EDUSAT LEARNING RESOURCE MATERIAL

Computer network
and
data communication

(For 5TH Semester CSE & IT)

Prepared
by
Er.Ramesh Chandra sahoo ,Sr.Lect , CSE/IT,
UCP Engg. School,Berhampur
Smt. Sumitra Mahapatra,PTGF, CSE/IT,
UCP Engg. School,Berhampur
Ms. Meenakshy sahu,PTGF, CSE/IT,
UCP Engg. School,Berhampur

Computer Network & Data Communication

Computer Network & Data Communication is the prime area of Application Development. Business applications need to store J_ process large volume of data. This paper teaches the methodology of storing & processing da for commercial application. It also deals in the security & other aspects of DBMS.

<u>BOOKS</u>:

1. Data Communication & Computer Networks by W.Stallings (PHI),

- Introduction to Comp. Network; M.Bhatia; Unv. S. Press
- Computer networks; Tanenbum; Pearson
- Data communication & network; Forouzen; TMH

1.0.Basic Of Data Communication

Contents

1.1 Introduction to Data Transfer

- Data Communication is the exchange of data (in the form of 0s and 1s) between two devices via some form of transmission medium (such as a wire cable).
- The purpose of data communication is to exchange information between two agents.
- The communicating device must be part of a communication system made up of a combination of hardware and software
- The effectiveness of a data communication system depends on three characteristics.

  Delivery: The system must deliver data to the correct destination.

  Accuracy: The system must deliver data accurately.

  Timeliness: The system must deliver data in a timely manner.
- The components of data communication system is made up of five components

  Message–the message is the information to be communicated.

  Sender -the sender is the device that sends the data message.

  Receiver -the receiver is the device that receive the message.

  Medium –the transmission medium is the physical path by which a message travels from sender to receiver.

  Protocol –A protocol is a set of rules that govern data communication.
- A network is a set of devices connected by a media links .A node can be a computer, printer or any other device capable of sending or receiving data generated by other nodes on the network.
- The three criteria necessary for an effective and efficient network

  Performance

  Reliability

  Security
- The factors that affect the performance of a network

  Number of users-The design of a given network is based on an assessment of the average number of users that will be communicating at any one time.

  Type of transmission medium-The medium defines the speed at which the data can travel through a connection. Today's network uses fiber-optic cable for faster and faster transmission.

Hardware-The types of hardware included in a network effect both speed and capacity of transmission.

Software- It used to process the data at the sender, receiver and intermediate node also.

- The Network reliability is measured by the following factors

  Frequency of failure- All networks fail occasionally.

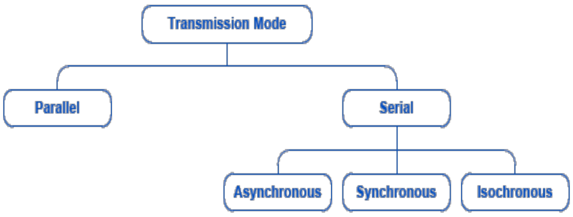
  Recovery time of a network after a failure- How long does it take to restore service? A network that recovery quickly

  Catastrophe- A network must be protected from catastrophic events such as fire, earthquake or theft.

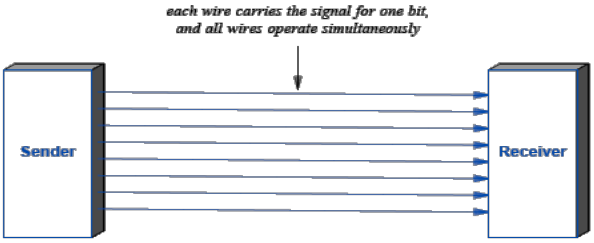
- Network security issues include protecting data from unauthorised access and viruses. Unauthorised access for a network to be useful, sensitive data must be protected from unauthorised access. Viruses A good network is protected from viruses by hardware and software designed specifically for that purpose

Digital data transmission

- Data transfer is the manner in which data is sent over the underlying medium.
- Transmission modes can be divided into two fundamental categories:
  1. **Serial transmission**
  2. **Parallel transmission**



Parallel transmission


each wire carries the signal for one bit, and all wires operate simultaneously
Sender
Receiver

- Parallel transmission allows transfers of multiple data bits at the same time over separate medium.
- Parallel transmission is used with a wired medium that uses multiple, independent wires.
- The signals on all wires are synchronized so that a bit travels across each of the wires at precisely the same time.
- In fig there are 8 wires used to send 8 data bits at the same time

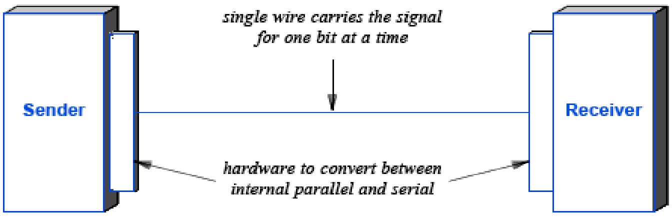
Advantages

- High speed: it can send N bits at the same time a parallel interface can operate N times faster than an equivalent serial interface.

- Match to underlying hardware: Internally, computer and communication hardware uses parallel circuitry; a parallel interface matches the internal hardware well.

Serial transmission

- Serial transmission sends one bit follows another.
- Most communication systems use serial mode
- We need only one communicating channel rather than *n* to transmit between two communicating device


single wire carries the signal
for one bit at a time
Sender
Receiver
hardware to convert between
internal parallel and serial

Advantages

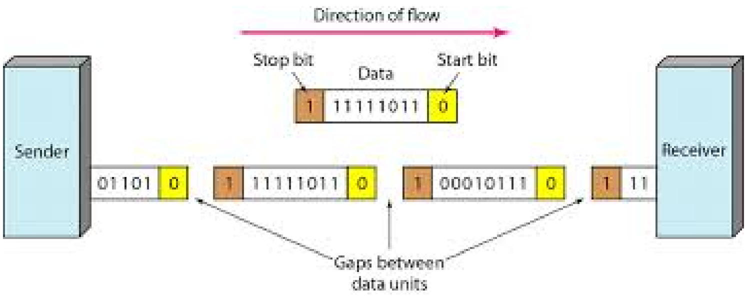
- Serial networks can be extended over long distances at much less cost .
- Using only one physical wire means that there is never a timing problem caused by one wire being slightly longer than another.

Serial transmission mechanisms can be divided into two broad categories

1. **Asynchronous transmission**
2. **Synchronous transmission**

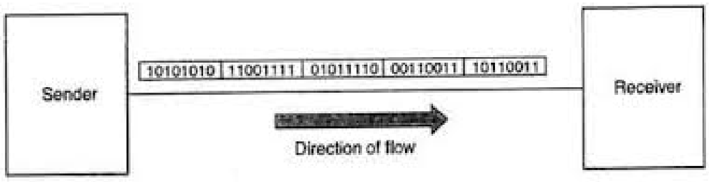
Asynchronous transmission

- Small blocks of bits are sent at a time without any time relation between consecutive bytes .when no transmission occurs a default state is maintained corresponding to bit 1.
- Due to arbitrary delay between consecutive bytes, the time occurrences of the clock pulses at the receiving end need to be synchronized for each byte.
- This is achieved by providing 2 extra bits start and stop.
- **Start bit:** Without a synchronizing pulse, the receiver can’t use timing to predict when the next group will arrive. To alert the receiver to the arrival of a new group, therefore an extra bit is added to the beginning of each byte. This bit usually a 0,is called a start bit
- **Stop bit:** To ensure the receiver know that the byte is finished; one or more additional bits are appended to end of the byte. These bits, usually 1s,are called stop bit



Synchronous Transmission

- In Synchronous transmission, we send bits one after another without start/stop bit or gapes. It is the responsibility of the receiver to group the bits.
- The advantage of the synchronous transmission is the speed. With no extra bits or gaps to introduce at the sending end and remove at the receiving end. Byte synchronization is accomplished in the data link layer



Synchronous Transmission

2.0 Reliable Data Transmission

Contents

Data Transfer rate

- The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time. In general, the greater the bandwidth of a given path, the higher the data transfer rate.

- In computers, data transfer is often measured in bytes per second. The highest data transfer rate to date is 14 terabits per second over a single optical fiber, reported by Japan's Nippon Telegraph and Telephone (NTT Do Como) in 2006.

Channel Capacity

- In computer science the term channel capacity refers to the maximum data (information) that can be supported by the communication media connected to the systems in the network.
- In simple words it indicates data traffic of channel(channel like co axial cable or optical fiber or any transmission media)
- the Shannon–Hartley theorem states the channel capacity *C*, meaning the theoretical tightest upper bound on the information rate of clean data that can be sent with a given average signal power *S* through an analog communication channel subject to additive white Gaussian noise of power *N*, is:

  $C = Blog_2\left(1 + \frac{S}{N}\right)$where

  1. *C* is the channel capacity in bits per second;
  2. *B* is the bandwidth of the channel in hertz ;
  3. *S* is the average received signal power over the bandwidth measured in watts ;
  4. *N* is the average noise or interference power over the bandwidth, measured in watts;*S/N* is the signal-to-noise ratio (SNR) or the carrier-to-noise ratio (CNR) of the communication signal to the Gaussian noise interference expressed as a linear power ratio (not as logarithmic decibels).

- Nyquist rate: In 1927, Nyquist determined that the number of independent pulses that could be put through a telegraph channel per unit time is limited to twice the bandwidth of the channel. In symbols

$$f_p \leq 2B$$

- where f_p is the pulse frequency and B is the bandwidth (in hertz). The quantity 2B later came to be called the Nyquist rate, and transmitting at the limiting pulse rate of 2B pulses per second as signalling at the Nyquist rate.
- Nyquist published his results in 1928 as part of his paper "Certain topics in Telegraph Transmission Theory."

2.2 Switching

- A switched network consist of a series of interlink nodes called switches.
- Switches are devices capable of creating temporary connection between two more devices linked to the switch.
- Switched networks are divide into three broad categories :
    1. circuit switched network
    2. packet-switched network
    3. .Message-switched network

circuit switched network

- A circuit switched network consist of a set of switches connected by a physical link.
- A connection between two station is a dedicated path made up one or more links.
- Each link is normally divided into n channels by using FDM or TDM.

Message-switched network

- In message switching, each switch stores whole message and forward it to the next switch.

2.2Packet Switching

- Packet switching can be used as an alternate to circuit switching. In the packet switched networks, data is sent in discrete units that have variable length. They are called as packets. There is a strict upper bound limit on the size of packets in a packet switch network. The packet contains data and various control information.

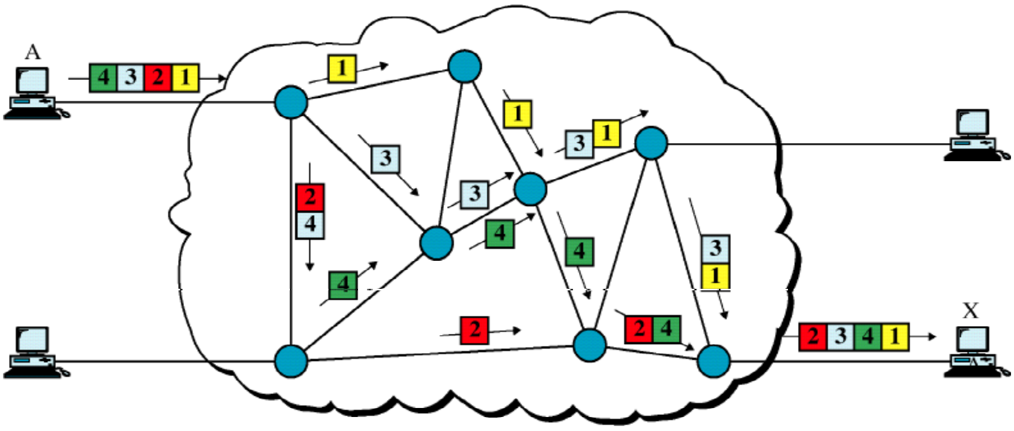
- The packet switched networks allow any host to send data to any other host without reserving the circuit. Multiple paths between a pair of sender and receiver may exist in a packet switched network.
- One path is selected between source and destination. Whenever the sender has data to send, it converts them into packets and forwards them to next computer or router. The router stores this packet till the output line is free.
- Then, this packet is transferred to next computer or router (called as hop). This way, it moves to the destination hop by hop. All the packets belonging to a transmission may or may not take the same route. The route of a packet is decided by network layer protocols.

Types of Packet Switching

The packet switching has two approaches: Virtual Circuit approach and Datagram approach.

Datagrams

- In datagram packet switching each packet is transmitted in any order.
- Every packet contain full packet of source and destination. Every packet is treated as individual, independent transmission.
- Even if a packet is a part of multi-packet transmission the network treats it as though it existed alone. Packets in this approach are called **datagrams.**
- Datagram switching is done at the network layer. Figure show how a datagram approach is used to deliver four packets from station A to station X. All the four packets belong to same message but they may travel via different paths to reach the destination *i.e.* station X.



- Datagram approach can cause the datagrams to arrive at their destination out of order with different delays between the packets.
- Packets may also be lost or dropped because of lack of resources. The datagram networks are also referred as connectionless networks. Here connectionless means that the switch does not keep information about connection state. There are no connection establishment or tear down phases.
- The datagram can arrive at the destination with a different order from the order in which they were sent. The source and destination address are used by the routers to decide the route for packets. Internet use datagram approach at the network layer.

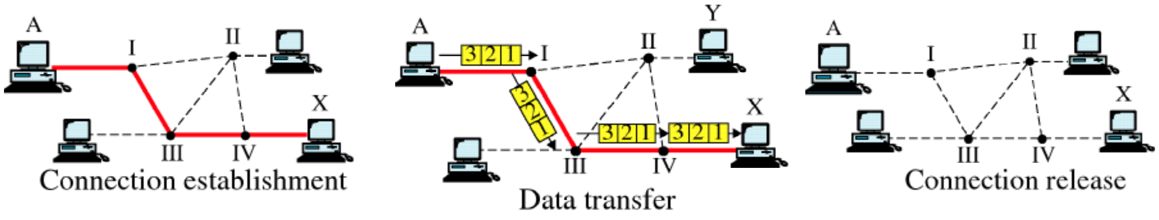
Virtual Circuit

- All the packets belonging to a message are preserved in order.
- A single route is chosen between sender and receiver at the beginning of the session.
- All packets transmitted one after another along that route
- Virtual circuit transmission is implemented in two formats:

1. Switched Virtual Circuits (SVC)
2. Permanent Virtual Circuits (PVC)

Switched Virtual Circuits (SVC)

- It can be compared to dial up lines in circuit switching.
- In this method, a virtual circuit is created when it is needed and exists only during the transmission.
- Suppose station A wants to send three packets to station X.
- First station A request to establish the connection to station X.
- Once the connection takes place, the packets are sent one after another in a sequential order.
- When the last packet is received, the station A is acknowledged and the connection is released.
- Each time when A whishes to communicate with X a new route is established.



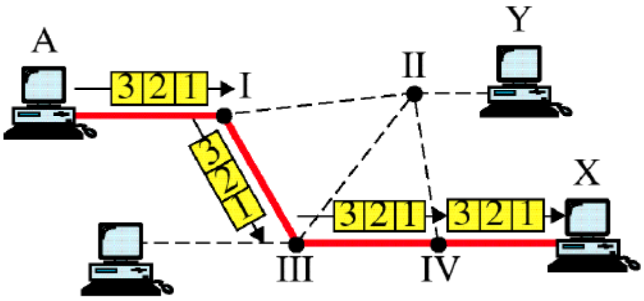
Connection establishment

Data transfer

Connection release

Permanent Virtual Circuits (PVC)

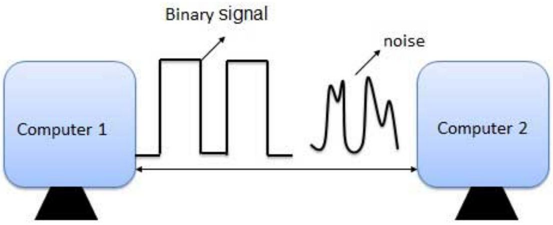
- It can be compared to leased lines in circuit switching
- In this method the same virtual circuit is provided between two users on a continues basis.
- The circuit is dedicated to specific users.
- Hence connection establishment and connection termination are not required



Data transfer

Different methods of Error Detection, Error Recovery or Error Correction

- Error means a condition when output information is not same as input information.
- When transmission of digital signals takes place between two systems such as a computer, the transmitted signal is combined with the "Noise".

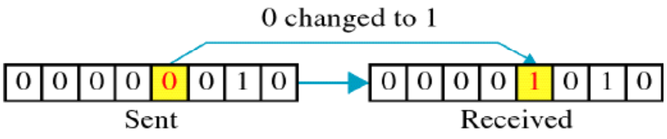


- The noise can introduce an error in the binary bits travelling from one system to other. That means 0 may change to 1 or a 1 may change to 0.Error must be detected and corrected.

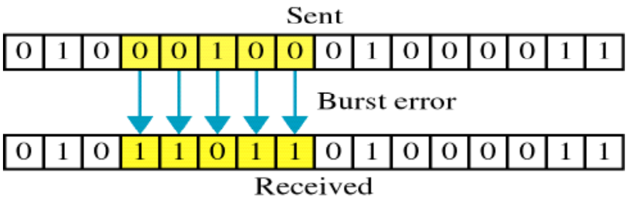
Types of errors

There are mainly two types of error occures

- **Single bit error:**
  In a single bit error, only one bit in the data unit has changed.



- **Burst error:**
  A burst error means two or more bits in the data unit have changed

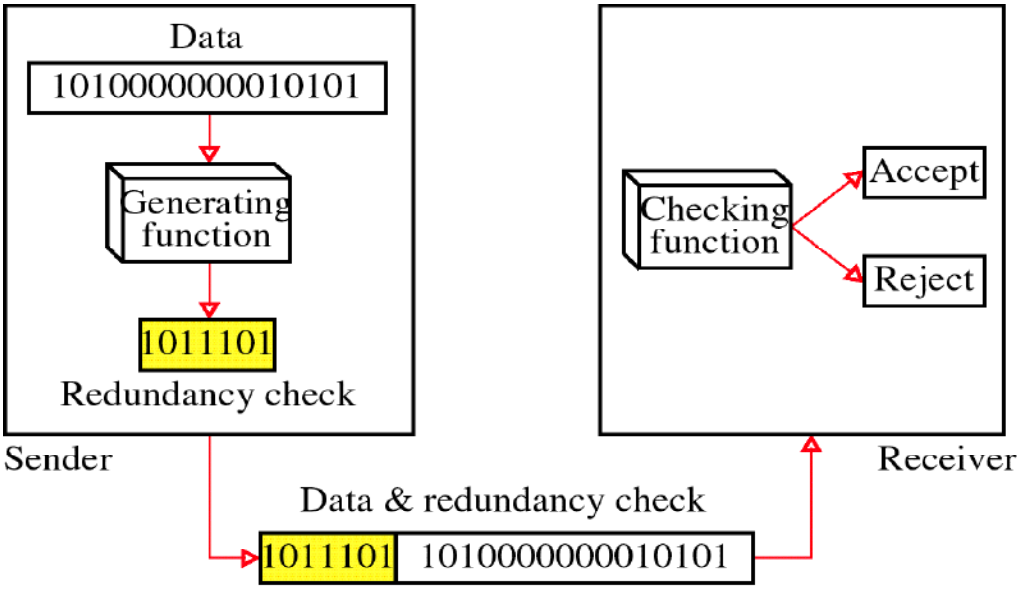


Detection

- The parity checking at the receiver can detect the presence of an error if the parity of the receiver signal is different from the expect parity.
- That means if is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity then the receiver can conclude that the received signal is not correct.
- If presence of error is detected then the receiver will ignore the received byte and request for retransmission of the same byte to the transmitter.

Redundancy

- All error detection/correction methods are based on redundancy. The redundancy bits are added with data, and then data with redundancy bit sent from source to destination. At the destination end using checking function check the data is correct or not, if correct then accept else reject.



Error Detection

- Four types of redundancy checks are used in data communication
    1. Vertical Redundancy Check (VRC)
    2. Longitudinal Redundancy Check (LRC)
    3. Cyclic Redundancy Check (CRC)
    4. Checksum

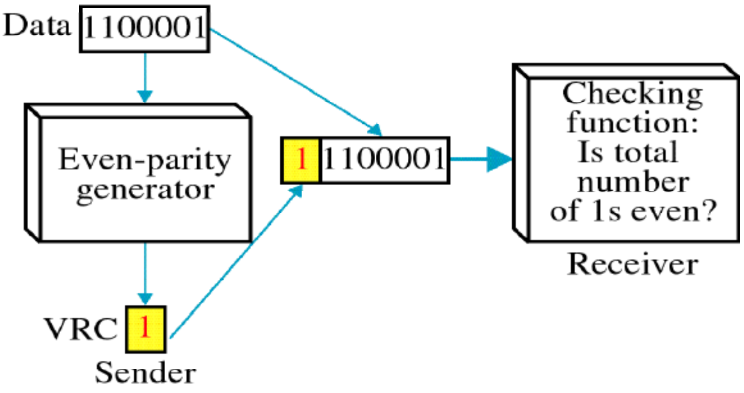
Vertical Redundancy Check (VRC)

- The most common and least expensive mechanism for error detection.In this technique a redundant bit, called a parity bit, is appended to every data unit. There are two types of parity bit used

1. **Even parity** -- Even parity means the number of 1's in the given word including the parity bit should be even (2,4,6,....).
2. **Odd parity** -- Odd parity means the number of 1's in the given word including the parity bit should be odd (1,3,5,....).

Use of Parity Bit

- The parity bit can be set to 0 and 1 depending on the type of the parity required.
- For even parity this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even.

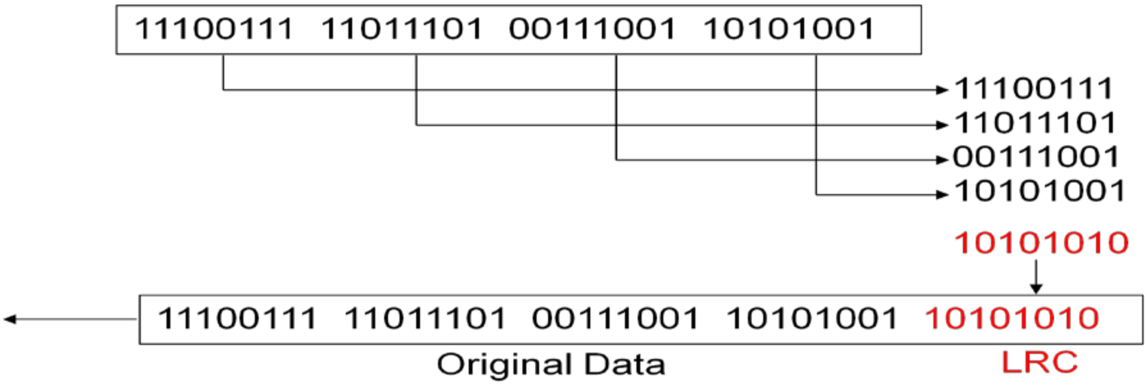


- For odd parity this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd.
- Append a single bit at the end of data block such that the number of ones is even.VRC is also known as **Parity Check**
- Performance:
    - Detects all odd-number errors in a data block

Longitudinal Redundancy Check (LRC)

In longitudinal redundancy check, a block of bits is divided into row and redundant row of bits, is added to a whole block

Original data**11100111 11011101 00111001 10101001**



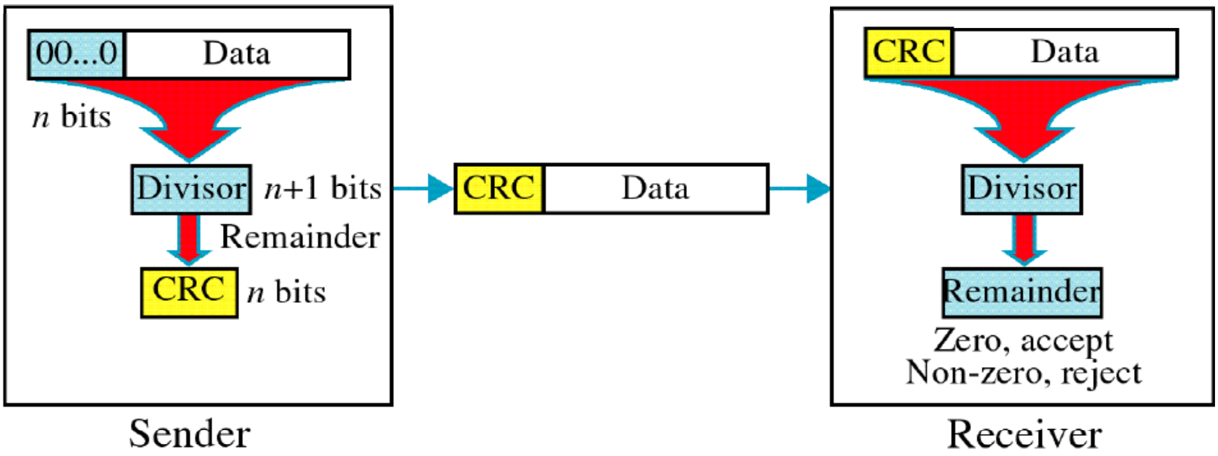
- Organize data into a table and create a parity for each column
- Then attach eight parity to the original data and send them to the receiver.
- At the receiving end, the receiver checks LRC using same method, some of the bits do not follow the even parity rule and the whole block is discarded.
- Some error patterns remain undetected:
  - e.g. 2 bits in the same position but in different rows change their values
- Performance:
  - LRC detects burst errors better than VRC

Cyclic Redundancy Check(CRC)

- It is most powerful method for error detection.
- A sequence of redundant bits, called the CRC or the CRC reminder is appended to the end of a data unit.
- CRC must have exactly one less bit then the divisor, and appending it to the end of the data string.
- There are three basic steps used

  1. A string of *n* 0s 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* bits
  2. The newly elongated data unit is divided by a divisor using a process called a binary division. The reminder resulting from this division is the CRC.

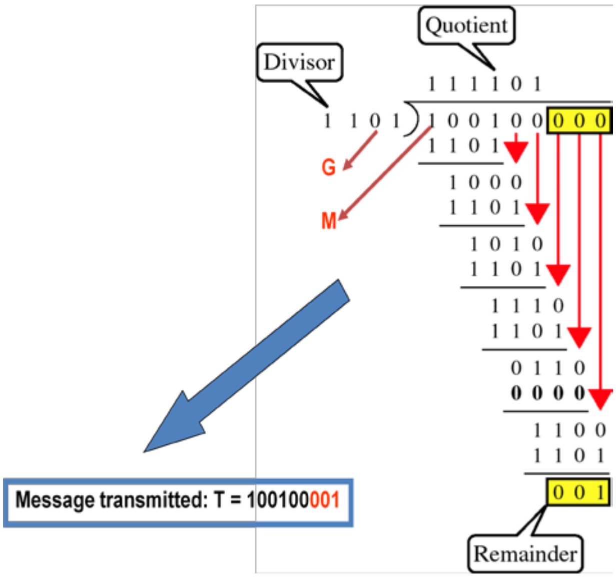
3. The CRC of n bits is derived in step2 replaces the appended 0s at the end of the data unit.



- ➢ At its destination, the incoming data unit is divided by the same devisor, if there is no reminder the data unit is accepted else rejected.

CRC Generator

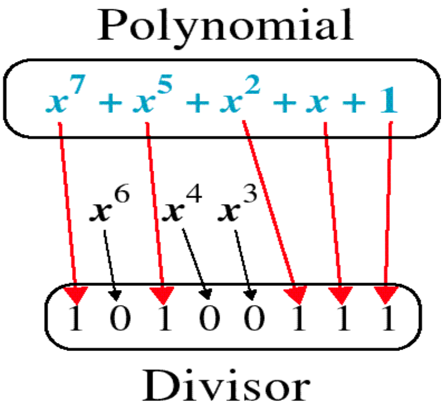
- ➢ It uses modulo-2 division .In first step the 4 bit divisor is subtracted from the first four bits of the dividend.
- ➢ Each bit of the divisor is subtracted from the from the corresponding bit of the dividend without disturbing the next higher



- ➢ The first bit of the reminder is dropped -If the second bit is also zero, it is retained, and the dividend for the next step will begin with 0.This process repeats until the entire dividend is used.

Polynomials

- It is most often represented not as a string of 1s and 0s,but as an algebraic polynomial.
- A polynomial is $x^6+x^4+x^3+x+1$
- The polynomial format is useful for two reasons
  1. It is short
  2. It can be used to proof the concept mathematically
- Associate bits with coefficients of a polynomial



Checksum

- Check sum is the method usedfor error detection mechanism. Checksum is used in the upper layers, while Parity checking and CRC is used in the physical layer. Checksum is also on the concept of redundancy.
- In the checksum mechanism two operations to perform.

Checksum generator

- Sender uses checksum generator mechanism. First data unit is divided into equal segments of n bits. Then all segments are added together using 1's complement. Then it complements ones again. It becomes Checksum and sends along with data unit.
- Exp: If 16 bits 10001010 00100011 is to be sent to receiver.
  So the checksum is added to the data unit and sends to the receiver. Final data unit is 10001010 00100011 01010000.

Checksum checker

- Receiver receives the data unit and divides into segments of equal size of segments. All segments are added using 1's complement. The result is completed once again. If the result is zero, data will be accepted, otherwise rejected.
- The final data is nonzero then it is rejected.

Error Correction

Error correction is handled by two ways

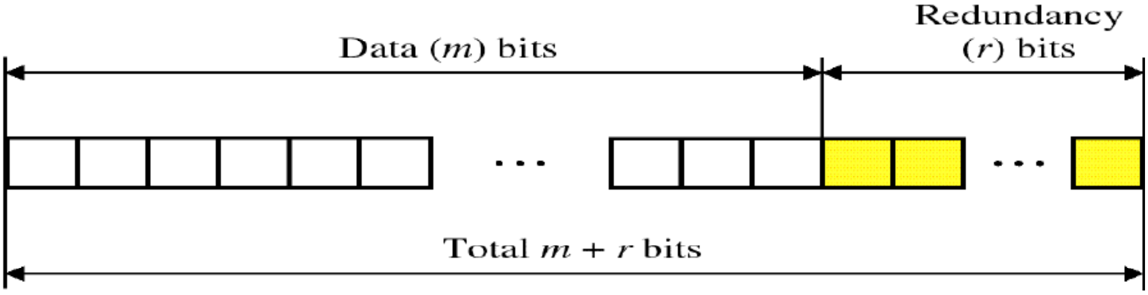
1. **Single bit error correction**
2. **Burst error correction**

Single bit error correction

- Let us take anASCII character of 7 Bits.
- The Situations occur may be: No error, Error in 1st bit, Error in 2nd bit, …, Error in 7th bit.

Redundancy bit

- At first glance, we would need 3 redundant bits to perform correction of 7 bit ascii character because three bits can show eight different states
- However, errors can affect the redundant bits, too.



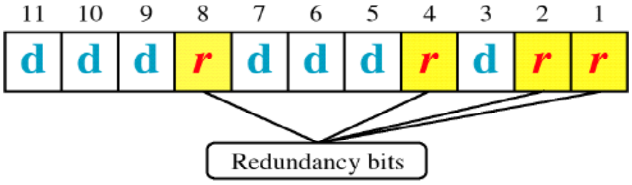
- Number of redundant bits r should be chosen in such a way that all single-bit errors, and these are m+r+1 ones, can be corrected.
- Since r bits can have 2^r different states, a sufficient condition is:

  2^r>= m+r+1

  - For example, for ASCII code (m=7) the smallest value of r is 4:
  - 16 = 2^4>= 7+4+1 = 12

Hamming code

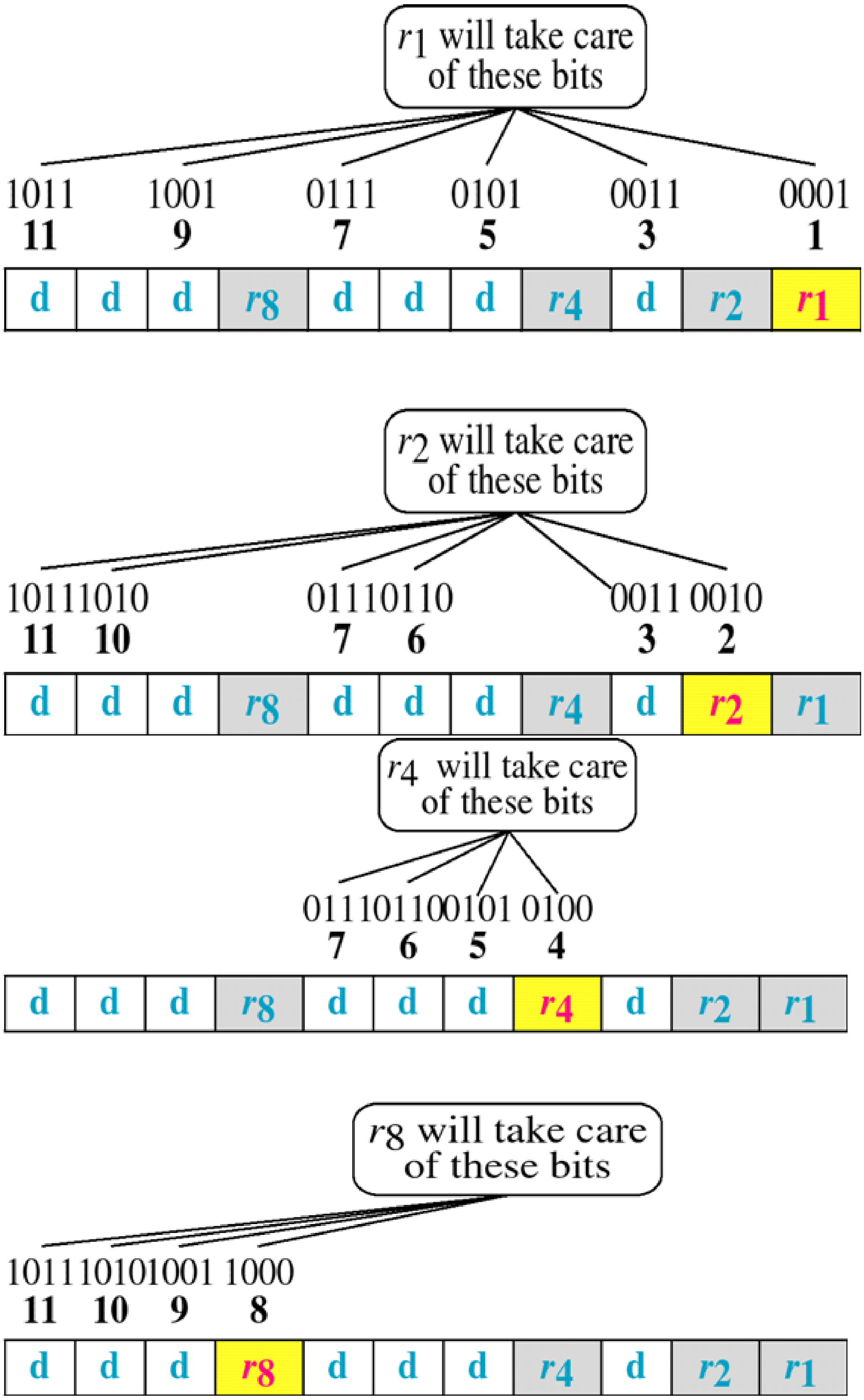
- Place the redundant bits (r-bits) in different positions.
- Each r-bit is the parity bit (or VRC bit) for a subset of the entire data.
- Receiver checks the parity bits again, and can identify the bit in error (if any).
- Placement of the r-bits for ASCII characters:



- r-bits are placed in positions which are power of 2.
- Details of the r-bit placement
- check bit r1 covers all odd numbered bits (e.g, 1, 3, 5, **. . .**)

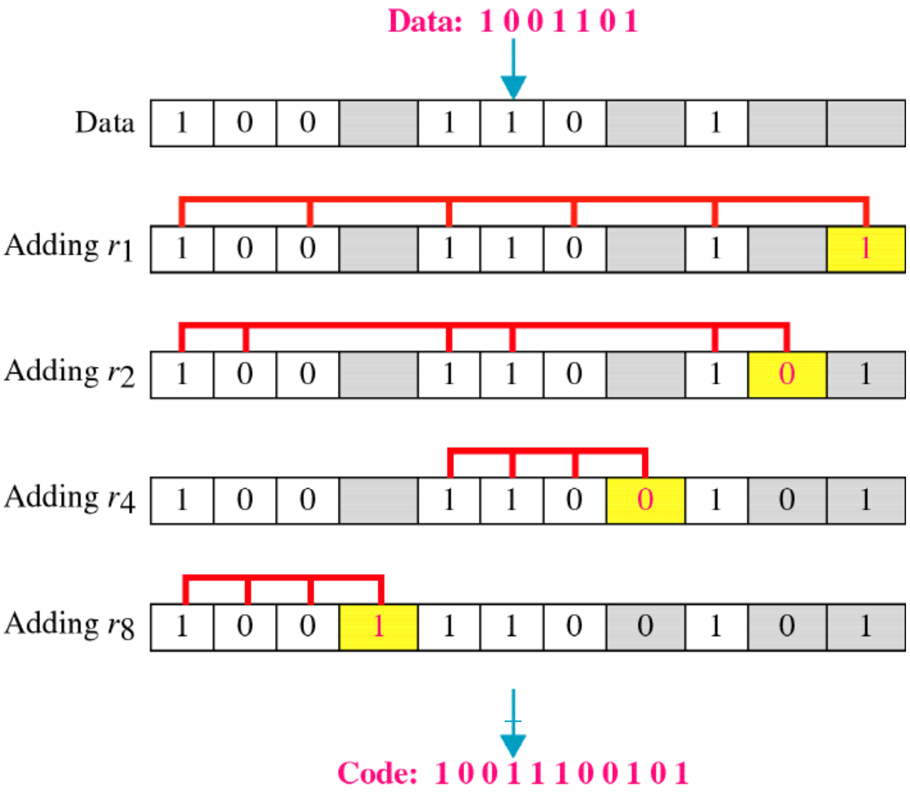
- check bit r2 covers bits 2, 3, 6, 7, 10, 11, . . .
- check bit r4 covers bits 4, 5, 6, 7, 12, 13, 14, 15, . . .

check bit r8 covers bits 8, 9, 10, 11, 12, etc.


r1 will take care of these bits
1011 11
1001 9
0111 7
0101 5
0011 3
0001 1
d d d r8 d d d r4 d r2 r1
r2 will take care of these bits
10111010 11 10
01110110 7 6
0011 0010 3 2
d d d r8 d d d r4 d r2 r1
r4 will take care of these bits
011101100101 0100 7 6 5 4
d d d r8 d d d r4 d r2 r1
r8 will take care of these bits
101110101001 1000 11 10 9 8
d d d r8 d d d r4 d r2 r1

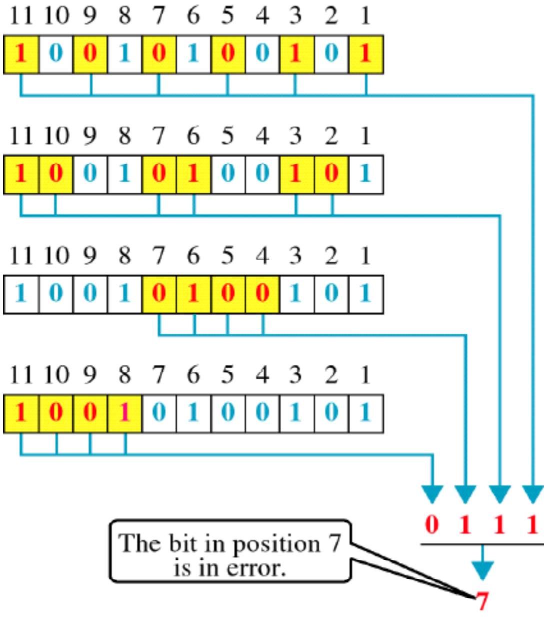
- ➢ Calculating the values of the r-bits in sender side.
- ➢ In first step, weplace each bit of the original character in its appropriate position in the 11 units.

- In the subsequent step we calculate the even parities for the various bit combinations.
- The parity value for each combination is the value of the corresponding r bit.
- For example,the value of r1 is calculated to provide even parity for a combination of bits 3,5,7,9 and 11.the value of r2 is calculated to provide even parity with bits 3, 6,7,10 and 11. the value of r4 is calculated to provide even parity with bits 4,5,6 and 7. The value of r8 is calculated to provide even parity with bits 8,9,10 and 11.



Error detection and correction

- The number 7 bit has been changed from 1 to 0.
- The receiver takes the transmission and recalculates 4 new VRCs using the same sets of bits used by the sender plus the relevant parity(r) bit for each set.
- Then it assembles the parity values into a binary number in order of r position (r8, r4, r2, r1).
- In our example this step gives us the



binary number 0111, which is precise location of the bit in error.

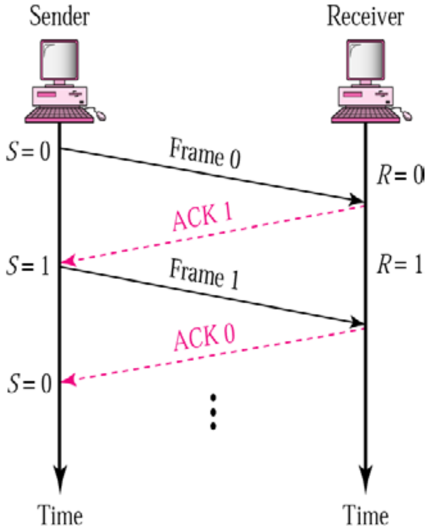
- Once the bit is identified the receiver can receive its value and correct the error.

Flow Control

- A flow control is asset of procedures that tells the sender how much data it can transmit before it must wait for an ACK from the receiver.
- The flow of data must not be allowed to overwhelm the receiver.
- Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily
- Two types of mechanism can be deployed in the scenario to control the flow:

Stop -and -Wait

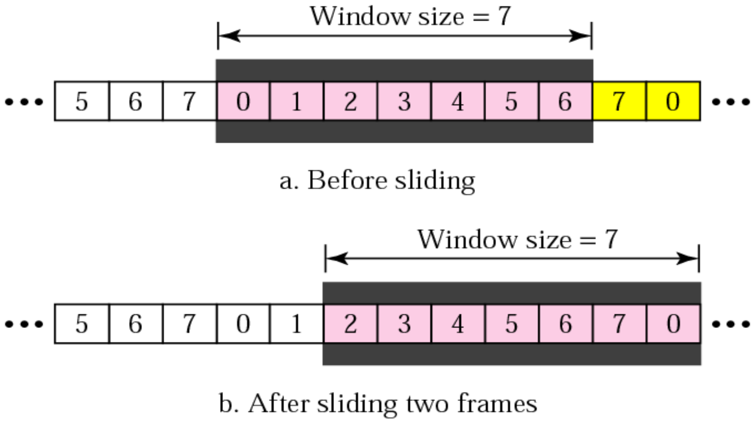
- In a stop- and- wait method of flow control, the sender waits for an ACK after every it sends.
- In the stop- and-wait method of flow control, the sender sends one frame and waits for an ACK before sending the next frame.
- Only when an ACK has been received is the next frame sent.
- This process of alternately sending and waiting repeats until the sender transmit an end of transmission frame
- The advantage of stop-and-wait is simplicity: each frame is checked and acknowledged before the next frame is sent.
- The disadvantage is inefficiency: the stop-and-wait is slow



Sliding Window

- In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgement.
- Frames can be sent one right after another.

- The receiver acknowledges only some of the frames using a single ACK to conform the receipt of multiple data frames
- In sliding window method of flow control, several frames can be in transit at a time.
- Sliding window refers imaginary box at both the sender and receiver.
- This window can hold frames at either end and provides an upper limit on the number of frames that can be transmitted before requiring an ACK.
- Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full.
- To keep track of which frames have been transmitted and which received, sliding window introduces the identification scheme based on the size of the window.



a. Before sliding

b. After sliding two frames

- The frames are numbered modulo-n, which means they are numbered from 0 to n-1.
- For example, if n=8 the frames are numbered 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1,...... The window is n-1 .
- When the receiver sends an ACK , it includes the number of the next frame it excepts to receive.
- In other words to acknowledge the receipt of a string of frames ending in frame 4,the receiver sends an ACK containing the number 5.
- When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

Sender Window

- At the beginning of the transmission the senders window contains n-1 frames.
- As frames are sent out the left boundary of the window moves in word, shrinking the size of the window. Given the window of the size w, if three frames have been transmitted since the last ACK, then the no of frames left in the window is w-3.
- Once an ACK arrives the window expands to allow in a number of new frames equal to the no of frames acknowledged by that ACK.

- Conceptually the sliding window of the sender shrinks from left when frames of data are sent, the sliding window of the sender expands when ACK are received.

Receiver window

- At the beginning of transmission, the receiver window contains not n-1 frames but n-1 spaces for frames.
- As new frames come in the size of the receiver window shrinks.
- The receiver window therefore represents not the no of frames received but the no of frames that may still be received before an ACK must be sent.
- Given a window size of w, if three frames are received without an ACK being returned, the no of spaces in the window is w-3.
- As soon as an ACK is sent the window expands to include places for a no of frames equal to the no of frames acknowledged.
- Conceptually, the sliding window of the receiver shrinks from the left when frames of data are received. The sliding window of the receiver expands to the right when ACKs are sent.

3.0 Connections and Interfacing

Contents

3.1 Introduction to serial and parallel connections

Parallel connection

- Parallel connections have multiple wires running parallel to each other and can transmit data on all the wires simultaneously.
- The speed of a parallel data link is equal to the number of bits sent at one time times the bit rate of each individual path; doubling the number of bits sent at once doubles the data rate.
- In practice, clock skew reduces the speed of every link to the slowest of all of the links.

Serial connections

- **Serial connections** have a single wire connected to each other and can transmit by sending data one bit at a time, sequentially, over a communication channel or computer bus.
- This is in contrast to parallel communication, where several bits are sent as a whole, on a link with several parallel channels.
- Keyboard and mouse cables and ports are almost invariably serial -- such as PS/2 port and Apple Desktop Bus and USB.
- Practically all long-distance communication transmits data one bit at a time, rather than in parallel, because it reduces the cost of the cable.
- The cables that carry this data (other than "the" serial cable) and the computer ports they plug into are usually referred to with a more specific name, to reduce confusion.

3.2 Half Duplex, Full Duplex

Simplex

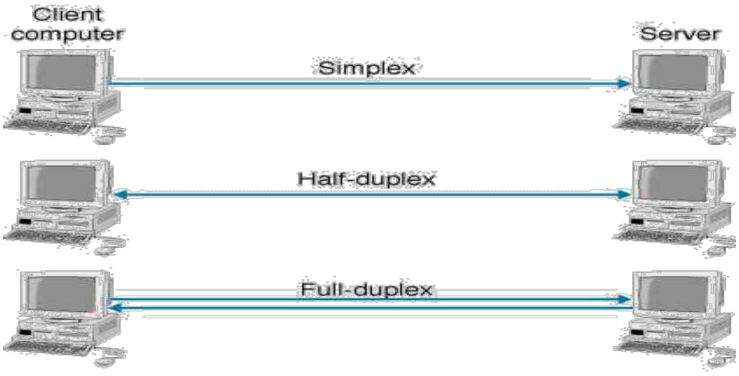
- In the broad band net work carries multiple signals in a single cable at a same time .
- The example of broad band network is cable TV. In a single cable carries multiple channels

Half duplex

- In half duplex communications two computer communicate over a long, data typical travels in only one directions at a time because the base band network used for most LAN's supports only a single signal. This is called half duplex communications

- An example of an Half duplex communications is two way radio set in which only one part can transmit at any one time and each pat must say 'over' to signal.

Full duplex



- The two systems that can communicate in both directions simultaneously are called full duplex mode communications
- The most common example of a full duplex network is once again the telephone system. Both part can speak simultaneously during the telephone call and each part can hear the other at the same time.

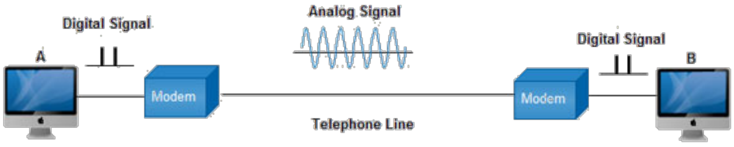
3.3 RJ-45

- **Registered Jack-45**, a **RJ-45** is an 8-pin connection used for Ethernet network adapters. This connector resembles the RJ-11 or 6-pin connector used with telephones in the United States, but they're completely different. The picture is of a RJ-45 connector separated from the cable.
- This connector is most commonly connected to the end of Cat5 cable, which is connected between a computer network card and a network device such as a network router.
- This makes it ideal for devices that need to transfer high levels of data in real-time, such as video devices.
- Registered Jack-45, an eight-wire connector used commonly to connect computers onto a local-area networks (LAN), especially Ethernets. RJ-45 connectors look similar to the ubiquitous RJ-11 connectors used for connecting telephone equipment, but they are somewhat wider.

3.3 Modular Connection Modem

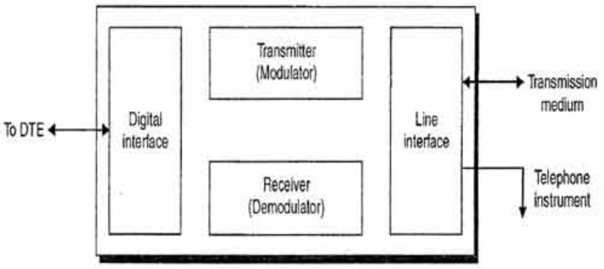
- Modem is abbreviation for Modulator – Demodulator**.** Modems are used for data transfer from one computer network to another computer network through telephone lines.
- The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

- **Modulator** converts information from digital mode to analog mode at the transmitting end and demodulator converts the same from analog to digital at receiving end.



Modulation/DeModulation

- The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is referred to as digitizing**.**



Building blocks of a modem

- When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.
- The modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier.
- This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.
- The transmission medium between the two modems can be dedicated circuit or a switched telephone circuit.
- If a switched telephone circuit is used, then the modems are connected to the local telephone exchanges.
- Whenever data transmission is required connection between the modems is established through telephone exchanges.

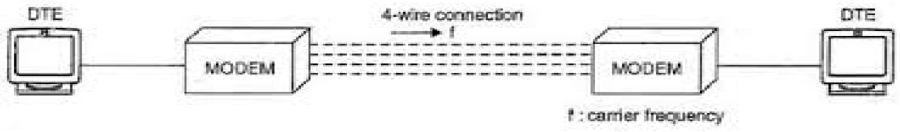
Modems can be of several types and they can be categorized in a number of ways.

- half duplex modem
- full duplex modem
- asynchronous modem
- synchronous modem.

Half duplex modem

- Half duplex modems use almost the entire bandwidth and so waste very little space.

- But because there is not then room for two channels, the information may only move one direction at a time.
- This means that time must be taken after each transmission to "turn around" the line, and extra interface signals are required to control which station is transmitting.



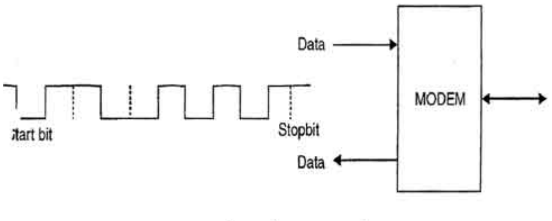
(a) Half Duplex

Full duplex modem

- A Full duplex modem can simultaneously transmit and receive on a connection.
- In other words, the river is divided into two channels in which information barges may travel in both directions at the same time.
- This is also true of the telephone line; some of the bandwidth is needed to separate the transmit and receive channels.
- This space is then wasted and cannot be used to carry information. As a result in most full duplex modems have relatively slow data transmission rates.

Asynchronous Modem

- Asynchronous modems can handle data bytes with start and stop bits.
- There is no separate timing signal or clock between the modem and the DTE.

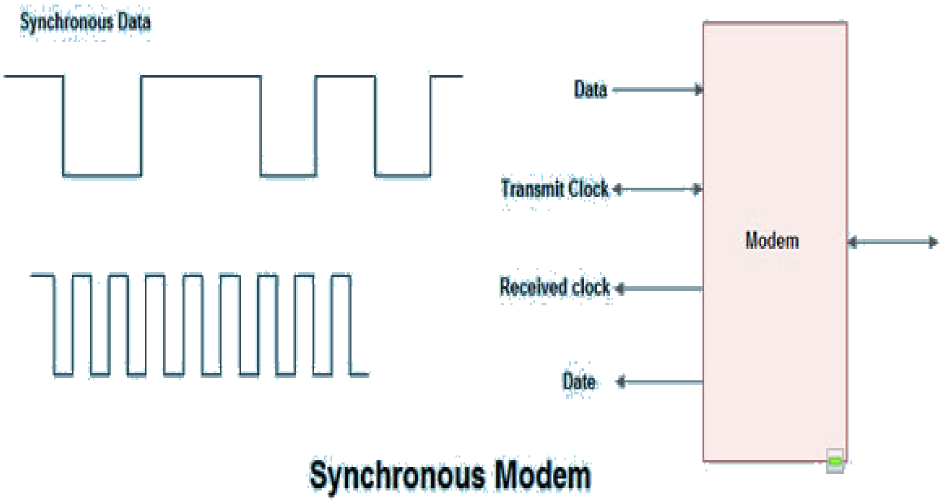


Asynchronous modem

- The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse .

Synchronous Modem

- Synchronous modems can handle a continuous stream of data bits but requires a clock signal.
- The data bits are always synchronized to the clock signal.
- There are separate clocks for the data bits being transmitted and received.
- For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem.



Synchronous Modem

Modulation techniques used for Modem

- The basic modulation techniques used by a modem to convert digital data to analog signals are
  1. Amplitude shift keying (ASK).
  2. Frequency shift keying (FSK).
  3. Phase shift keying (PSK).
  4. Differential PSK (DPSK).

These techniques are known as the binary continuous wave (CW) modulation.

Modems are always used in pairs. Any system whether simplex, half duplex or full duplex requires a modem at the transmitting as well as the receiving end.

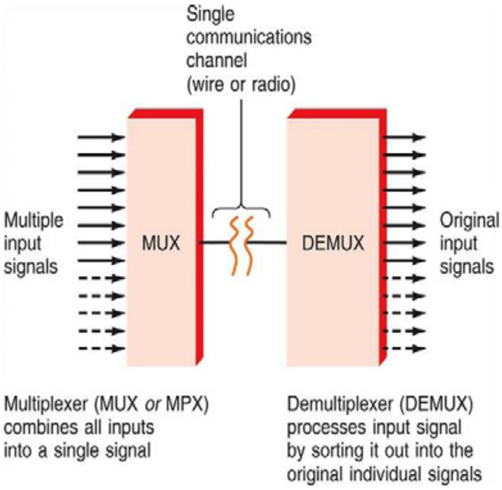
Thus a modem acts as the electronic bridge between two worlds - the world of purely digital signals and the established analog world.

4.0 Multiplexing

Contents

4.1 Concept of Multiplexing

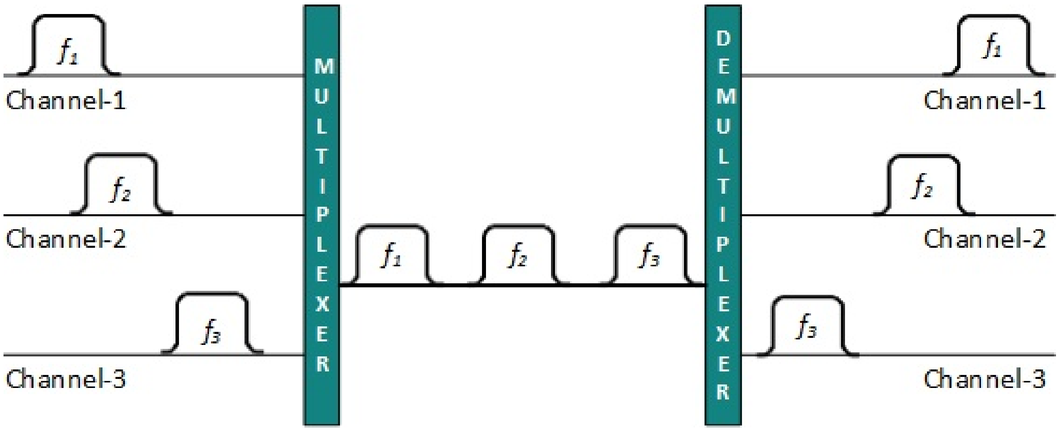
- Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.
- Communication is possible over the air (radio frequency), using a physical media (cable) and light (optical fiber). All mediums are capable of multiplexing.
- When more than one senders tries to send over single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and send to different receivers.


Single communications channel (wire or radio)
Multiple input signals
MUX
DEMUX
Original input signals
Multiplexer (MUX *or* MPX) combines all inputs into a single signal
Demultiplexer (DEMUX) processes input signal by sorting it out into the original individual signals

- Transmitting two or more signals simultaneously can be accomplished by running multiple cables or setting up one transmitter receiver pair for each channel , but this is an expensive approach.
- A single cable or radio link can handle multiple signals simultaneously using a technique known as multiplexing.Multiplexing permits hundreds or even thousands of signals to be combined and transmitted over a single medium.
- A device called a multiplexer (often shortened to "mux") combines the input signals into one signal. When the multiplexed signal needs to be separated into its component signal s (for example, when your email is to be delivered to its destination), a device called a d emultiplexer (or "demux") is used.
- Multiplexing was originally developed in the 1800s for telegraphy. Today, multiplexing is widely used in many telecommunications applications, including telephony, Internet com munications, digital broadcasting and wireless telephony.

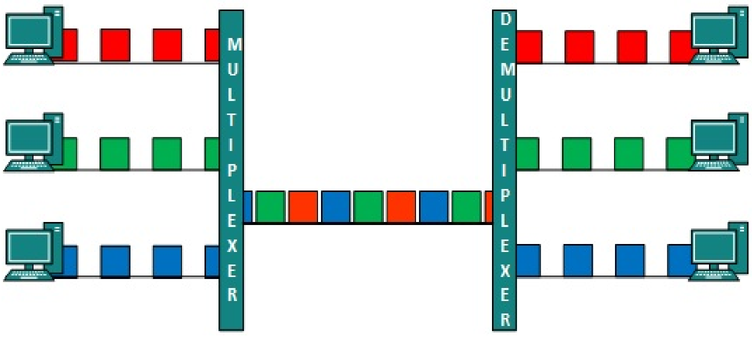
Frequency Division Multiplexing

- When the carrier is frequency, FDM is used.
- FDM is an analog technology.
- FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.
- Each user can use the channel frequency independently and has exclusive access of it.
- All channels are divided such a way that they do not overlap with each other. Channels are separated by guard bands.
- Guard band is a frequency which is not used by either channel.



Time Division Multiplexing

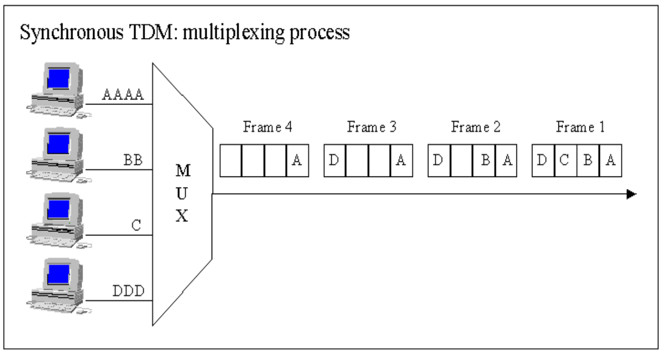
- TDM is applied primarily on digital signals but can be applied on analog signals as well.
- In TDM the shared channel is divided among its user by means of time slot.
- Each user can transmit data within the provided time slot only.



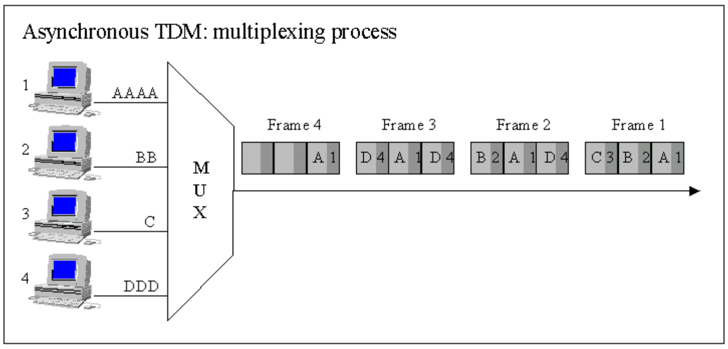
- Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.
- TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.

- When at one side channel A is transmitting its frame, on the other end De-multiplexer providing media to channel A.
- As soon as its channel A's time slot expires this side switches to channel B.
- On the other end De-multiplexer behaves in a synchronized manner and provides media to channel B. Signals from different channels travels the path in interleaved manner.
- 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.

1. **Synchronous TDM:** Time slots are pre assigned and are fixed. Each source is given its 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.

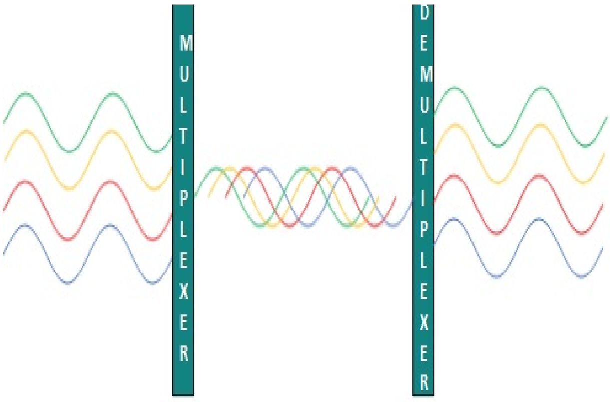


2. **Asynchronous TDM:** In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission.



Wavelength Division Multiplexing

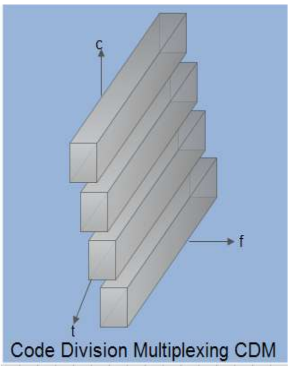
- Light has different wavelength (colors).
- In fiber optic mode, multiple optical carrier signals are multiplexed into on optical fiber by using different wavelengths.
- This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



- Further, on each wavelength Time division multiplexing can be incorporated to accommodate more data signals.

Code Division Multiplexing

- Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique Code. CDM uses orthogonal codes to spread signals.
- Each station is assigned with a unique code, called chip. Signals travels with these codes independently travelling inside the whole bandwidth. The receiver in this case, knows in advance chip code signal it has to receive signals.
- CDM is widely used in so-called second-generation (2G) and third-generation 3G wireless communications. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands. This is a combination of analog-to-digital conversion and spread spectrum technology.
- CDM may be defined as a form of multiplexing where the transmitter encodes the signal using a pseudo-random sequence. CDM involves the original digital signal with a spreading code. This spreading has the effect of spreading the spectrum of the signal greatly and reducing the power over anyone part of the spectrum. On the other hand, the receiver knows about the code generated and transmitted by the transmitter and therefore, can decode the received signal. Each different random sequence corresponds to a different communication channel from multiple stations.
- Code Division Multiplexing assigns each channel its own code to make them separate from each other. These unique underlying codes, which ~hen decoded restore' the original desired signal while totally removing the effect of the other coded channels. Guard spaces are realized by using codes with orthogonal codes..Figure explains how all channels C_i, use the same frequency at the same time for transmission.



Code Division Multiplexing CDM

- It may be understood that a single bit may be transmitted by modulating a series of signal elements at different frequencies in some particular order. These numbers of different frequencies per bit are called as the chip rate. If one or more bits are transmitted at the same frequency, it is called as frequency hopping. This will happen only when the chip rate ,is less than one because chip rate is the ratio of frequency and bit. At the receiving side, receiver decodes a 0 or a 1 bit by checking these frequencies in the correct order.

Disadvantage

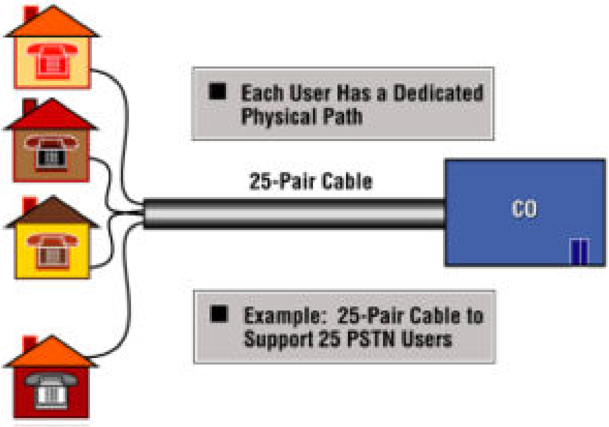
- A disadvantage of CDM is that each user's transmitted bandwidth is enlarged than the digital data rate of the source. The result is an occupied bandwidth approximately equal to the coded rate. Therefore, CDM and spread spectrum are used interchangeably. The transmitter and receiver require a complex electronic circuitry.

Advantage

- The main advantage of CDM is protection from interference and tapping because only the sender the receiver knows the spreading code.

Space-Division Multiplexing

- When we want to transmit multiple messages, the goal is maximum reuse of the given resources: time and frequency. Time-Division Multiplexing (TDM), operates by dividing the time up into time slices, so that the available time can be reused. Frequency-Division Multiplexing (FDM), operates by dividing up the frequency into transmission bands, so that the frequency spectrum can be reused. However, if we remember our work with directional antennas, we can actually reuse both time and frequency, by transmitting our information along parallel channels. This is known as **Space-Division Multiplexing**.


■ Each User Has a Dedicated Physical Path
25-Pair Cable
CO
■ Example: 25-Pair Cable to Support 25 PSTN Users

- Space division multiplexing (SDM) is nothing more than the provision of multiple fixed bandwidth channels by multiple physical paths (i.e., pairs of wires or optical fibers). A good example of SDM is the use of a 25-pair cable to carry the conversations of 25 individual users from the customer's premises to the local telephone company's central office location.
- SDM is not the most efficient technique from the standpoint of outside plant resources, but it does play a role in all carrier networks. A given copper or fiber facility has a finite capacity for information. When that capacity is exhausted, SDM is the only alternative.
- By some arguments, SDM is not a multiplexing scheme at all, since it does not support multiple communication channels on a single medium. However, the concept is an important one because it occurs both in the deployment of transmission facilities as well as the internal architecture of some switches.

5.0 Network Applications

Contents

5.1 Networks users

- Based on the roles of the computers attached to the networks, network users are divided into two types:
- **Server-based Network user**
- **Domain-based network user**

Server-based Network user

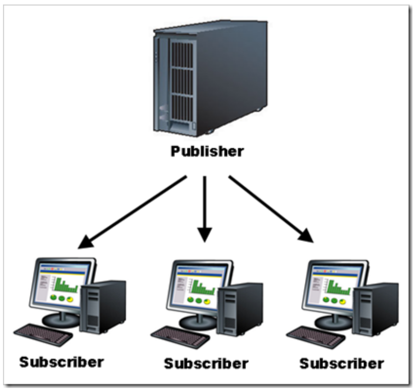
- Users log in once to access resources.
- Stronger security because of server management
- Shared files by members
- Shared printers and other resources
- E-mail capability through an email server
- Applications stored in a central location
- Backups scheduled and performed from a central location
- Shared resources can reflect the work patterns of subgroups.
- More efficient software upgrades
- Server-based networks are defined by the presence of servers on a network that provide security and administration of the network.
- Server-based networks divide processing tasks between clients and servers. Clients request services, such as file storage and printing, and servers deliver them.
- Server computers typically are more powerful than client computers, or are optimized to function as servers.

Domain-based network user

- In Windows NT, server-based networks are organized into what are called *domains*.
- Domains are collections of networks and clients that share security trust information.
- Domain security and logon permission are controlled by special servers called domain controllers.

- There is one master domain controller, called the Primary Domain Controller (PDC), which may be assisted by secondary domain controllers called Backup Domain Controllers (BDC) during busy times or when the PDC is not available for some reason.
- No computer users can access the resources of servers in a domain until they have been authenticated by a domain controller.

5.1Central Servers



- A central server is a computer system that provides local area networking services to multiple users.
- It consists of one or more high speed computers that store official application and data files that can be shared by many different people.
- Central Server provides IT hosting services such as cloud computing, shared hosting, e-mail and online backup for the Brazilian market.
- As a pioneer of cloud computing services in Brazil, Central Server has been able to leverage key partnerships with market leaders such as Microsoft (SPLA) and VMware (vCloud Powered) to create hosting plans that span from virtual servers to full fledged Software Defined Data Centres (SDDC).
- We offer a managed platform that supports multiple programming languages for Windows Server and Linux environments, including: ASP, ASP.Net, PHP, CGI, Java; in addition to several database options.
- Our proven email services are trusted by thousands of companies that rely on advanced features, such as: personalized webmail, email marketing, mail archiving and antispam protection for their mission critical communication.
- Central Server uses of two state-of-the-art data centres in the southern city of Curitiba, connected to multiple internet backbones and enabled to provide high availability, business continuity and disaster recovery solutions.

5.2 LAN Environment

- The local area network (LAN) modelling features of networks are designed to investigate connectionless networks in which data is transmitted between devices in discrete units called packets.
- A valid path may not exist between a source and destination in this type of network.

- A connectionless network relies on forwarding or routing algorithms running in various network devices to forward a packet appropriately through the network to its final destination.
- In a typical LAN model network, you might have collections of Computing Device models - Workstation, Server, and Printer models -connected to a Hub or Media model representing a single LAN and a series of LANs linked by Bridge or Router models.
- The Workstation and Server models generate packets destined for other Computing Device models throughout the model network, and Router and Bridge models are responsible for forwarding packets between subnetworks.
- The LAN environment is less mature than the telecom environment of the netWorks application, and therefore it offers comparably less flexibility and functionality than its connection-oriented sibling.
- You can, however, still perform very interesting and useful LAN simulations using this environment.

LAN Components

- The LAN equipment models are developed around the premise that a LAN architecture consists of equipment connected to a transmission media through a network interface card (NIC).
- The default equipment models provided in the LAN environment are very different from the telecom equipment models, both in terms of structure and functionality. The four categories of LAN models are

    1. Network Adapter
    2. Network Medium
    3. Cable Connectors
    4. Power supply
    5. Hub/Switch/Router
    6. Network Software

Network Adapter (NA)

- A computer needs a network adapter to connect a network .it converts computer data into electronic signals.
- The network access element of its job is called media access control (MAU). The physical address of every computer on network is called its MAC address.
- All Internetwork and Computing Device models contain at least one NIC that is used to connect the model (through arcs) to a Transmission Media model to form a model LAN.

Network Medium (NM)

- Unshielded twisted pair cable used as a medium. It is generally referred to as network cable or Ethernet cable.
- Other cables are used i.e. shielded twisted pair cable, single mode and multi mode fiber optic cable.

Cable connector (CA)

- In wired network the most common format connector is RJ-45.
- It is otherwise called as RJ-45 port.

Power supply (PW)

- Both wired and wireless networks need a power supply.
- A wireless n/w uses the current to generate radio waves. a cable network sends data as an electronic pulses.

Hub/switch/router

- A hub is little more than a spliter.It repeats any signal coming into one of its ports out unto all its another port.
- A switch is more sophisticated version of a hub. It only send the signal onto the computer with the address written in the arriving message.
- Router is much more complicated and able to forward the message.

Network Software (NS)

- It uses the software like: server software, workstation software.
- In a network the computer connects with a server or main computer known as workstation. It also use the operating system which manages the workload with number of various type of software attached to it.
- LAN OS are novel Netware, Win NT, Win 2000, UNIX.
- All Internetwork and Computing Device models contain at least one NIC that is used to connect the model (through arcs) to a Transmission Media model to form a model LAN.
- All LAN equipment models also have reliability controls for simulating equipment failure and restoration.

Print Servers

- In a network printing can be done centrally because a network can:-
    - Allow users to share printers
    - Allow you to place printers where convenient, not just near individual computers
    - Achieve better workstation performance by using high-speed network data transfer, print queues, and spooling
    - Allow users to share network fax services

- Print services manage and control printing on a network, allowing multiple and simultaneous access to printing facilities.
- The network operating system achieves this by using print queues, which are special storage areas where print jobs are stored and then sent to the printer in an organized fashion.
- The user can then continue working in an application while the network takes care of the printing.
- Network printing also cuts costs by allowing shared access to printing devices. This is especially important when it comes to the more expensive varieties of printers. High-quality color printers, high-speed printers, and large-format printers and plotters tend to cost a lot.
- Another print service is fax services.
- With network print services, you can fax straight from your workstation to a receiving fax machine. This way, you can eliminate the step of printing a hard copy and scanning it into a fax machine.
- From an application, you can send a document to a fax queue, which then takes care of the faxing.
- Furthermore, with a fax server, you can receive faxes directly on your workstation.

Application Server

- Application services allow client PCs to access and use extra computing power and expensive software applications that reside on a shared computer. You can add specialized servers to provide specific applications on a network. For example, if your organization needed a powerful database, you could add a server to provide this application.

Message Servers

- Message servers provide message services in a wide variety of communication methods that go far beyond simple file services. With file services, data can pass between users only in file form. With message services, data can take the form of graphics, digitized video, or audio, as well as text and binary data. As hypertext links (electronic connections with other text, images, sounds, and so on) become more common in messages, message services are becoming an extremely flexible and popular means of transmitting data across a network.
- Message services must coordinate the complex interactions between users, documents, and applications. For example, with message services, you can send an electronic note, attached to a voice-mail message, to a fellow user on a network.
- There are four main types of message services:

  - Electronic mail
  - Workgroup applications
  - Object-oriented applications
  - Directory services

Database Servers

- Database services can provide a network with powerful database capabilities that are available for use on relatively weak PCs.
- Most database systems are client-server based. This means that the database applications run on two separate components:
  - The client-end portion of the application runs on the client, providing an interface and handling less intensive functions, such as data requests.
  - The server-end portion of the application handles the intensive performance of database operations. It runs on the database server, managing the database, processing queries, and replying to clients.

Directory service

- A **directory service** is the software system that stores, organizes, and provides access to information in a computer operating system's directory. In software engineering, a directory is a map between names and values. It allows the lookup of named values, similar to a dictionary.
- As a word in a dictionary may have multiple definitions, a directory service can associate a name with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.
- Directories may be very narrow in scope, supporting only a small set of node types and data types, or they may be very broad, supporting an arbitrary or extensible set of types. In a telephone directory, the nodes are names and the data items are telephone numbers. In the DNS the nodes are domain names and the data items are ip addresses (and alias, mail server names, etc.).
- In a directory used by a network operating system, the nodes represent resources that are managed by the OS, including users, computers, printers and other shared resources. Many different directory services have been used since the advent of the internet but this article focuses mainly on those that have descended from thex.500 directory service.
- A network service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and

peripheral devices such as printers. Ideally, the directory service should make the physical

- Network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected.
- There are a number of directory services that are used widely. Two of the most important ones are ldap, which is used primarily for e-mail addresses, and Netware directory service (NDS), which is used on Novel Netware networks. Virtually all directory services are based on the x.500 ITU standard, although the standard is so large and complex that no vendor complies with it fully.

Implementations of directory services

- Directory services were part of an Open Systems Interconnection (OSI) initiative to get everyone in the industry to agree to common network standards to provide multi-vendor interoperability.
- In the 1980s, the ITU and ISO came up with a set of standards - X.500, for directory services, initially to support the requirements of inter-carrier electronic messaging and network name lookup. The Lightweight Directory Access Protocol, LDAP, is based on the directory information services ofX.500, but uses the TCP/IP stack and a string encoding scheme of the X.500 protocol DAP, giving it more relevance on the Internet.
- There have been numerous forms of directory service implementations from different vendors. Systems developed before the advent of X.500 include:
- Domain Name System: (DNS), the first directory service on the Internet, which is still used everywhere today.
- Hesiod: was based on DNS and used at MIT's Project Athena.
- Network Information Service: (NIS), originally named Yellow Pages (YP), was Sun Microsystems' implementation of a directory service for Unix network environments. It served a similar role as Hesiod.
- Net Info: was developed by NeXT in the late 1980s for NEXTSTEP. After being acquired by Apple, it was released as open source and used as the directory service for Mac OS X before being deprecated in favour of the LDAP-based Open Directory. Support for Net Info was completely removed with the release of 10.5 Leopard.
- Banyan VINES: were the first scalable directory services offering.

- NT Domains: was developed by Microsoft to provide directory services for Windows machines prior to the release the LDAP-based Active Directory in Windows 2000. Windows Vista continues to support NT Domains, but only after relaxing the minimum authentication protocols it supports.

Advantages of Networks

File Sharing

- The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so.
- This saves him/her the hassle of carrying a storage device every time data needs to be transported from one system to another. Further, a central database means that anyone on that network can access a file and/or update it.
- If files are stored on a server and all of its clients share that storage capacity, then it becomes easier to make a file available to multiple users.

Resource Sharing

- Resource sharing is another important benefit of a computer network.
- For example, if there are twelve employees in an organization, each having their own computer, they will require twelve modems and twelve printers if they want to use the resources at the same time.
- A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing.
- All the computers can be interconnected using a network, and just one modem and printer can efficiently provide the services to all twelve users.

Inexpensive Set-Up

- Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses.
- A particular software can be installed only once on the server and made available across all connected computers at once.
- This saves the expense of buying and installing the same software as many times for as many users.

Flexible Handling

- A user can log on to a computer anywhere on the network and access his files.
- This offers flexibility to the user as to where he should be during the course of his routine.
- A network also allows the network administrator to choose which user on the network has what specific permissions to handle a file.
- For example, the network administrator can allot different permissions to User A and User B for File XYZ. According to these permissions, User A can read and modify File XYZ, but User B cannot modify the file.
- The permission set for User B is read-only. This offers immense flexibility against unwarranted access to important data.

Increased Storage Capacity

- Since there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent.
- A standalone computer might fall short of storage memory, but when many computers are on a network, the memory of different computers can be used in such a case.
- One can also design a storage server on the network in order to have a huge storage capacity.

Disadvantages of Networks

Security Concerns

- One of the major drawbacks of computer networks is the security issues that are involved.
- If a computer is a standalone computer, physical access becomes necessary for any kind of data theft.
- However, if a computer is on a network, a hacker can get unauthorized access by using different tools. In case of big organizations, various network security software need to be used to prevent theft of any confidential and classified data.

Virus and Malware

- If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too.

- Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply.
- Similarly, if malware gets accidentally installed on the central server, all clients in the network that are connected to that server will get affected automatically.

Lack of Robustness

- If the main file server of a computer network breaks down, the entire system becomes useless. If there is a central linking server or a bridging device in the network, and it fails, the entire network will come to a standstill.
- In case of big networks, the file server should be a powerful computer, which often makes setting up and maintaining the system doubly expensive.

Needs An Efficient Handler

- The technical skills and know-how required to operate and administer a computer network is considerably high. Any user with just the basic skills cannot do this job.
- Also, the responsibility that comes with such a job is high, since allotting username-passwords and permissions to users in the network are also the network administrator's duties.
- Similarly, network connection and configuration is also a tedious task, and cannot be done by an average user who does not have advanced knowledge of computers and/or networking.

Lack of Independence

- Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.
- Computer networks have had a profound effect on the way we communicate with each other today, and have made our life easier.
- From the World Wide Web to your local office LAN, computers have become indispensable in daily life, and networks have become a norm in most businesses.
- If networks are designed and configured keeping in mind its pros and cons , they are the best piece of facility you could ever have.

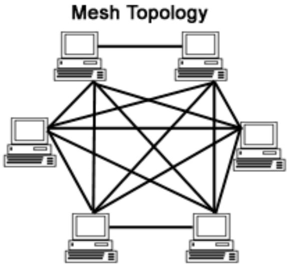
6.0 Network Structures

Contents

6.1 Topologies

- The way in which the connections are made of the physical devices is called the topology of the network.
- Network topology specifically refers to the physical layout of the network, especially the locations of the computers and how the cable is run between them.
- It is important to select the right topology for how the network will be used.
- Each topology has its own strengths and weaknesses.
- The four most common topologies are
  - Mesh topology
  - Bus topology
  - Star topology
  - Ring topology
  - Tree Topology
  - Hybrid Topology

Mesh topology



- A network setup where each computer and network device is interconnected with one another, allowing for most transmissions to be distributed, even if one of the connections go down.
- This topology is not commonly used for most computer networks as it is difficult and expensive to have redundant connection to every computer. However, this topology is commonly used for wireless networks.

Advantages of Mesh topology

- Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.
- Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.

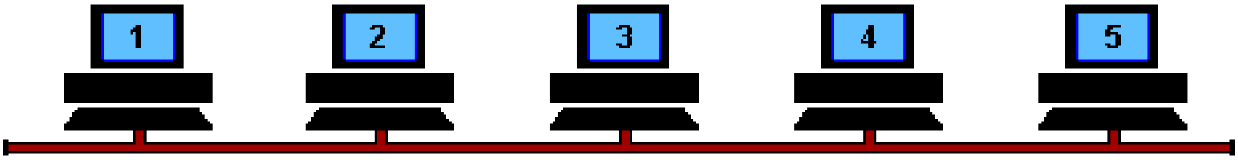
- Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

- There are high chances of redundancy in many of the network connections.
- Overall cost of this network is way too high as compared to other network topologies.
- Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

Bus Topology

- The bus topology is often used when a network installation is small, simple, or temporary.
- On a typical bus network, the cable is just one or more wires, with no active electronics to amplify the signal or pass it along from computer to computer.
- This makes the bus a passive topology**.**
- When one computer sends a signal up (and down) the wire, all the computers on the network receive the information, but only one (the one with the address that matches the one encoded in the message) accepts the information. The rest disregard the message.
- Only one computer at a time can send a message; therefore, the number of computers attached to a bus network can significantly affect the speed of the network. A computer must wait until the bus is free before it can transmit.
- These factors also affect star and ring networks**.**



- Another important issue in bus networks is termination. Since the bus is a passive topology, the electrical signal from a transmitting computer is free to travel the entire length of the cable. Without termination, when the signal reaches the end of the wire, it bounces back and travels back up the wire.
- When a signal echoes back and forth along an unterminated bus, it is called ringing. To stop the signals from ringing, you attach terminators at either end of the segment. The terminators absorb the electrical energy and stop the reflections.
- Cables cannot be left unterminated in a bus network.
- *Ethernet 10Base2 (also known as thinnet) is an inexpensive network based on the bus topology.*

Advantages of Bus Topology

- There are several advantages to a bus topology:
  - The bus is simple, reliable in very small networks, easy to use, and easy to understand.
  - The bus requires the least amount of cable to connect the computers together and is therefore less expensive than other cabling arrangements.
  - It is easy to extend a bus. Two cables can be joined into one longer cable with a BNC barrel connector, making a longer cable and allowing more computers to join the network.
  - A repeater can also be used to extend a bus; a repeater boosts the signal and allows it to travel a longer distance.

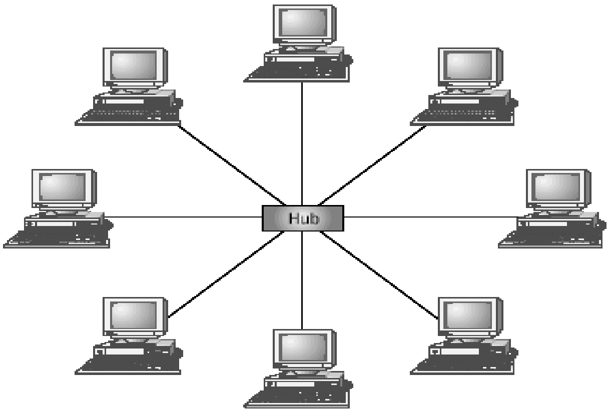
Disadvantages of Bus Topology

- Heavy network traffic can slow a bus considerably. Because any computer can transmit at any time, and computers on most bus networks do not coordinate with each other to reserve times to transmit, a bus network with a lot of computers can spend a lot of its bandwidth (capacity for transmitting information) with the computers interrupting each other instead of communicating. The problem only gets worse as more computers are added to the network.
- Each barrel connector weakens the electrical signal, and too many may prevent the signal from being correctly received all along the bus.
- It is difficult to troubleshoot a bus. A cable break or malfunctioning computer anywhere between two computers can cause them not to be able to communicate with each other. A cable break or loose connector will also cause reflections and bring down the whole network, causing all network activity to stop.

Star Topology

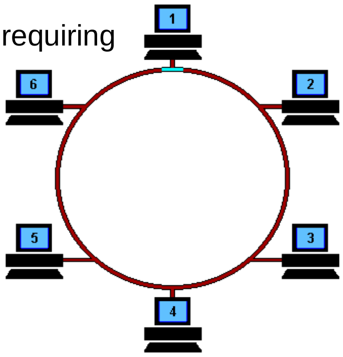
- In a star topology, all the cables run from the computers to a central location, where they are all connected by a device called a hub.
- Each computer on a star network communicates with a central hub that resends the message either to all the computers (in a broadcast star network) or only to the destination computer (in a switched star network). The hub in a broadcast star network can be active or passive.
- An active hub regenerates the electrical signal and sends it to all the computers connected to it. This type of hub is often called a multiport repeater. Active hubs and switches require electrical power to run.

- A passive hub, such as wiring panels or punch-down blocks, merely acts as a connection point and does not amplify or regenerate the signal.
- Passive hubs do not require electrical power to run.
- You can use several types of cable to implement a star network. A hybrid hub can accommodate several types of cable in the same star network.
- In a star topology the computers are all connected by cables to a central point.



Ring Topology

- In a ring topology, each computer is connected to the next computer, with the last one connected to the first.
- Rings are used in high-performance networks, networks requiring that bandwidth be reserved for time-sensitive features such as video and audio, or when even performance is needed when a large number of clients access the network.



- In a ring topology computers are connected in a circle.
- Every computer is connected to the next computer in the ring, and each retransmits what it receives from the previous computer. The messages flow around the ring in one direction. Since each computer retransmits what it receives, a ring is an *active* network and is not subject to the signal loss problems a bus experiences. There is no termination because there is no end to the ring.
- Some ring networks do token passing. A short message called a token is passed around the ring until a computer wishes to send information to another computer.
- That computer modifies the token, adds an electronic address and data, and sends it around the ring.

- Each computer in sequence receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin.
- The receiving computer returns a message to the originator indicating that the message has been received. The sending computer then creates another token and places it on the network, allowing another station to capture the token and begin transmitting. The token circulates until a station is ready to send and captures the token.
- This all happens very quickly: a token can circle a ring 200 meters in diameter at about 10,000 times a second. Some even faster networks circulate several tokens at once. Other ring networks have two counter-rotating rings that help them recover from network faults.
- FDDI is a fast fiber-optic network based on the ring topology

Advantages of Ring topology

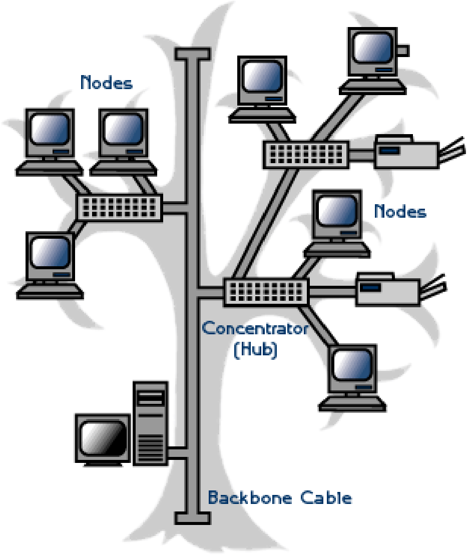
- The ring topology offers the following advantages:
  - Because every computer is given equal access to the token, no one computer can monopolize the network.
  - The fair sharing of the network allows the network to degrade gracefully (continue to function in a useful, if slower, manner rather than fail once capacity is exceeded) as more users are added.

Disadvantages of Ring topology

- The ring topology has the following disadvantages:
  - Failure of one computer on the ring can affect the whole network.
  - It is difficult to troubleshoot a ring network.
  - Adding or removing computers disrupts the network.

Tree topology

- A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See fig).
- Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.



Advantages of a Tree Topology

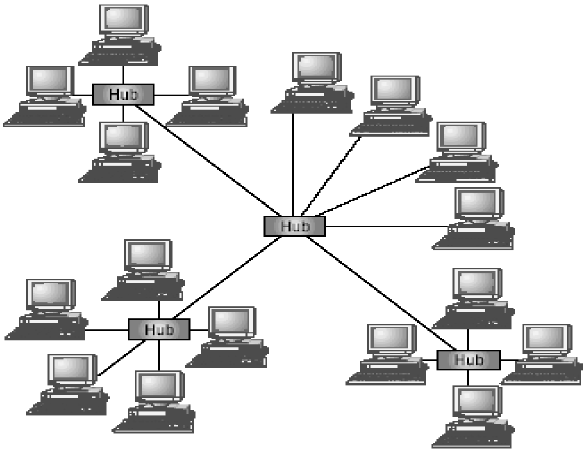
- Point-to-point wiring for individual segments.
- Supported by several hardware and software vender.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Hybrid topology

- You can expand a star network by placing another star hub where a computer might otherwise go, allowing several more computers or hubs to be connected to that hub. This creates a *hybrid star* network, like the one shown.



Advantages

- It is easy to modify and add new computers to a star network without disturbing the rest of the network. You simply run a new line from the computer to the central location and plug it into the hub. When the capacity of the central hub is exceeded, you can replace it with one that has a larger number of ports to plug lines into.
- You can use several cable types in the same network with a hub that can accommodate multiple cable types.
- The center of a star network is a good place to diagnose network faults.
- Intelligent hubs (hubs with microprocessors that implement features in addition to repeating network signals) also provide for centralized monitoring and management of the network.
- Single computer failures do not necessarily bring down the whole star network. The hub can detect a network fault and isolate the offending computer or network cable and allow the rest of the network to continue operating.

Disadvantages

- If the central hub fails, the whole network fails to operate.
- Many star networks require a device at the central point to rebroadcast or switch network traffic.
- It costs more to cable a star network because all network cables must be pulled to one central point, requiring more cable than other networking topologies.

6.2 Structured Wiring System, Media Twisted Pair, Coaxial cable, Fiber Optics

Network Components

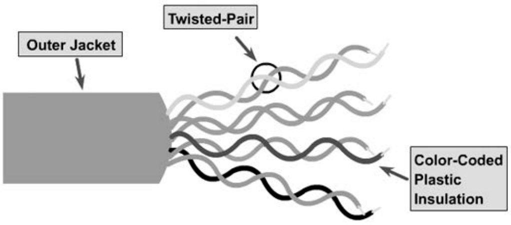
- Cabling
  - Cable is used to interconnect computers and network components together.
  - There are three main cable types used today
    - Twisted pair
    - Coaxial cable
    - Fiber optics
  - The choice of cable depends upon a number of factors, like
    - Cost
    - Distance
    - Number of computers involved
    - Speed
    - Requirements [bandwidth] i.e., how fast data is to be transferred
- Physical matter that carries transmission
  - Guided media:
    - Transmission flows along a physical guide (Media guides the signal))
    - Twisted pair wiring, coaxial cable and optical fiber cable
  - Wireless media (aka, radiated media)
    - No wave guide, the transmission just flows through the air (or space)
    - Radio (microwave, satellite) and infrared communications

Twisted-Pair Cable

- Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks.
- A pair of wires forms a circuit that can transmit data.
- The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.

- When electrical current flows through a wire, it creates a small, circular magnetic field around the wire.
- When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields.
- Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.
- Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP).

Unshielded Twisted Pair (UTP)



- UTP cable is a medium that is composed of pairs of wires.
- UTP cable is used in a variety of networks.
- Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other.
- UTP cable often is installed using a Registered Jack 45 (RJ-45) connector .
- The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.
- Commonly used types of UTP cabling are as follows:

Category 1—Used for telephone communications. Not suitable for transmitting data.

Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).

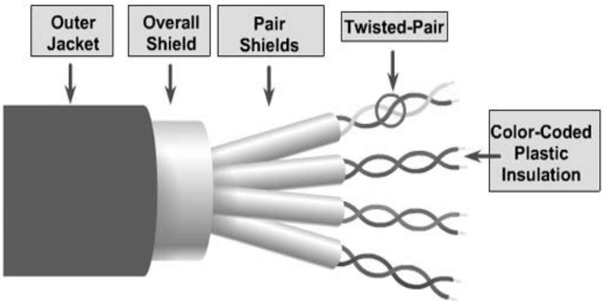
Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.

Category 5—Can transmit data at speeds up to 100 Mbps.

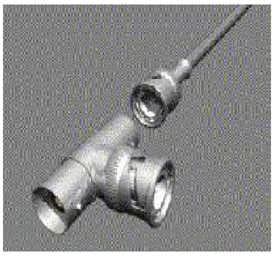
Shielded Twisted-Pair Cable

- Shielded twisted-pair (STP) cable combines the techniques of shielding, cancellation, and wire twisting.

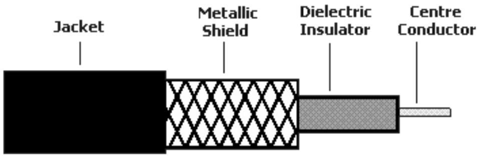


- Each pair of wires is wrapped in a metallic foil .
- The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable.
- As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI).
- STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses.
- Although STP prevents interference better than UTP, it is more expensive and difficult to install.

Coaxial Cable



- Coaxial cable so as named because it contains two conductors within the sheath.
- At the centre of the cable is the copper core that actually carries the electrical signals.
- Surrounding the core is a layer of insulation and also it is called second conductor.
- The second conductor works as ground.
- There are two types of coaxial cable



1.RG8 used in LAN also known as thick Ethernet.

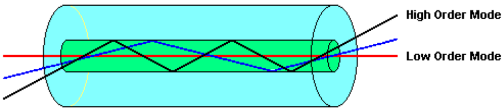
2.RG-58 used for LAN and known as thin Ethernet.

Advantage

- Less prone to interference than TP (due to (shield)
- More expensive than TP (quickly disappearing)
- used mostly for CABLE TV

Fiber Optic Cable

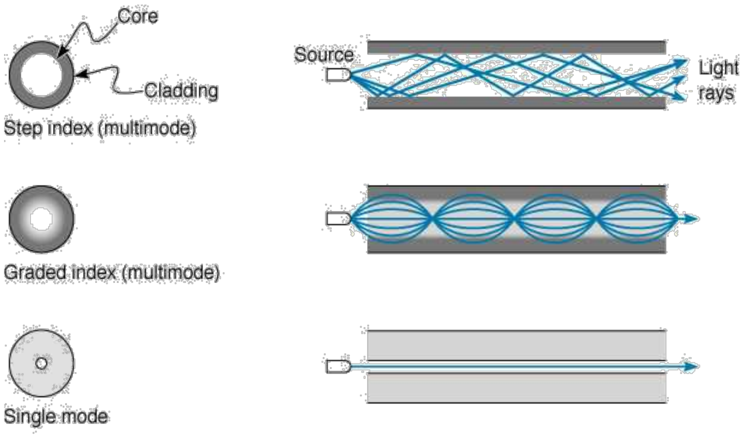
- Completely different.
- Instead of Electrical signal it transmits pulses of light over a glass or plastic element.
- Has extremely high capacity, ideal for broadband
- Fiber optic cable structure (from center):
  - Core (v. small, 5-50 microns, ~ the size of a single hair)
  - Cladding, which reflects the signal
  - Protective outer jacket



Types of Optical Fiber

- Multimode (core diameter 62.5 microns)
  - Earliest fiber-optic systems
  - LED is using instead of laser and carries multiple wave lengths. Cannot span distances as long as single mode but it bends at corner. As is much cheaper.
- Graded index multimode
  - Reduces the spreading problem by changing the refractive properties of the fiber to refocus the signal
  - Can be used over distances of up to about 1000 meters
- Single mode (core diameter 8.3 microns)
  - Transmits a single wave length direct beam through the cable
  - Signal can be sent over many miles without spreading
  - Expensive (requires lasers; difficult to manufacture)
  - It cannot be bend around the corner.

Optical Fiber



Fiber optic is often used to overcome distance limitations. It can be used to join two hubs together, which normally could not be connected due to distance limitations. In this instance, a UTP to Fiber transceiver (often referred to as a FOT) is necessary.

ST connector and SC connector are used

The features of fiber-optic cable system

- expensive
- used for backbones (linking LAN’s together) or FDDI rings (100Mbps)
- high capacity (100Mbps)
- immune to electromagnetic interference
- low loss
- difficult to join
- connectors are expensive

7.0 Standards

Contents

7.1 Introduction to OSI reference Model

- The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model in 1977 and finally 1983.
- It has since become the most widely accepted model for understanding network communication.
- The OSI model attempts to define rules that apply to the following issues:
  - How network devices connect and communicate each other even their languages are different at the same time how it makes a connection between the each device.
  - The methods is used for which device on a network knows when the data to be transmitted and when the data not to be transmitted.
  - Methods to ensure that network transmissions are received correctly and by the right recipient
  - How the physical transmission media are arranged and connected
  - How to ensure that network devices maintain a proper rate of data flow
  - How bits are represented on the network media
  - The OSI model does not work or perform any particular functions in the communications process but the actual work is done by the SW and HW.
  - It also defines which tasks need to be done and which protocols will handle those tasks each of the seven layers.
  - It divides the tasks into several subtasks.
  - The subtasks will be fulfilled by the specific protocols at the specific layer of the OSI model.
  - Protocol stack is also possible i.e when protocols are grouped together to complete a task
  - Each layer of the OSI model has a different protocols are with it. When more than one protocol is need to complete a task, that time the protocols are grouped e.g TCP/IP

Protocols

- The network consists of many other computing platforms running on different version, different Operating System and Application software. So that the network cannot find out which computer has which operating system and AS, So that the common languages is needed to understand each other in different computer.
- That's why the common languages are made, that languages are called protocol. It is a standard set of instructions and procedures according to communication take place.
- Through this protocol the computer agreed upon ways that computers exchange information.

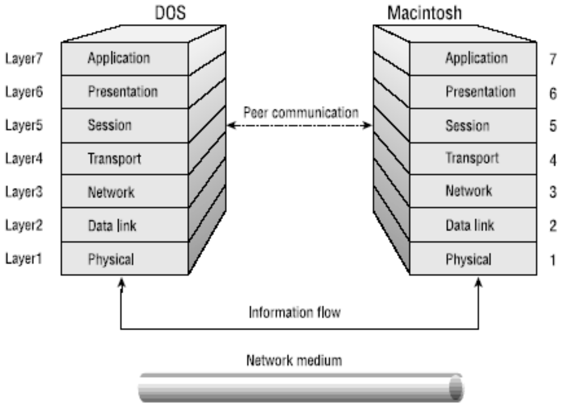
Hardware Protocols

- Hardware protocols define how hardware devices operate and work together. The 10baseT Ethernet protocol is a hardware protocol specifying exactly how two 10baseT Ethernet devices will exchange information and what they will do if it is improperly transmitted or interrupted. It determines such things as voltage levels and which pairs of wires will be used for transmission and reception. There is no program involved; it is all done with circuitry.

Software Protocol

- Programs communicate with each other via software protocols. Network client computers and network servers both have protocol packages that must be loaded to allow them to talk to other computers. These packages contain the protocols the computer needs to access a certain network device or service.

Protocol Stack



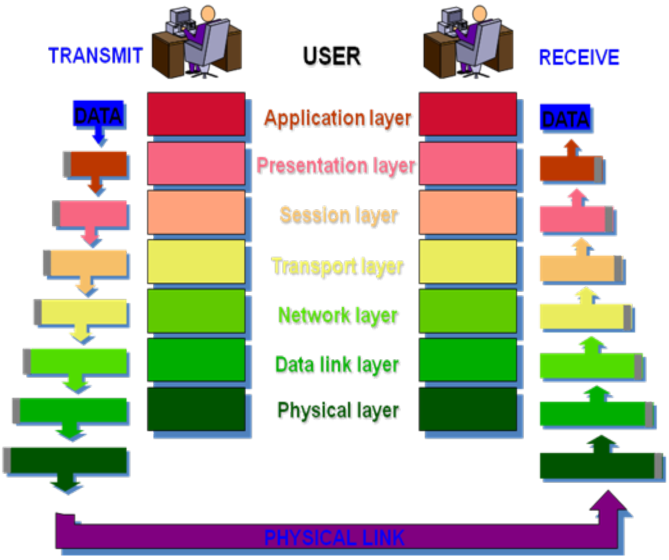
- A protocol stack is a group of protocols arranged on top of each other as part of a communication process. Each layer of the OSI model has different protocols associated with it. When more than one protocol is needed to complete a communication process, the protocols are grouped together in a stack.
- Each layer in the protocol stack receives services from the layer below it and provides services to the layer above it.

- For two computers to communicate, the same protocol stacks must be running on each computer. Each layer of the protocol stack on one computer communicates with its equivalent, or peer, on the other computer.
- The computers can have different operating systems and still be able to communicate if they are running the same protocol stacks. For example, a DOS machine running TCP/IP can communicate with a Macintosh machine running TCP/IP.

Open Systems Interconnection (OSI)

- "The OSI model for network protocols is well-designed and very interoperable."
- "It was developed too late to be accepted by the principal communications customers in industry and the military, who had already invested heavily in TCP/IP."
- And while serving as a good framework for protocols it is not ideal for actual high speed implementations.

THE 7 LAYERS OF OSI

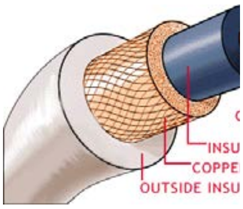


Physical Layer

This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres, copper wire or wireless etc. The following are the main functions of the physical layer:

- **Hardware Specification:** The details of the physical cables, network interface cards, wireless radios, etc are a part of this layer.

Coaxial Cable

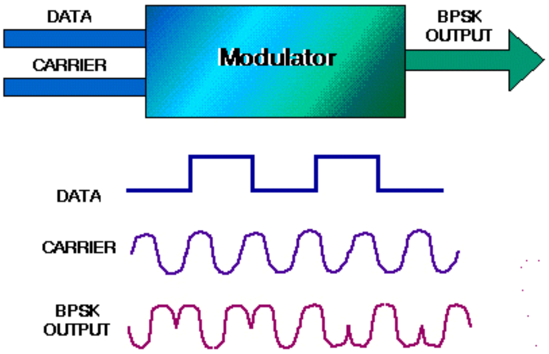


Hybrid Cable

Wireless Card

Network Card

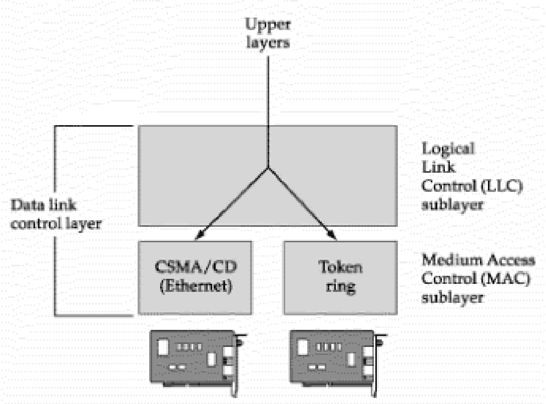
- **Encoding and Signalling:** How are the bits encoded in the medium is also decided by this layer. For example, on the copper wire medium, we can use different voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer. eg, we may use Binary phase shift keying for the representation of '1' and '0' rather than using different voltage levels if we have to transfer in RF waves.



- **Data Transmission and Reception:** The transfer of each bit of data is the responsibility of this layer. This layer assures the transmission of each bit with a high probability. The transmission of the bits is not completely reliable as there is no error correction in this layer.
- **Topology and Network Design:** The network design is the integral part of the physical layer. Which part of the network is the router going to be placed, where the switches will be used, where we will put the hubs, and how many machines is each switch going to handle, what server is going to be placed where, and many such concerns are to be taken care of by the physical layer. The various kinds of network topologies that we decide to use may be ring, bus, star or a hybrid of these topologies depending on our requirements.

Data Link Layer

This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :


Upper layers
Logical Link Control (LLC) sublayer
Data link control layer
CSMA/CD (Ethernet)
Token ring
Medium Access Control (MAC) sublayer

- **Framing:** Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.
- **Acknowledgment:** Sent by the receiving end to inform the source that the frame was received without any error.
- **Sequence Numbering:** To acknowledge which frame was received.
- **Error Detection:** The frames may be damaged, lost or duplicated leading to errors. The error control is on **link to link** basis.
- **Retransmission:** The packet is retransmitted if the source fails to receive acknowledgment.
- **Flow Control:** Necessary for a fast transmitter to keep pace with a slow receiver.

Network Layer

- The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
- **Routing:** This deals with determining how packets will be routed (transferred) from source to destination.
- **Subnet traffic control**: routers can Instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- **Frame fragmentation**: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- **Logical-physical address mapping**: translates logical addresses, or names,into physical addresses.
- **Subnet usage accounting:** has accounting functions to keep track of frames Forwarded by subnet intermediate systems, to produce billing information.

Transport Layer

- **Fragmentation and Re-assembly:** The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.

- **Types of service:** The transport layer also decides the type of service that should be provided to the session layer. The service may be perfectly reliable, or may be reliable within certain tolerances or may not be reliable at all. The message may or may not be received in the order in which it was sent. The decision regarding the type of service to be provided is taken at the time when the connection is established.
- **Error Control:** If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on **end to end** basis.
- **Flow Control:** A fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information.
- **Connection Establishment / Release:** The transport layer also establishes and releases the connection across the network. This requires some sort of naming mechanism so that a process on one machine can indicate with whom it wants to communicate.

Session Layer

- It deals with the concept of **Sessions** i.e. when a user logins to a remote server he should be **authenticated** before getting access to the files and application programs.
- Another job of session layer is to establish and maintain sessions. If during the transfer of data between two machines the session breaks down, it is the session layer which re-establishes the connection. It also ensures that the data transfer starts from where it breaks keeping it transparent to the end user. e.g. In case of a session with a database server, this layer introduces **check points** at various places so that in case the connection is broken and re-established, the transition running on the database is not lost even if the user has not committed. This activity is called **Synchronization**.
- Another function of this layer is **Dialogue Control** which determines whose turn is it to speak in a session. It is useful in video conferencing.

Presentation Layer

- This layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate data structures to be exchanged can be defined in abstract way along with standard encoding. It also manages these abstract data structures and allows higher level of data structures to be defined an exchange. It encodes the data in standard agreed way (network format).
- **Character code translation**: for example, ASCII to EBCDIC.
- **Data conversion**: bit order, CR-CR/LF, integer-floating point, and so on.
- **Data compression**: reduces the number of bits that need to be transmitted on the network.
- **Data encryption:** encrypt data for security purposes. For example, password encryption.

Application Layer

- The application layer enables the user, whether human or software, to access the network. It provides user interface and support for services such as electronic mail, remote access and transfer, shared database management, and other types of distributed information services.
- The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.DNS client/server program can support an e-mail program to find the IP address of an e-mail recipient.
- specific services provided by the application layer includes the following
  1. **Network virtual terminal**

     A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. The application creates a software emulation of a terminal at the remote host. The user’s computer talks to the software terminal which, in turn, talks to the host, and vice versa.
  2. **File transfer, access, and management**

     This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in a local computer and to manage or control files.
  3. **Mail services**

     This application provides the basis for e-mail forwarding and storage.

4. **Directory services**

   This application provides distributed database sources and access for global information about various objects and services.

7.2 Advantage of Layering & Existing Standards

Advantages of Using a Layered Model

- Allows a layer to be changed without impacting the rest of the model.
- Interoperability between network applications is improved by using a standard interface.
- Design and development efforts can be made in a modular fashion.
- Network operations and troubleshooting can be simplified.
- **Reduces complexity**

  It breaks network communication into smaller, simpler parts. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
- **Standardizes interfaces:**

  It standardizes network components to allow multiple vendor development and support.
- **Facilitates modular engineering:**

  It allows different types of network hardware and software to communicate with each other.
- **Interoperability between Vendors**

  It allows multiple-vendor development through standardization of network components. Defines the process for connecting two layers together, promoting interoperability between vendors It Allows vendors to compartmentalize their design efforts to fit a modular design, which eases implementations and simplifies troubleshooting
- **Ensures interoperable technology**:

  It prevents changes in one layer from affecting the other layers, allowing for quicker development.
- **Accelerates evolution:**

  It provides for effective updates and improvements to individual components without affecting other components or having to rewrite the entire protocol.
- **Simplifies teaching and learning:**

  It breaks network communication into smaller components to make learning easier. Provides a teaching tool to help network administrators understand the communication process used between networking components

- **Five Conversion Steps of Data**
  Encapsulation **Data** >> **Segments** >> **Packets** >> **Frames** >> **Bits**
- Upper layers convert and format the information into **data** and send it to the Transport Layer.
- The Transport layer turns the data into **segments** and adds headers then sends them to the Network layer.
- The Network layer receives the segments and converts them into **packets** and adds header information (logical addressing) and sends them to the Data Link Layer.
- The Data Link layer receives the packets and converts them into **frames** and adds header information (physical source and destination addresses) and sends the frames to the Physical Layer.
- The Physical layer receives the frames and converts them into **bits** to be put on the network medium.

8.0 LAN Signaling and Access

Contents

8.1 Signaling Base band

Bandwidth

- Bandwidth is the capacity of a medium to convey data.. One example of bandwidth is automobile traffic. A two-lane road with a speed limit can accommodate only so many cars before there are too many and a traffic jam results. You can increase the bandwidth of a road by making the cars travel more quickly (which corresponds to using a faster transmission method in networks) or by making the road wider (which corresponds to using more wires in networks).

Base Band

- The cable connecting the computer can carry one signal at a time, and all the system take turn using it. This type of network is called Base band network.
- In the base band network, when a computer transmits data it might be broken into many packet and transmits separately. The receiving system reassembles them back into original. This is called packet switching network.
- Baseband refers to the original frequency range of a transmission signal before it is converted, or modulated, to a different frequency range.
- For example, an audio signal may have a baseband range from 20 to 20,000 hertz. When it is transmitted on a radio frequency (RF), it is modulated to a much higher, inaudible, frequency range.
- A baseband signal or low pass signal is a signal that can include frequencies that are very near zero, by comparison with its highest frequency (for example, a sound waveform can be considered as a baseband signal, whereas a radio signal or any other modulated signal is no).

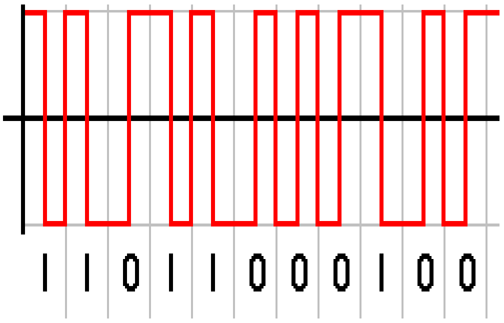
- A signal "at baseband" is usually considered to include frequencies from near 0 Hz up to the highest frequency in the signal with significant power.
- There are few communications media that will pass low frequencies without distortion. Then, the original, low frequency components are referred to as the baseband signal.
- Some signals can be treated as baseband or not, depending on the situation. For example, a switched analog connection in the telephone network has energy below 300 Hz and above 3400 Hz removed by
- band pass filtering; since the signal has no energy very close to zero frequency, it may not be considered a baseband signal.

8.2. Manchester encoding and Differential Manchester encoding

- The idea of RZ and the idea of NRZ-L are combined into the Manchester encoding scheme.

- In Manchester encoding, the duration of the bit is divided into 2 halves .the voltage remains at one level during the 1^{st} half and moves to the other level in 2^{nd} half. The transmission at the middle of the bit provides synchronization.

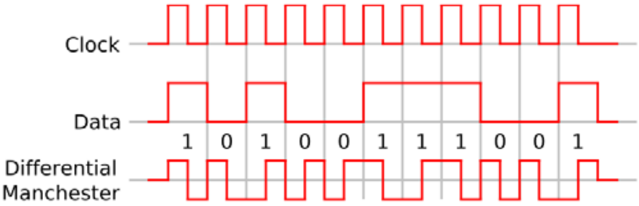
- In the Manchester encoding shown, logic 0 is indicated by a 0 to 1 transition at the centre of the bit and a logic 1 is indicated by a 1 to 0 transition at the centre of the bit. Note that signal transitions do not always occur at the 'bit boundaries' (the division between one bit and another), but that there is always a transition at the centre of each bit.
- The following diagram shows a typical Manchester encoded signal with the corresponding binary representation of the data (1, 1, 0, 1, 0, 0) being sent.



- The waveform for a Manchester encoded bit stream carrying the sequence of bits 11011000100.
- Manchester scheme overcomes several problems associated with NRZ-L.

Differential Manchester Encoding

- In differential Manchester encoding combines the idea of RZ and NRZ-I.
- There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1 there is none.
- Differential Manchester scheme overcomes several problems associated with NRZ-I.



- Differential Manchester encoding is a line code in which data and clock signals are combined to form a single 2-level self-synchronizing DataStream. It is a differential encoding, using the presence or absence of transitions to indicate logical value.

Advantages

- A transition is guaranteed at least once every bit, allowing the receiving Device to perform clock recovery.
- Detecting transitions is often less error-prone than comparing against a Threshold in a noisy environment.

8.3. Modulation Techniques

Modulation

- In electronics and telecommunications**,** modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal (high frequency signal), with a modulating signal that typically contains information to be transmitted.
- In telecommunications, modulation is the process of conveying a message signal, for example a digital bit stream or an analog audio signal, inside another signal that can be physically transmitted. Modulation of a sine waveform transforms a baseband message signal into a pass band signal.
- Today vast amounts of information are communicated using radio communications systems. Both analogue radio communications systems and digital or data radio communications links are used.
- There are many ways in which a radio carrier can be modulated to carry a signal, each having its own advantages and disadvantages. The choices of modulation have a great impact on the radio communications system.

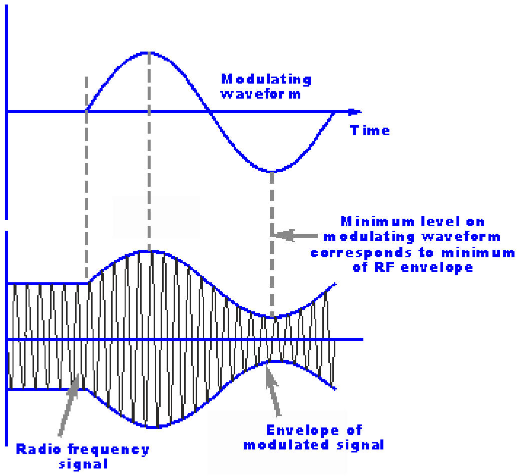
- Some forms are better suited to one kind of traffic whereas other forms of modulation will be more applicable in other instances. Choosing the correct form of modulation is a key decision in any radio communications system design.

Basic Type Of Modulation

- There are three main ways in which a radio communications or RF signal can be modulated:

Amplitude Modulation(Am)

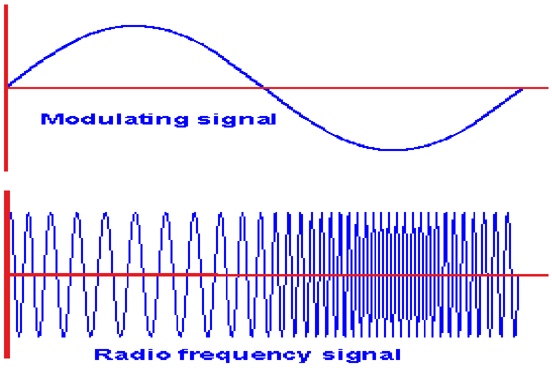
- In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitudes of the modulating signal.
- The frequency and phase of the carrier remain same; only the amplitude changes to follow variations in the information. The modulating signal is the envelope of the carrier.
- AM is normally implemented by using a simple multiplier because the amplitude of the carrier signal needs to be changed according to the amplitude of the modulating signal. As the name implies, this form of modulation involves modulating the amplitude or intensity of the signal.


Modulating waveform
Time
Minimum level on modulating waveform corresponds to minimum of RF envelope
Radio frequency signal
Envelope of modulated signal

- Amplitude modulation was the first form of modulation to be used to broadcast sound, and although other forms of modulation are being increasingly used, amplitude modulation is still in widespread use.

Frequency modulation(FM)

- In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level of modulating signal.
- The peak amplitude and phase of the carrier signal remain constant, but as the amplitude of the information signal changes, the frequency of the carrier changes correspondingly.

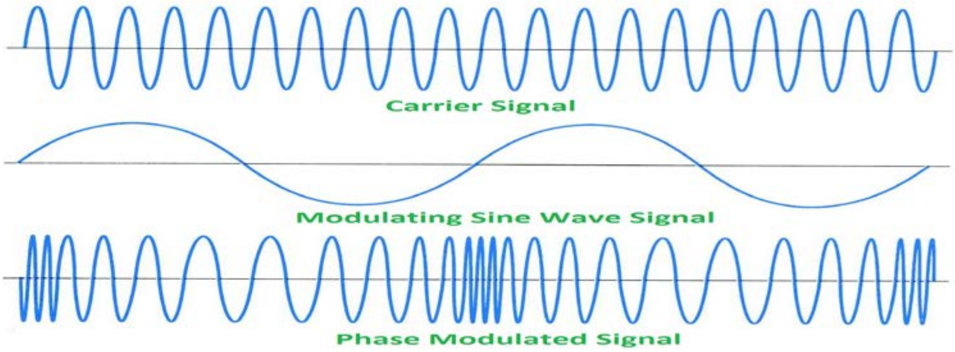


- FM is normally implemented by using a voltage-controlled oscillator as with FSK.The frequency of the oscillator changes according to the input voltage which is the amplitude of the modulating signal

- Frequency modulation has the advantage that, as amplitude variations do not carry any information on the signal, it can be limited within the receiver to remove signal strength variations and noise. As a result is form of modulation has been used for many applications including high quality analogue sound broadcasting.

Phase modulation(PM)

- In PM transmission, the phase of the carrier signal is modulated to follow the changing voltage level of the modulating signal.
- The peak amplitude and frequency of the carrier signal remain constant, but as the amplitude of the information signal changes, the phase of the carrier changes correspondingly.
- It can be proved mathematically that PM is the same as FM with one difference. In FM, the instantaneous change in the carrier frequency is proportional to the amplitude of the modulating signal; In PM the instantaneous change in the carrier frequency is proportional to the derivative of the amplitude of the modulating signal.
- The frequency of the oscillator changes according to the derivative of the input voltage which is the amplitude of the modulating signal.
- Phase modulation, PM, is used in many applications to carry both analogue and digital signals. Keeping the amplitude of the signal constant, the phase is varied to carry the required information or signal.



- Phase modulation is widely used for transmitting radio waves and is an integral part of many digital transmission coding schemes that underlay a wide range of technologies like Wi-Fi, GSM and satellite television.

- Although phase modulation is used for some analogue transmissions, it is far more widely used as a digital form of modulation where it switches between different phases. This is known as phase shift keying, PSK, and there are many flavours of this.

8.4 BROADBAND

- The term broadband refers to the wide bandwidth characteristics of a transmission medium and its ability to transport multiple signals and traffic types simultaneously.
- The medium can be coaxial cable, optical fiber, twisted pair, DSL local telephone networks or wireless. In contrast, baseband describes a communication system in which information is transported across a single channel.

Simplex communication

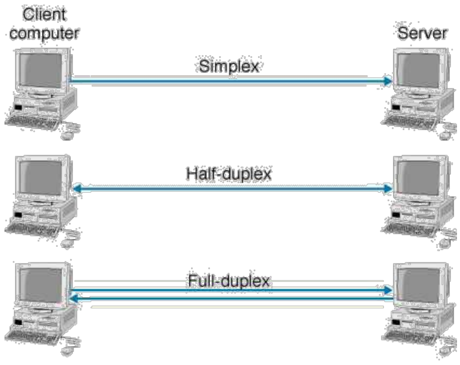
- In the broad band net work carries multiple signals in a single cable at a same time.
- The example of broad band network is cable TV. In a single cable carries multiple channels

Half duplex communications

- In half duplex communications two computer communicate over a long, data typical travels in only one directions at a time because the base band network used for most LAN’s supports only a single signal. This is called half duplex communications
- An example of an Half duplex communications is two way radio set in which only one part can transmit at any one time and each pat must say ‘over’ to signal.

Full duplex communications

- The two systems that can communicate in both directions simultaneously are called full duplex mode communication.
- The most common example of a full duplex network is once again the telephone system. Both parts can speak simultaneously during the telephone call and each part can hear the other at the same time.



8.5 Carrier sense Multiple Access(CSMA)

- It was developed to minimize the chance of collision and to increase the performance.
- It requires that each station first listen to the medium before sending.
- It is based on the principle sense before transmit or listen before talk.

- It can reduce the possibility of collision, but it cannot eliminate it.
- In CSMA a station senses the carrier on the channel before starting its own transmission.
- The vulnerable time for CSMA is the propagation time Tp.
- propagation time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. When a channel is sense to be idle, a station can take one of the three different approaches to transmit a packet on to the channel. These three protocols are as follows:

Non-persistent CSMA

- In non-persistent CSMA, when a station having a packet to transmit and finds that the channel is busy, it backs off for a fixed interval of time.
- It then checks the channel again and if the channel is free then it transmits.
- The back-off delay is determined by the transmission of a frame, propagation time and other system parameter.
- 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. But it waits a random period of time and again check for activity.

1-Persistent CSMA

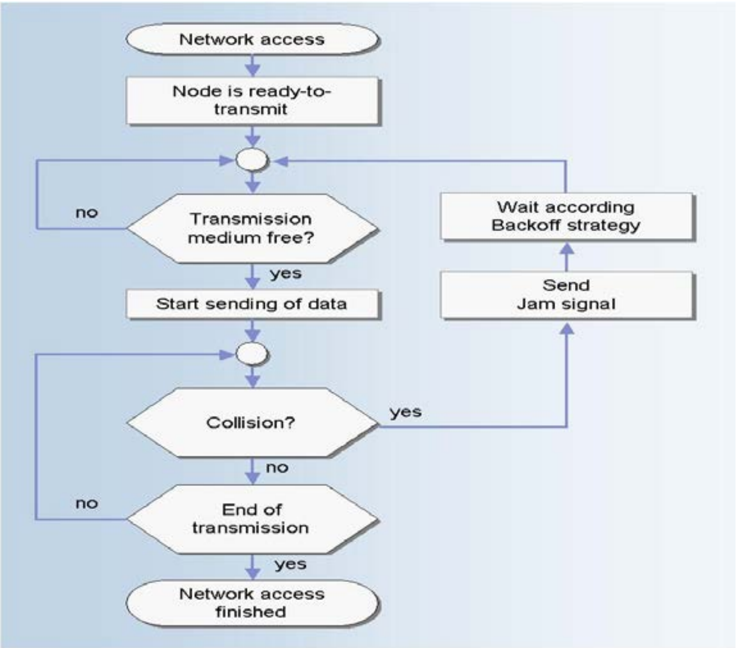
- Any station wishing to transmit, monitor the channel continuously until the channel is idle and then transmit with probability one, hence the name 1-persistent.
- When two or more stations are waiting to transmit, a collision is guaranteed. Since each station will transmit immediately at the end of busy period. In this case each will wait a random amount of time and will then reattempt to transmit.
- As in the case with non-persistent CSMA, the performance of 1-persistent CSMA protocol depends only on the channel delay time.

P-Persistent CSMA:-

- To reduce the probability of collision in 1-persistent CSMA, not all allowed transmitting immediately, after the channel is idle.
- When a station becomes ready to send and its sense the channel to be idle, it either transmits with a probability p or it defers transmission by one time slot with a probability q=1-p.if the differed slot is also idle, the station either transmits with probability p or defers again with a probability q.this process is repeated until either packets are transmitted of the channel is busy.

CSMA with collision detection (CSMA/CD)

- CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specifications were developed jointly by digital equipment corporation (DEC), Intel, and Xerox. This network is called as Ethernet. The IEEE802.3
- CSMA/CD stands for LAN are based on Ethernet specification.
- The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may send its message. If no station was sending at the time that it first listened, the station may send its message immediately. The term carrier sense indicates this listening before transmitting behaviour.
- **Carrier Sense Multiple Access/Collision Detect** (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks.
- **Carrier-sense multiple access with collision detection** describes how the Ethernet protocol regulates communication among nodes
- On Ethernet, any station can send a frame at any time. Each station senses whether the medium is idle and therefore available for use. If it is, the station begins to transmit its first frame. If another station also tries to transmit at the same time, a collision occurs and the frames are discarded and then a jamming signal is sent throughout the network in order to notify all stations of the collision.
- Each station then waits for a random period of time and retries. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off. The stations retry until successful transmission of the frame.CSMA/CD is specified in the IEEE 802.3 standard.



- The **jam signal** is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.
- **Transmit** – The stations (nodes) sends the frames to other stations (nodes)
- **Carrier Sense** – The stations (nodes) listen to the medium if it is idle for transmission
- **Back off** – After collision occurs, a jam signal is sent to notify all stations of the collision. After the jam signal is sent, the stations (nodes) wait for a random period of time called Back off period.
- If two or more stations have message to send at the same time and they are separated by significant distances on the bus/channel. each may begin transmitting at roughly the same time without being aware of the other station .the signal from each station will superimpose on the channel and is garbled beyond the decoding ability of the receiving station .this is termed as collision .
- A protocol is required for transmitting station to monitor the channel while sending each of its messages and to detect such collisions.
- When a collision has been detected, each of sending stations must cease transmitting, wait for a random length of time, and then try again. Because of quick termination of transmission time and bandwidth is saved. Therefore CSMA/CD is more efficient than ALOHA and CSMA. CSMA/CD network work best on a bus, multipoint topology with busty asynchronous transmission.CSMA/CD has totally decentralized control and is based on connection access.

CSMA with collision avoidance (CSMA/CA)

Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain.

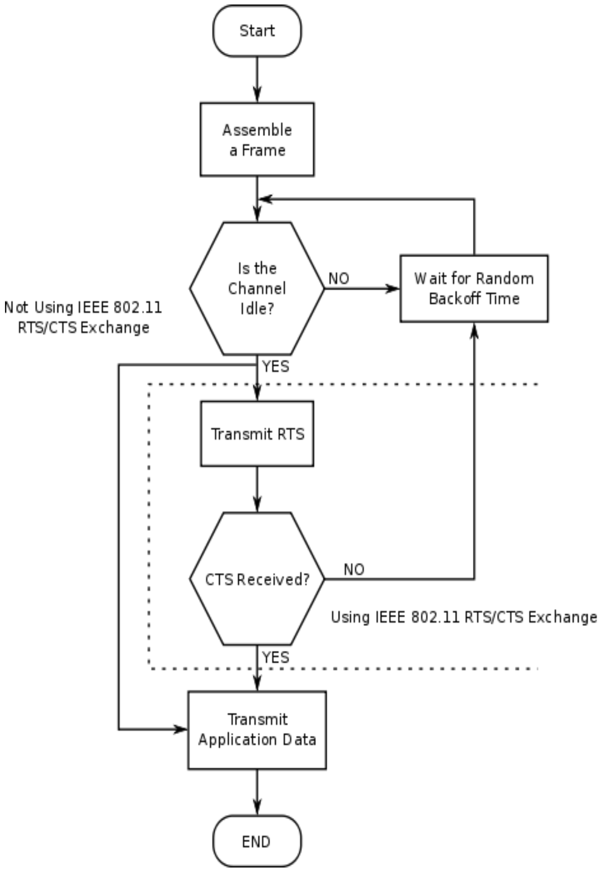
1. Carrier Sense

- Prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not.

2. Collision Avoidance

- If another node was heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.

- Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the shared medium. This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network, the Access Point only issues a Clear to send to one node at a time.
- Transmission: if the medium was identified as being clear or the node received CTS to explicitly indicate it can send, it sends the frame in its entirety.
- Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its transmission will dwarf any attempt to listen).
- Although CSMA/CA has been used in a variety of wired communication systems, it is particularly beneficial in a wireless LAN due to a common problem of multiple stations being able to see the Access Point, but not each other. This is due to differences in transmitting power, and receives sensitivity.


Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

- CSMA/CA performance is based largely upon the modulation technique used to transmit the data between nodes. Studies show that under ideal propagation conditions (simulations), Direct Sequence Spread Spectrum (DSS) provides the highest throughput for all nodes on a network when used in conjunction with CSMA/CA and the IEEE 802.11 RTS/CTS exchange under light network load conditions.

8.6 TOKEN RING

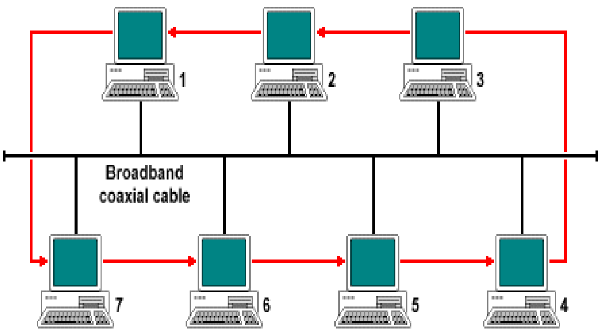
- Token ring local area network (LAN) technology is a protocol which resides at the data link layer (DLL) of the OSI model.
- It used a special three-byte frame called a token that travels around the ring. Token-possession grants the possessor permission to transmit on the medium.
- Initially used only in IBM computers, it was eventually standardized with protocol IEEE 802.5.

- Stations on a token ring LAN are logically organized in a ring topology with data being transmitted sequentially from one ring station to the next with a control token circulating around the ring controlling access.
- Physically, a token ring network is wired as a star, with 'MAUs' and arms out to each station and the loop going out-and-back through each.

Token frame

- When no station is transmitting a data frame, a special token frame circles the loop. This special token frame is repeated from station to station until arriving at a station that needs to transmit data. When a station needs to transmit data, it converts the token frame into a data frame for transmission.
- Once the receiving station receives its own data frame, it converts the frame back into a token. If a transmission error occurs and no token
- frame, or more than one, is present, a special station referred to as the active monitor detects the problem and removes and/or reinserts tokens as necessary.
- On 4 Mite/s token rings, only one token may circulate; on 16 Mbit/s token rings, there may be multiple tokens.
- A data token ring frame is an expanded version of the token frame that is used by stations to transmit media access control (MAC) management frames or data frames from upper layer protocols and applications.
- Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start
- delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field.

Token Bus



- Token Bus is described in the IEEE 802.4 specification, and is a Local Area
- Network (LAN) in which the stations on the bus or tree form a logical ring.
- Each station is assigned a place in an ordered sequence, with the last station in the sequence being followed by the first, as shown below. Each station knows the address of the station to its "left" and "right" in the sequence.

- Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable.
- A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring.
- Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. Token bus was used by General Motors for their Manufacturing Automation Protocol (MAP) standardization effort.
- This is an application of the concepts used in token ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring.
- Due to difficulties handling device failures and adding new stations to a network, token bus gained a reputation for being unreliable and difficult to upgrade.
- In order to guarantee the packet delay and transmission in Token bus protocol, a modified Token bus was proposed in Manufacturing Automation Systems and flexible manufacturing system (FMS).
- A means for carrying Internet Protocol over token bus was developed.
- The IEEE 802.4 Working Group is disbanded and the standard has been withdrawn by the IEEE.

Token Passing

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

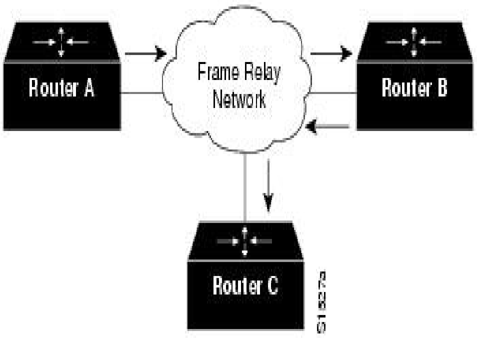
Demand Priority

- Demand priority is a media-access method used in 100BaseVG, a 100 megabit per second (Mbit/s) Ethernet implementation proposed by Hewlett-Packard (HP) and AT&T Microelectronics.

- Demand priority shifts network access control from the workstation to a hub. This access method works with a star topology. In this method, a node that wishes to transmit indicates this wish to the hub and also requests high- or regular-priority service for its transmission.
- After it obtains permission, the node begins transmitting to the hub.
- The hub is responsible for passing the transmission on to the destination node; that is, the hub is responsible for providing access to the network. A hub will pass high priority transmissions through immediately, and will pass regular-priority transmissions through exactly at the same time the opportunity arises.
- Demand priority helps increase bandwidth in the following ways: A node does not need to keep checking whether the network is idle after transmitting.
- In current Ethernet implementations, a wire pair is dedicated to this task. By making network checking unnecessary, demand priority frees a wire pair.
- With demand priority, the hub needs to pass a transmission on only to its destination, so that overall network traffic is decreased. This means there is more bandwidth available for heavy network traffic.
- Demand Priority was discovered by Albert J. Sofinski at Cornell University. He came up with the idea after feeding his dog and going on a walk. Upon returning, he quickly wrote down the idea, and it persists to this day.

Fast Switching

- Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding.
- Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching.
- To configure fast switching, perform the tasks described in the following sections:
  1. Enabling AppleTalk Fast Switching
  2. Enabling IP Fast Switching
  3. Enabling Fast Switching on the Same IP Interface
  4. Enabling Fast Switching of IPX Directed Broadcast Packets
  5. Enabling SMDS Fast Switching



1. Enabling AppleTalk Fast Switching

- AppleTalk access lists are automatically fast switched. Access list fast switching improves the performance of AppleTalk traffic when access lists are defined on an interface.

2. Enabling IP Fast Switching

- Fast switching involves the use of a high-speed switching cache for IP routing.
- Destination IP addresses is stored in the high-speed cache to expedite packet forwarding. In some cases, fast switching is inappropriate, such as when slow-speed serial links (64K and below) are being fed from higher- speed media such as T1 or Ethernet.

3. Enabling Fast Switching on the Same IP Interface

- You can enable IP fast switching when the input and output interfaces are the same interface. This normally is not recommended, though it is useful when you have partially meshed media such as Frame Relay.

- Figure illustrates a scenario where enabling fast switching on the same IP interface is desirable. Router A has a data-link connection identifier (DLCI) to Router B, and Router B has a DLCI to Router C. There is no DLCI between Routers A and C; traffic between them must go in and out of Router B through the same interface.

4. Enabling Fast Switching of IPX Directed Broadcast Packets

- By default, Cisco IOS software switches IPX packets that have been directed to the broadcast address. To enable fast switching of these IPX-directed broadcast packets, use the following command in global configuration mode:

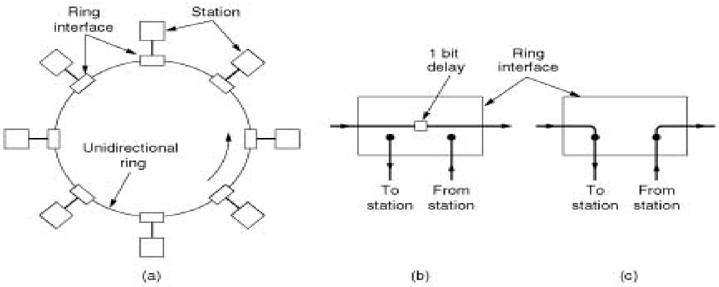
5. Enabling SMDS Fast Switching

- SMDS fast switching of IP, IPX, and AppleTalk packets provides faster packet transfer on serial links with speeds above 56 kbps. Use fast switching if you use high-speed, packet-switched, datagram-based WAN technologies such as Frame Relay offered by service providers.
- By default, SMDS fast switching is enabled.
- Fast packet switching is a variant of packet switching that increases the throughput by eliminating overhead associated with flow control and error correction functions, which are either offloaded to upper layer networking protocols or removed altogether.

- ATM and Frame Relay are two major implementations of fast packet switching.

Slotted Ring

- In slotted ring protocol, the ring is slotted into a number of fixed-size frames, where each frame contains a bit that tells whether it is full or empty. When a station wants to transmit, it waits for an empty frame, marks it as full, and puts its data in this frame.
- A performance analysis of the slotted ring protocol for a voice/data integrated network environment is presented. At each node two types of packet generation (data and voice) are assumed and a model to provide dedicated buffers for storing each type of packet is constructed.



- Packet transmission is performed according to the slotted ring protocol with priority given to the voice packets. In particular, an on-off model reflecting real behaviour for the generation of voice packets is defined and finite capacities for the packet buffers are assumed to allow for the calculation of buffer overflow probabilities.
- In particular, an on-off model reflecting real behaviour for the generation of voice packets is defined and finite capacities for the packet buffers are assumed to allow for the calculation of buffer overflow probabilities.
- An approximate delay analysis of a slotted ring medium access protocol is represented. The operation is based on a continuous stream of slots circulating around the ring.
- The delay model is represented. Assuming that a slot is reserved with a reassumed probability, an expression for the z-transform of the number waiting in the queue is derived by using the embedded technique.
- From this the expression for the average access delay is obtained. The approximation of the probability is then found and the average delay can be solved. The incoming traffic is assumed to be Poisson. Numerical results are discussed.

9.0 Popular LAN Standards

Contents

9.1 Different LAN standards: IEEE 802.3, 10base5, 10base2, 10baseT, Switched Ethernet, IEEE802.4, IEEE 802.5, Token Structure, IEEE 802.6, IEEE 802.1, Physical Layout, Data Encoding and Transmission, FDDI,ATM

Introduction

IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.

IEEE 802.4: Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).

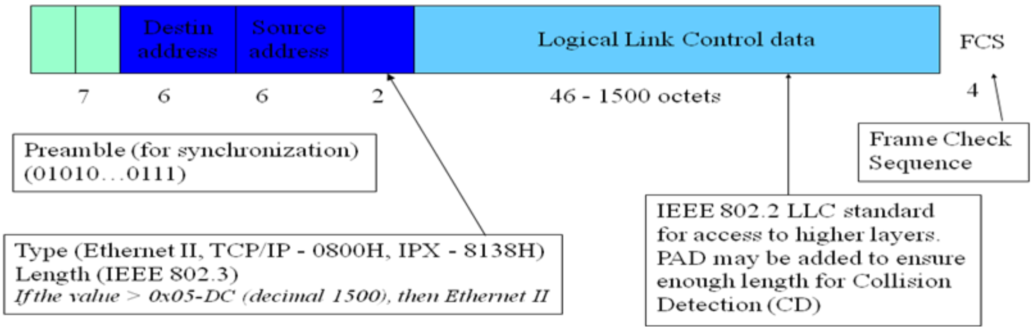
IEEE 802.5: Defines the MAC layer for token-ring networks.

IEEE 802.6: Standard for Metropolitan Area Networks (MANs)

802.3 Ethernet

Now that we have an overview of the OSI model, we can continue on these topics. I hope you have a clearer picture of the network model and where things fit on it.

Ethernet/IEEE 802.3 Frame


Destn address
Source address
Logical Link Control data
FCS
7
6
6
2
46 - 1500 octets
4
Preamble (for synchronization) (01010…0111)
Frame Check Sequence
IEEE 802.2 LLC standard for access to higher layers. PAD may be added to ensure enough length for Collision Detection (CD)
Type (Ethernet II, TCP/IP - 0800H, IPX - 8138H)
Length (IEEE 802.3)
If the value > 0x05-DC (decimal 1500), then Ethernet II

- 802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

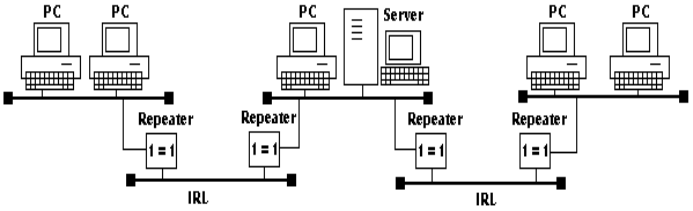
- CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.
- The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.
- Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.
  The most common topology for Ethernet is the star topology.

10 Base-5 (Thick Ethernet)

IEEE-spec	802.3
Max. speed	10 Mbps
Cable	Standard Ethernet Coax Cable
Connectors	N-type
Terminators	50 ohm
Max. length of a segment	500m/1640ft
Max. number of taps per segment	100
Max. number of stations per network	1024
Min. distance between taps	2.5m/8.3ft
Max. length of transceiver cable	50m/164ft
Max. number of repeaters	4
Topology	Bus

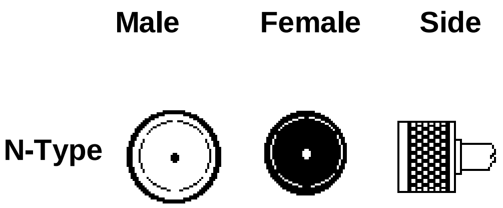
Maximum Topology

- 10Base-5 is a bus topology.
- A thick coaxial cable runs through the building and stations are attached to this cable by transceivers.



- The maximum amount of repeaters in a network is four. Since a segment may be up to 500 meters the total network length can be 2500 meter.

- There is little catch in this because 2 of the total of 5 segments may not be occupied. This doesn't matter for the length, but it does for the way you position your computers.
- The 2 non-occupied segments are only ment for extending the network and are called IRLs (Inter Repeater Links). For larger distances you need fiber optic repeaters or bridges or routers.



Cabling

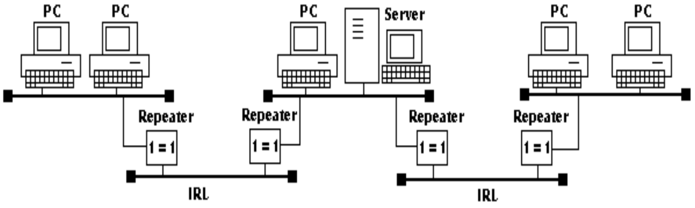
- 10Base-5 uses standard coaxial cable, the cable is about 1cm thick and yellow (normal cable) or orange (plenum cable) coloured. The connector type used is N-type.
- A segment can be one cable length with only two N-type connectors at the far ends, or it can be composed of several pre-terminated cables. The two last N-type connectors on the cable need to have a 50 ohm terminator installed. One of the terminators should be grounded. A segment is defined as all the cable between two terminators.
- Devices are attached to the segment (or backbone cable) by means of transceivers. A transceiver can be intrusive (N-type) or non-intrusive (vampire type). A transceiver always has a Sub-D15 male AUI (Attachment Unit Interface) connector.
- An IEEE802.3 10Base-5 compatible device has a female Sub-D15 female AUI (Attachment Unit Interface) connector that normally connects to a transceiver by means of a transceiver cable (also called AUI or drop cable). The transceiver cable is ALWAYS a male-female cable.

10 BASE-2 (Thin Ethernet)

IEEE-norm	802.3
Maximum speed	10 Mbps
Cable	RG58
Connectors	BNC
Terminators	50 ohm
Max. length of a segment	185m/607ft
Max. number of taps per segment	30
Max. amount of stations per network	1024

Min. distance between taps	0.5m/1.65ft
Max. number of repeaters	4
Topology	Bus

Maximum Topology

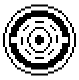
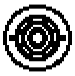
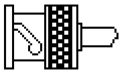


- 10Base-2 is a bus topology.
- The cable runs from computer to computer, like a daisy-chain. All devices are connected to the cable through a T-connector.
- The transceiver is on the Ethernet card in the device. This means that no cable is allowed between the T-connector and the device.

  A complete 10BASE-2 network (one collision domain) may consist of five segments interconnected by four repeaters.
- Only three of those five segments may have network devices connected to them
- The other two segments function as Inter Repeater Links (IRLs) and their only function is to extend the network. This allows for a maximum of 925m/3035ft (5x185m) of network cable if you stick to 10Base-2 cable. For larger distances you need 10Base-5 or fiber optic repeaters or bridges or routers.

Cabling

- Thin Ethernet is also called Cheaper net. Thin Ethernet uses RG58 coaxial cable and BNC connectors.

	Male	**Female**	**Side**
BNC			

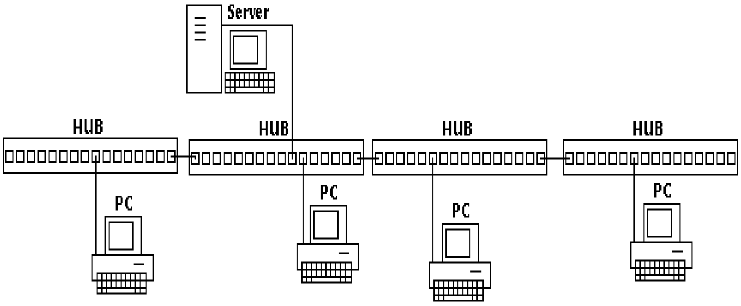
- An IEEE802.3 10Base-2 compatible device has a female BNC connector that connects to the coax cable by means of a FMF BNC T-connector.
- The T-connector connects directly to the device. It is not allowed to have any length of cable between the BNC T-connector and the device.
- The two last BNC T-connectors need to have a 50 ohm terminator installed on the un-used (open) side. One of the terminators should be grounded. A segment is defined as all the cable plus T-connectors between two terminators.

10BASE-T(Twisted-Pair Ethernet)

IEEE-spec	802.3
Wire speed	10 Mbps
Cable type	UTP CAT 3, 4 and 5
Connector type	RJ45
Used pins	1 & 2, 3 & 6
Max. length of a segment	100m/328ft
Max. number of taps per segment	2
Max. amount of stations per network	1024
Max. amount of repeaters	4
Topology	Star

Maximum Topology

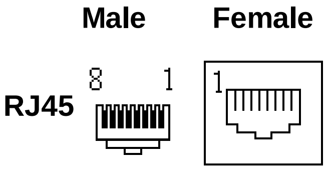
- A segment is defined as the cable between the hub and a workstation.
- According to the EIA/TIA this length has a maximum of 100m separated in: 5m from HUB to patch panel, 90 meters from patch panel to wall outlet, and 5 meters from wall outlet to the workstation.



- A complete 10Base-T network (one collision domain) may consist of 4 repeaters between the two far most workstations. Meaning the maximum length of a 10Base-T Network can be 500m/1500ft. To exceed this maximum you need Fiber Optic Repeaters or Bridges or Routers.

Cabling

- 10Base-T uses Category 3, 4 or 5 UTP cable and RJ45 connectors.

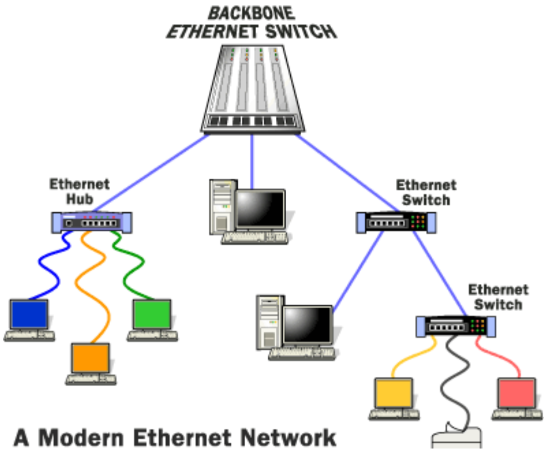


- Any IEEE802.3 10Base-T compatible device has a female RJ45 connector that normally connects to a hub or concentrator using UTP cable. The cabling is more or less a DTE/DCE situation. The workstation is a DTE and the HUB is a DCE. Connecting a workstation to an HUB requires a straight cable. Connecting two hubs or two workstations together requires a crossed cable.

- 10Base-T only uses 4 wires. In general the cable that is installed will be an 8-wire cable. The pins 4, 5, 7 and 8 are simply not used.

Switched Ethernet

- It refers to the use of switches in an Ethernet network .This term was more commonly used when networks were being transitioned from hubs to switches. Today ,Ethernet switches are the norm ,even low cost 5-port unit is switch rather then a hub.
- An Ethernet LAN that uses switches to connect individual hosts or segments.
- In the case of individual hosts, the switch replaces the repeater and effectively gives the device full 10 Mbps bandwidth (or 100 Mbps for Fast Ethernet) to the rest of the network.
- This type of network is sometimes called a *desktop switched Ethernet.* In the case of segments, the hub is replaced with a switching hub. Traditional Ethernets, in which all hosts compete for the same bandwidth, are called shared Ethernets*.*
- Switched Ethernets are becoming very popular because they are an effective and convenient way to extend the bandwidth of existing Ethernets.
- Modern Ethernet implementations often look nothing like their historical counterparts.
- Where long runs of coaxial cable provided attachments for multiple stations in legacy Ethernet, modern Ethernet networks use twisted pair wiring or fiber optics to connect stations in a **radial pattern**.
- Where legacy Ethernet networks transmitted data at 10 megabits per second (Mbps), modern networks can operate at 100 or even 1,000 Mbps!



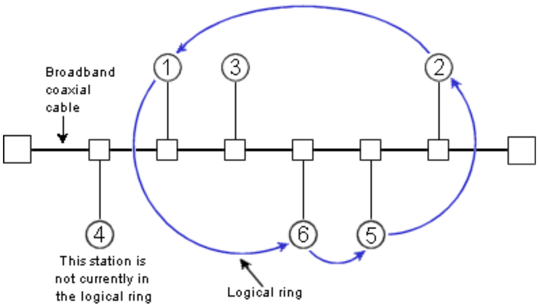
A Modern Ethernet Network

- Perhaps the most striking advancement in contemporary Ethernet networks is the use of **switched Ethernet**.
- Switched networks replace the shared medium of legacy Ethernet with a dedicated segment for each station.
- These segments connect to a switch, which acts much like an Ethernet bridge, but can connect many of these single station segments.

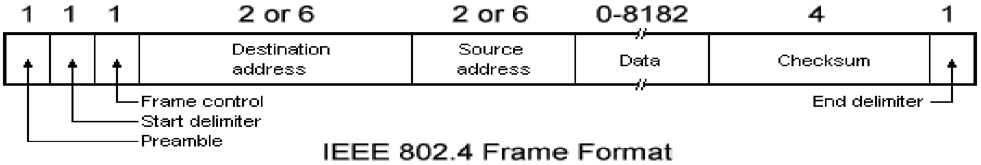
- Some switches today can support hundreds of dedicated segments. Since the only devices on the segments are the switch and the end station, the switch picks up every transmission before it reaches another node.
- The switch then forwards the frame over the appropriate segment, just like a bridge, but since any segment contains only a single node, the frame only reaches the intended recipient. This allows many conversations to occur simultaneously on a switched network.

IEEE 802.4: Token Bus Network

- In this system, the nodes are physically connected as a bus, but logically form a ring with tokens passed around to determine the turns for sending. It has the robustness of the 802.3 broadcast cable and the known worst case behaviour of a ring. The structure of a token bus network is as follows:



Frame Structure



IEEE 802.4 Frame Format

A 802.4 frame has the following fields:

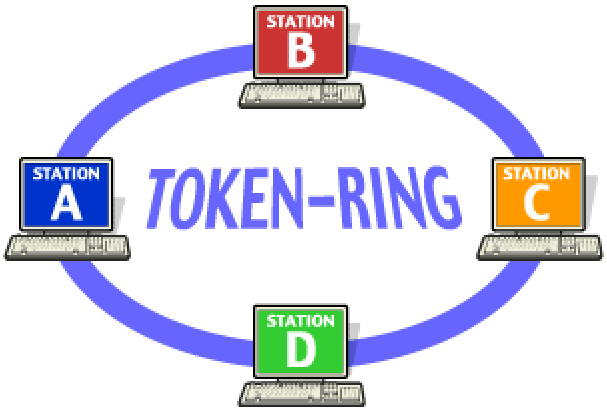
- Preamble: The Preamble is used to synchronize the receiver's clock.
- Starting Delimiter (SD) and End Delimiter (ED): The Starting Delimiter and Ending Delimiter fields are used to mark frame boundaries. Both of them contain analog encoding of symbols other than 1 or 0 so that they cannot occur accidentally in the user data. Hence no length field is needed.
- Frame Control (FC): This field is used to distinguish data frames from control frames. For data frames, it carries the frame's priority as well as a bit which the destination can set as an acknowledgement. For control frames, the Frame Control field is used to

specify the frame type. The allowed types include token passing and various ring maintenance frames.

- Destination and Source Address: The Destination and Source address fields may be 2 bytes (for a local address) or 6 bytes (for a global address).
- Data: The Data field carries the actual data and it may be 8182 bytes when 2 byte addresses are used and 8174 bytes for 6 byte addresses.
- Checksum: A 4-byte checksum calculated for the data. Used in error detection.

IEEE 802.5 Token Ring

- The most common local area network alternative to Ethernet is a network technology developed by IBM, called **token ring**.
- Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, token ring implements a strict, orderly access method.
- A token-ring network arranges nodes in a logical ring, as shown below. The nodes forward frames in one direction around the ring, removing a frame when it has circled the ring once.
- The ring initializes by creating a **token**, which is a special type of frame that gives a station permission to transmit.



- The token circles the ring like any frame until it encounters a station that wishes to transmit data.
- This station then "captures" the token by replacing the token frame with a data-carrying frame, which encircles the network.
- Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token and forwards that token on to the next node in the ring.
- Token-ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting.
- Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token-ring networks typically transmit data at either 4 or 16 Mbps.

- There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber.

  Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

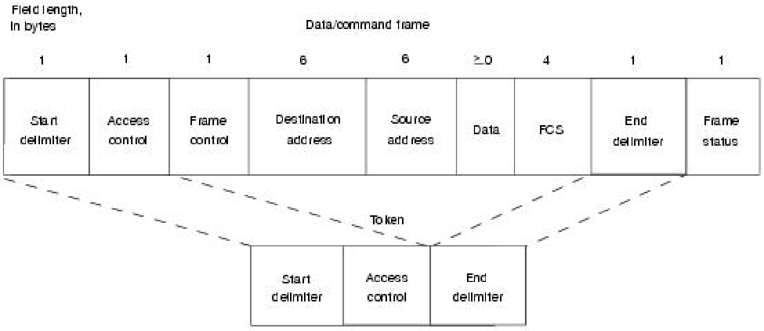
Token Ring Operation

- Token Ring and IEEE 802.5 are two principal examples of token-passing networks (FDDI is the other). Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit.
- If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.
- If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks. If early token release is supported, a new token can be released when frame transmission is complete.
- The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.
- Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. This feature and several reliability features, which are discussed in the section "Fault-Management Mechanisms," later in this article, make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important. Factory automation environments are examples of such applications.

Priority System

- Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: the priority field and the reservation field.
- Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

Frame Fromat



- Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames.
- Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.
- Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols. Both formats are shown in Figure: IEEE 802.5 and Token Ring Specify Tokens and Data/Command Frames

Token Frame Fields

The three token frame fields illustrated in Figure 9-3 are summarized in the descriptions that follow:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

- **End delimiter** - Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields illustrated in Figure 9-3 are described in the following summaries:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **Frame-control bytes** - Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** - Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data** - Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS)** - Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter** - Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame Status** - Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

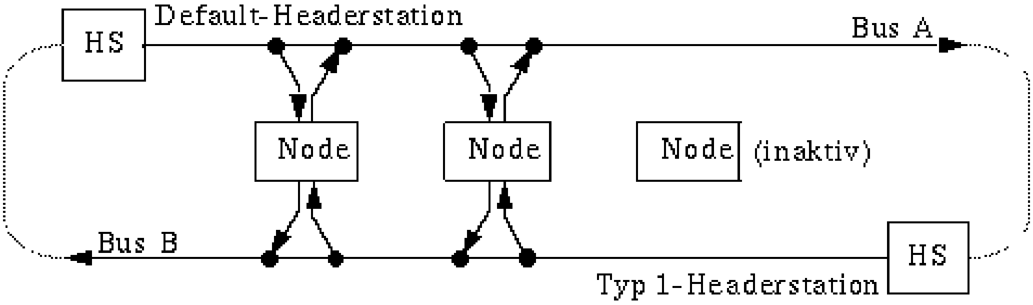
802.6 DQDB

- The IEEE Standard 802.6 *(*Distributed Queue Dual Bus *(DQDB) Sub network of a* Metropolitan Area Network (MAN)) permits sub network reconfiguration, usually without loss of communication ability, whenever there are bus faults. The Configuration Control Protocol (CCP) is the protocol which enables this to occur.
- **IEEE 802.6** is a standard governed by the ANSI for Metropolitan Area Networks (MAN). It is an improvement of an older standard (also created by ANSI) which used the Fiber distributed data interface (FDDI) network structure.

- The FDDI-based standard failed due to its expensive implementation and lack of compatibility with current LAN standards. The IEEE 802.6 standard uses the Distributed Queue Dual Bus (DQDB) network form. This form supports 150 Mbit/s transfer rates.
- It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fiber optic cable with an optical wavelength of 1310 nm. This standard has also failed, mostly due to the same reasons that the FDDI standard failed.
- Most MANs now use Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) network designs, with recent designs using native Ethernet or MPLS.

The DQDB Physical Layer

- The Head of Bus (HOB)s act a slot generators so that the bus is never quiet.
- Nodes are located logically adjacent to the bus and are promiscuous readers. They read all slots that come off the bus but may not necessarily alter any of the data.
- Nodes may be passive readers or, in an active system, they may act as repeaters so as to forestall attenuation.
- If Node 2 wishes to send data in the direction of Node n then it will use Bus A. This implies that it must first reserve a slot by placing a request on Bus B.
- If Node 2 wishes to send data in the direction of Node 1 it must first reserve a slot using Bus A and then send the data on Bus B.



DQDB Operation

- The DQDB configuration is independent of the number of nodes and of the distances involved making DQDB ideal for high-speed transmissions
- DQDB uses 53-byte packets (52 data bytes and one access control byte) for transmissions called slots.
- Slots from different nodes are intermingled in the network traffic.

- The head node (the first node connected to the external fiber) is responsible for creating empty slots and sending these down the line to the other nodes to use.
- The down line nodes indicate how many slots are needed using the secondary bus to the head node which then creates empty slots and sends these down the line.
- As the slots move down the line, they are taken by the nodes that have requested them.

IEEE 802.1

- It is a working group of the IEEE 802 project of the IEEE Standards Association.
  It is concerned with:
- 802 LAN/MAN architecture
- internetworking among 802 LANs, MANs and wide area networks
- 802 Link Security
- 802 overall network management
- protocol layers above the MAC & LLC layers

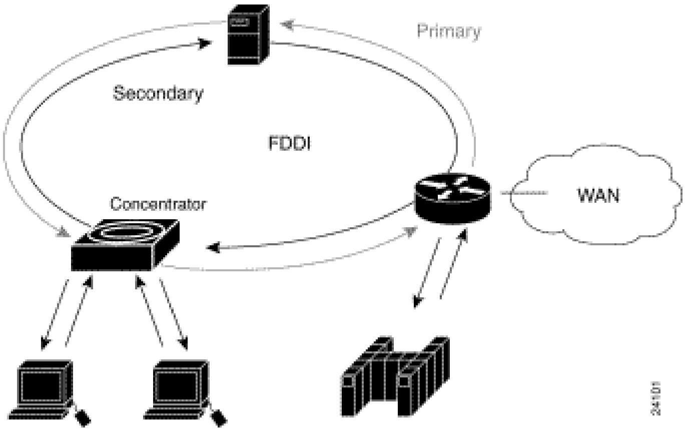
Fiber-Distributed Data Interface (FDDI)

- FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100-Mbps Ethernet, which is cheaper and easier to administer, FDDI has waned in popularity.
- FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.
- An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).
- FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols. FDDI-II is a version of FDDI that adds the capability to add circuit-switched service to the network so that voice signals can also be

handled. Work is underway to connect FDDI networks to the developing Synchronous Optical Network.

Function of FDDI

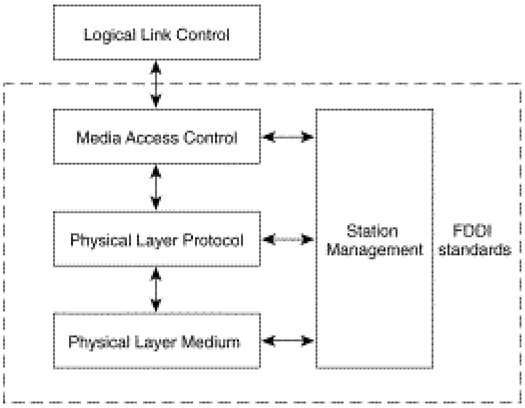
- The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper.
- FDDI uses a dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating).



- The dual-rings consist of a primary and a secondary ring.
- During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle.
- The primary purpose of the dual rings, as will be discussed in detail later in this chapter, is to provide superior reliability and robustness. Figure 1 shows the counter-rotating primary and secondary FDDI rings.

FDDI Specifications

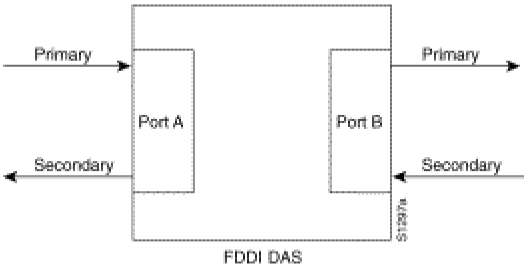
- FDDI specifies the physical and media-access portions of the OSI reference model.
- FDDI is not actually a single specification, but it is a collection of four separate specifications each with a specific function.
- Combined, these specifications have the capability to provide high-speed connectivity between upper-layer protocols such as TCP/IP and IPX, and media such as fiber-optic cabling.
- FDDI's four specifications are the Media Access Control (MAC), Physical Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT).



- The MAC specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and error-recovery mechanisms.
- The PHY specification defines data encoding/decoding procedures, clocking requirements, and framing, among other functions. The PMD specification defines the characteristics of the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors.
- The SMT specification defines FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.
- FDDI is similar to IEEE 802.3 Ethernet and IEEE 802.5 Token Ring in its relationship with the OSI model. Its primary purpose is to provide connectivity between upper OSI layers of common protocols and the media used to connect network devices.

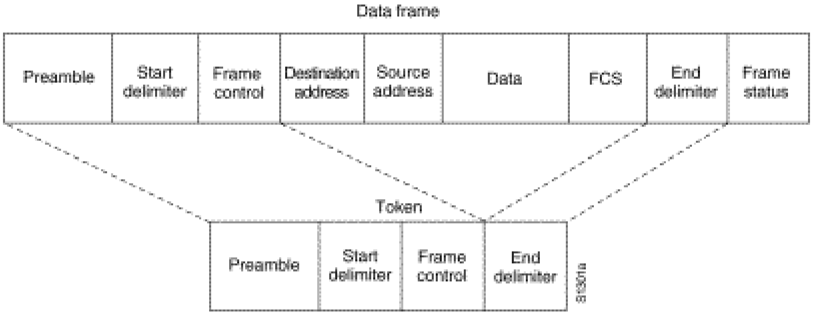
FDDI Station-Attachment Types

- One of the unique characteristics of FDDI is that multiple ways actually exist by which to connect FDDI devices. FDDI defines three types of devices: single-attachment station (SAS), dual-attachment station (DAS), and a concentrator.
- An SAS attaches to only one ring (the primary) through a concentrator. One of the primary advantages of connecting devices with SAS attachments is that the devices will not have any effect on the FDDI ring if they are disconnected or powered off. Concentrators will be discussed in more detail in the following discussion.



- Each FDDI DAS has two ports, designated A and B. These ports connect the DAS to the dual FDDI ring. Therefore, each port provides a connection for both the primary and the secondary ring. As you will see in the next section, devices using DAS connections will affect the ring if they are disconnected or powered off. Figure 3 shows FDDI DAS A and B ports with attachments to the primary and secondary rings.
- An FDDI concentrator (also called a *dual-attachment concentrator* [DAC]) is the building block of an FDDI network. It attaches directly to both the primary and secondary rings and ensures that the failure or power-down of any SAS does not bring down the ring.

- This is particularly useful when PCs, or similar devices that are frequently powered on and off, connect to the ring. Figure 4 shows the ring attachments of an FDDI SAS, DAS, and concentrator.
- FDDI Frame Format
- The FDDI frame format is similar to the format of a Token Ring frame. This is one of the areas where FDDI borrows heavily from earlier LAN technologies, such as Token Ring. FDDI frames can be as large as 4,500 bytes. Following fig. shows the frame format of an FDDI data frame and token.



Asynchronous transfer mode

- A final network technology that bears mentioning is **asynchronous transfer mode**, or ATM.
- ATM networks blur the line between local and wide area networking, being able to attach many different devices with high reliability and at high speeds, even across the country.
- ATM networks are suitable for carrying not only data, but voice and video traffic as well, making them versatile and expandable. While ATM has not gained acceptance as rapidly as originally predicted, it is nonetheless a solid network technology for the future.
- Ethernet's popularity continues to grow. With almost 30 years of industry acceptance, the standard is well known and well understood, which makes configuration and troubleshooting easier.
- As other technologies advanced, Ethernet has evolved to keep pace, increasing in speed and functionality.**ATM** is a high-speed networking standard designed to support both voice and data communications.
- ATM is normally utilized by Internet service providers on their private long-distance networks. ATM operates at the data link layer (Layer 2 in the OSI model) over either fiber or twisted-pair cable.
- ATM differs from more common data link technologies like Ethernet in several ways. For example, ATM utilizes no routing.
- Hardware devices known as ATM switches establish point-to-point connections between endpoints and data flows directly from source to destination. Additionally,

instead of using variable-length packets as Ethernet does, ATM utilizes fixed-sized cells. *ATM cells* are 53 bytes in length, that includes 48 bytes of data and five (5) bytes of header information.

- The performance of ATM is often expressed in the form of OC (Optical Carrier) levels, written as "OC-xxx." Performance levels as high as 10 Gbps (OC-192) are technically feasible with ATM. More common performance levels for ATM are 155 Mbps (OC-3) and 622 Mbps (OC-12).
- ATM technology is designed to improve utilization and quality of service (QoS) on high-traffic networks. Without routing and with fixed-size cells, networks can much more easily manage bandwidth under ATM than under Ethernet, for example. The high cost of ATM relative to Ethernet is one factor that has limited its adoption to backbone and other high-performance, specialized networks.

The structure of an ATM cell

- An ATM cell consists of a 5-byte header and a 48-byte payload. The payload size of 48 bytes was chosen as described above.
- ATM defines two different cell formats: UNI (User-Network Interface) and NNI (Network-Network Interface). Most ATM links use UNI cell format.

Diagram of the UNI ATM Cell

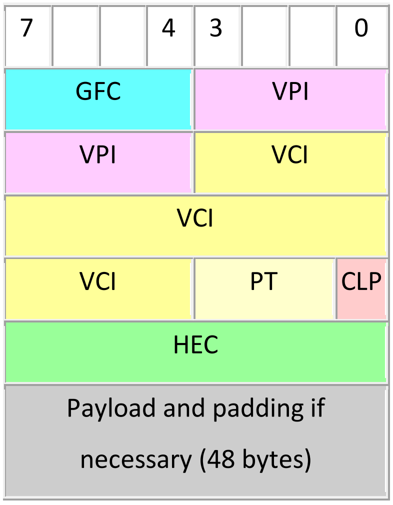
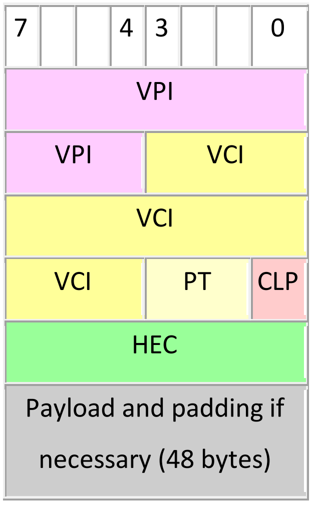


Diagram of the NNI ATM Cell



GFC = Generic Flow Control (4 bits) (default: 4-zero bits)

VPI = Virtual Path Identifier (8 bits UNI, or 12 bits NNI)

VCI = Virtual Channel identifier (16 bits)

PT = Payload Type (3 bits)

CLP = Cell Loss Priority (1-bit)

HEC = Header Error Control (8-bit CRC, polynomial = $X^8 + X^2 + X + 1$)

- ATM uses the PT field to designate various special kinds of cells for operations, administration and management (OAM) purposes, and to delineate packet boundaries in some ATM adaptation layers (AAL).
- Several ATM link protocols use the HEC field to drive a CRC-based framing algorithm, which allows locating the ATM cells with no overhead beyond what is otherwise needed for header protection. The 8-bit CRC is used to correct single-bit header errors and detect multi-bit header errors. When multi-bit header errors are detected, the current and subsequent cells are dropped until a cell with no header errors is found.
- A UNI cell reserves the GFC field for a local flow control/sub multiplexing system between users. This was intended to allow several terminals to share a single network connection, in the same way that two Integrated Services Digital Network(ISDN) phones can share a single basic rate ISDN connection. All four GFC bits must be zero by default.
- The NNI cell format replicates the UNI format almost exactly, except that the 4-bit GFC field is re-allocated to the VPI field, extending the VPI to 12 bits. Thus, a single NNI ATM interconnection is capable of addressing almost 2^{12} VPs of up to almost 2^{16} VCs each (in practice some of the VP and VC numbers are reserved).

10.0 Interconnection

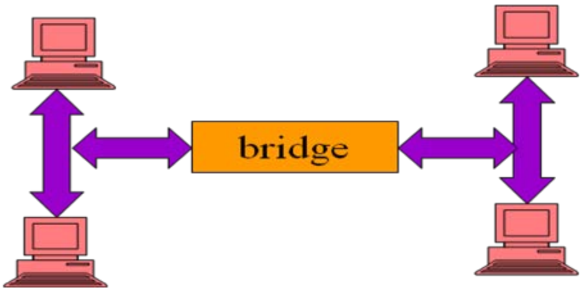
Contents

10.1 Use of Repeaters, Bridges, Router, Gateways, Public Network, X.25, Frame Relay

Use of Repeaters

- A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss.
- Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.
- In a data network, a repeater can relay messages between sub networks that use different protocols or cable types.
- Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.
- Network **repeaters** regenerate incoming electrical, wireless or optical signals. With physical media like Ethernet or Wi-Fi, data transmissions can only span a limited distance before the quality of the signal degrades.
- Repeaters attempt to preserve signal integrity and extend the distance over which data can safely travel.
- A repeater connects two segments of your network cable.
- It retimes and regenerates the signals to proper amplitudes and sends them to the other segments.
- When talking about, Ethernet topology, you are probably talking about using a hub as a repeater.
- Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row.
- Many network architectures limit the number of repeaters that can be used in a row.
- Repeaters work only at the physical layer of the OSI network model.
- Actual network devices that serve as repeaters usually have some other name.
- **Active hubs**, for example, are repeaters. Active hubs are sometimes also called "multiport repeaters," but more commonly they are just "hubs."
- Other types of "passive hubs" are not repeaters. In Wi-Fi, access points function as repeaters only when operating in so-called "repeater mode."

Bridge



- Bridge is physical device typically a box of two port which connect two network at Data Link Layer.
- A Bridge provides packet filtering at Data link layer .
- A bridge to join to existing LAN or two split one LAN in to two segment. Bridge operate in promiscuous mode.
- Data packet enter the bridge through either one of the port and the bridge then read the destination address in each packet header and decides how to process that packet . This is called packet filtering.
- If the destination address of a packet arriving from one network segment is that of a computer on the other segment, the bridge Tx it out from other port.
- If the destination address of a computer on a same network segment as the computer that generated it, the bridge discard the packet.

Bridges &Collision

- A collisions domain is a network that is constructed so that when two computers transmit packet at the same time a collision occurs. When we add the new hub in existing network that the same collision domain as the original network because Hub relay the signal without filtering the packet
- Bridge do not relay the signals to other network until they have receive the entire packet. For this reason two computer on different side of the bridge do not cause to conflict.
- Bridge maintain the internal address table that listed the hardware address of the computer on both segment . When bridge receive the packet and read the destination address DLL header. It check the address against its lists. If the address is associated with the segment other than that from which the packet arrived, the bridge relay it to that segment there are two type of bridge

  (a) Local Bridge

  (b)Translation Bridge

  (c) Remote Bridge

Local Bridge

- Standard type of bridge use to connect network segment of same type and same location is called local bridge. This is simplest type of bridge ,it does not modify the data in packet. It simply read the address in the data link layer protocol and pass the packet or discard it.

Translation bridge

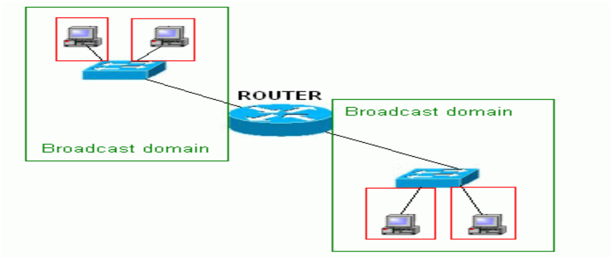
- It is DLL device that connect network using different network media or different protocol. This bridge is more complicated than local bridge. The bridge can thus connect an Ethernet segment to FDDI (Fiber Distributed Data Interface) segment or connect two different type of Ethernet type segment such as (100BaseTx).

Remote Bridge

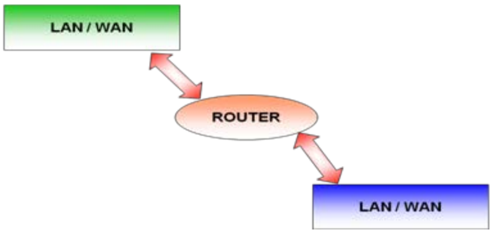
- Remote bridge is designed to connect two network segment at distance locations using some form of wide area network link. The link can be a modem connection leased telephone line or any type of WAN technology. The advantage of using a bridge in this manner is that you reduce the amount of traffic passing over the WAN link., which is usually far slower and more expensive than the local Network.

Router

- Routers are packet forwarding devices or it is a device that forwards data packet along network.
- Routers are located at gateway the places where two or more networks connect. .

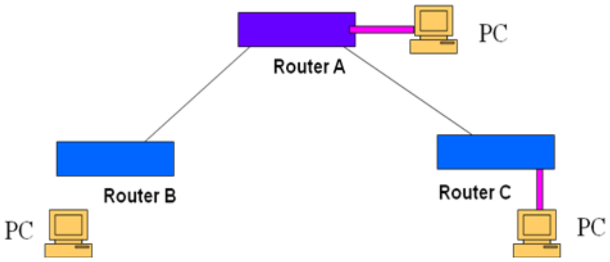


- A router is connected to at least two networks, commonly two LANs or WAN or a LAN and its ISP's network. Routers allow transmission of data between network segments.
- Routers are specialized computers that send your messages and those of every other Internet user speeding to their destinations along thousands of pathways.



Function Of Router

- Routing is the process of moving data throughout a network , passing through several network segments.
- Router gets information about which path to take from files on the routers called routing tables. These table contain information about which router network interface to place information on in order to send it to a particular network segment. Routers will not pass unknown or broadcast packets. A router will route a packet only if it has a specific destination.



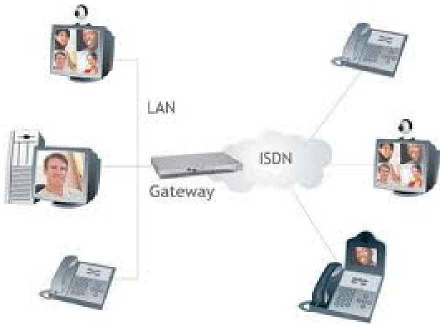
- Keeping the messages moving
- Transmitting packets
- Knowing where to send data
- Understanding the protocols
- Tracing message

The main difference between routers, bridges

- A router passes packets by looking up the destination in it's routing table of an incoming packet. Bridges work at layer 1/2 physical media where everything is passed from one port to another with no regard for source, destination, or network address.
- Routers work at layer 3 moving packets from one port to another based on the L3 address - i.e. IP address, IPX address, etc.

Gateway

- A gateway can translate information between different network data formats or network architectures.
- It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers.
- Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model.

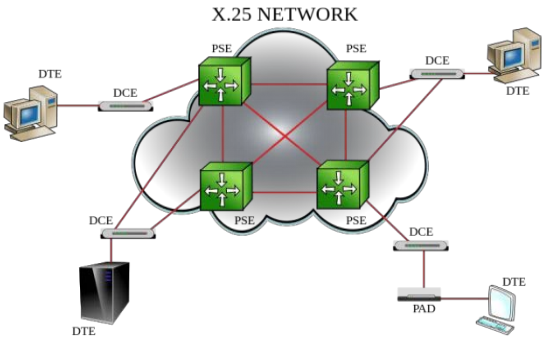


- Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model.
- To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

X.25

- **X.25** is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.
- X.25 was originally defined by the International Telegraph and Telephone Consultative Committee (CCITT, now ITU-T) in a series of drafts and finalized in a publication known as The Orange Book in 1976.
- .X.25 is a family of protocols that was popular during the 1980s with telecommunications companies and in financial transaction systems such as automated teller machines.

- X.25 is a standard suite of protocols used for packet switching across computer networks. The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model.
- Each X.25 packets contains up to 128 bytes of data. The X.25 network handles packet assembly at the source device, delivery, and then dis-assembly at the destination. X.25 packet delivery technology includes not only switching and network-layer routing, but also error checking and re-transmission logic should delivery failures occur. X.25 supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.



- Based upon existing analog copper lines that experience a high number of errors
- Uses the virtual circuit approach
- An X.25 WAN consists of packet-switching exchange (PSE) nodes as the networking hardware, and leased lines, plain old telephone service connections or ISDN connections as physical links
- Provides a way to send packets across a packet-switched public data network
- The redundant error checking is done at each node
- X.25 was originally designed more than 25 years ago to carry voice over analog telephone lines (dialup networks). Typical applications of X.25 today include automatic teller machine networks and credit card verification networks. X.25 also supports a variety of mainframe terminal/server applications.
- With the widespread acceptance of Internet Protocol (IP) as a standard for corporate networks, many X.25 applications are now being migrated to cheaper solutions using IP as the network layer protocol and replacing the lower layers of X.25 with Ethernet or ATM hardware.

Architecture

- The X.25 specification defines only the interface between a subscriber (DTE) and an X.25 network (DCE). X.75, a very similar protocol to X.25, defines the interface between two X.25 networks to allow connections to traverse two or more networks.

- X.25 originally defined three basic protocol levels or architectural layers. The layer numbers were dropped to avoid confusion with the OSI Model layers.

Physical layer

- This layer specifies the physical, electrical, functional and procedural characteristics to control the physical link between a DTE and a DCE.
- Common implementations use X.21, EIA-232, EIA-449 or other serial protocols.

Data link layer

- The data link layer consists of the link access procedure for data interchange on the link between a DTE and a DCE.
- In its implementation, the, link accessed procedure balanced (lapb) is a data link protocol that manages a communication session and controls the packet framing.
- It is a bit-oriented protocol that provides error correction and orderly delivery.

Packet layer

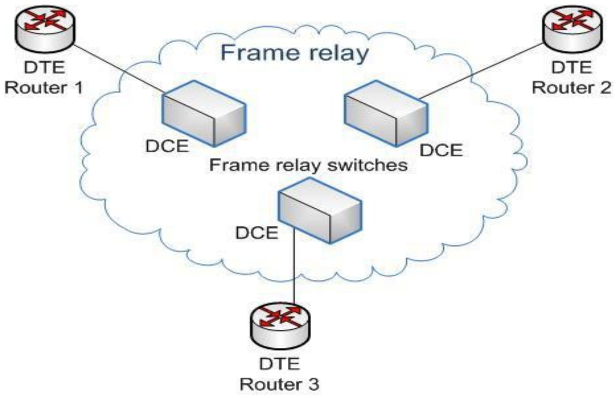
- This layer defined a packet-layer protocol for exchanging control and user data packets to form a packet-switching network based on virtual calls, according to the packet layer.
- X.25 provides a set of user facilities defined and described in ITU-T Recommendation X.2. The X.2 user facilities fall into five categories:
  1. Essential facilities;
  2. Additional facilities;
  3. Conditional facilities;
  4. Mandatory facilities.
  5. Optional facilities.

Frame Relay

- Frame relay is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN in late 1980s and early 1990s.
- Prior to frame relay, some organizations were using a virtual-circuit switching network called X.25 that performed switching at the network layer.However,X.25 has several drawbacks:-
  - a.) X.25 has a low 64 kbps data rate. By the 1990s.there was a need for higher data rate WANs.
  - b.) X.25 has extensive flow and error control at both the data link layer and the network layer. Similar to X.25, but does not have the added framing and processing overhead to provide guaranteed data transfer.
- In response to the above drawbacks, Frame relay was designed. Frame relay is a wide-area network with the following features:-

1. Frame relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).this means that it can easily be used instead of a mesh of T-1 or T-3 lines.
2. Frame relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocol that already have a network layer protocol, such as the Internet.
3. Frame relay allows bursty data.
4. Frame relay allows a frame size of 9000 bytes, which can accommodate all local area network frame sizes.
5. Frame relay is less expensive than other traditional WANs.
6. Frame relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.

- Frame Relay only operates at the first two layers of the OSI model. FR is basically "dumb" and relies upon customer equipment or DTE gear to monitor and govern flows and do error correction.
- Link-to-link reliability is not provided – if a frame is corrupted, it is silently discarded
- Upper-level protocols such as TCP must detect and recover discarded frames
- Frame Relay call control signalling is carried out separate from the actual data connection. This eliminates nodes having to store tables of routing information
- An entire OSI layer is non-existent with Frame Relay.



- There is no low or hop control, or error correction. Other applications operating above Frame Relay must carry this out.
- Frame Relay can operate upto 2Mbps (32 timeslots), rather than the 64kbps of X25 (1 timeslot).
- Frame relay provides permanent virtual circuits and switched virtual circuits. A virtual circuit in frame relay is identified by a number called a data link connection identifier (DLCI).

11.0 Iteroperability

TCP/IP protocol suite

- This section presents an in-depth introduction to the protocols that are included in TCP/IP. Although the information is conceptual, you should learn the names of the protocols.
- TCP/IP" is the acronym that is commonly used for the set of network protocols that compose the Internet Protocol suite. Many texts use the term “Internet” to describe both the protocol suite and the global wide area network.

Protocol Layers and the Open Systems Interconnection Model

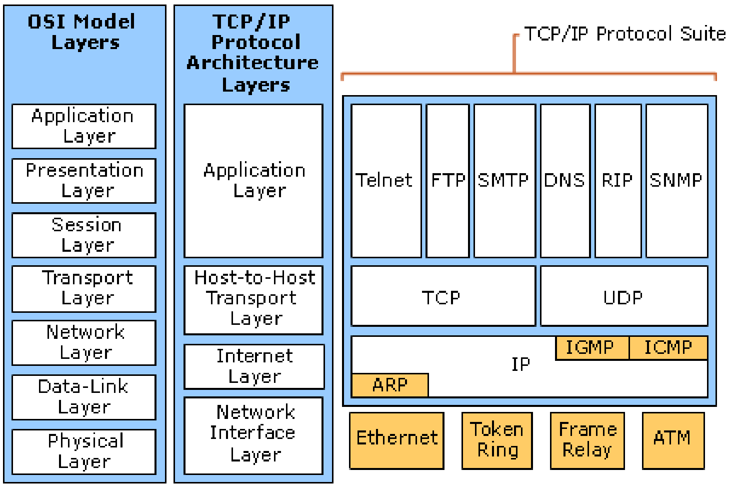
- Most network protocol suites are structured as a series of layers, sometimes collectively referred to as a protocol stack. Each layer is designed for a specific purpose.
- Each layer exists on both the sending and receiving systems. A specific layer on one system sends or receives exactly the same object that another system's peer process sends or receives.

Architecture Model

The OSI model describes idealized network communications with a family of protocols. TCP/IP does not directly correspond to this model. TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all.

TCP/IP Model Layers

The TCP/IP model uses four layers that logically span the equivalent of the top six layers of the OSI reference model; this is shown (The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stack and the underlying networking hardware.) The following are the TCP/IP model layers, starting from the bottom.



Physical network layer

- The physical network layer specifies the characteristics of the hardware to be used for the network.
- For example, physical network layer specifies the physical characteristics of the communications media.
- The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

- The data-link layer identifies the network protocol type of the packet, in this instance TCP/IP.
- The data-link layer also provides error control and "framing."
- Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Network Layer

- The Internet layer, also known as the network layer or IP layer, accepts and delivers packets for the network.
- This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

- The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

IP addressing

- The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.
- Host-to-host communications – IP determines the path a packet must take, based on the receiving system's IP address.

ARP Protocol

- The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers.

- ARP assists IP in directing datagram’s to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

- The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:
- Dropped packets – Packets that arrive too fast to be processed
- Connectivity failure – A destination system cannot be reached

Transport Layer

- The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets.
- This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service.
- UDP provides unreliable datagram service.

TCP Protocol

- TCP enables applications to communicate with each other as though they were connected by a physical circuit.
- TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

SCTP Protocol

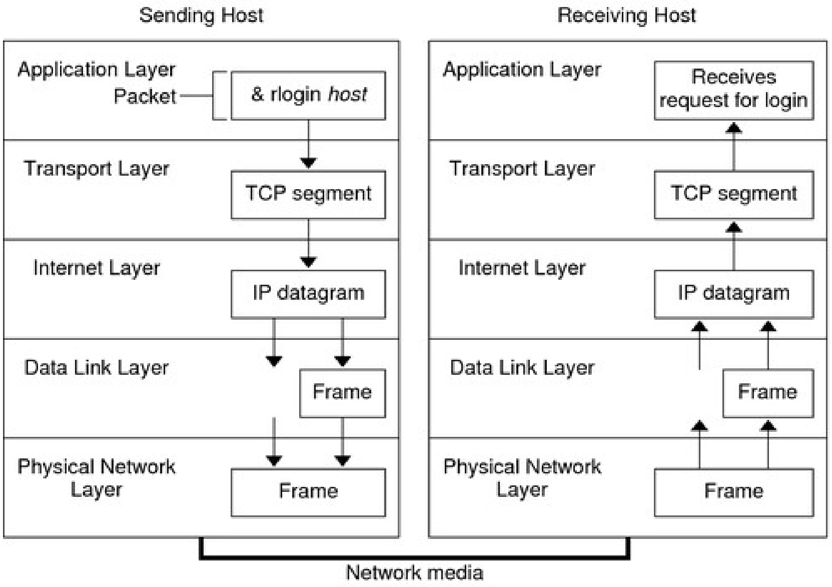
- SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP.
- Moreover, SCTP can support connections between systems that have more than one address, or multihued.
- The SCTP connection between sending and receiving system is called an association.

Application Layer

- The application layer defines standard Internet services and network applications that anyone can use.
- These services work with the transport layer to send and receive data. Many application layer protocols exist.
- The following list shows examples of application layer protocols:
  1.Standard TCP/IP services such as the ftp, tftp, and telnet commands

2. UNIX “r” commands, such as rlogin and rsh
3. Name services, such as NIS and the domain name system (DNS)
4. Directory services (LDAP)
5. File services, such as the NFS service
6. Simple Network Management Protocol (SNMP), which enables network management
7. Data Encapsulation and the TCP/IP Protocol Stack
8. The packet is the basic unit of information that is transferred across a network.

- The basic packet consists of a header with the sending and receiving systems' addresses, and a body, or payload, with the data to be transferred.
- As the packet travels through the TCP/IP protocol stack, the protocols at each layer either add or remove fields from the basic header.
- When a protocol on the sending system adds data to the packet header, the process is called data encapsulation. Moreover, each layer has a different term for the altered packet, as shown in the following figure.



The receiving side also follow the same layering procedure

Application Layer

- Where a Communication Originates
- The packet's history begins when a user on one system sends a message or issues a command that must access a remote system.
- The application protocol formats the packet so that the appropriate transport layer protocol, TCP or UDP, can handle the packet.

Transport Layer

- Where Data Encapsulation Begins
- When the data arrives at the transport layer, the protocols at the layer start the process of data encapsulation.
- The transport layer encapsulates the application data into transport protocol data units.
- The transport layer protocol creates a virtual flow of data between the sending and receiving application.

Data-Link Layer

- Where Framing Takes Place
- Data-link layer protocols, such as PPP, format the IP datagram into a frame. These protocols attach a third header and a footer to "frame" the datagram.
- The frame header includes a cyclic redundancy check (CRC) field that checks for errors as the frame travels over the network media. Then, the data-link layer passes the frame to the physical layer.

Physical Network Layer

- Where Frames Are Sent and Received
- The physical network layer on the sending host receives the frames and converts the IP addresses into the hardware addresses appropriate to the network media.
- The physical network layer then sends the frame out over the network media.

CNDC Sample questions

Short Question-2 mark

1. What is data transfer rate?
2. What is parallel transmission?
3. Write two advantage of parallel transmission?
4. What is serial transmission?
5. Give the name of different serial transmission with an example?
6. Write two advantage of serial transmission?
7. What is synchronous transmission?
8. What is asynchronous transmission?
9. Give two advantage & disadvantage of asynchronous transmission?
10. What is data channel?
11. What is channel capacity?
12. What is switching? Give the name of different switching circuit?
13. What is packet switching?
14. What is circuit switching?
15. What is datagram?
16. Give the name of different phase of virtual circuit?
17. Explain flow control.
18. Write three conditions for error correction and error detection?
19. How encoder and decoder will work for error correction?
20. Define dataflow.
21. What is networking? Write two advantage & disadvantage of networking?
22. What are the different criteria for networking?
23. W hat is half duplex?
24. What is full duplex?
25. What is simplex?
26. Give the name of one connector and explain its work?
27. How the modems are work?
28. What is multiplexing? Mention the name of different multiplexing?
29. Write the work of multiplexer and demultiplexor?
30. What is bandwidth?
31. What is FDM? Which signal technique is used for FDM?
32. What is TDM? Which signals are transmitted in case of TDM?
33. Explain WDM.
34. What is demultiplexing?
35. What is SDM? How it is flexible?
36. Explain CDM.
37. What are the different types of network model?
38. Explain about LAN, WAN, MAN shortly.
39. What are topologies? Give the name of different types of topology?
40. What is mesh topology?
41. What is bus topology? How many bus topologies are there?
42. Write the work of tap or connector? Which topology is best for tap or connector?
43. Which types of signals are transmitted in case of circuit switching and packet switching?

44. What is structured wiring system?
45. How many type of copper cable are used and what are those?
46. Write the work of coaxial cable?
47. What is shielded twisted pair cable?
48. What is unshielded twisted pair cable?
49. How the fiber optic cables are made? Which signals are transferred in fiber optic cable?
50. What is OSI reference model? Give the name of 7 layer of OSI model?
51. How the data are transmitted in case of physical layer and how the data bits are send in case of data link layer?
52. Which type of protocols is used for transport layer?
53. What is the work of presentation &session layer?
54. What is the work of application layer?
55. Which protocols are used for application layer?
56. Write some advantage of layering & existing standard?
57. What is signal?
58. What is signaling base band?
59. What is NRZ &RZ?
60. Write two difference between NRZ-L & NRZ-I?
61. What is Manchester encoding?
62. What is differential Manchester encoding?
63. What is error? How many type of error is there and what are those?
64. What is modulation technique? Write the name of different modulation technique?
65. Define broadband.
66. Define carrier band.
67. Write two differences between broadband & carrier band?
68. What is token ring?
69. What is token passing?
70. What is the work of token bus?
71. Define demand priority.
72. What is fast switching?
73. Write some points on IEEE 802.3, IEEE 802.4 &IEEE 802.5?
74. Define ATM.
75. How the FDDI will work for network?
76. Define frame relay.
77. Define X.25.
78. Write two differences between TCP and UDP?
79. Why TCP/IP is so called connection oriented?
80. Why we use repeater?
81. What is the work of router?
82. What is gate way?
83. Write the work of modem?
84. Define IP format.

LONG QUESTION (6 Mark)

1. What is data transfer rate? Explain different types of data transmission with diagram.
2. Define data transfer, data transfer rate, data channel & channel capacity.
3. What is switching? Explain about different types of switching circuit.
4. What is error? What are the different types of methods are used for error detection?
5. Explain error correction method briefly using one example.
6. How error recovery will do explain it briefly?
7. Explain serial and parallel connection with diagram. Write the advantage of serial and parallel connection?
8. What is data flow? Explain half duplex, full duplex and simplex briefly.
9. What is multiplexing? Define various types of multiplexing.
10. Write the short note on SDM and CDM?
11. What is network? Explain about network user briefly.
12. Define central server and print server neatly.
13. Discuss about LAN environment with WAN and MAN?
14. What is directory? Explain the work of directory service.
15. What is networking? Write the different advantage & disadvantage of networking briefly?
16. What is topology? Discuss about various types of topologies?
17. Define structured wired system briefly?
18. Why copper cable is required for networking? Explain co-axial cable briefly?
19. What is the work of twisted pair cable? Explain UTP & STP.
20. Write the work of fiber optic cable? Define where it is used?
21. What is OSI reference model? Explain the 7 layers of OSI model briefly.
22. Describe about different line coding scheme?
23. Write the several difference between NRZ-L & NRZ-I?
24. Define Manchester encoding and differential Manchester encoding scheme?
25. Give the short note on
    1. Signaling baseband
    2. Broad band
    3. Carrier band
26. What is modulation? Explain about different modulation technique briefly.
27. What is CSMA? Discuss about various types of CSMA with diagram?
28. What is CSMA? Define CSMA/CD & CSMA/CA with flow chart.
29. Give the short note on:-
    1. Token passing
    2. Token ring
    3. Token bus
    4. Slotted ring
30. Define about demand priority and fast switching.
31. Explain IEEE 802.5.
32. Explain IEEE 802.6 briefly.
33. Explain the work of FDDI.
34. Define asynchronous transfer mode (ATM) briefly.

35. Write the work of frame relay?
36. Define repeater, bridge, router and gateway with example briefly.
37. Define the work of public network. explain about X.25.
38. Give the 6 difference between TCP & UDP?
39. Define error control with example briefly.
40. Explain TCP/IP protocol suite with IP address format with neat diagram.

LONG QUESTION (8 marks)

1. What is data transfer rate? Explain about the different data transmission with neat diagram.
2. Define switching. Discuss about the various type of switching circuit with suitable example?
3. What is packet switching? Explain datagram and virtual circuit switching network.
4. Explain error detection method with suitable example briefly.
5. What is error? Explain error control mechanism briefly.
6. What is data flow? Explain about simplex, half-duplex, full-duplex and parallel connection briefly.
7. What is multiplexing? Discuss about various type of multiplexing with neat diagram?
8. Define network users. Explain print server and central server.
9. Define LAN enviournment with WAN & MAN.
10. Give the sort note on:-
    a) Device sharing
    b) Directory service
    c) Central server
    d) Print server
11. What is networking? Discuss various advantage and disadvantage of networking?
12. What is topology? Explain different types of network topologies with neat diagram briefly.
13. What is twisted pair cable? Explain UTP & STP properly.
14. What is OSI reference model? Explain about 7 layer of OSI model.
15. Explain line coding scheme briefly.
16. Define Manchester encoding and differential Manchester encoding scheme.
17. Define CSMA? Explain about the different types of CSMA with diagram.
18. Explain CSMA with collision detection.
19. Explain CSMA with collision avoidance.
20. Write the short note on:-
    a) Token passing
    b) Token ring
    c) Token bus
    d) Slotted ring
21. Explain about different LAN standard with example briefly.
22. Discuss frame relay and asynchronous transfer mode with neat diagram?
23. What do you mean by repeater? Explain the work of router and gateway.
24. Explain the work of X.25 for networking with diagram.
25. Explain about TCP/IP protocol suite briefly with neat diagram.