 is signified here as 200 metres maximum segment length (actually 185 metres).

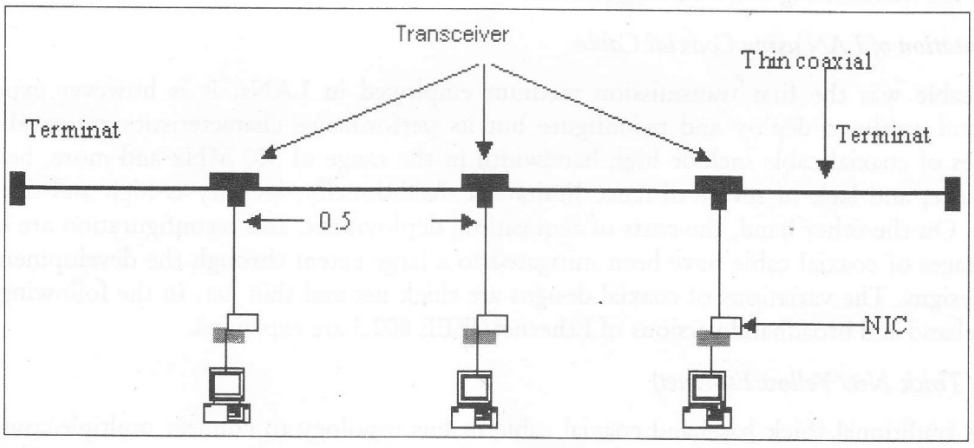


Figure 6.9: Hardware Configurations 10Base2

A BNC (Bayonet Neil Connector) or a T-connector is used to connect a cable and terminals or terminators. Note also that the NIC for 10Base2 can be connected directly to a T-connector because this NIC has a built-in transceiver. Only up to 30 nodes per segment can be connected. The minimum allowable distance is 0.5 metres between consecutive connections.

Implementation of Ethernet using Twisted Pair

Recently twisted pair has become very popular as a LAN medium. Although its performance characteristics are less appealing, its low cost and high availability certainly are attractive. Unshielded Twisted-Pair (UTP) performs nicely at low data rates using the same cable for LANs as is used for telephone terminals, hence the current tendency to deploy Category 5 UTP pairs to each jack so that voice and data terminals can share a common wiring system. Additionally, UTP has been proved to perform at very high data rates (100 Mbps) over short distances.

Shielded twisted-pair (STP) sometimes is used in LAN applications. STP might be used in an environment in which UTP data transmission might be especially susceptible to EMI/RFI, or might cause interference on adjacent pairs. Implementations of different LANs using UTP Cables are explained below.

10BaseT (Twisted Pair Ethernet)

This uses Cat 3, 4, or 5 UTP. 10BaseT translates to 10 Mbps, baseband twisted pair. 10BaseT actually is a wire hub that serves as a multiport repeater, as well as a central point of interconnection. Figure 6.10 shows the hardware configuration of 10BaseT. A star type topology is used. The device shown at the centre is known as hub. A connector known as RJ45 is connected at each end of the cable. The hub has multiple ports, each of which is connected to node using NIC via the UTP cable. Each of the NIC for the 10BaseT has a built-in transceiver as do those of the 10Base2. The maximum distance between the 10BaseT hub and the attached device is 100 metres/segment.

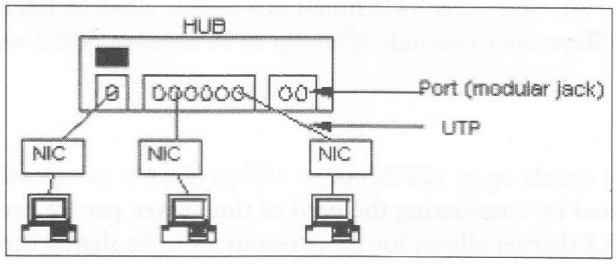


Figure 6.10: Hardware Configuration 10BaseT

Ethernet Specification

Table 6.1: Ethernet Specifications

	10Base5	10Base2	10BaseT
Transmission speed	10Mbps	10Mbps	10Mbps
Transmission medium	Coaxial cable	Coaxial cable	UTP cat3,4,5
Maximum segment length	500metre	185 metre	100metre
Maximum node/segment	100	30	-
Minimum length between node	2.5 metre	0.5 metre	-
Repeaters/Series	4	4	4
Maximum network length	2500 metre	925 metre	500 metre

Table 6.1 shows the major Ethernet specifications described so far. Note that the maximum network length means the maximum allowable distance between nodes.

Fast Ethernet

With the advancement of time and intensive use of LAN, more workstations and more active users have resulted in more LAN traffic. Increased use of graphics and other bandwidth-intensive applications have increased LAN traffic. Other applications like video conferencing and multimedia have created a demand for fast LANs. Bandwidth of 10 Mbps, 16 Mbps and even 20 Mbps are becoming a bottleneck. In response to this, Fast LANs have been developed, offering bandwidth of 100 Mbps and soon to 1 Gbps. Fast LAN options currently include:

- 100BaseT or Fast Ethernet
- Iso-Ethernet (Isochronous Ethernet Integrated Services)
- 100VG-AnyLAN
- FDDI (Fibre Distributed Data Interface) – This has already been explained
- ATM (Asynchronous Transfer Mode) – This too has also been explained.

100BaseT (Fast Ethernet)

100BaseT is a high-speed LAN standard and is considered a variation of 10BaseT. This is standardized as IEEE 802.3u. This operates with an access mechanism as CSMA/CD and provides a transmission speed of 100 Mbps through an Ethernet switching hub. Multiple 10 Mbps connections are supported through multiple ports on the switch. Cat 3, 4, or 5 UTP can be used in 4-pair configuration. Cat 5 UTP is generally used for a maximum LAN diametre of 500 metres. Three pairs are used for transmission, with the fourth pair used for signaling and control (CSMA/CD) in half-duplex mode. Connections to nodes, servers and other switching hubs are provided at 100 Mbps, supporting ten 10-Mbps channels. The 100 Mbps media include fibre (up to 30 miles or 50km without repeaters) and Cat 5 UTP at 100 metres.

Gigabit Ethernet

Gigabit Ethernet that has speeds up to 1000Mbps or 1Gbps (gigabit per second) is 10 times faster than 100Base-T. This was created by considering the need of time when people needed to process large files across a network. Gigabit Ethernet allows for more resources to be shared throughout a network. The enormous potential of optical fibre cable made it possible to transfer huge files or large network intensive work because of latent power of bandwidth and its speed. Gigabit Ethernet can run in half-duplex or full-duplex mode. It looks similar to Ethernet from the Data Link layer upward. The physical layer is defined in the IEEE 802.3z 1000BASE-T standard, which is the standard for Gigabit Ethernet over the Category 5 or 6 cabling and uses all four of the Category 5 or 6 pairs for sending and receiving data simultaneously.

Gigabit Media Types

There are three types of media for Gigabit Ethernet. These are longwave, shortwave, and copper medium.

1. *1000BaseLX or longwave:* Single-mode and multimode fibre along with longwave laser is used. The 1000BaseLX GigaBit Interface Converter (GBIC) interfaces can pass data up to 3 kms.
2. *1000BaseSX or shortwave (SW):* It uses multimode fibre with shortwave laser. It has distance limitation up to 550 metres with the GBIC interfaces.

3. *1000BaseCX:* It is defined in the IEEE 802.3z specification and uses shielded 150-ohm copper. This can be used only for short distances because this cabling method has a distance limitation up to 25 metres.

6.2.4 CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Protocol

Protocols in which stations listen for a carrier or transmissions and act accordingly are called carries sense protocols.

The first carrier sense protocol is called 1-persistent CSMA. When a station has data to send, it first listens to the channel to see if anyone lese is transmitting at that moment. If the channel is busy, the station waits until it become idle when the station detects an idle channel, it transmit a frame of a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent because the station transmits with a probability of 1 whenever if finds the channel idle.

A second carrier sense protocol is nonpersistent CSMA. In this protocol, before sending a frame the station sense the channel, if no one is sending the station begins transmissions. However, if the channel is already in use, the station does not continuously sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits for a random period of time and then reports the algorithm.

The last protocol is p-persistent CSMA which applies to slotted channels. When a station becomes ready to send, it senses the channel. If it is idle, it transmit with a probability p. With a probablity q= 1-p, it waits until the next slot. If that slot is also idle, it either transmits or waits again, with probability p and q respectively. The process is repeated until either the frame has been transmitted or another station has begun transmitting. In the latter case, it acts as if there had been a collision. If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm once again.

Datagrams are used to transmit the messages across the network. Many nodes on a same physical wire line may start sending their datagrams simultaneously and thereby causing collision. In order to avoid this, the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol are devised to ensure that two datagrams aren't sent out at the same time, and if they are, it acts as a mediator to retransmit. In CSMA/CD mechanism, if a channel is busy on the network, other stations cannot transmit. It is therefore prone to slow the communication process in a network environment.

Managing Access to Networks

You may think if all the stations at a time begin to access network, there would be some sort of chaos. Therefore, there are many methods of managing access to a network. If all network stations tried to send data at once, the messages would become unintelligible, and no communication could occur. It necessitates to device mechanism to avoid such deadlocks. Some of important methods are listed and discussed below:

- Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)
- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Token Passing
- Polling

Carrier Sense Multiple Access: In this case when a user wishes to transmit, he first listens to the medium to ensure whether another transmission is in progress or not. It is known as carrier sense. If the channel is in use, he must wait. If the medium is idle, he may transmit. If channel is busy, he has to

wait for a random period of time before trying to listen. This has been explained in detail in other part of the tutorial.

CSMA with Collision Detection

The most commonly used medium access control technique for bus and star topology is Carrier Sense Multiple Access with collision detection' (CSMA/CD). The original version of this technique was developed by Xerox as part of the Ethernet LAN, which formed the basis for the IEEE 802.3 standard. The basic rules for CSMA/CD are also following:

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, then transmit immediately.
3. If a collision is detected during transmission, transmit a brief jamming signal to ensure that all stations know that there has been a collision and then cease transmission.
4. After transmitting the jamming signal, wait a random amount of time, then attempt to transmit once again (Repeat from step 1).

The following process of transmission under CSMA/CD can be explained with the help of a flow diagram as shown Figure 6.11.

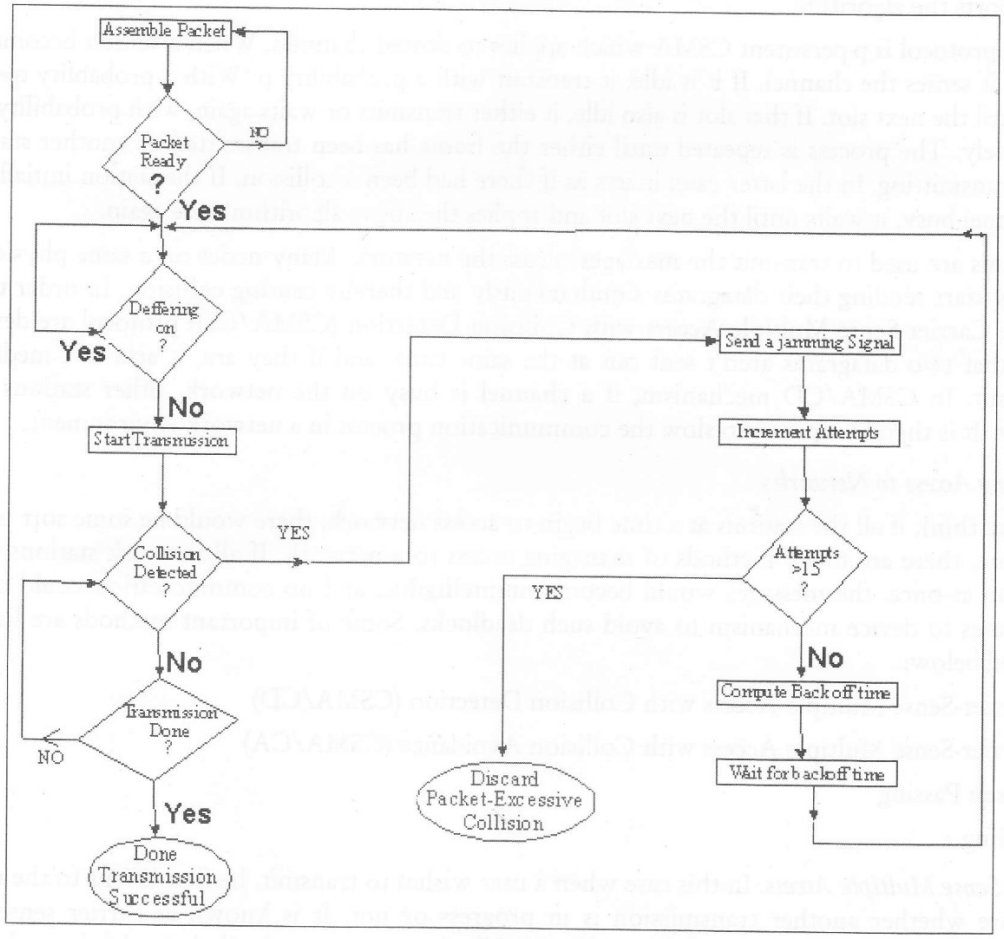


Figure 6.11

Hence, when as CSMA/CD station senses that a collision has occurred, it immediately ceases transmission and sends a brief jamming signal to notify all stations of this collision. Collisions are detected by monitoring the analog waveform directly from the channel. When signals from two or more stations are present simultaneously, the composite waveform is distorted from that of a single station, resulting in the form of larger than normal voltage amplitude on the cable.

If a collision is detected, the stations about the packet being transmitted and sends a jamming signal. After the jamming signal has been transmitted, the station involved in colliding packets wait random amount of time and then try to send their packets again. By using a random delay, the colliding stations try to minimize the change of another collision during the wait for transmission. However to maintain stability a method known as "Binary Exponential Algorithm" is used in ethernet. In the method, a station will persist in trying when there are repeated collisions. There retries will continue until the transmission in successful or 16 attempts (the original plus 15 retries) have made unsuccessful. At this point (after 16^{th} attempt) the packet is discarded and the event is reported as an error.

In summary, If a user desires to transmit, he first listens to ensure whether the channel is free or not. If the channel is idle, he transmits. If the channel is busy, he keeps on listening until the channel is free, then transmits immediately. During the transmission, he continues listening to detect collision. If a collision is detected, he stops transmitting immediately, and waits a random period of time before goes back to step transmit again. Basically CSMA/CD has three states. These are transmission period, contention period and idle period.

6.2.5 IEEE 802.4 Token Bus

IEEE 802.4 standard defines token bus access method for LAN that uses the token passing technology. In toke bus networks nodes or computers are logically connected in a ring that is nothing but a physically connected common bus. Tokens are broadcasted to every station in the network to provide access and data exchange rights however, only the station with the destination address after seeing request for its machine responds to the source machine as indicated in the token as source address. After completing the transmission of data, the token is passed to the next logical station in the ring. There is always a maximum limit on the amount of data to be transmitted from any machine. If the node holding the token is not ready to transmit, it immediately passes the token to its successor without wasting bandwidth. The advantage of the token passing schemes ensures efficient use of the bandwidth under moderate to high load. It also provides a fairly good chance to every node to communicate. However, token passing scheme may also assign priority to different types of traffic and a maximum time between token accesses can be fixed.

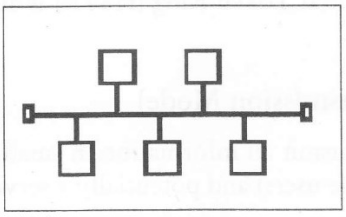


Figure 6.12: Token Bus

There are two general types of token passing schemes. They are token ring and token bus. Figure 6.12 shows the token bus configuration. Next section describes token ring schemes. However, for clarity between token bus and token, the token ring is essentially a closed set of point-to-point connections

between active repeaters that forward packets around the ring. In token ring network, one node's successor is the next node in the link and the free token does not contain the address of the successor and traffic on the ring flows in one direction only.

Figure 6.12 shows the token bus with a logical ring is created on a physical bus. Machines or computers are attached to the bus similarly to Ethernet. The difference is that each station keeps in a table the address of its current successor and predecessor to forward the free token in a packet addressed to its successor for access. Thus, only active stations participate in the token passing logical ring. When a node completes exchange of data, it sends a packet containing its own address and the address of its current successor so that other inactive nodes in the network those are ready to transmit could update their table, if there is any new node in the network. Thereafter the active node leaves the token for inactive nodes with an address in the range to be captured by a node, which is ready to transmit. If a node holding the token is ready to become inactive, it forwards a message to its predecessor listing its successor and leaves the token to this successor.

6.2.6 IEEE 802.5 Token Ring

Token Ring is a ring topology created by IBM in the 1970s and is defined as the IEEE 802.5 standards. It describes a token-passing network in a ring topology. In this mechanism, a stream of data, called a token, is passed around the network. This token indicates that any station with a message or data to transmit waits until it receives a free token. Once the free token is captured by any node, it then changes to a busy token and transmits a block of data called a frame. This is similar to an Ethernet frame. The receiving station copies the data from the frame and the frame continues around the ring, making a complete round trip back to the original transmitting station. The transmitting station now knows the frame has been received. That station then issues a new free token on the ring for others to use.

The advantage of this mechanism is that it prevents collision by ensuring that only one station at a time is transmitting. It also ensures the delivery of the frame. The Token Ring topology uses Layer 1 and Layer 2 with STP wiring. A central hub called Multistation Access Unit (MSAU) is used to connect each station in a star type of topology. The MSAU uses electromechanical relays to make the physical star into a logical ring. In this manner each station receives signals from its Nearest Active Upstream Neighbour (NAUN) and repeats them to its downstream neighbours. In this topology, a priority scheme can also be configured by the network administrator for high-priority stations to use the network more frequently. The frame has two fields namely the priority field and the reservation field. Earlier IBM Token Ring products were available with speeds of 4Mbps and 16Mbps. With the advancement of technology, High-speed Token Ring (HSTR) is also available with speeds of 100Mbps and 1Gbps.

6.2.7 ATM (Asynchronous Transmission Mode)

The basic idea behind ATM is to transmit all information in small, fixed-size packets called cells. ATM is both a technology (hidden from the users) and potentially a service (visible to the users).

Main reasons for choosing cell switching:

- It is highly flexible and can handle both constant rate traffic (audio, video) and variable rate traffic (data) easily.

- At the very high speeds envisioned (gigabits), digital switching of cells is easier than using traditional multiplexing techniques.
- It can provide broadcasting which is essential for TV distribution and many other applications.

ATM networks are connection-oriented. Cell delivery is not guaranteed, but their order is Intended speeds for ATM networks: 155 Mbps (used by AT&T's SONET for high definition TV), 622 Mbps (for carrying four 155-Mbps channels), and gigabits speed later.

At the physical layer, ATM does not prescribe a particular set of rules for the physical medium, but instead says that ATM cells may be sent on a wire or fiber by themselves, but they may also be packaged inside the payload of other carrier systems.

In other words, ATM has been designed to be independent of the transmission medium.

The ATM layer defines the layout of a cell, deals with establishment and release of virtual circuits, and congestion control.

The AAL (ATM Adaptation Layer) provides an interface to allow users to send packets larger than a cell.

6.3 HARDWARE ADDRESSING AND FRAME TYPE IDENTIFICATION

Hardware Addressing Scheme is processed b many network technologies for identifying the network stations. Each transmitted frame, along with it, carries a hardware address. We discuss below the related concepts.

6.3.1 Specifying a Recipient

With the growth of wireless communication, the growth of laptop with mobile Internet connection is imminent. The mobile hosts have different sets of requirements for routing a packet to a mobile host. Generally, this requirement is accomplished through creation of two LAN foreign agent and home agent. When a mobile host connects to the network, it collects a foreign agent packet or creates a request for foreign agent. Consequently, a connection is set up between them and the mobile host provides to the foreign agent its home and some other details relating to security. Subsequently, the foreign agent contacts the mobile host's home agent and delivers the message about the mobile host.

The home location agent maintains user information in the form of static and dynamic information. The static information is the International Mobile Subscriber Identity (IMSI), account status, service subscription information authentication key and options etc. The dynamic information is the current location area of the mobile subscriber which is the identity of the currently serving foreign agent to enable the routing of mobile-terminated calls. As soon as a mobile user leaves its current location area the information in the home location agent is updated so that the mobile user can be localized in the GSM network.

When a foreign agent contacts home location agent, the home agent verifies the received information. If verification is found to be correct, it permits the foreign agent to proceed. Consequent to this, the foreign agent enables the mobile host into its routing table. When the packets for the mobile host arrive, its home location register encapsulates it and redirects to the foreign agent where the mobile

host is residing. Thereafter, foreign agent returns encapsulation data to the router so that all next packets would be directly sent to correspondent router (foreign agent).

6.3.2 Broadcasting

In broadcasting, the source machine intends to send messages to many or all other hosts. For example, stock exchange reports, sports news like cricket match score, flights schedules, etc. Hence sending the same message to several recipients is broadcast and the algorithm doing so is called broadcast algorithm. To accomplish the task the following methods are proposed:

"The simplest method is that source machine sends the packet to all the necessary destination machines. In doing so, the source machine needs to maintain the complete list of the addresses of destination machines. It also involves wastage of the bandwidth. It is one of the most undesirable methods."

6.3.3 Multicasting

Sometimes, there are groups that are working and exchanging information among group members. Hence, sending information to well-defined groups that have large members, but small compared to the network, as a whole is called multicasting and the routing algorithm making it possible is called multicast routing. If the group is small, sending messages point to point will suffice but if the group is large, point to point transferring messages would be inefficient. In such a situation broadcasting will also not be proved efficient because messages may not be of interest of all the recipients and messages may also be classified.

Multicast Addressing

To multicast an audio or video program, a source must first acquire a class D multicast address (from a distributed database), which acts like a station frequency or channel number.

Multicast Group Management

- Periodically, each mrouter sends out broadcast packet limited to its island asking who is interested in which channel.
- Hosts wishing to receive one or more channels send another packet back in response.
- Each m router keeps a table of which channels it must put out onto its LAN.

The multicast routing algorithm involves update list of all process in a group available with source or host machine. Further, the router should contain a list or table to know which of their hosts belong to which group. This update is accomplished either by router to query their hosts periodically to know about the new members in groups or by the hosts informing their routers about changes in-group membership.

In multicast routing, each router computes a spanning tree for all other routers in the subnet. On receipt of a multicast packet for a group at a router, that router examines its spanning tree and prunes the multicast packet so that all lines that do not lead to hosts that are members of the group could be removed. The pruning of the spanning tree involves Link State routing when each router is aware of the complete subnet topology including which hosts belong to which groups. Thereafter, the spanning tree is pruned from beginning at the end to each path and moving towards the root. Thus all routers that do not belong the group are removed.

The major disadvantage of this algorithm is that it scales inefficiently to large networks. To overcome this problem, another method, a core-base tree is used. This computes a single spanning tree per group with the root (the core) near the middle of the group. A host sends a multicast message to the core, which then performs the multicast along the spanning tree. The advantage of this method is reduction in storage costs from multiple trees to one tree per group.

6.3.4 Frame Headers and Frame Format

Frame Format is allocated to many lan technologies such as token ring and token bus.

Frame Header shows the address and identifies the other related information.

Frame Format of Token Bus

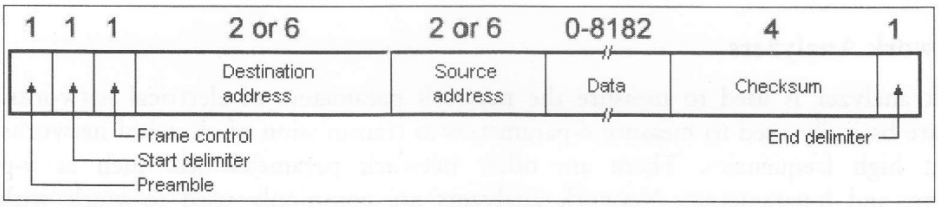


Figure 6.13: Token Bus Frame Format

Each field in a Token bus is described below:

- *Preamble:* It is used to synchronize the receiver's clock.
- *Starting Delimiter (SD) and End Delimiter (ED):* They are used to mark frame boundaries. Both of them contain analog encoding of symbols other than 1 or 0 so that they cannot occur accidentally in the user data. Hence no length field is needed.
- *Frame Control (FC):* It is used to distinguish data frames from control frames including the frame's priority and acknowledgement.
- *Destination and Source Address:* They contain2 bytes for a local address or 6 bytes for a global address.
- *Data:* It contains 8182 bytes when 2 byte addresses are used and 8174 bytes for 6 byte addresses.
- *Checksum:* It is used in error detection.

Frame Format of Token Ring

Each field in a Token ring is described below:

- *Start Delimiter:* It is used to inform each station of a token and uses a unique coding for the frame.
- *Access-Control Byte:* It is a series of bits that circulate throughout the ring and are used by the active monitor to ensure delivery. Within it a priority bit indicates the priority of the frame or token. It has also a reservation bit indicating the priority required for the next token to gain access to the ring. A token bit differentiates a token from a data or command frame. The monitor bit determines whether a frame is circling the ring endlessly. Active monitor employs a mechanism for detecting and compensating for network fault.

- *Frame Control:* It is used to indicate the frame type and contains the frame type bit, the reserved bit, and the control bits.
- *Destination Address:* It indicates the address of the receiver.
- *Source Address:* It has the address of the sender.
- *Data:* This field is used to send the information.
- *Frame Control Sequence:* It guarantees that all the frames are delivered without damage.
- *End Delimiter:* It describes the end of the token or frame and contains bits to indicate if a frame is damaged.
- *Frame Status:* It ends the frame and ensures that the frame has been copied to the destination address.

6.3.5 Network Analyzers

A network analyzer is used to measure the network parameters of electrical networks. Network analyzers are basically used to measure s-parameters as transmission of electrical networks is easy to measure at high frequencies. There are other network parameter sets such as y-parameters, z-parameters, and h-parameters. Network analyzers are commonly used to work with two-port networks such as amplifiers and filters, but they can be used on networks with an arbitrary number of ports.

Network analyzers mostly work at high frequencies. But there are some special types of network analyzers that can cover lower frequency ranges down to 1 Hz. These network analyzers can be used for example for the measurement of audio and ultrasonic components.

The two main types of network analyzers are:

Scalar Network Analyzer (SNA): It is used to measure amplitude properties only.

Vector Network Analyzer (VNA): It is used to measure both amplitude and phase properties.

Check Your Progress

1. What is Ring topology?
2. How is LAN implemented using coaxial cable?

6.4 LET US SUM UP

Briefly, 802.2 LLC sublayer or the 802 LAN's intends to provide for a best-effort datagram service. LLC aims to provide unreliable datagram service, acknowledged datagram service and reliable connection oriented service. The LLC header is derived from the older HDLC protocol. IEEE 802.3 and Ethernet standards are very popular and distinct LAN standards. However, they can be used interchangeably.

By now you may have understood the differences between ring, star, and LAN topologies along with the respective examples for each topology. Besides you would have learnt as to how each is used in the network, and that Token Ring uses a ring topology, while Ethernet uses a star topology when using CAT 5 cabling. There are various versions of Ethernet technology and their advantages, disadvantages

and limitations. The application and implementation of various network components, which has been explained earlier, has again been stressed in this unit. IEEE 802.3 Standards also explains cabling schemes for Ethernet. It uses CSMA/CD with Manchester encoding.

The reasons why Ethernet technology is widely used are many. They include its efficiency, and low cost factor, which have made it popular over other technologies. With the advancement of technology and increasing demand for faster processing, Ethernet technology is constantly evolving to maintain its status and to stay ahead of the network demands. Ethernet is fairly easy to install because of the wide variety of equipment in the market and the standards that accompany it. Ethernet speed ranges from 10Mbps to 10,000Mbps, to accommodate the wide variety of networks. Gigabit Ethernet is the latest armament of Ethernet technology. IBM's Token Ring is also in the race. It is the second most widely used technology in today's networks. IEEE 802.4 Token Bus is an arbitrary linear or tree topology and is more reliable and efficient than token ring. In token bus, nodes are uniquely numbered from highest to lowest and token then pass accordingly. It works in broadcast domain. IEEE 802.5 Token Ring uses a ring topology and a Token-passing method to access the physical medium, which consist of a virtual ring. Token ring technology is also available starting from 4 Mbps to 1 Gbps. The principle used in the token ring network is that a token is circulating in the ring and whichever node gets that token first will have right to transmit the data. The advantage of the scheme is that the token rotates in the ring, hence it guarantees that every node gets the token with in some specified time.

The routing algorithms that require selecting a path or route from many possible routes in the network are part of the router software. They are of two basic types namely non-adaptive or static and dynamic or adaptive. Selection of routing algorithms depends on the minimum mean delay for the packets and number of hop before reaching to the destination machine. Flooding algorithms have very limited use mostly with distributed systems or systems with tremendous robustness requirements at any instance. Broadcast and multicast routings are used to forward a single packet to several recipients depending on whether they belong to broadcast or multicast group.

6.5 KEYWORDS

10Base2 (Thin Net/Black Ethernet): Uses coaxial of thinner gauge of 5mm in diametre and bus topology.

10Base5 (Thick Net/Yellow Ethernet): This uses traditional thick baseband coaxial cable in bus topology to connect multiple computers.

10BaseT (Twisted pair Ethernet): Uses Cat 3, 4, or 5 UTP.

Bus: All devices on network are attached to a single cable in a bus topology LAN.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Protocol ensures that two datagrams aren't sent out at the same time, and if they are, it acts as a mediator to retransmit.

Ethernet: It is the least expensive high-speed LAN alternative in which data is transferred between wiring closets using either a heavy coaxial cable (thick net) or fibre optic cable.

Logical Link Control Layer (LLC): It belongs to the upper portion of the Data Link Layer and defines Logical Link Control (LLC) for local area networks.

Ring: All the nodes or devices in the network are attached to the network on the same cable but in a circular fashion where the first nodes attach to the last node in cyclic mode.

Star: Each node in a star topology connects to a dedicated link where the other end connects to a switch or hub.

Token Bus: In toke bus networks nodes or computers are logically connected in a ring that is nothing but a physically connected common bus.

Token Rin: In this mechanism, a stream of data, called a token, is passed around the network.

6.6 QUESTIONS FOR DISCUSSION

1. How does the frame format of token ring differ from Ethernet?
2. What is the Ethernet protocol and how does it compare with the Token ring protocol in terms of delay?
3. How can a collision be avoided in CSMA/CD network?
4. Discuss various types of LAN Topologies.
5. How broadcasting is different from multicasting?

Check Your Progress: Model Answers

1. All the nodes or devices in the network are attached to the network on the same cable but in a circular fashion where the first nodes attach to the last node in cyclic mode in a ring topology.
2. Coaxial cable was the first transmission medium employed in LANs. It is however expensive to acquire and costly to deploy and reconfigure but its performance characteristics are excellent.

6.7 SUGGESTED READINGS

Anuranjan Misra, *Computer Networks*, Acme Learning Pvt. Ltd. Publications

Rajneesh Agrawal and Bhata Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

UNIT IV

LESSON

7

NETWORK HARDWARE

CONTENTS

7.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Know network hardware concept
- Discuss LAN wiring with its physical topology
- Understand fiber modems
- Discuss switches, repeaters, and bridges
- Explain network hardware

7.1 LAN WIRING

7.1.1 Local Area Networks

This technology connects people and machines within a site. A Local Area Network (LAN) is a network that is confined to a relatively small area as shown in Figure 7.1. Local Area Networks (LANs) are most often described as privately owned networks that offer reliable high speed communication channels optimized for connecting information processing equipment in a limited geographical area, namely, an office, buildings, schools or campus.

A LAN is a form of local (limited distance), shared packet network for computer communications. LANs interconnect computers and peripherals over a common medium in order that users might share access to host computers, databases, files, applications, and peripherals. They can also provide a connection to other networks either through a computer, which is attached to both networks, or through a dedicated device called a gateway.

The components used by LANs can be divided into cabling standards, hardware, and protocols. Various LAN protocols are Ethernet, Token Ring: TCP/IP, SMB, NetBIOS and NetBeui, IPX/SPX, Distributed Fiber Data Interchange (FDDI) and Asynchronous Transfer Mode (ATM).

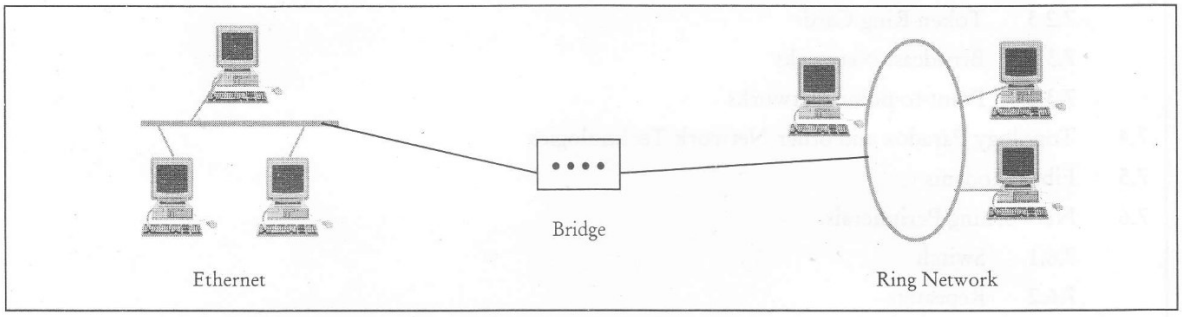


Figure 7.1: Local Area Network

Briefly, based on size, transmission technology and topology LAN is characterized as below:

1. *Size:* usually a diameter of not more than a few kilometers, with bounded and known worst-case transmission time, making special design and simple management possible.
2. *Transmission technology:* LAN uses a shared cable running at speeds of 10 to 100 Mbps (and even higher), with delay of tens of microseconds and few errors.
3. *Topology:* It may have topologies as bus (e.g., Ethernet) as shown in Figure 7.1, ring (e.g., IBM token ring), etc.

Allocation of the shared channel:

(i) Each machine is statically allocated a time slot to transmit, and gets its turn by round robin.

(ii) Each machine is dynamically allocated a time slot on demand.

(iii) Centralized method uses an arbitration unit to determine who goes next.

(iv) Decentralized method allows each machine to decide for itself.

(v) Cable is the medium through which information usually moves from one network device to another. There are several types of cable, which are commonly used with LANs. In some cases, a network will utilize only one type of cable; other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Wireless LANs
- Cable Installation Guides

7.1.2 Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission or by satellite. Wireless networks are very important for allowing laptop computers or remote computers to connect to the LAN. They are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are **line-of-sight** and **scattered broadcast. Line-of-sight communication** means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. Some several disadvantages are:

- They provide poor security.
- They are susceptible to interference from lights and electronic devices.
- They are also slower than LANs using cabling.

7.1.3 Cable Installation Guides

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.

- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both the ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

7.2 NETWORK INTERFACE CARDS

The Network Interface Card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes, which are attached to a serial port or a SCSI port. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The three most common network interface connections are Ethernet cards, Local Talk connectors, and Token Ring cards. According to a International Data Corporation study, Ethernet is the most popular, followed by Token Ring and Local Talk (Sant'Angelo, R. (1995). NetWare Unleashed, Indianapolis, IN: Sams Publishing).

7.2.1 Ethernet Cards

Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both) (See Figure 7.2). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.

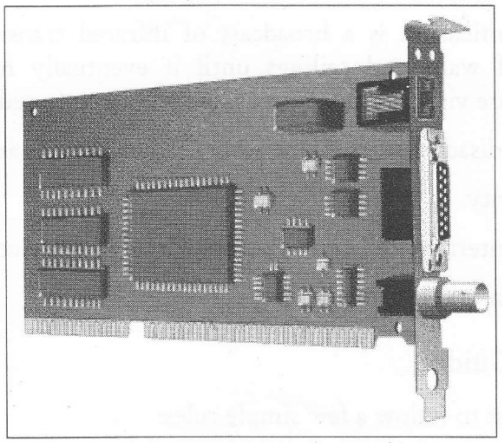


Figure 7.2

7.2.2 Local Talk Connectors

Local Talk is Apple's built-in solution for networking Macintosh computers. It utilizes a special adapter box and a cable that plugs into the printer port of a Macintosh A major disadvantage of Local Talk is that it is slow in comparison to Ethernet. Most Ethernet connections operate at 10 Mbps (Megabits per second). In contrast, Local Talk operates at only 230 Kbps (or .23 Mbps).

Table 7.1: Ethernet Cards vs. Local Talk Connections

Ethernet	Local Talk
Fast data transfer (10 to 100 Mbps)	Slow data transfer (.23 Mbps)
Expensive - purchased separately	Built into Macintosh computers
Requires computer slot	No computer slot necessary
Available for most computers	Works only on Macintosh computers

7.2.3 Token Ring Cards

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

7.3 NETWORK HARDWARE

There are two important dimensions for classifying networks — transmission technology and scale.

Transmission technology can be classified into two types:

1. Broadcast networks.
2. Point-to-point networks.

7.3.1 Broadcast networks:

These networks have a single communication channel shared by all the machines on the network. They work as follows:

- All the others receive packets sent by any machine.
- An address field within the packet specifies for whom it is intended.
- Upon receiving a packet, a machine checks the address field. If it is intended for itself, it processes the packet; otherwise, it is just ignored.
- It is also possible to address all broadcasting or multicasting a subset of the machines.
- The address consisting of all 1 bits is reserved for broadcast.
- All addresses with the high-order bit set to 1 are reserved for multicasting.
- The remaining addresses bits form a bit map corresponding to groups.
- Each machine can subscribe to any or all of the groups.