Chapter 1

OSI Layers

LEARNING OBJECTIVES

- *Computer network*
- *LAN*
- *LAN topologies*
- *CSMA/CD*
- *WAN*
- *The OSI reference model*
- *LAN technologies*
- *Physical layer*
- *Data link layer*
- *Types of error*
- *MAC sub layer*
- *FDM/TDM*

Computer Network

Computer network is the collection of two or more computers that are interconnected with each other to perform data communication using the data communication protocol through communications media (wired or wireless) .So these computers can share information, data, programs, and use of hardware together. Data communications that can be done include text data, images, video and sound.

Or

A computer network, often simply referred, as a network is a collection of computers and devices interconnected by communication channels that facilitate communication and allow sharing of resources and information among interconnected devices. There are different networks:

1. LAN
2. MAN
3. WAN

LAN

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a lab, school, or building. LAN Computers rarely spans more than a mile apart.

In a typical LAN configuration, one computer is designated as the file server. It stores all the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On many LANs, cables are used to connect the network interface cards in each computer. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU which executes programs and it is also able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

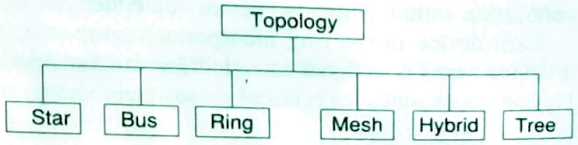
Three characteristic features of LAN

1. The size of a LAN network.
2. The topology of the local area network.
3. The technology used for transmission.

In simple LAN configuration, a single cable runs through the entire set up and the peripherals and computers are attached to the cable. Traditional LAN speeds are 10 Mbps to 100 Mbps. Modern LAN cables are capable of much higher data transfer per second.

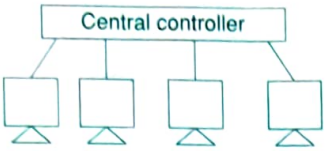
In case two or more systems need to use the LAN at the same time, then an arbitration mechanism is deployed to resolve the conflict. A first come first serve policy or a prioritized approach may be chosen.

LAN topologies



Star Topology Each device has a dedicated point-to-point link to a central controller called a hub. Most used LAN topology.

If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device as shown in the figure.



Each device needs only one link and one I/O port to connect it to any number of others.

Advantages

1. Robust, if one link fails, only that link is affected. All other links remain active.
2. As long as hub is working, it can monitor link problems and by pass defective links.

Disadvantages

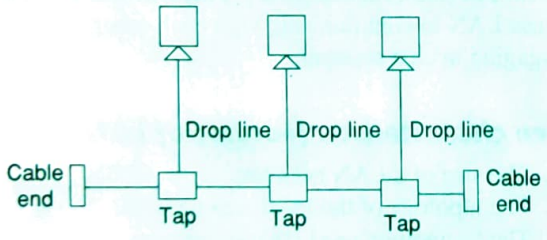
1. If hub goes down, the whole system dead.
2. More cabling is required in a star than ring or bus.

Bus Topology A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the accessing technique used.

The traffic can go in either direction, i.e., it is bidirectional.

Nodes are connected to the bus cable by drop lines and taps as shown in the figure.



Advantages

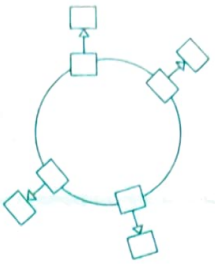
1. Ease of installation.
2. Require less cabling than mesh or star topologies.

Disadvantages

1. Difficult to add new devices.
2. A fault in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring Topology Each device has a dedicated point-to-point connection with only the two devices on either side of it.

Each device in the ring incorporates a repeater; when a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



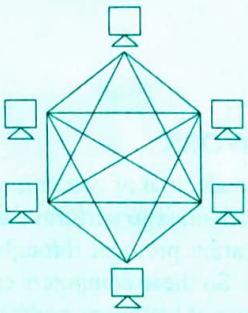
Advantages

1. Easy to install and reconfigure.
2. Fault isolation is simplified as it issues alarm which alerts the network operator to the problem and its location.

Disadvantages

1. A break in the ring can disable the entire network.
2. It is not relevant for higher-speed LANs.

Mesh topology Every station is interconnected to every other station as shown in the figure.



$n(n-1)/2$ (duplex mode) links are required for communication in both directions. Each device on the network must have $(n-1)$ I/O ports to be connected to the other $(n-1)$ stations.

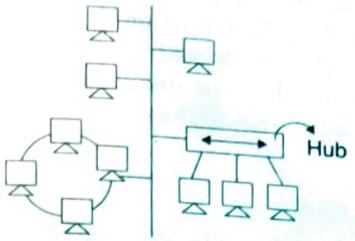
Advantages

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problems.
2. This topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is advantage of security, only the intended recipient sees the message on the dedicated line.
4. Fault identification and fault isolation is easy because of point-to-point links.

Disadvantages

1. As the hardware(cables) required for connection is more, it is expensive.
2. Installation and reconnection are difficult.
3. The sheer bulk of the wiring can be greater than the available space.

Hybrid Topology More than one topology in a network.



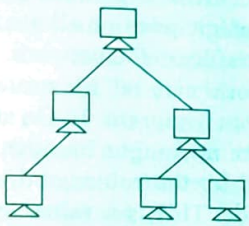
Advantages

1. Fault detection is easier.
2. We can add new stations without affecting the original architecture.

Disadvantages

1. As different topologies are combined so complexity of design increases. Very less practical implementation.
2. The hub which is used to connect different topologies is very costly. Moreover the cost of whole infrastructure is very high.

Tree Topology This topology uses the combination of star and bus topology.



Advantages

1. Expansion is easier; one can add new stations easily.
2. Errors can be easily detected.
3. Robust, if one link fails the remaining system is in communication.

Disadvantages

1. With the increase in the number of nodes, complexity and maintenance become difficult.

Examples: The most common type of local area network is an Ethernet LAN. The smallest home LAN can have exactly two computers; a large LAN can accommodate thousands of computers. Many LANs are divided into logical groups called subnets. An Internet Protocol (IP) 'Class A' LAN can in theory accommodate more than 16 million devices organized into subnets.

MAN

A metropolitan area network is a computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

WAN

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.

A WAN is complicated; it uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN. As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth.

A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LAN to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Residences typically employ one LAN and connect to the Internet WAN via an Internet Service Provider (ISP) using a broadband modem. The ISP provides a WAN IP address to the modem, and all of the computers on the home network use LAN (so-called private) IP addresses. All computers on the home LAN can communicate directly with each other but must go through a central gateway, typically a broadband router, to reach the ISP.

THE OSI REFERENCE MODEL

The concept of how a modern day network operates can be understood by dissecting it into seven layers. This seven layer model is known as the OSI Reference Model and defines how the vast majority of the digital networks on earth function. OSI is the acronym for Open Systems Interconnection. The important concept to realize about the OSI Reference Model is that it does not define a network standard, but rather provides guidelines for the creation of network standards.

Physical Layer

The first layer of a network is the Physical Layer. The Physical Layer is literally what its name implies: the physical infrastructure of a network.

This includes the cabling or other transmission medium and the network interface hardware placed inside computers

and other devices which enable them to connect to the transmission medium.

The purpose of the Physical Layer is to take binary information from higher layers, translate it into a transmission signal or frequency, transmit the information across the transmission medium, receive this information at the destination and finally translate it back into binary before passing it up to the higher layers.

Transmission signals or frequencies vary between network standards and can be as simple as pulses of electricity over copper wiring or as complex as flickers of light on optical lines or amplified radio frequency transmissions.

The information that enters and exits the Physical Layer must be bits; either 0s or 1s in binary. The higher layers are responsible for providing the Physical Layer with binary information. Since almost all information inside a computer is already digital, this is not difficult to achieve.

The Physical Layer does not examine the binary information nor does it validate it or make changes to it. The Physical Layer is simply intended to transport the binary information between higher layers located at points A and B.

Data Link Layer

The second layer in the OSI Model is the Data Link Layer, the only layer in the OSI model that specifically addresses both hardware and software.

The Data Link Layer receives information on its software side from higher layers, places this information inside 'frames', and finally gives this frame to the Physical Layer, Layer 1, for transmission as pure binary.

A frame essentially takes the information passed down from a higher layer and surrounds it with Physical Address information. This information is important for the Data Link Layer on the receiving end of the transmission.

When the frame, in binary form, arrives at the destination node, it is passed from the transmission medium to the Data Link Layer (Layer 2) by the Physical Layer (Layer 1).

The Data Link Layer on the receiving node checks the frame surrounding the information received to see if it's Physical Address matches that of its own. If the Physical Address does not match, the frame and its encapsulated data is discarded. If the Physical Address is a match, then the information is removed from the frame and passed up to the next highest layer in the OSI Model.

The Physical Addressing system allows multiple nodes to be on the same network medium, but retain the ability to address only a specific node with a transmission.

The Physical Address used in the Data Link Layer's Physical Addressing system is known as a MAC address and is embedded physically into the node's Network Interface Card during manufacturing.

Every NIC's MAC address is unique in order to prevent addressing conflicts. It is this relationship that causes the Data Link Layer to be known as the only layer that addresses both hardware and software.

In this layer the information on the network makes the move from the physical infrastructure of the network into the software realm. The remainders of the OSI reference model's layers are entirely software.

Network Layer

OSI Layer 3 is known as the Network Layer. The purpose of the Network Layer is to direct network traffic to a destination node who's Physical Address is not known. This is achieved through a system known as Logical Addressing.

Logical Addresses are software addresses assigned to a node at Layer 3 of the OSI Model. Since these addresses are able to be defined by software rather than being random and permanent like Physical Addresses, Logical Addresses are able to be hierarchical. This allows extremely large networks to be possible.

A smart device working at Layer 3 that handles network signals from each node directly rather than nodes just blindly repeating packets at Layer 1 until they happen to reach their destination. Such a device is known as a network router.

A network router sits in the center of a network with all nodes having a direct link to it rather than being linked to each other. This strategic position allows the router to intercept and direct all traffic on the network.

A routed network can be illustrated by a star formation, as shown in Diagram 1. On a routed network, Layer 3 packets are no longer broadcasted to all nodes, but rather received by the router and passed on only to the appropriate node. This is a valuable concept because it allows for the collision free-transport of packets across a network.

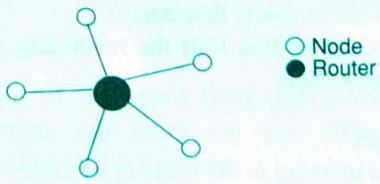


Figure 1

As being linked directly to all nodes in a local network, a router can be linked directly to other routers. This allows groups of nodes separated by distance to communicate with each other in a practical way.

It would not be practical to have nodes separated by a great distance all connected to a single router. The amount of cabling required would be immense and depending on the number of nodes involved, the router may not posses the required number of physical connections.

Routers can be chained in a line, or as shown in Diagram 2, can be connected by a central router. This concept is virtually infinitely scalable and is very efficient.

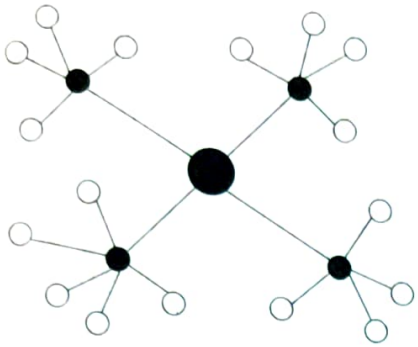


Figure 2

When a node starts a transmission, the OSI Layer 3 protocol takes the information passed down from higher layers and encapsulates it with the logical address of the destination node in a unit called a packet.

This packet, then passes through the remaining lower layer protocols, is transmitted over the network medium from the node to the router. This router reads the logical address that the packet contains and compares it to a list of physical addresses of nodes that are directly connected to it.

If the packet's destination address matches an entry in this list, the packet is transmitted directly on the line that leads straight to the destination node.

If the router does not know of a direct connection to the destination node, the packet is transmitted on a line leading directly to another router. This router then treats the packet much like the first router did upon receipt.

The packet's logical address is checked for matches against the list of logical addresses belonging to nodes directly connected to the router.

If the packet reaches a router with connections only to other routers, as shown in Diagram 2, the router uses the logical address's orderly numbering scheme to try and determine the closest router to the destination node and then transmits the packet to that router.

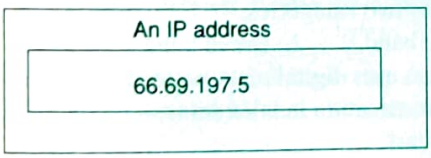


Figure 3

In IP, logical addresses look like four sets. Diagram 3 shows an example of an IP address. IP addresses are orderly on four levels, from left to right. The first section of the IP address refers to a top level router, or a router that is at the highest level of this particular branch of the network. In Diagram 3, the first number is 66. Therefore all IP addresses between 66.0.0.1 and 66.255.255.255 are managed by this router. Only one router is required in a routed network, but more may exist. A router may have a maximum of 255 nodes, which may be either ordinary nodes or other routers. This effectively means that each branch of a network, a group of nodes that have the first set of numbers in their IP address in common, could theoretically have over sixteen million end nodes.

Transport Layer

OSI Layer 4 is known as the Transport Layer, all information transferred is assumed to be at the correct destination node and is being passed up to Layer 4.

The Transport Layer is responsible for the reliability of the link between two end users and for dividing the data that is being transmitted by assigning port numbers to its Layer 4 packages, known as segments.

Ports can be thought of as virtual destination mailboxes or outlets. When information reaches a Layer 4 protocol, the segment is examined to determine the destination port of the data it contains. Once the port is determined, just as all of the past layers have done, the wrapper is discarded and the payload data passed up to the next layer's protocol.

Higher layer protocols that provide services such as email, web browsing, text chat, file transfer and more, each operate on their own unique Layer 4 port, allowing all of these protocols to be operated at once without interference.

On the reliability front, Transport Layer protocols are be capable of running a checksum on the payload data, which they carry. This allows the protocol to determine the integrity of incoming payload data. If this data has been corrupted, the Layer 4 protocol will request the segment to be retransmitted.

Session Layer

OSI Layer 5, known as the Session Layer, still serves a purpose in the OSI Reference Model. The Session Layer draws the outline for protocols that manage the combination and synchronization of data from two separate higher layers.

Layer 5 protocols are responsible for ensuring that the data is Synchronized and consistent before transmitted. A good example is the streaming of live multimedia audio and video, where perfect synchronization between video and audio is desired.

Presentation and Application Layers

The sixth and seventh layers in the OSI Reference Model are the Presentation Layer and the Application Layer. The primary purpose of these layers is to facilitate the movement of formatted information between applications interacting with end users on nodes.

Commonly used top layer protocols are HTTP (for the secure transfer of web page related files), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP, used for sending email messages), and SSH (Secure Shell), used to secure remote shell access for a computer operating system.

OSI reference model concept

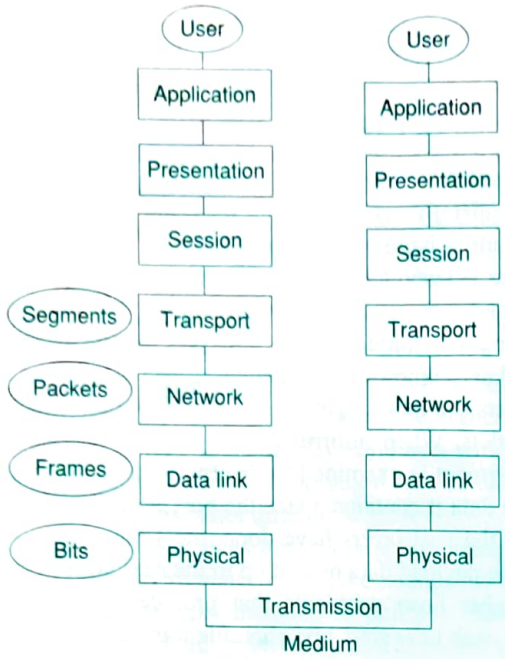


Figure 4

The OSI Reference Model exists not to make hard rules or to shape the industry, but to provide a logical, well-researched, and tested model after which the world's best communication protocol stacks are modeled. The TCP/IP stack is very well-known for being the driving force behind most of the internet, and represents the third (IP) and fourth (TCP) layers of the OSI Model. Every layer in the OSI Model is a reference for a protocol which must facilitate communication between both higher and lower layers. The 'U-shaped' example shown in Diagram 4 provides a visual concept of how two users may be linked on a given network in reference to the OSI Model. Data starts and ends with the user. From the Application Layer of the first user, it must travel down through layers 7 to 1, across the transmission medium, then back up to layers 1 to 7 to be presented at the Application Layer to the user on the end of the transmission. Diagram 4, shows an example of a path between two nodes. Protocols defined by this reference are dependent on the next lowest layer protocol. So, for example, one could not run an Application Layer protocol on a node without the presence of Layer 1 through 6, protocols also being utilized on the node.

LAN TECHNOLOGIES

IEEE standard for networking

IEEE standard project 802 is designed for the enter – connectivity between LAN's

IEEE 802 maps to physical and data link layer

Example: Ethernet, Token ring etc, the IEEE standards for the different groups are

802.1 – Higher layer LAN Protocol
802.3 – Ethernet
802.11 – Wireless LAN
802.15 – WPAN
802.16 – Broad band wireless Access
802.17 – Resilient packet Ring
802.18 – Radio Regulatory TAG
802.19 – Co existence TAG
802.20 – Mobile Broad band wireless access
802.21 – Media independent Hand off

} Active working grourp

802.2 – Logical link control working group
802.4 – Token Bus
802.5 – Token Ring
802.7 – Broad band area Network
802.8 – Fiber optic TAG
802.9 – Integrated service LAN
802.10 – Security working group
802.12 – Demand priority working group
802.14 – Cable modern working group

} In active or dis-banded working groups

Ethernet

We have

10 Mbps – Ethernet
100 Mbps – Fast ethernet
1 Gbps – Gigabit Ethernet
10 GE – 10 Gigabit Ethernet

Best suited for LAN because it is capable of handling high speed bandwidth.

- Ethernet medium:
  Thick wire – 10B5
  Thin wire – 10B2
  Twisted pair – 10BT, 100BT, 1000BT
  Fibre – 10BF, 100BF, 1000BF
  CAT 4 – 10 Mbps
  CAT 5 – 10/100 Mbps
  CAT 6 – 10/100/1000 Mbps
- Fundamental is CSMA/CD, Standard is 802.3.
- It defines two categories:
  1. Base band. 2. Broad band
- Baseband uses digital manchester encoding techniques.
- IP communication in ethernet is of 3 types:
  (i) Unicast
  (ii) multi cast
  (iii) broadcast
- When user sends data he puts destination and source address.
  (i) In unicast, only intended users responds, however all can get the signal (individual MAC).
  (ii) In multicast, group of users will get the data (group MAC).
  (iii) In broadcast, all users on Ethernet can see the data (all MAC).
- Every computer accepts 3 types of packets, to his own, to the group it belongs, to all.

CSMA/CD

CSMA (Carrier Sense Multiple Access)

CSMA protocols performance is better than ALOHA—Monitor the channel before and/or during data transmission.

1-Persistent Check whether the channel is free before transmitting the data. If busy, wait until it becomes free and then immediately start Re-transmitting.

Non-Persistent When the channel is busy, wait for a random period of time before trying again

If the waiting time is too long, the channel utilization decreases.

P-Persistent Used in slotted systems, If the channel is idle during the current slot, transmit with probability P, and defer until next slot with probability $(1 - P)$

Two or more computers can get connected on same physical medium. All computers can communicate whenever they feel like. Any computer want to communicate, it senses the medium, if medium is free and not used by anyone it captures the medium and puts its data on to the channel.

All computers listens to the sent data but only intended computer/system will respond. At this instance, sending computer is owner of the medium; no other system can be owner or can send the data. When two or more computers try to send data at same time by sensing the medium, collision occurs, which will be sensed by all the computers, then they keep integral wait unit of time for next transmission of data. Once the sending machine gets the corrupted collision message it retransmits using integral time.

MAC sublayer

The medium Access control (MAC) sub layer is the bottom half of the Data link layer. The upper half is commonly called logical link control (LLC) sublayer.

Frame format

Preamble	SFD	Destination address	Source address	Length or type	Data and padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1500 bytes	4 bytes

Preamble The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enables it to synchronize its input timing.

Start frame delimiter (SFD) The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that, this is the last chance for synchronization. The last 2-bits is 11 and alerts the receiver that the next field is the destination address.

Destination address (DA) The DA field is 6 bytes and contains the physical address of the destination station to receive the packet.

Source address (SA) The SA field is also 6 bytes and contains the physical address of the sender of the packet.

Length field The original ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard uses it as the length field to define the number of bytes in the data field.

Data This field contains data encapsulated from the upper layer protocols. It is of minimum 46 bytes and a maximum of 1500 bytes.

Ethernet follows **binary exponential back off** algorithm to give waiting time for stations, which are involved in collisions. After collisions, waiting time for the stations will be K * 51.2 μ sec, where K is randomly picked up from 0 to $2^n - 1$, 'n' is the collision number. But after 10 collisions, the randomization internal is frozen at a maximum of 1023 slots.

If each station transmits during a contention slot with probability p, the probability A that some station acquires the channel in that slot is

$$A = Kp\,(1-p)^{k-1}$$

A is maximized when $p = 1/k$, with $A \to 1/e$ as $K \to \infty$

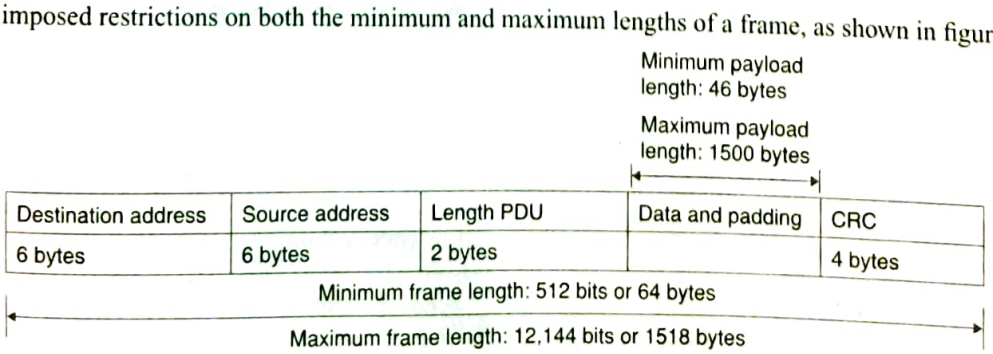
The probability that the contention internal has exactly j slots in it is $A(1-A)^{j-1}$, hence mean number of slots per contention is given by

$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}$$

CRC The last field contains error detection information.

Frame length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in figure below:.



Minimum length of frame is 512 bytes or 64 bytes. If we count 18 bytes of header and trailer, then minimum length of data from the upper layer is 64 – 18 = 46 bytes.

If the upper layer packet is less than 46, padding is added to make up the difference and used to find out collision. Maximum length of the frame is 1518 bytes. If we substract 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

- The maximum length restriction has two reasons.
- First, memory was very expensive when ethernet was designed, a maximum length restriction helped to reduce the size of the buffer.
- Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Since each slot has a duration $2T$, the mean contention internal, w, is $2T/A$. Assuming optional p, the mean number of contention slots is never more than e, so w is atmost $2Te = 5.4$ T.

$$\text{Channel efficiency} = \frac{p}{p + 2T/A}$$

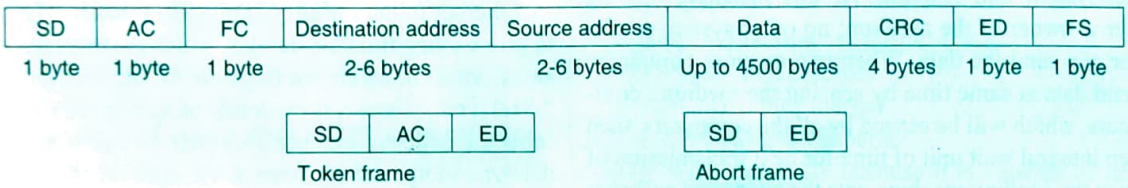
$$= \frac{1}{1 + 2B\dfrac{Le}{cF}}$$

Where F = Frame length
B = Network bandwidth
L = Cable length
C = Speed of signal propagation
E = Contention slots per frame

802.5 TOKEN Ring

Here ring topology is used and devices are physically arranged to form a ring. A token is passed among stations. If a station wants to send data, it must wait and capture the token. Only the token holders are permitted to transmit frame. Token ring allows each station to send one frame per turn.

Frame formats



802.5 Token ring uses differential Manchester digital signal encoding. It supports data rates upto 16 mbps. Tokens ring protocol specifies three types of frames: Data, token, and abort.

The token and abort frames are both truncated data frames.

Data frame

Start delimiter (SD) It is one byte long and is used to alert the receiving station for the arrival of a frame as well as to synchronize it's timing.

Access control (AC) It is one byte long and includes subfields. It has the format PPPTMRRR. First 3-bits are priority field. T denotes whether this is a data frame, token or an abort frame. Token bit is followed by monitor bit. The last 3 bits are the reservation field that can be set by stations wishing to resume access to ring.

Frame control This field is one byte long and contains two fields. The first is a one bit field used to indicate the type of information (whether it is a control information or data). The second uses the remaining seven bits of the byte and contains information used by the token ring logic.

Destination address (DA) The six byte DA field contains the physical address of the frame's next destination.

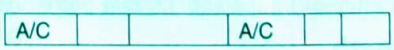
Source address (SA) The six byte SA field contains the physical address of the sending station.

Data contains LLC data unit Data contains 0 or more bytes, maximum size of the data depends upon taken holding time.

CRC The CRC field is 4 byte long and contains a CRC – 32 bit error detection sequence.

End delimiter (ED) ED is a second flag field of one byte and indicates the end of the sender's data and control information.

Frame status It is one byte long



A: Addressed recognized bit
C: Copies bit

It can be set by the receiver to indicate that the frame has been read/copied etc.

When a frame arrives at the station with the destination address, the station turns A bits to 1. If station copies the frame to the station it also turns on the C bit. A station might fail to copy a frame due to lack of frame buffer or other reason.

When the sending station receives the frame, it examines the A and C bits.

Three combinations are possible:

1. $A = 0$, $C = 0$: destination not ready /present.
2. $A = 1$, $C = 0$: destination present byte frame not accepted.
3. $A = 1$, $C = 1$: destination present and frame copied.

Token frame

It includes only 3 fields: SD, AC and ED

1. The SD indicates, the frame is coming
2. The AC indicates that the frame is a token and includes priority and reservation fields. $T = 0$ for token in AC.
3. The ED indicates the end of the frame.

Abort frame

An abort frame contains no information at all just starting and ending delimiters. It can be generated by the sender to stop its own transmission. Each station has a priority code, as a frame passes by, a station waiting to transmit may reserve the next open token by entering its priority code in the Access control field (AC) of the token or data frame. A station with a higher priority may remove a lower priority reservation and replace it with its own. Among stations of equal priority, the process is first come, first served. Through this mechanism, the station holding the reservation gets the opportunity to transmit as soon as the token is free, whether or not it comes next physically on the ring.

Monitor station Several problems may appear to disrupt the operation of a token ring network. If the token is destroyed by noise there will be no token on the ring and no station can send data. To solve such a problem, one station on the ring is designated as a monitor. The monitor sets a time, each time the token passes. If the token does not appear in the allotted period of time, it is assumed to be lost and the monitor generates a new token and introduces it to the ring. The monitor detects the orphan frames, by setting the monitor bit in the access control byte.

As the frame passes, the monitor checks the status field. If the monitor bit is set, something is wrong since the frame has passed the monitor twice, so monitor discards it. The monitor then destroys the frame and puts a token on the ring. If monitor fails, the protocol ensures that another station is quickly selected as monitor. Every station has the capability of becoming the monitor. While the monitor is functioning properly, it alone is responsible for seeing that the ring operates correctly.

When station notices that either of its neighbors appears to be dead it transmits BEACON frame giving the address of the dead station.

Physical Layer

Physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1-bit, it is received by the other side as 1-bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

Types of Medium

Medium can be classified into two categories:

1. Guided Media: Guided media means that signals are guided by the presence of physical media i.e., signals are under control and remains in the physical wire. For example, copper wire.
2. Unguided Media: Unguided media means that there is no physical path for the signal to propagate. Unguided media has essentially electromagnetic waves. There is no control on flow of signal. For example, radio waves.

Transmission Media

In Guided transmission media, generally two kinds of materials are used.

1. Copper
   - Coaxial cable
   - Twisted pair
2. Optical Fiber

Coaxial cable

Coaxial cable consists of an inner conductor and an outer conductor which are separated by an insulator. The inner conductor is usually copper. The outer conductor is covered by a plastic jacket. It is named coaxial because the two conductors are coaxial. Typical diameter of coaxial cable lies between 0.4 inches to 1 inch.

Twisted pair

A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, the purpose of twisting is to reduce cross talk interference between several pairs. Twisted pair is much cheaper than coaxial cable but it is susceptible to noise and electromagnetic interference and attenuation is large.

Optical fiber

In optical Fiber light is used to send data. In general terms presence of light is taken as bit-1 and its absence as bit 0. Optical fiber consists of either glass or plastic core which is surrounded by cladding of the same material but of different refractive index. This cladding is surrounded by a plastic jacket which prevents optical fiber from electromagnetic interference and harshly environments. It uses the principle of total internal reflection to transfer data over optical fibers. Optical fiber is much better in bandwidth as compared to copper wire, since there is hardly any attenuation or electromagnetic interference in optical wires. Hence there is

less requirement to improve quality of signal, in long distance transmission. Disadvantage of optical fiber is that end points are fairly expensive.

Communication Links

In a network nodes are connected through links. The communication through links can be classified as

Simplex Communication can take place only in one direction.
Example: TV broadcasting.

Half duplex Communication can take place in one direction at a time. Suppose node A and B are connected then half duplex communication means that at a time data can flow from A to B or from B to A but not simultaneously.
Example: Two persons talking to each other such that when one speaks the other listens and vice versa, walkie-talkies, citizens band radios.

Full duplex Communication can take place simultaneously in both directions.
Example: telephone network.

Links can be further classified as:

Point-to-Point In this communication only two nodes are connected to each other. When a node sends a packet then it can be received only by the node on the other side and none else.

Multi-Point It is a kind of sharing communication in which signal can be received by all nodes. This is also called broadcast.

Digital Data to Digital Signals

A digital signal is sequence of discrete, discontinuous voltage pulses. Each pulse is a signal element. Encoding scheme is an important factor in knowing that how successfully the receiver interprets the incoming signal.

Encoding techniques

Following are several ways to map data bits to signal elements:

Non-return-to-zero (NRZ): NRZ codes share the property that voltage level is constant during a bit interval. High level voltage = bit 1 and low level voltage = bit 0. A problem arises when there is a long sequence of 0's and 1's and the voltage level is maintained at the same value for a long time.

This creates a problem on the receiving end because now, the clock synchronization is lost due to lack of any transitions and hence, it is difficult to determine the exact number of 0's and 1's in this sequence.

The two variations are as follows:

1. *NRZ–Level*: In NRZ–L encoding, the polarity of the signal changes only when the incoming signal changes from a '1' to a '0' or from a '0' to a '1'. NRZ – L method, looks just like the RZ method, except for the first input one data bit. This is because NRZ does not consider the first data bit to be a polarity change, where NRZ–L does.
2. *NRZ–Inverted*: Transition at the beginning of bit interval = bit 1 and no transition at the beginning of bit interval = bit 0 or vice versa. This technique is known as differential encoding.

Digital Data Communication Techniques

For two devices linked by a transmission medium to exchange data, a high degree of co-operation is required. Typically data is transmitted one bit at a time. The timing (rate, duration, spacing) of these bits be same for transmitter and receiver. There are two options for transmission of bits.

Parallel All bits of a byte are transferred simultaneously on separate parallel wires. Synchronization between multiple bits is required which becomes difficult over large distance. Parallel communication gives large bandwidth but expensive, possible only for devices which are close to each other.

Serial Bits transferred serially one after other. Serial communication gives less bandwidth but cheaper, suitable for transmission over long distances.

Manchester encoding

Manchester encoding is used in Ethernet (IEEE 802.3) it is a line code in which bit encoding has at least one transition and consumes the same time.

It ensures frequent line voltage transitions, which are directly proportional to clock rate

It is not dependent on data, so it will not carry any information.

Transmission Techniques

Asynchronous

Small blocks of bits (generally bytes) 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 two extra bits, start and stop.

Start Bit It is prefixed to each byte and equals 0. Thus it ensures a transition from 1 to 0 at onset of transmission of byte. The leading edge of start bit is used as a reference for generating clock pulses at required sampling instants. Thus each onset of a byte results in resynchronization of receiver clock.

Stop Bit To ensure that transition from 1 to 0 is always present at beginning of a byte it is necessary that default state be 1, but there may be two bytes one immediately following the other and if last bit of first byte is 0, transition from 1 to 0 will not occur. Therefore a stop bit is suffixed to each byte equaling 1. It's duration is usually 1, 1.5, 2 bits. Asynchronous transmission is simple and cheap but requires an overhead of 3 bits i.e., for 7 bit code 2(start, stop bits) + 1 parity bit implying 30% overhead. However this percentage can be reduced by sending larger blocks of data but then timing errors between receiver and sender cannot be tolerated beyond [50/number. of bits in block]%. It will not only result in incorrect sampling but also misaligned bit count. i.e., a data bit can be mistaken for stop bit if receiver's clock is faster.

Synchronous

Larger blocks of bits are successfully transmitted. Blocks of data are either treated as sequence of bits or bytes. To prevent timing, drift clocks at two ends need to be synchronized. This can be done in two ways.

1. Provide a separate clock line between receiver and transmitter. (or)
2. Clocking information is embedded in data signal i.e., Biphase coding for digital signals.

Still another level of synchronization is required so that receiver determines beginning or end of block of data. Hence each block begins with a start code and end with a stop code. These are in general same, known as flag that is unique sequence of fixed number of bits. In addition some control characters encompass data within these flags. Data and control information is called a frame. Since any arbitrary bit pattern can be transmitted, there is no assurance that bit pattern for flag will not appear inside the frame, thus destroying frame stuffing.

Channel Allocation A large class of networks is built on broadcast channels, a number of stations will share the same channel, if one station sends, all other stations have to hear it.

Problem occurs when, 2 stations want to start data transmission at the same time, in this situation 2 fames collide.

To avoid frame collision, allocate the channel to one of the stations.

There are 3-strategies for channel allocation:

1. Let a station try to use the channel, and when the collision occurs, that is taken care of later.
2. Each station in turn is allowed to use the channel. This is applied in token-based systems. Only the station that has the token can use the channel.
3. Reserve the channel in prior, It is used in slotted systems. The problem is how to make a reservation.

Data Link Layer

Data link layer provides interface to the network layer, determines the number of bits of the physical layer to be grouped into frames, detects transmission error and regulates the flow of frames.

Functions of data link layer:

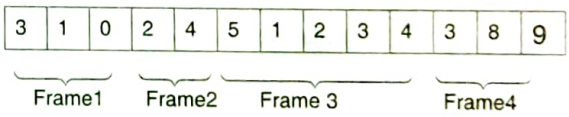
1. Framing
2. Physical addressing
3. Flow control
4. Error control
5. Access control

Various methods of Framing are

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

Time gaps Framing is done by inserting time gaps between frames, very similar to the way of spacing between words in ordinary text. It is risky to count on timing to mark the start and end of each frame.

Character count It uses a field in the header to specify the number of characters in the frame. Thus at the destination by seeing the character count it knows how many characters follows and where the end of the frame exists.



Problem If count of any frame changes, destination will get out of synchronization and is unable to locate start of next frame.

Starting and ending characters, with character stuffing Each frame starts with the ASCII character sequence DLESTX and ends with the sequence DLEETX. If destination looses track of the frame boundaries, all it has to do is to look for DLESTX or DLEETX character

Starting and ending flags, with bit stuffing

Bit Stuffing: Suppose ou r flag bits are 01111110. So the transmitter will always insert an extra 0 bit after each occurrence of five 1s (except for flags). After detecting a starting flag the receiver monitors the bit stream. If pattern of five 1's appear, the sixth bit is examined and if it is 0 it is deleted; else if it is 1 and next bit is 0 the combination is accepted as a flag. Similarly byte stuffing is used for byte oriented transmition. Here we use an escape sequence to prefix a byte similar to flag and two escape sequences if byte itself is an escape sequence.

Has arbitrary number of bits and allows character codes with an arbitrary number of bits per character. Every frame begins and ends with a special bit pattern, 01111110, called a flag byte.

As soon as the sender's data link layer encounters five consecutive one's in the data, it stuffs a 0 bit into the outgoing bit stream.

Receiver de-shifts the 0 bit of the five consecutive incoming 1 bits, followed by a 0 bit.

If the user data is 01111110, transmitted as 011111010 but stored at receiver as 01111110.

Physical layer coding violations Applied to the networks in which the encoding on the physical medium contains some redundancy.

1 → high – low pair

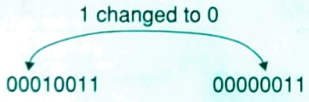
0 → low – high pair

Here high-high, low-low not used for data.

Every data bit has a transition in the middle, thus easy for the receiver to locate the bit boundaries.

Types of Errors

Single bit error The term single bit error means that only one bit in the data unit has changed, it can either be from 1 to 0 or from 0 to 1.



Single bit error correction

A single bit error occurs when a bit changes in value from 0 to 1 (or) from 1 to 0 while storing (or) while performing read (or) write operation. If that error bit is identified, that can be corrected by complementing.

Hamming codes

In hamming codes, K parity bits are added to an n-bit data word, that forms a new word of $(n + k)$ bits. The bit positions are numbered in sequence from 1 to $n + k$. These positions numbered with powers of 2 are reserved for the parity bits; the remaining bits are the data bits.

Example: Consider the given 8-bit data word 11000100, we include four party bits with this word and arrange the bits as follows.

Bit position

1	2	3	4	5	6	7	8	9	10	11	12
$P1$	$P2$	1	$P4$	1	0	0	$P8$	0	1	0	0

The parity bits are in positions, 1, 2, 4, 8. Each parity bit is calculated as

$P1$ = XOR of bits (3, 5, 7, 9, 11) = $1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$P2$ = XOR of bits (3, 6, 7, 10, 11) = 0

$P4$ = XOR of bits (5, 6, 7, 12) = 1

$P8$ = XOR of bits (9, 10, 11, 12) = 1

⇒ If there is odd number of 1s, XOR gives 0

⇒ If there is even number of 1s, XOR gives 1

The values $P1 = 0$, $P2 = 0$, $P4 = 1$, $P8 = 1$ are substituted in 12-bit composed word

Bit position

1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	1	1	0	0	1	0	1	0	0

Check for errors:

$C1$ = XOR of bits (1, 3, 5, 7, 9, 11)

$C2$ = XOR of bits (2, 3, 6, 7, 10, 11)

$C4$ = XOR of bits (4, 5, 6, 7, 12)

$C8$ = XOR of bits (8, 9, 10, 11, 12)

Since the bits were written with even parity, the result $C = C8\ C4\ C2\ C1 = 0000$

∴ Indicates that no error has occurred.

- The code can be used with words of any length.

Burst Error The term burst means that two or more bits in the data unit have changed, either changed, from 1 to 0 or changed from 0 to 1.

Sent:

010011010000-sent bits corrupted by burst error

010001111000 Received

Parity bit

Parity bit is an error detecting code. This bit is added to data words depending on number of 1's in the data word; It could be even parity and odd parity.

n-bit data word is transformed to $(n + 1)$ bit code word with the addition of a bit. Even parity makes even number of 1's in a code word, similarly odd parity makes odd number of 1's in a code word.

Let us illustrate with example

Data word – 1 0 1 1 Parity bit

Code word – 1 0 1 1 1 parity bit (even parity)

Code word: 1 0 1 1 0 (odd parity)

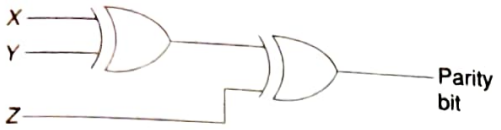
At the receiver side, when the code is received, the receiver checks the same as it is done by the generator. But here it adds all the bits which results in syndrome. If the syndrome is 0 then the number of 1's in code word is even, else number of 1's is odd.

Decision logic analyzer will decide, whether the code word is correct or not, based on syndrome value.

Parity bit generator

The parity bit generator for a 3-bit data word is given below.

The message is in the form of $X\,Y\,Z$



Parity bit generator

When the message is passed through the above circuit, the parity will be generated accordingly.

Error correction code

When data is transmitted form the source to destination, there is a chance of error introduction into the data. Error detection will detect the errors in data, while error correction will rebuild the original data,

Error correction code can be implemented in 2 ways

1. Forward error correction (FEC)
2. Automatic repeat request (ARQ)

In FEC, when sender is sending data, sender adds redundant data (encoded information) to the original data. At the receiver side this redundant data is used to recover the original data, when original data is tampered [error data].

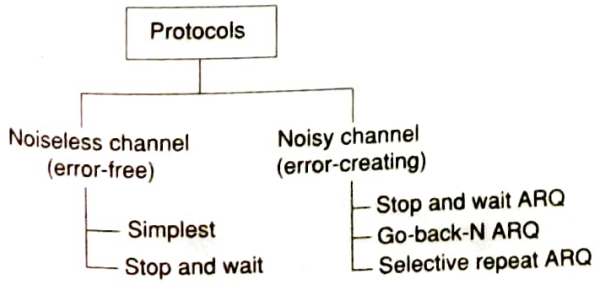
In ARQ, the receiver requests for the retransmission of the data packets, which are corrupted. Receiver will check the data using some error detection code.

Flow Control

It regulates the flow of frames so that slow receivers are not affected by the fast sender or vice versa.

It tell the sender how much data it should transmit before it waits for an acknowledgement from the receiver. Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Error control in the data link layer is often implemented simply. Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).



All the protocols we discuss as unidirectional in the sense that data frames travels from sender to receiver. Although special frames called acknowledgment (ACK) and negative acknowledgment (NAK) can flow in the opposite direction for flow and error control purposes, data flow is in only one direction. In real life network, the data link protocols are implemented as bidirectional, data flow in both directions. In these protocols flow and error control information such as ACKs and NAKs are included in the data frames in a technique called piggybacking.

Stop and wait Sender sends one frame, stops until it receives confirmation from the receiver. Error correction in stop and wait ARQ is done by keeping a copy of the sent frame and retransmitting the frame when the timer expires.

Only 2 sequence numbers 0 and 1 are used.
Window size is 1.
No ACK for lost or damaged frames.

$$\text{Throughput} = \frac{\text{One packet}}{RTT}$$

$$\text{Utilization} = \frac{L}{L + BR}$$

L = packet length
B = Bandwidth
R = RTT
If $L < BR$, Efficiency > 50
$L > BR$, Efficiency = 50

$$\mu = \frac{1}{1+2a},\ a = \frac{\text{propagation time}}{\text{Transmission time}}$$

Link utilization is low in stop and wait.

GBN protocol We can send several frames before receiving acknowledgements; we keep a copy of these frames with the acknowledgment.

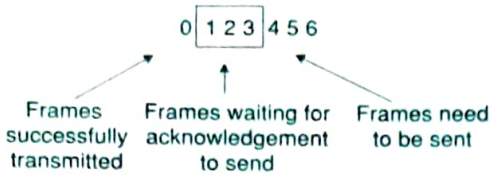
- Sequence numbers ranges from $2^m - 1$.
- m – number of bits for sequence numbers.
- The sender window slides one or more slots when a valid acknowledgment arrives.
- It uses cumulative acknowledgement or piggy backing wherever possible to acknowledge the frames.
- It discards duplicate and out of order packets.
- Receiving window size is 1.
- If the sender receives a NAK, it resends all frames in the sender window.

If a single packet is lost, damaged or acknowledgement is lost, it will resend all the packets.

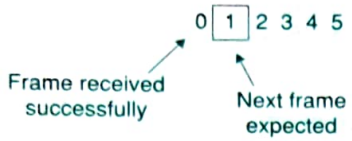
$$\text{Link efficiency} = \frac{1-p}{1-p+p^w}$$

Where, p is the packet loss probability
w is the sender's window size.

Sender:



Receiver:



- If N is maximum sequence number, then sender window size = N, Receiver window size = 1.
- If N is the number of sequence number, sender window size = $N-1$, Receiver window size = 1.

Selective repeat More efficient for noisy links but processing at the receiver is more complex. Receiver window size is same as of sender window size. Sender window maximum size is 2^{m-1}, receiver window maximum size is 2^{m-1}. Sender and receiver window must be at most one half of 2^m.

Receives out of order packets because receiver's window size is greater than 1.

It uses cumulative or independent or piggyback ACK whenever possible. If sender receives a NAK, it resends just the frame specified by the NAK.

If N is maximum sequence number,

$$\text{Sender window size} = \frac{N+1}{2},$$

$$\text{Receiver window size} = \frac{N+1}{2}$$

If N is the number of sequence numbers, sender window size $= \frac{N}{2}$, Receiver window size $= \frac{N}{2}$.

Medium Access Control Sublayer

Multiplexing

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

Frequency Division Multiplexing (FDM)

This is possible in the case where transmission media has a bandwidth higher than the required bandwidth of signals to be transmitted. A number of signals can be transmitted at the same time. Each source is allotted a frequency range in which it can transfer it's signals, and a suitable frequency gap is given between two adjacent signals to avoid overlapping. This type of multiplexing is commonly seen in the cable TV networks.

Time Division Multiplexing (TDM)

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

Synchronous TDM Time slots are pre. Assigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle or several turns per cycle, if it has a high data transfer rate, or may be once in a number 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.

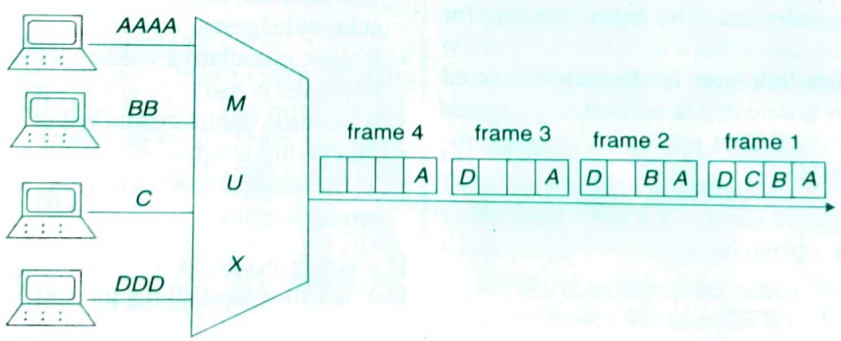


Figure 5 Synchronous TDM: Multiplexing process

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.

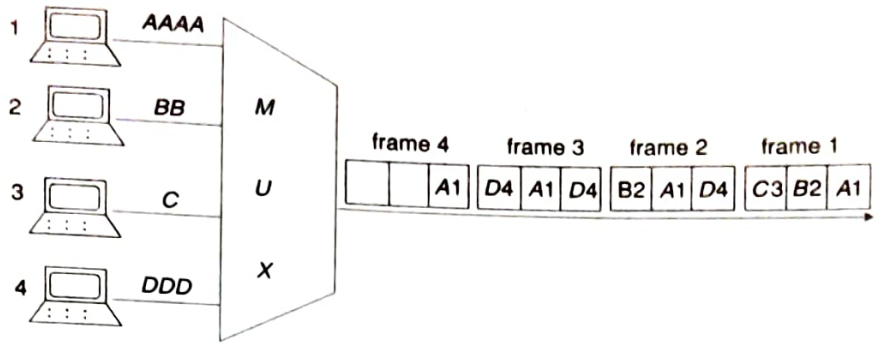


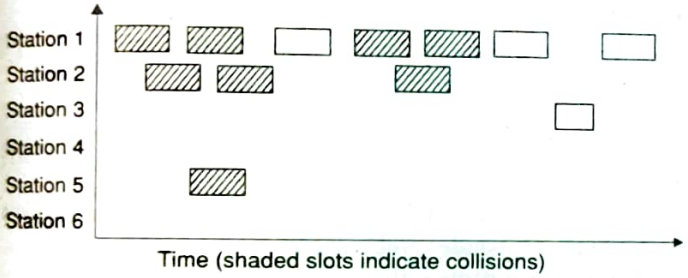
Figure 6 Asynchronous TDM

Aloha Protocols

The Aloha Protocol was designed to provide data transmission between computers on several islands using radio transmission.

Pure aloha

Pure Aloha is an unslotted, fully decentralized protocol. It is extremely simple and trivial to implement. The ground rule is 'when you want to talk, just talk!' So, a node which wants to transmit, will go ahead and sends the packet on its broadcast channel, with no consideration of who so ever to any body else is transmitting (or) (not).

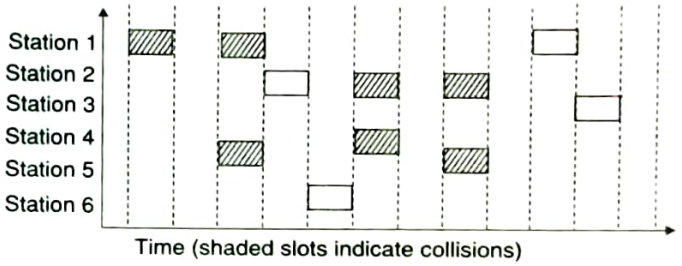


One serious drawback here is that, you don't know whether what you are sending, has been received properly or not. To resolve this in pure Aloha, when one node finishes speaking it expects an acknowledgement in a finite amount of time otherwise it simply retransmits the data. This scheme works well in small networks where the load is not high. But in large, load intensive networks where many nodes may want to transmit at the same time, this scheme fails miserably. This led to the development of slotted Aloha.

Slotted Aloha

This is quite similar to pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at the demand time, the sender waits for some time. This delay is specified as follows–the timeline is divided into equal slots and then it is required that transmission should take place only at slot boundaries. To be more precise, the slotted Aloha makes the following assumptions.

- All frames consist of exactly L bits.
- Time is divided into slots of size L/K seconds. (i.e., a slot equals the time to transmit one frame)
- Nodes start to transmit frames only at the beginning of slots.
- The nodes are synchronized so that each node knows when the slots begin.
- If two or more frames collide in a slot, then all the nodes detect the collision event before slot ends.



In this, way the number of collisions that can possibly take place is reduced by a huge margin. And hence, the performance became much better compared to pure Aloha. Collisions may only take place with nodes that are ready to speak at the same time.

Virtual private network

Virtual Private Networking (VPN) Internet protocol security (IP sec) is one of the most complete, secure, standards-based protocol developed for transporting data.

A VPN is a shared network, where private data can be accessed only by the intended recipient.

The term VPN is used to describe a secure connection over the Internet.

VPN is also used to describe private networks such as Frame Relay and Asynchronous Transfer Mode (ATM).

The purpose of data security is that the data flowing across the network is protected by encryption technologies.

IP sec-based VPNs use encryption to provide data security, that increases the networks resistance to data tampering.

IP sec-based VPNs can be created over any type of IP Network, including Internet, ATM, Frame Relay, among all only Internet is inexpensive.

Uses of VPN

Intranets Intranets connect an organization's locations. These locations could be head quarters offices, branch offices, Employees home which is located in some Remote area.

This connectivity is used for e-mails, sharing files etc.

The cost of connecting remote home users is very expensive compared to Internet access technologies because of this organizations have moved their networks to the Internet.

Remote access It enables telecommuters and mobile workers to access e-mail and business applications.

A dial-up connection to an organizations modem pool is one method to access remote workers. It is expensive, because of long distance telephone and service costs.

IP sec

IP sec is an Internet Engineering Task Force (IETF) standard suite of protocols that provide data authentication, integrity, and confidentiality between 2 communication points across IP-Network.

It provides data security at the IP-packet level.

IP sec protects against possible security exposures by protecting data while in transit.

Features

IP sec was designed to provide the following security features when transferring packets across networks.

1. Authentication: Verifies that the packet received is actually from the correct sender or not.
2. Integrity: Ensures that the contents of packet did not change while transmitting data.
3. Confidentiality: Conceals the message content through encryption.

Components of IP sec

ESP: (Encapsulating security payload), It provides confidentiality, authentication and integrity.

AH: (Authentication Header) provides Authentication and Integrity.

IKE: (Internet key Exchange) provides key management and security Association (SA) management.

ESP:

- Most importantly, it provides message content protection.
- IP sec provides an open frame work for implementing standard algorithms such as SHA and MD5.
- The algorithms IP sec uses produces a unique identifier for each packet, which is a data equivalent to a finger print.
- This Finger Print allows the device to determine whether a packet has been tampered with.
- Packets that are not authenticated are discarded and not delivered to the intended receiver
- ESP also provides all encryption services in IP sec.
- Encryption/decryption allows only the sender and the authorized receiver to read the data.
- The authentication performed by ESP is called ESP authentication.
- ESP provides authentication and integrity for the payload and not for the IP-header

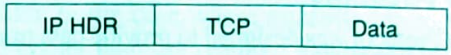
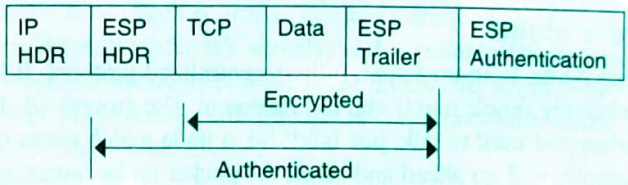


Figure 7 Original packet



The ESP Header is inserted into the packet between the IP-header and any subsequent packet contents.

- ESP encrypts the data, the payload is changed.
- ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

AH:

Provides optional anti-replay protection, which protects against unauthorized retransmission of packets.

The authentication header is inserted into the packet between the IP-header and any sub sequent packet contents.

AH does not protect the data's confidentiality.

For added protection in certain cases, AH and ESP can be used together.

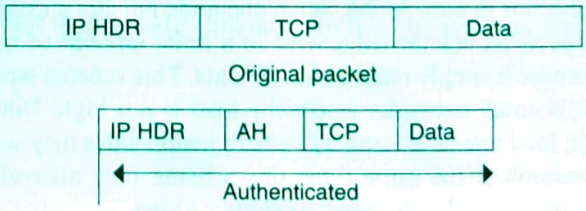


Figure 8 Packet with IP sec Authentication Header.