UNIT I

NETWORK ARCHITECTURE, PERFORMANCE :

Bandwidth and Latency, High Speed Networks, Network-Centric View, Error Detection, Reliable Transmission, Ethernet and Multiple Access Networks, Overlay Networks: Routing Overlays, Peer-to-Peer Networks and Content Distribution Networks, Client-Server Networks, Delay-Tolerant Networks

1.1 Network Architecture

Q1. Write about different types of computer network architectures. **(Imp.)**

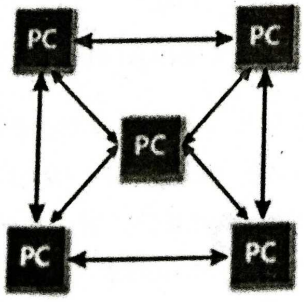
Ans :

Meaning

The design and setup of a computer network is called Computer Network Architecture. It is the organization and arrangement of different network devices (i.e., the clients such as PCs, desktops, laptops, mobiles etc.) at both physical and logical levels in order to fulfil the needs of the end user/ customer.

1. Peer-to-Peer Network

- The peers referred to here are the individual devices linked together directly, having equal responsibilities and equal powers without the presence of any central authority.
- Due to the absence of a central device in charge of tasks, this architecture is also known as decentralized architecture.



- Each computer has special rights for resource sharing, however this might cause issues if the computer with the resource is unavailable.
- Useful in smaller environments with less number of computers.

Advantages

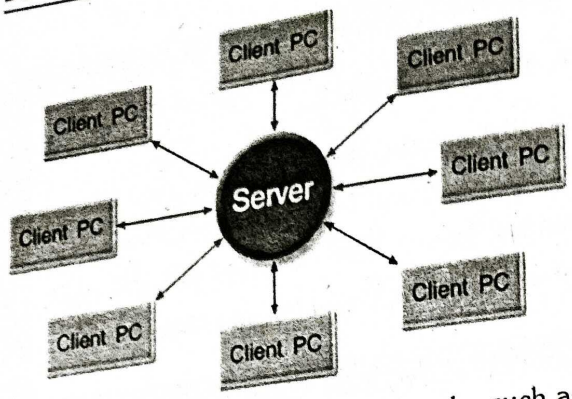
- No particular device is a client or a server, the tasks and responsibilities of servers are distributed among all the devices, which also act as clients.
- Very inexpensive to set up, as there is no requirement of a centralized server, and this also ensures that in case of any failure in the network, all unaffected devices continue to operate normally.
- It's simple to set up and maintain because each computer runs independently.

Disadvantages

- No centralized system, thus difficult to keep a backup of the data in case of any fault.
- It has a security flaw because the computers are self-managed.
- With a growth in the number of machines on this network, performance, security, and access may all become big issues.

2. Client-Server Architecture

- This is also known as centralized architecture, as one powerful central computer is in charge of serving all the requests from the client computers. This central computer is a server.
- The client computers connect to the server as and when they require the use of shared resources or shared data. All of the shared data is stored solely in the server, and not on any other computer.



- A server handles all of the key tasks, such as security and network administration.
- All of the clients interact with one another via a server.

Advantages

- This type of architecture is much easier to scale since it is much more convenient to add more server computers than configure the network on each and every computer (as is the case in peer-to-peer architecture).
- Much faster network speeds.
- Because a single server manages the shared resources in a Client/Server network, there is improvement in security.
- Backing up data is easy because of the centralized system.
- The server provides a customised Network Operating System (NOS) to offer resources to a large number of users that want them.

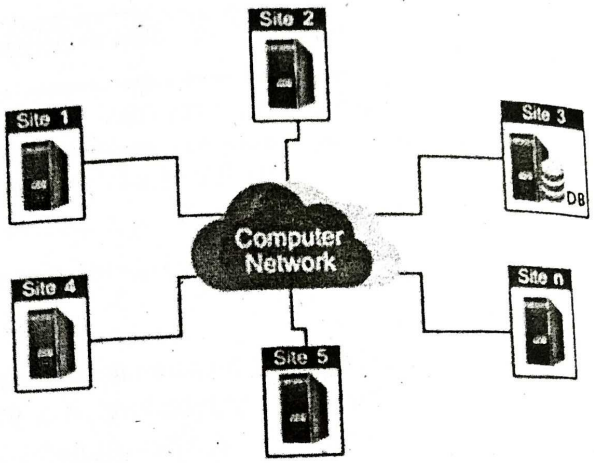
Disadvantages

- More prone to downtime because if the server fails, none of the client machines are able to get their requests served.
- Requirement of a dedicated network administrator to handle all of the resources.
- It is far more expensive than P2P. This is due to the requirement for a server with more RAM, as well as the necessity for several networking devices such as hubs, routers, switches, and so on.

There are some more lesser-known computer architectures:

3. Centralized Computing Architecture

One powerful computer is utilized to service one or more low-powered computers in centralized computing architecture. The nodes under the centralized architecture are not linked; they are only connected to the server.

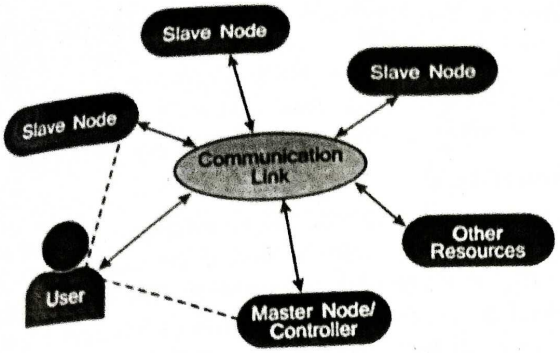


The centralized computing architecture includes the following components:

- The primary, mainframe computer which handles all processing.
- Terminals are connected to a central computer and function as input/output devices.
- Linking of at least two mainframe computers together via networks. Terminals communicate solely with the mainframe and never with one another.

4. Distributed Computing Architecture

A distributed architecture connects one or more nodes, which are personal computers. It supports a variety of functions, including file sharing, hardware sharing, and network sharing. The nodes in the distributed architecture can manage their own data and rely on the network for administration rather than data processing.

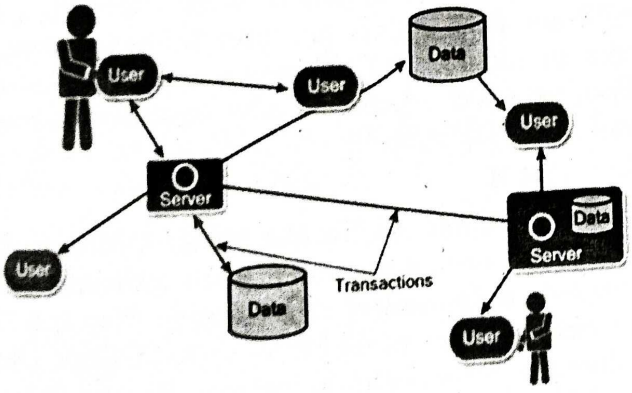


The following components are found in distributed computing architecture:

- Different computers are effective at performing independently.
- Completion of tasks on multiple computers locally.
- Networks enable computers to exchange data and services, but they do not offer processing help.

5. Collaborative Computing Architecture

The collaborative computing architecture is a hybrid of centralised and decentralised computing. Individual members of a network can process their users fundamental needs under the collaborative model.



A database server, such as an MSSQL server or an ORACLE server, for example, observes or manages all database-related operations on all network nodes. The model will, however, execute requests that are not from the database.

1.2 Performance

1.2.1 Bandwidth and Latency

Q2. Explain about bandwidth and Latency.

Ans :

Bandwidth

Bandwidth, or precisely network bandwidth, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time. That simply means that higher is the bandwidth of a network, larger is the amount of data network can be sending to and from across its path. Be careful not to confuse bandwidth with closely related terms such as the data rate and the throughput. Bandwidth is something that deals with the measurement of capacity and not the speed of data transfer.

Units of Measurement

Bandwidth is usually measured in bits transferred per second through a path or link. The common units of bandwidth we come across are as follows.

bps (Bits per second)

Mbps (Megabits per second)

Gbps (Gigabits per second)

Example :

Here, a bandwidth of 10 bps for a channel, is just another way of saying that a maximum of 10 bits can be transferred using that link for any given time. It has no relation with the transfer speed of the channel.

Latency

- Being simple latency means whenever you have given input to the system and the total time period it takes to give output so that particular time period/interval is known as latency.
- Actually, latency is the in-between handling time of computers, as some of you may think that whenever some system connects with another system it happens directly but no it isn't, the signal or data follows the proper traceroute for reaching its final destination.

- Nowadays fiber optic cables are used for transmitting the signals/data from one place to another with the speed of light but obviously before reaching to the final destiny the data/signal has to pass from many checkpoints or posts and follow a proper traceroute so it takes some time to get respond from the receiver and that total round of time is known as latency.
- If you want to know the fastest possible network connection you could have from one place to another then we will suppose light as a medium because light just takes 100milli seconds(approx.) to take a round of earth. So according to the data if you let light as a medium then you can send 20 packets per second across the other sides of the world.

1.2.2 High Speed Networks

Q3. Explain about High Speed Networks.

Ans :

1. Switched Ethernet

Switched Ethernet relies on centralized multiport switches to provide a physical link between multiple LAN segments. Inside each intelligent switch, high-speed circuitry supports wire-speed virtual connections between all the segments for maximum bandwidth allocation on demand. Adding new segments to a switch increases the aggregate network speed while reducing overall congestion, so Switched Ethernet provides superior configuration flexibility. It also gives you an excellent migration path from 10- to 100-Mbps Ethernet because both segments can often operate via the same switch.

Benefits

It's a cost-effective technique for increasing the overall network throughput and reducing congestion on a 10-Mbps network. Other than the addition of the switching hub, the Ethernet network remains the same the same network interface cards, the same client software, the same LAN cabling.

100BASE-T (IEEE 802.3u)

100BASE-T retains the familiar CSMA/CD media access technique used in 10-Mbps Ethernet networks. It also supports a broad range of cabling options: two standards for twisted pair, one for fiber. 100BASE-TX supports 2-pair Category 5 UTP or Type 1 STP cable. 100BASE-T4 uses 4-pair Category 3 or 4 cable. And 100BASE-FX supports fiber optic links via duplex multimode fiber cable.

Benefits

It retains CSMA/CD, so existing network management systems don't need to be rewritten. It can easily be integrated into existing 10-Mbps Ethernet LANs, so your previous investment is saved. It's also backed by hundreds of manufacturers in the high-speed networking industry.

100VG (IEEE 802.12)

100VG uses an encoding scheme called Quartet Signaling to transmit data simultaneously over all four pairs in the network cable, so it achieves a full tenfold increase in transmission speeds over 10BASE-T. It also replaces the CSMA/CD media access control protocol with Demand Priority to optimize network operation and eliminate the overhead of packet collisions and recovery. Demand Priority works like this: The hub directs all transmissions, acknowledging higher-priority packet requests before normal-priority requests. This effectively guarantees bandwidth to time-sensitive applications like voice, video, and multimedia applications.

Benefits

It uses a transmission frequency very similar to traditional Ethernet, works on any conventional cabling system (Category 3, 4, or 5 UTP, Type 1 STP, and fiber optics), and uses the same connectors. In addition, 100VG may soon support Token Ring networks a potential advantage over its rival standard 100BASE-T.

2. ATM

Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication technique that supports data-transfer rates ranging from sub-T1 speeds (less than 1.544 Mbps) up to 10 Gbps. Like other packet-switching services (Frame Relay, SMDS), ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. Instead, it relies on the inherent integrity of digital lines to ensure data integrity.

Benefits

Networks are extremely versatile. An ATM

network can be treated as a single network, whether it connects points in a building or across the country. Its fixed-length cell-relay operation, the signaling technology of the future, offers more predictable performance than variable-length frames. And it can be integrated into an existing network as needed without having to upgrade the entire LAN.

3. FDDI

FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the token ring protocol.

In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network(WAN).

An FDDI network contains two token rings, one for possible backup in case the essential ring falls flat.

The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps

Characteristics

- FDDI gives 100 Mbps of information throughput.
- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

Advantages of FDDI

- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

Disadvantages

- FDDI is complex. Thus establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically since fiber optic cable, connectors and concentrators are exceptionally costly.

4. Frame Relay

Frame Relay (frame relay) is a packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection.

It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends. It makes it more efficient than X.25, and a higher process speed achieved (it can transmit over 2,044 Mbps).

If the traffic is hefty, with a large number of small packages, its performance is more excellent than X25.

If large files transferred at high speeds, the price/performance ratio is higher in X25.

Frame relay has evolved from X.25 packet switching and objective is to reduce network delays, protocol overheads and equipment cost. Error correction is done on an end-to-end basis

rather than a link -to-link basis as in X.25 switching. Frame relay can support multiple users over the same line and can establish a permanent virtual circuit or a switched virtual circuit.

Frame relay is considered to be a protocol, which must be carried over a physical link. While useful for connection of LANs, the combination of low throughput, delay variation and frame discard when the link is congested will limit its usefulness to multimedia.

- Packet switching was developed when the long distance digital communication showed a large error rate.
- To reduce the error rate, additional coding bits were introduced in each packet in order to introduce redundancy to detect and recover errors.
- But in the modem high speed telecommunication a system, this overhead is unnecessary and infect counter productive.
- Frame relay was developed for taking the advantage of the high data rates and low error rates in the modem communication system.
- The original packet switching networks were designed with a data rate at the user end of about 64 kbps.
- But the frame relay networks are designed to operate efficiently at the user's data rates upto 2 Mbps.
- This is possible practically because most of the overhead (additional bits) are striped off.
- Frame relay is a virtual circuit wide area network which was designed in early 1990s.
- Frame relay also is meant for more efficient transmission scheme than the X.25 protocol.
- Frame Relay is used mostly to route Local Area Network protocols such as IPX or TCP/IP.

Characteristics

1. Frame Relay service is a service that supports the transport of data
2. Frame relay is a connectionless service, meaning that each data packet passing through the network contains -address information
3. Frame relay is a service that is provided with a variety of speeds from 56 Kbs up to 25 Mbs.
4. Even though the most used speeds for the service are currently 56 Kbs and 1.544 Mbs
5. Frames are variable in length and goes up to 4,096 bytes
6. Frame Relay is considered to be a Broadband ISDN service
7. One of the unique facets of frame relay service is that the service supports variable size data packets.

Features

Some important features of frame relay are :

1. Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).
2. Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
3. It allows the bursty data.
4. It has a large frame size of 9000 bytes. So it can accommodate all local area network frame sizes.
5. Frame relay can only detect errors (at the data link layer). But there is no flow control or error control.
6. The damaged frame is simply dropped. There is no retransmission. This is to increase the speed. So frame relay needs a reliable medium and protocols having flow and error control.

5. SONET

The synchronous optical network or SONET is a standardized form of protocol that is used in digital communication between the sender and the receiver. SONET protocol uses fiber optic medium (optical fibers) to transmit a huge amount of data across a large distance. One of the main advantages that a synchronous optical network provides is that it can be used to transfer multiple streams of

data simultaneously (at the same time) using optical fibers.

Some of the important points related to SONET are:

- SONET is used in the physical layer of the OSI model for broadband synchronized transmission of data such as voice, video, etc.
- It was developed by Bellcore in the mid-1980s and it was developed for the public telephone network.
- It is used in the North American region.
- SONET is standardized by the American National Standards Institute (ANSI).
- SONET is efficient and costs low for a few channels because of higher transmission rates.
- SONET is somewhat similar to the SDH which is used in the regions like Japan and Europe.
- At the higher capabilities, there is a problem with bandwidth efficiency.
- There is more overhead related to the SONET protocol as it is complex to implement and we have to work with multiple channels.
- There is no standard compatible with the SONET protocol.
- Tributary services are used for transporting and switching payloads and for the tributary services, the mux services of SONET are necessary.

Advantages

- Transmits data to large distances
- Low electromagnetic interference
- High data rates
- Large Bandwidth

Disadvantages

- No standard that is compatible.
- SONET mux services are necessary for tributary services.
- Low cost and efficient for few channels.
- The SONET/SDH network management system is inadequate for managing and using the DWDM technique.
- At higher capacities, bandwidth efficiency is a problem.
- There must be more overhead.

1.2.3 Network-Centric View

Q4. What is Net-Centric Computing? Explain about its areas.

Ans : **(Imp.)**

Meaning

Net-Centric Computing (NCC) is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network. Net-centric Computing focuses on large-scale distributed computing systems and applications that communicate through open, wide-area networks like the Internet. General examples of large-scale network-centric systems are the World-Wide Web and Computational Grids.

Net-centric computing refers to an emerging technology architecture and an evolutionary stage of client/server computing. It is a common architecture built on open standards that supports in different ways for different people to collaborate and to reach different information sources.

The evolutionary nature of net-centric computing links technological capabilities and strategic opportunities, helping people in facing today's new problems and providing the flexibility to meet tomorrow's challenges.

Areas

There is a wide array of subject areas, the most important of which are;

1. Web Applications

A web application (or web app) is an application software that runs on a web server. Web applications are accessed by the user through a web browser with an active network connection. Some examples of commonly-used web applications can be stated as web-mail, online retail sales, online banking, and online auctions. Web applications can be designed for a wide variety of users and can be used by anyone for numerous reasons.

Functionality

For proper functioning a web application requires three elements; a web server to handle requests from the client, an application server to execute the tasks requested by the user and a data-

base to store information. Typical web application flow can be described in five steps;

1. User presents a request to the web server over the Internet, through a web browser or the application's user interface.
2. Web server sends this request to the appropriate web application server.
3. Web application server performs the requested task and then generates the results of the requested data.
4. Web application server sends results to the web server with the requested information or processed data.
5. Web server responds to the client with the requested information that then appears on the user's display.

Development

Development of a web application has two phases as front-end and back-end development. Front-end development is the client-side development and scripting languages like JavaScript, HTML5, or Cascading Style Sheets (CSS) are commonly used for the process.

Design

Web application design is an important stage in building a web application. It focuses on the appearance and feel of the web application to the user. This stage encompasses several different aspects, including user interface design (UI), usability design(UX), content production, and graphic design. UI stands for User Interface. UI is the part of the web application with which a user interacts. Simply, it's everything you see and touch, such as buttons, colors, fonts, navigation, etc. UX stands for User Experience. UX focuses on users' experience and feeling towards their journey through the web app. Was the web application hard to use, was it slow, was the user disappointed when using it? are the criteria mainly considered by a UX designer.

Security

Attacks against web apps range from database manipulation to large-scale network disruption. Some of the common methods of attack are;

- Cross site scripting (XSS)
- SQL injection (SQi)
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Buffer overflow
- Cross-site request forgery (CSRF)
- Data breach

General yet some of important steps in ensuring security and gaining the customer trust, can be stated as using up-to-date encryption, requiring proper authentication, continuously patching discovered vulnerabilities, and having good software development hygiene.

2. Distributed Systems

Introduction

A distributed system is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another from any system in order to appear as a single system to the end-user. The computers that are in a distributed system can be physically together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible components, such as mainframes, personal computers, workstations, minicomputers, and so on. Common use cases of a distributed systems are electronic banking systems, massive multiplayer online games, and sensor networks.

Functionality

There are two general ways that distributed systems function :

1. Each component of the system works to achieve a common goal and the end-user views results as one combined unit.
2. Each component has its own end-user and the distributed system facilitates sharing resources or communication services.

Architectural models

Distributed systems generally consist of four different basic architectural models :

1. **Client-server :** Clients contact the server for data, then format it and display it to the end-user.
2. **Three-tier :** Information about the client is stored in a middle tier rather than on the client, to simplify application deployment.
3. **n-tier :** Generally used when the server needs to forward requests to additional enterprise services on the network.
4. **Peer-to-peer :** There are no additional nodes used to provide services or manage resources. Responsibilities are uniformly distributed among components in the system, known as peers, which can serve as either client or server.

3. Cloud Computing

Cloud computing is the delivery of different computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet without direct active management by the user. Simply stating, cloud computing means storing and accessing data and programs over the internet instead of ones' computer's hard drive. Organizations are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics, and customer-facing web applications. As an example, healthcare services use the cloud to develop more personalized treatments for patients. Financial services are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to players around the world.

Security

Cloud security is a discipline of cyber security committed to secure cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms. Cloud security is a key concern for cloud storage providers. Major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, insecure application program interfaces (APIs) and Distributed denial of service (DDoS) attacks. Some common methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections.

4. Semantic Web

"The Semantic Web is a webby way to link data" — Dave Beckett

Introduction

The Semantic Web is an extension of the existing World Wide Web, extended with the goal of the making network data machine-understandable. In other words, the current Web is transformed from being machine-readable to machine understandable. The Semantic Web provides much smarter and more effortless customer experiences by giving content in the forms compatible to a customer's need. It not only improves traditional search, but is facilitating more seamless, intelligent, and integrated customer experience journeys as well. Semantic Web represents the next vital evolution in connecting information.

1.2.4 Error Detection

Q5. What are different types of errors? Explain error detection techniques.

Ans : **(Imp.)**

Errors in Communication

When the information received at the receiver end does not match the sent data. At the time of transmission, errors are introduced into the binary data sent from the sender to the receiver due to noise during transmission. This means that a bit having a 0 value can change to 1 and a bit having a 1 value can change to 0.

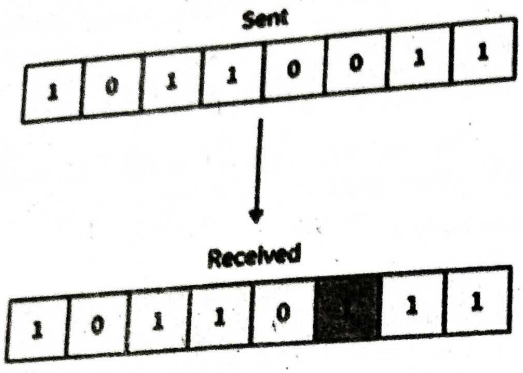
Types of Errors

Some errors that occur during communication are given below:

1. Single-bit Error

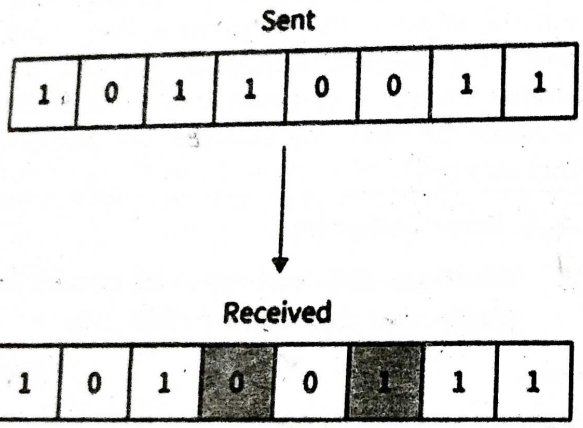
Typically, only one bit of the frame received is corrupt, and the corrupted bit can be located anywhere in the frame.

Refer to the below image for the single-bit error



2. Multiple-bit Error

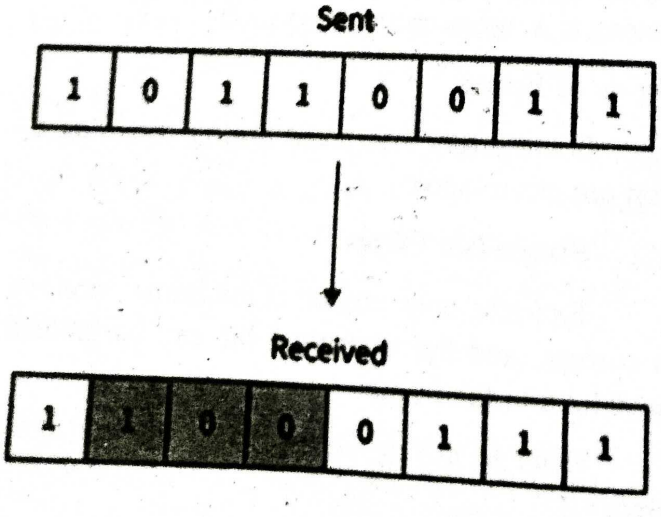
More than one bit received in the frame is found to be corrupted. Refer to the below image for the multiple-bit error



3. Burst Error

More than one consecutive bit is corrupted in the received frame.

Refer to the below image for the burst-bit error



Error Detection techniques

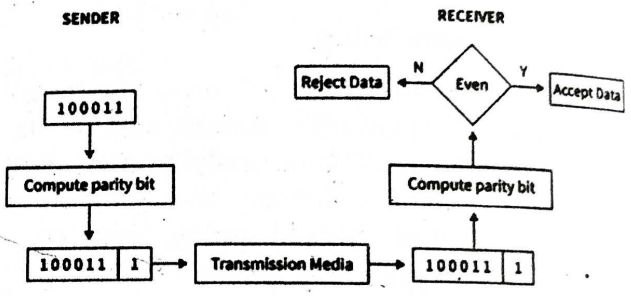
1. Simple Parity Check

Data sent from the sender undergoes parity check :

- 1 is added as a parity bit to the data block if the data block has an odd number of 1's.
- 0 is added as a parity bit to the data block if the data block has an even number of 1's.

This procedure is used for making the number of 1's even. And this is commonly known as even parity checking.

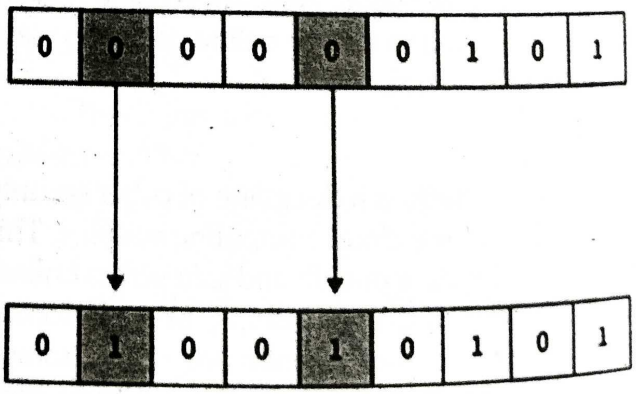
Refer to the below image for the simple parity-checking method :



Disadvantage

- Only single-bit error is detected by this method, it fails in multi-bit error detection .
- It can not detect an error in case of an error in two bits.

Refer to the below image for the disadvantage simple parity checking method

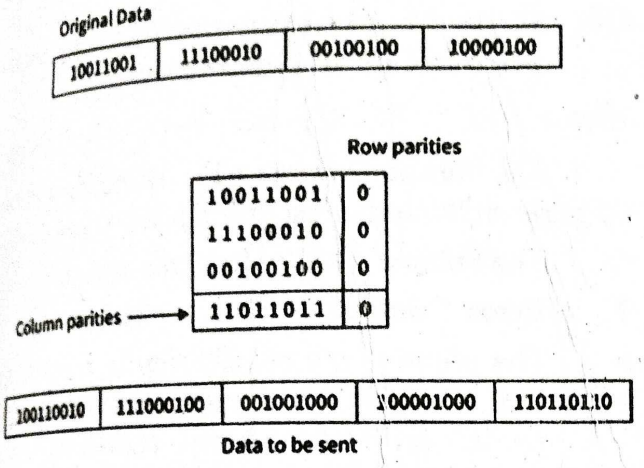


2. Two-Dimensional Parity Check

For every row and column, parity check bits are calculated by a simple method of parity check. Parity for both rows and columns is transmitted with the data sent from sender to receiver. At the receiver's

side, parity bits are compared with the calculated parity of the data received.

Refer to the below image for the two-dimensional parity checking method



Disadvantages

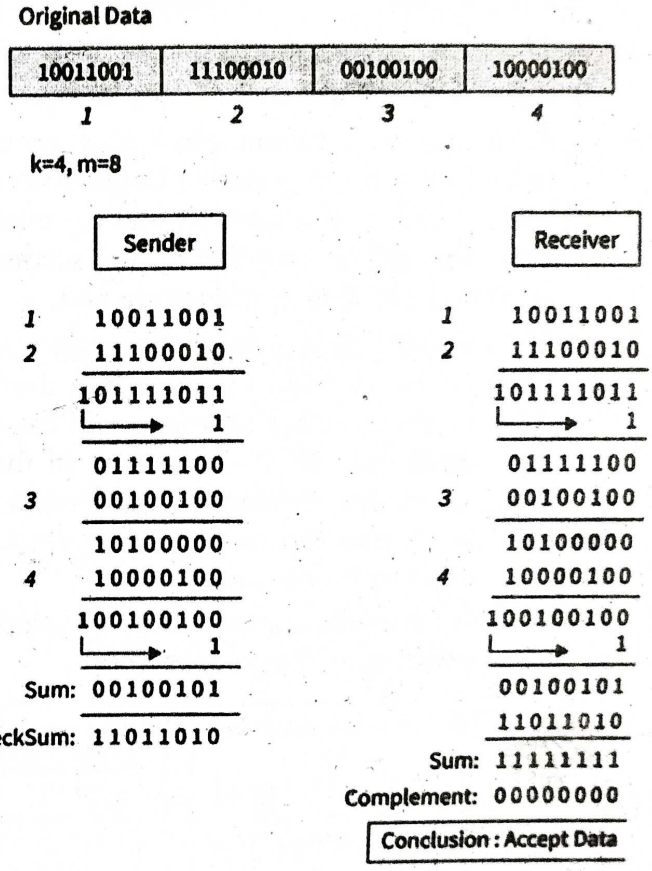
- If 2 bits are corrupted in 1 data unit and another data unit exactly at the same position is corrupted then this method is not able to detect the error.
- Sometimes this method is not used for **detecting 4-bit **errors or more than 4-bit errors.

3. Checksum

Checksum is a error detection which detects the error by dividing the data into the segments of equal size and then use 1's complement to find the sum of the segments and then sum is transmitted with the data to the receiver and same process is done by the receiver and at the receiver side, all zeros in the sum indicates the correctness of the data.

1. First of all data is divided into k segments in a checksum error detection scheme and each segment has m bits.
2. For finding out the sum at the sender's side, all segments are added through 1's complement arithmetic. And for determining the checksum we complement the sum.
3. Along with data segments, the checksum segments are also transferred.
4. All the segments that are received on the receiver's side are added through 1S complement arithmetic to determine the sum. Then complement the sum also.
5. The received data is accepted only on the condition that the result is found to be 0. And if the result is not 0 then it will be discarded.

Refer to the below image for the checksum method

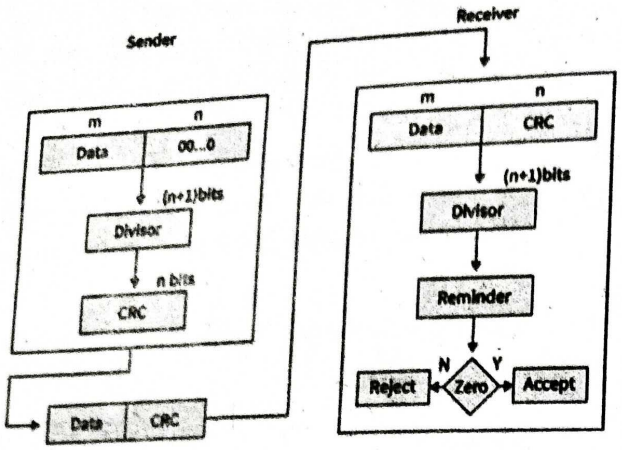


Disadvantages

In checksum error is not detected, if one sub-unit of the data has one or more corrupted bits and corresponding bits of the opposite value are also corrupted in another sub-unit. Error is not detected in this situation because in this case the sum of columns is not affected by corrupted bits.

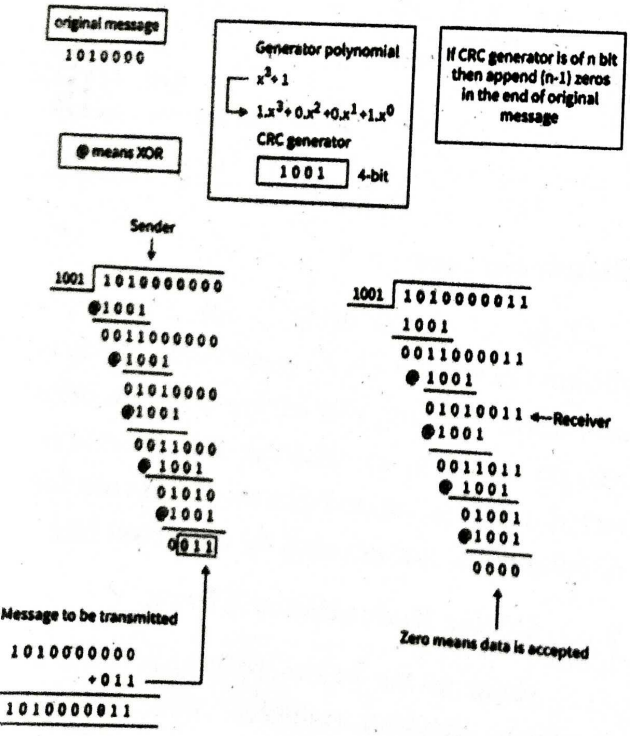
4. Cyclic Redundancy Check

Refer to the below image for the cyclic redundancy checking method



- The checksum scheme uses the addition method but CRC uses binary division.
- A bit sequence commonly known as cyclic redundancy check is added to the end of the bits in CRC. This is done so that the resulting data unit will be divisible by the second binary number that is predetermined.
- The receiving data units on the receiver's side need to be divided by the same number. These data units are accepted and found to be correct only on the condition of the remainder of this division is zero. The remainder shows that the data is not correct. So, they need to be discarded.

Refer to the below image for the example of the cyclic redundancy checking method



Disadvantages

Cyclic Redundancy Check may leads to overflow of data.

1.2.5 Reliable Transmission

Q6. Write about various reliable services provided by transport layer.

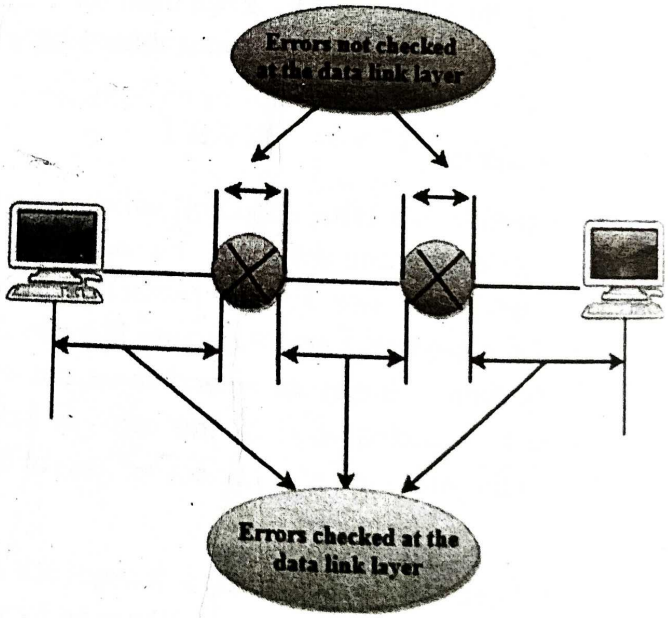
Ans : (Imp.)

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects :

1. Error Control

- The primary role of reliability is Error Control. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.



- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

2. **Sequence Control**

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

3. **Loss Control**

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

4. **Duplication Control**

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

5. **Flow Control**

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Q7. What is multiplexing? Write about stop and wait protocol.

Ans :

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.

Stop and Wait protocol

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

The primitives of stop and wait protocol are:

Sender side

Rule 1:

Sender sends one data packet at a time.

Rule 2:

Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

Receiver side

Rule 1:

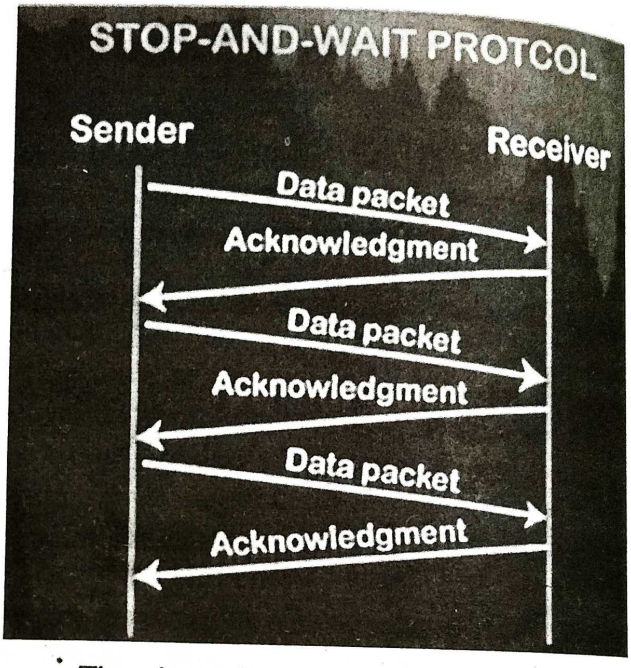
Receive and then consume the data packet.

Rule 2:

When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.

Working of Stop and Wait protocol

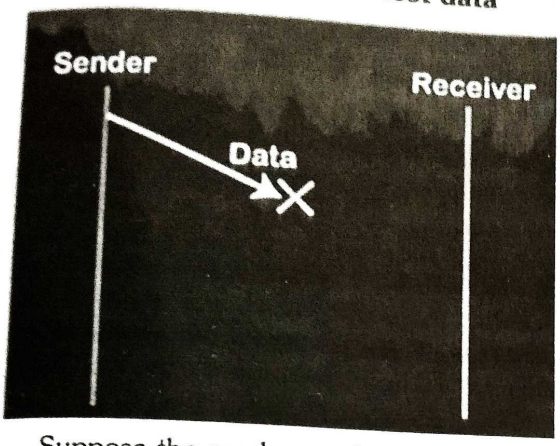


The above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Disadvantages

The following are the problems associated with a stop and wait protocol:

1. Problems occur due to lost data

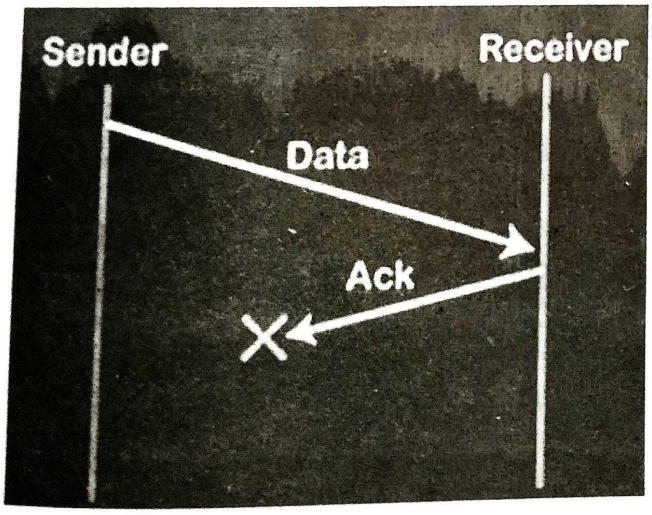


Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

- Sender waits for an infinite amount of time for an acknowledgment.
- Receiver waits for an infinite amount of time for a data.

2. Problems occur due to lost acknowledgment

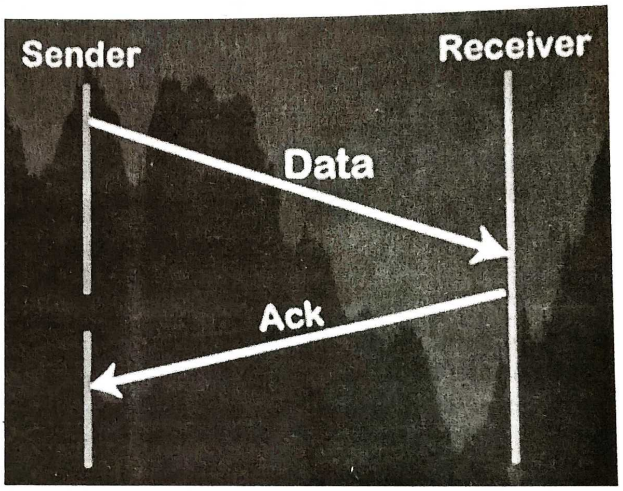


Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

In this case, one problem occurs

- Sender waits for an infinite amount of time for an acknowledgment.

3. Problem due to the delayed data or acknowledgment



Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.

Q8. Explain Sliding window protocol.

Ans :

A sliding window is also known as windowing. A sliding window is a method for controlling sending data packets between two network devices where dependable and sequential delivery of data packets is needed, such as using the Data Link Layer (OSI model) or Transmission Control Protocol (TCP).

In the sliding window technique, each data packet (for most data link layers) and byte (in TCP) includes a unique consecutive sequence number

used by the receiving computer to place data in the correct order. The objective of the sliding window technique is to use the sequence numbers to avoid duplicate data and to request missing data.

Following are the two types of Sliding Window Protocol :

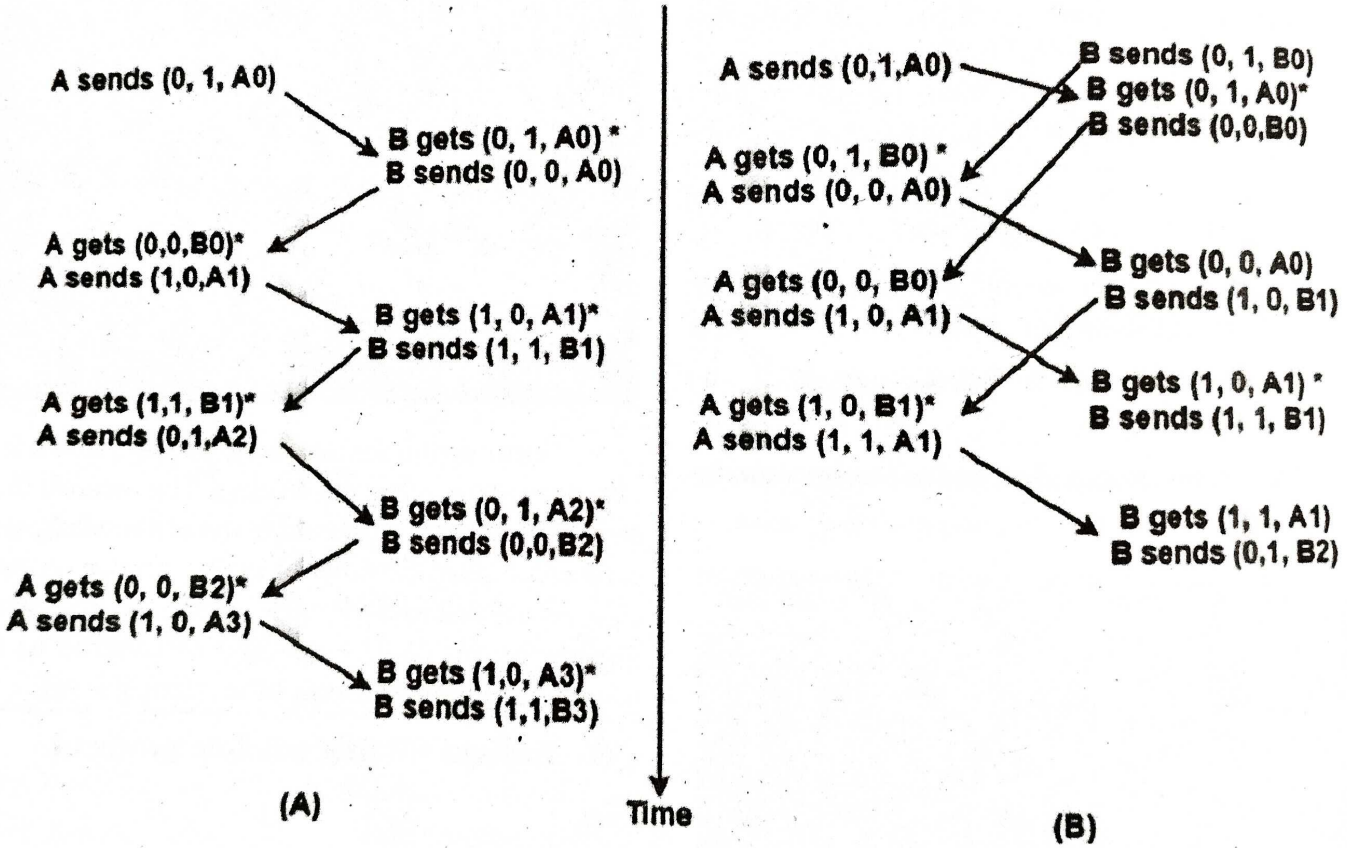
Go Back-n Protocol

Go-Back-N Automatic Repeat Query (ARQ) protocol is also referred to as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that helps a sliding window method. In this, if any frame is manipulated or lost, all subsequent frames have to be sent again.

For example, in GO- Back –N, the N is the sender's window size; if it is GO-Back-5, the sender will send frame 1 to 5 before receiving the knowledge of frame 1.

All the frames are numbers to deal with the most and duplicate frames. If the sender does not receive the receiver's acknowledgement, then all the frames available in the current window will be re-transmitted.

The design of the Go-Back-N protocol is shown below :



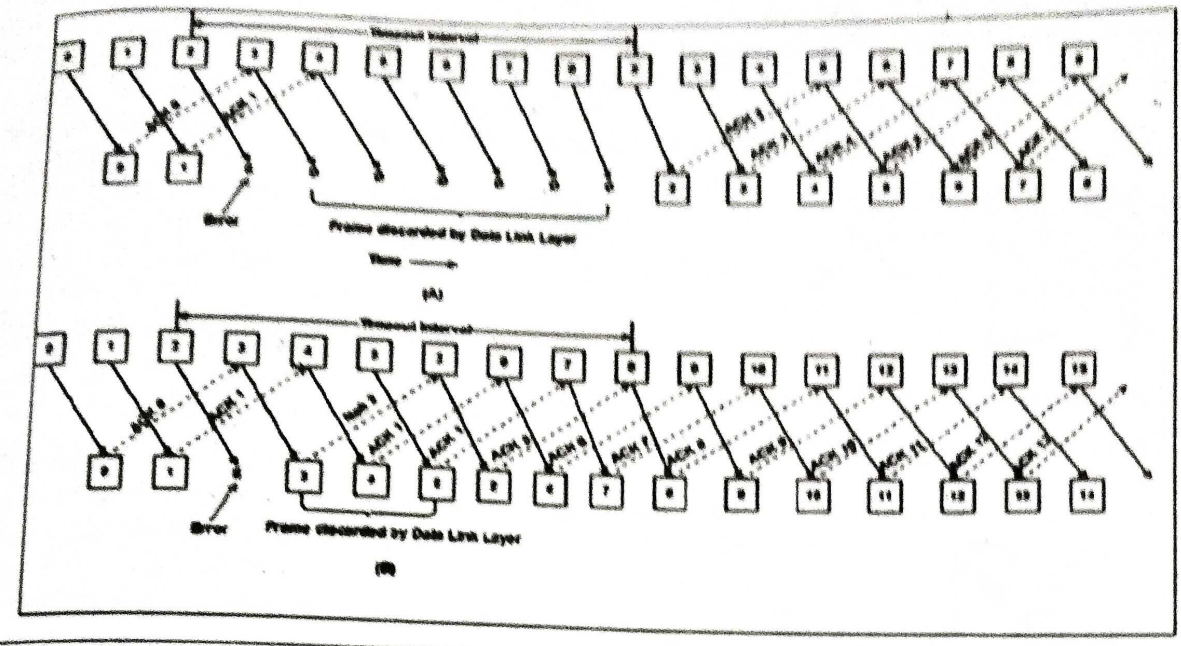
Selective Repetitive ARQ

Selective Repeat ARQ is also referred to as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that facilitates a sliding window method. The Goback-N ARQ protocol operates well if it has fewer errors.

In this protocol, the sender window size is always similar to the size of the receiver window. The size of the sliding window is continually greater than 1.

If the receiver obtains a corrupt frame, it does not directly remove it. It sends a negative acknowledgement to the sender. The sender sends that frame again immediately, receiving a negative acknowledgement. There is no waiting for any time-out to share that frame.

The structure of the Selective Repeat ARQ protocol is demonstrated below :



1.2.6 Ethernet And Multiple Access Networks

Q9. Explain about multi access networks.

Ans :

The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD).

As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link.

The Ethernet has its roots in an early packet radio network, called Aloha, developed at the University of Hawaii to support computer communication across the Hawaiian Islands. Like the Aloha network, the fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently (in Aloha, the medium was the atmosphere, while in the Ethernet the medium was originally a coax cable). The core idea in both Aloha and the Ethernet is an algorithm that controls when each node can transmit.

Physical Properties

Ethernet segments were originally implemented using coaxial cable of length up to 500 m. (Modern Ethernets use twisted copper pairs, usually a particular type known as "Category 5," or optical fibers, and in some cases can be quite a lot longer than 500 m.) This cable was similar to the type used for cable TV. Hosts connected to an Ethernet segment by tapping into it. A *transceiver*, a small device directly attached to the tap, detected when the line was idle and drove the signal when the host was transmitting. It also received incoming signals. The transceiver, in turn, connected to an Ethernet adaptor, which was plugged into the host. This configuration is shown in Figure.

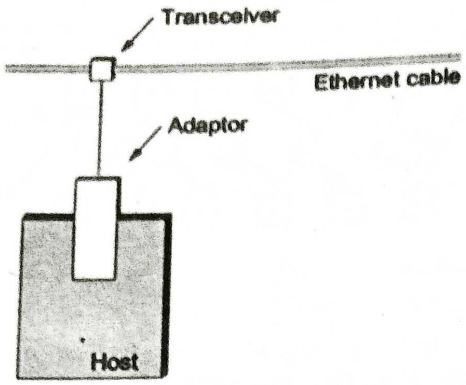


Fig.: Ethernet transceiver and adaptor

Multiple Ethernet segments can be joined together by repeaters (or a multi-port variant of a repeater, called a hub). A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals; repeaters do not understand bits or frames. No more than four repeaters could be positioned between any pair of hosts, meaning that a classical Ethernet had a total reach of only 2500 m. For example, using just two repeaters between any pair of hosts supports a configuration similar to the one illustrated in Figure, that is, a segment running down the spine of a building with a segment on each floor.

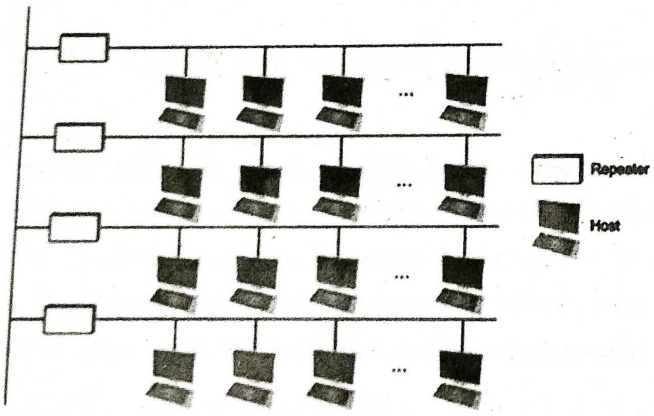


Fig.: Ethernet repeater, interconnecting segments to form a larger collision domain.

Any signal placed on the Ethernet by a host is broadcast over the entire network; that is, the signal is propagated in both directions, and repeaters and hubs forward the signal on all outgoing segments. Terminators attached to the end of each segment absorb the signal and keep it from bouncing back and interfering with trailing signals. The original Ethernet specifications used the Manchester encoding scheme described in an earlier section, while 4B/5B encoding (or the similar 8B/10B) scheme is used today on higher speed Ethernets.

It is important to understand that whether a given Ethernet spans a single segment, a linear sequence of segments connected by repeaters, or multiple segments connected in a star configuration, data transmitted by any one host on that Ethernet reaches all the other hosts.. The multi-access part of the Ethernet is all about dealing with the competition for the link that arises in a collision domain.

Access Protocol

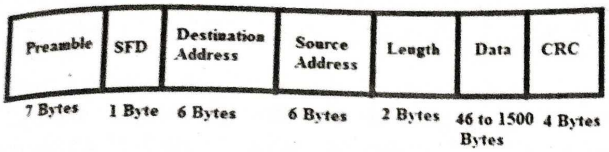
We now turn our attention to the algorithm that controls access to a shared Ethernet link. This algorithm is commonly called the Ethernet's media access control (MAC). It is typically implemented in hardware on the network adaptor. We will not describe the hardware per se, but instead focus on the algorithm it implements. First, however, we describe the Ethernet's frame format and addresses.

Ethernet Protocol Frame Structure

Generally, the structure of the Ethernet frame is defined within the IEEE 802.3 standard. But there are numerous optional frame formats are being employed for Ethernet to expand the capacity of the protocol. The Early frame versions were very slow but the latest Ethernet versions operate at 10 Gigabits/sec. So this is the very fastest Ethernet version.

The frame structure at the data link layer in the OSI model is almost the same for all Ethernet speeds. The structure of the frame simply adds headers & trailers in the region of the Layer 3 PDU (Protocol Data Unit) to summarize the message. The frame structure of Ethernet is shown below and it begins with the Preamble that functions at the physical layer

Ethernet header includes both Source & Destination MAC address, after which the frame's payload is present. The end field is Cyclical Redundancy Checking, used to notice the error. The following diagram shows the structure of the frame & fields.



Ethernet Frame Structure

Preamble

The first pattern of the Ethernet Protocol frame is 7-Bytes of Preamble where alternative 0's and 1's in this frame indicate the beginning of the frame & permit the sender & receiver to set up bit-level synchronization. At first, a Preamble in the above frame was introduced to permit for the few bits loss because of signal delays.

However, present high-speed-based Ethernet doesn't require Preamble for protecting the frame bits. Preamble specifies the receiver that frame is coming & lets the receiver lock on the data stream before the genuine frame starts.

Start of Frame Delimiter

The start of frame delimiter (SFD) is a 1-Byte field with 10101011 values that indicates that upcoming bits are the beginning of the frame, which is the address of the destination. The start of the frame delimiter is mainly designed to split the pattern of the bit to the preamble & signal the beginning of the frame.

Sometimes, the start of frame delimiter is considered as the main part of the preamble, so this is the main reason that Preamble is expressed as 8 Bytes in several places. The SFD gives a warning to stations that this is the final opportunity for synchronization.

Destination Address

The Destination Address Field is a 6-bytes field in the above Ethernet frame. The address within the frame & the device MAC address is compared. If both the addresses are matched, then the device simply allows the frame. This MAC address is a unicast, multi-cast, or broadcast.

Source Address

The source address is a 6-Byte field, including the source machine's MAC address. Once the address of source is an individual address or Unicast always, then LSB of an initial byte will be always.

Length

This field size is 2-byte long that specifies the entire Ethernet frame length. The length value held by the 16-bit field ranges from 0 to 65534, however, the length cannot be higher than 1500 due to some own Ethernet limitations.

Data Field

Data field is the location where actual data can be added and it is also called Payload. Here, both the data & IP header will be inserted if IP is used over Ethernet. So, the highest data available may be 1500 Bytes. If the data length is below the minimum length of 46 bytes, then padding zeros can be included to reach the minimum achievable length.

CRC Field

The CRC in the frame is the last pattern with 4 Bytes. This field includes 32-bits of data hash code, which is produced over the Source Address, Destination Address, Length, and Ethernet Protocol's Data field. If the checksum is calculated through a destination that is not similar to the sent checksum value, then received data can be corrupted.

Here, the frame size for IEEE 802.3 Ethernet standard changes from 64 bytes – 1518 bytes with 46 to 1500 bytes of data length.

Addresses

Each host on an Ethernet—in fact, every Ethernet host in the world—has a unique Ethernet address. Technically, the address belongs to the adaptor, not the host; it is usually burned into ROM. Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons. Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped. For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address

00001000000000000010101111100100101100010000000010

To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build. For example, Advanced Micro Devices has been as-

signed the 24-bit prefix 080020 (or 8:0:20). A given manufacturer then makes sure the address suffixes it produces are unique.

Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet. Each adaptor recognizes those frames addressed to its address and passes only those frames on to the host. (An adaptor can also be programmed to run in *promiscuous* mode, in which case it delivers all received frames to the host, but this is not the normal mode.) In addition to these *unicast* addresses, an Ethernet address consisting of all 1s is treated as a *broadcast* address; all adaptors pass frames addressed to the broadcast address up to the host. Similarly, an address that has the first bit set to 1 but is not the broadcast address is called a multicast address. A given host can program its adaptor to accept some set of multicast addresses. Multicast addresses are used to send messages to some subset of the hosts on an Ethernet (e.g., all file servers). To summarize, an Ethernet adaptor receives all frames and accepts

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode

It passes to the host only the frames that it accepts

1.3 Overlay Networks

1.3.1 Routing Overlays

Q10. Write about overlay networks.

Ans :

An overlay network is a virtual or logical network that is created on top of an existing physical network. The internet, which connects many nodes via circuit switching, is an example of an overlay network.

An overlay network is any virtual layer on top of physical network infrastructure. This may be as simple as a virtual local area network (VLAN) but typically refers to more complex virtual layers from software-defined networking (SDN) or a software-defined wide area network (SD-WAN).

The overlay creates a new layer where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links. Overlays enable administrators to define and manage traffic flows, irrespective of the underlying physical infrastructure.

Overlay networks and SDN

SDN is a quickly growing network strategy where the network operating system separates the data plane (packet handling) from the control plane (the network topology and routing rules). SDN acts as an overlay, running on the distributed switches, determining how packets are handled, instead of a centralized router handling those tasks.

SDN enables more flexible virtual networking that enables a more hands-off approach without changes to the physical underlay. SDN is an example of distributed computing where the actual processing is spread across multiple nodes, a departure from client-server computing where those routes were hardcoded.

Overlay network structure and protocols

Overlay network protocols include Virtual Extensible LAN (VXLAN), Generic Routing Encapsulation, Network Virtualization using GRE, Stateless Transport Tunneling and Network Virtualization Overlays.

Most network overlays work at Layer 3 in the Open Systems Interconnection (OSI) model, handling all traffic through the IP address. But, if a VLAN is created as an overlay, then the overlay would be done at Layer 2 with media access control (MAC) addresses.

In the case of SDN, the most common protocol for communication is OpenFlow, an open standard protocol that provides interoperability and is used in some fashion by most SDN tools.

Advantages

Network overlays provide some key benefits to networking, including the following:

- **Flexibility :** The overlay provides a more flexible networking approach by removing the hardcoded constraints of a physical network,

which enables configuration tied to usage or function.

- **Management :** Overlays offer better access management by segmenting and joining devices logically instead of managing these components physically.
- **Security :** Overlay networks enhance security by segmenting traffic and restricting access by groups, individuals or devices. In the case of a network compromise — when using SDN as an overlay — an attacker's traffic can be detected and stopped more easily.
- **Redundancy and efficiency :** With an overlay, traffic has an easier time changing routes based on either traffic saturation or network interruptions.

Disadvantages

Despite the advantages of overlay networks, organizations should heed the potential challenges or disadvantages as well, including the following:

- **Extra layers of management :** IT would have to manage two different network layers daily. Most importantly, the layers must be managed in unison as the topology that the overlay expects needs to be accurately represented in the underlay.
- **Troubleshooting :** Again, this must occur for both the underlay and overlay.
- **Potential security exposure.** The negative effects of misconfiguration can be amplified across a wider set of devices or users.

Examples and uses of overlay networks

Some examples of overlay network deployments include virtual private networks, peer-to-peer networks, content delivery networks, voice over IP services and non-native software-defined networks. Other examples and uses of overlay networks are the following:

- **VLAN or VXLAN :** These networks are created at Layer 2 or encapsulated with Layer 2 to create logical segments for routing traffic.
- **Hypervisor and virtual servers :** Virtual networking creates virtual switches and virtual network cards that create an overlay for communicating between virtual machines or between the hypervisor and the rest of the network.
- **SD-WAN :** SD-WAN creates an overlay that manages a communication tunnel between two networks so that all the communications do not need to be hardcoded to the connection.
- **SDN :** SDN uses protocols like OpenFlow to create a virtual overlay that sits on top of network switches, enabling the switches to handle more of the data routing functions, optimizing data flow.

Q11. Explain about routing overlays.

Ans :

The simplest kind of overlay is one that exists purely to support an alternative routing strategy; no additional application-level processing is performed at the overlay nodes. You can view a virtual private network (VPN) as an example of a routing overlay, but one that doesn't so much define an alternative strategy or algorithm as it does alternative routing table entries to be processed by the standard IP forwarding algorithm.

As hosts they are probably connected to the Internet by only one physical link, but as a node in the overlay they would be connected to multiple neighbours via tunnels.

Since overlays, almost by definition, are a way to introduce new technologies independent of the standardization process, there are no standard overlays we can point to as examples..

Experimental Versions of IP

Overlays are ideal for deploying experimental versions of IP that you hope will eventually take over the world. For example, IP multicast started off as an extension to IP and even today is not enabled in many Internet routers. The MBone (multicast backbone) was an overlay network that implemented IP multicast on top of the unicast routing provided by the Internet. A number of multimedia conference tools were developed for and deployed on the Mbone.

Like VPNs, the MBone used both IP tunnels and IP addresses, but unlike VPNs, the MBone implemented a different forwarding algorithm—forwarding packets to all downstream neighbors in the shortest path multicast tree. As an overlay, multicast-aware routers tunnel through legacy routers, with the hope that one day there will be no more legacy routers.

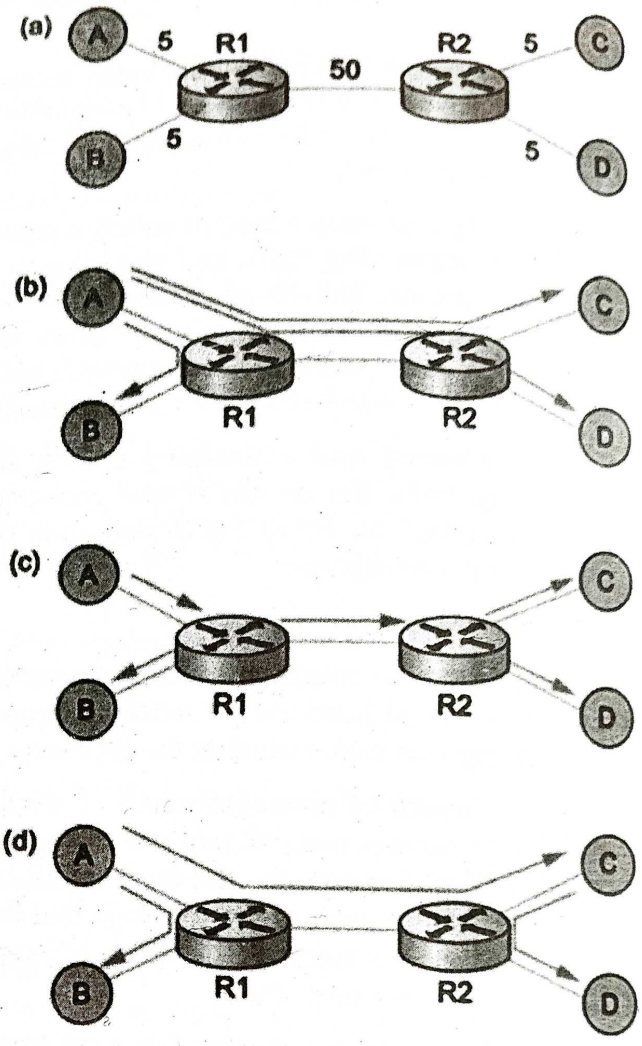
The 6-BONE was a similar overlay that was used to incrementally deploy IPv6. Like the MBone, the 6-BONE used tunnels to forward packets through IPv4 routers. Unlike the MBone, however, 6-BONE nodes did not simply provide a new interpretation of IPv4's 32-bit addresses. Instead, they forwarded packets based on IPv6's 128-bit address space. The 6-BONE also supported IPv6 multicast.

End System Multicast

Although IP multicast is popular with researchers and certain segments of the networking community, its deployment in the global Internet has been limited at best. In response, multicast-based applications like video conferencing have recently turned to an alternative strategy, called end system multicast. The idea of end system multicast is to accept that IP multicast will never become ubiquitous and to instead let the end hosts that are participating in a particular multicast-based application implement their own multicast trees.

Before describing how end system multicast works, multicast assumes that only Internet hosts (as opposed to Internet routers) participate in the overlay. Moreover, these hosts typically exchange messages with each other through UDP tunnels rather than IP tunnels, making it easy to implement as regular application programs.

This makes it possible to view the underlying network as a fully connected graph, since every host in the Internet is able to send a message to every other host. Abstractly, then, end system multicast solves the following problem: Starting with a fully connected graph representing the Internet, the goal is to find the embedded multicast tree that spans all the group members.



Since we take the underlying Internet to be fully connected, a naive solution would be to have each source directly connected to each member of the group. In other words, end system multicast could be implemented by having each node send unicast messages to every group member. To see the problem in doing this, especially compared to implementing IP multicast in routers, consider the example topology in Figure.

Figure, depicts an example physical topology, where R1 and R2 are routers connected by a low-bandwidth transcontinental link; A, B, C, and D are end hosts; and link delays are given as edge weights. Assuming A wants to send a multicast message to the other three hosts, Figure 1 shows how naive unicast transmission would work. This is clearly undesirable because the same message must traverse

the link A-R1 three times, and two copies of the message traverse R1-R2.

Figure, depicts the IP multicast tree constructed by the Distance Vector Multicast Routing Protocol (DVMRP). Clearly, this approach eliminates the redundant messages. Without support from the routers, however, the best one can hope for with end system multicast is a tree similar to the one shown in Figure 1. End system multicast defines an architecture for constructing this tree.

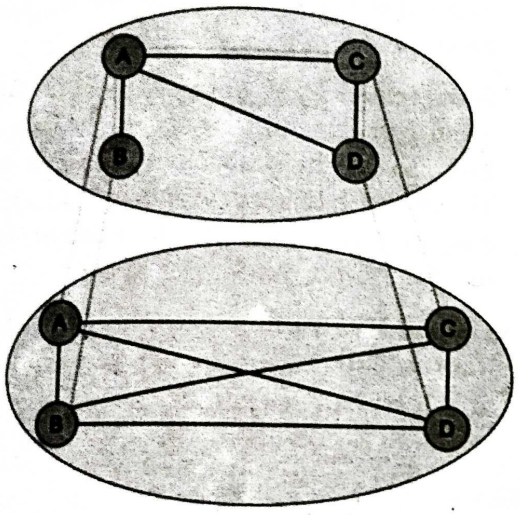


Fig.: Multicast tree embedded in an overlay network

The general approach is to support multiple levels of overlay networks, each of which extracts a subgraph from the overlay below it, until we have selected the subgraph that the application expects. For end system multicast, in particular, this happens in two stages: First we construct a simple mesh overlay on top of the fully connected Internet, and then we select a multicast tree within this mesh.

The idea is illustrated in Figure 2, again assuming the four end hosts A, B, C, and D. The first step is the critical one: Once we have selected a suitable mesh overlay, we simply run a standard multicast routing algorithm (e.g., DVMRP) on top of it to build the multicast tree.

The key to constructing the intermediate mesh overlay is to select a topology that roughly corresponds to the physical topology of the underlying Internet, but we have to do this without anyone telling us what the underlying Internet actually looks like since we are running only on end hosts and not routers. The general strategy is for the end hosts to measure the roundtrip latency to other nodes and decide to add links to the mesh only when they like what they see. This works as follows.

First, assuming a mesh already exists, each node exchanges the list of all other nodes it believes is part of the mesh with its directly connected neighbours. When a node receives such a membership list from a neighbour, it incorporates that information into its membership list and forwards the resulting list to its neighbours. This information eventually propagates through the mesh, much as in a distance vector routing protocol.

When a host wants to join the multicast overlay, it must know the IP address of at least one other node already in the overlay. It then sends a "join mesh" message to this node. This connects the new node to the mesh by an edge to the known node. In general, the new node might send a join message to multiple current nodes, thereby joining the mesh by multiple links. Once a node is connected to the mesh by a set of links, it periodically sends "keepalive" messages to its neighbours, letting them know that it still wants to be part of the group.

When a node leaves the group, it sends a "leave mesh" message to its directly connected neighbours, and this information is propagated to the other nodes in the mesh via the membership list described above. Alternatively, a node can fail or just silently decide to quit the group, in which case its neighbours detect that it is no longer sending "keep alive" messages. Some node departures have little effect on the mesh, but should a node detect that the mesh has become partitioned due to a departing node, it creates a new edge to a node in the other partition by sending it a "join mesh" message.

As described so far, we will end up with a mesh that is a subgraph of the original fully connected Internet, but it may have suboptimal performance because

1. Initial neighbour selection adds random links to the topology.
2. Partition repair might add edges that are essential at the moment but not useful in the long run.
3. Group membership may change due to dynamic joins and departures.
4. Underlying network conditions may change.

What needs to happen is that the system must evaluate the value of each edge, resulting in new edges being added to the mesh and existing edges being removed over time.

To add new edges, each node i periodically probes some random member j that it is not currently connected to in the mesh, measures the round-trip latency of edge (i, j), and then evaluates the utility of adding this edge. If the utility is above a certain threshold, link (i, j) is added to the mesh. Evaluating the utility of adding edge (i, j) might look something like this:

1.3.2 Peer-to-Peer Networks and Content Distribution Networks

Q12. Write about peer to peer network.

Ans :

A peer-to-peer network is a simple network of computers. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

History

Before the development of P2P, USENET came into existence in 1979. The network enabled the users to read and post messages. Unlike the forums we use today, it did not have a central server. It is used to copy the new messages to all the servers of the node.

- In the 1980s the first use of P2P networks occurred after personal computers were introduced.
- In August 1988, the internet relay chat was the first P2P network built to share text and chat.
- In June 1999, Napster was developed which was a file-sharing P2P software. It could be used to share audio files as well. This software was shut down due to the illegal sharing of files. But the concept of network sharing i.e P2P became popular.
- In June 2000, Gnutella was the first decentralized P2P file sharing network. This allowed users to access files on other users' computers via a designated folder.

Types

1. **Unstructured P2P networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content. For example, Napster, Gnutella, etc.
2. **Structured P2P networks:** It is designed using software that creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set up but can give easy access to users to the content. For example, P-Grid, Kademlia, etc.
3. **Hybrid P2P networks:** It combines the features of both P2P networks and client-server architecture. An example of such a network is to find a node using the central server.

Features

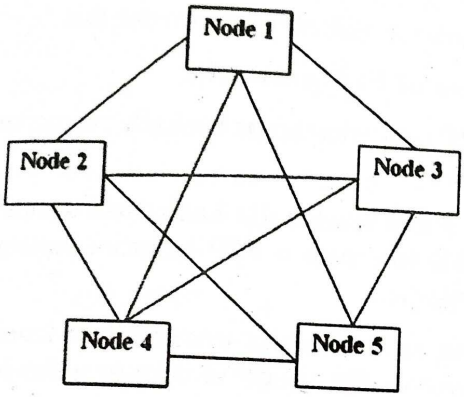
- These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.
- Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network.
- Since the nodes act as clients and servers, there is a constant threat of attack.
- Almost all OS today support P2P networks.

P2P Network Architecture

In the P2P network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printers.

- Each computer in the network has the same set of responsibilities and capabilities.
- Each device in the network serves as both a client and server.

- The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.
- Each computer in the network has the ability to share data with other computers in the network.
- The architecture is usually composed of workgroups of 12 or more computers.



How Does P2P Network Work?

Let's understand the working of the Peer-to-Peer network through an example. Suppose, the user wants to download a file through the peer-to-peer network then the download will be handled in this way:

- If the peer-to-peer software is not already installed, then the user first has to install the peer-to-peer software on his computer.
- This creates a virtual network of peer-to-peer application users.
- The user then downloads the file, which is received in bits that come from multiple computers in the network that have already that file.
- The data is also sent from the user's computer to other computers in the network that ask for the data that exist on the user's computer.

Thus, it can be said that in the peer-to-peer network the file transfer load is distributed among the peer computers.

How to Use a P2P Network Efficiently?

Firstly secure your network via privacy solutions. Below are some of the measures to keep the P2P network secure:

- **Share and download legal files:** Double-check the files that are being downloaded before sharing them with other employees. It is very important to make sure that only legal files are downloaded.
- **Design strategy for sharing:** Design a strategy that suits the underlying architecture in order to manage applications and underlying data.
- **Keep security practices up-to-date:** Keep a check on the cyber security threats which might prevail in the network. Invest in good quality software that can sustain attacks and prevent the network from being exploited. Update your software regularly.
- **Scan all downloads:** This is used to constantly check and scan all the files for viruses before downloading them. This helps to ensure that safe files are being downloaded and in case, any file with potential threat is detected then report to the IT Staff.
- **Proper shutdown of P2P networking after use:** It is very important to correctly shut down the software to avoid unnecessary access to third persons to the files in the network. Even if the windows are closed after file sharing but the software is still active then the unauthorized user can still gain access to the network which can be a major security breach in the network.

Q13. State the applications of P2P Network.

Ans :

Below are some of the common uses of P2P network:

- **File sharing:** P2P network is the most convenient, cost-efficient method for file sharing for businesses. Using this type of network there is no need for intermediate servers to transfer the file.
- **Blockchain:** The P2P architecture is based on the concept of decentralization. When a peer-to-peer network is enabled on the blockchain it helps in the maintenance of a complete replica of the records ensuring the

accuracy of the data at the same time. At the same time, peer-to-peer networks ensure security also.

- **Direct messaging:** P2P network provides a secure, quick, and efficient way to communicate. This is possible due to the use of encryption at both the peers and access to easy messaging tools.
- **Collaboration:** The easy file sharing also helps to build collaboration among other peers in the network.
- **File sharing networks:** Many P2P file sharing networks like G2, and eDonkey have popularized peer-to-peer technologies.
- **Content distribution:** In a P2P network, unline the client-server system so the clients can both provide and use resources. Thus, the content serving capacity of the P2P networks can actually increase as more users begin to access the content.
- **IP Telephony:** Skype is one good example of a P2P application in VoIP.

Q14. Explain the advantages and disadvantages of P2P Network.

Ans :

Advantages of P2P Network

- **Easy to maintain:** The network is easy to maintain because each node is independent of the other.
- **Less costly:** Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
- **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
- **Adding nodes is easy:** Adding, deleting, and repairing nodes in this network is easy.
- **Less network traffic:** In a P2P network, there is less network traffic than in a client/server network.

Disadvantages of P2P Network

- **Data is vulnerable:** Because of no central server, data is always vulnerable to getting lost because of no backup.
- **Less secure:** It becomes difficult to secure the complete network because each node is independent.
- **Slow performance:** In a P2P network, each computer is accessed by other computers in the network which slows down the performance of the user.
- **Files hard to locate:** In a P2P network, the files are not centrally stored, rather they are stored on individual computers which makes it difficult to locate the files.

Examples of P2P networks

P2P networks can be basically categorized into three levels.

- The first level is the basic level which uses a USB to create a P2P network between two systems.
- The second is the intermediate level which involves the usage of copper wires in order to connect more than two systems.
- The third is the advanced level which uses software to establish protocols in order to manage numerous devices across the internet.

Some of the popular P2P networks are Gnutella, BitTorrent, eDonkey, Kazaa, Napster, and Skype.

Q15. What is a Content Distribution Network and how does it work?

Ans :

A CDN is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content. A CDN-

1. Manages servers that are geographically distributed over different locations.
2. Stores the web content in its servers.
3. Attempts to direct each user to a server that is part of the CDN so as to deliver content quickly.

How does CDN work?

To minimize the distance between the visitors and your website's server, a CDN stores a cached

version of original content in multiple geographical locations (a.k.a., points of presence/ PoPs). Each PoP contains a number of caching servers known as edge servers that are responsible for content delivery to visitors within its proximity. CDN caches content in many places at once, ensuring quick delivery of content.

Let's consider an example:

Suppose you are hosting a website, wherein your origin server(server containing the primary source of your website's data, where website files are hosted) is located in Australia and a company XYZ provides you the CDN service.

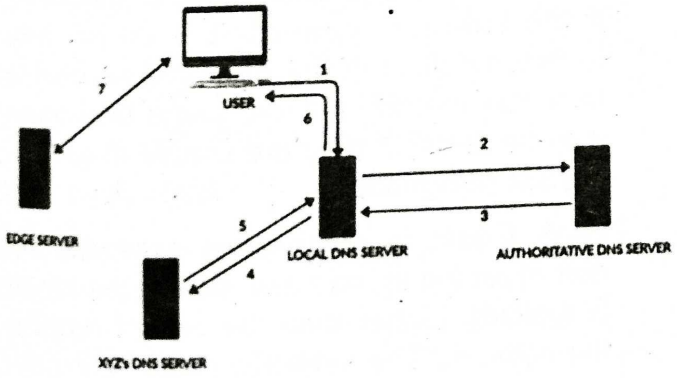
When a user in India clicks on a video on your website, the request goes to the user's local DNS server(See DNS), which relays the request to the authoritative DNS server of your website.

The authoritative DNS server then identifies that the user is situated far away and therefore relays the request to its XYZ's DNS server. Now the DNS query enters XYZ's network which provides the address of the edge server that is closest to the user to the Local DNS server. The video is delivered by this edge server.

From this point onwards the local DNS server knows the address of the edge server. So whenever users within its network send a request for content from your website, the local DNS server shall relay the request to the edge server.

CDN thus minimizes the number of hops required to deliver the data to a user's browser due to the POPs that are located near the user.

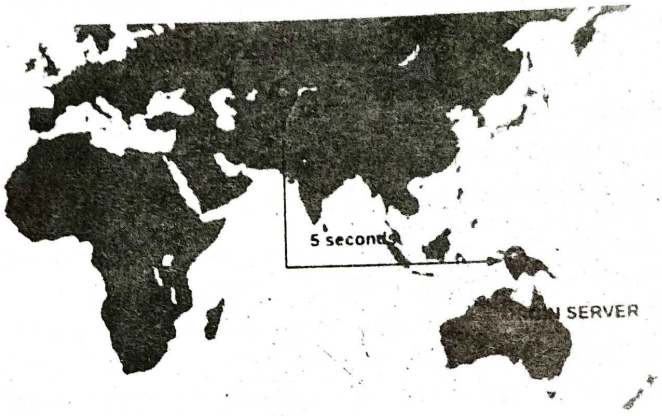
Following image depicts the same:



Following Image depicts the difference between how a request is handled with and without a CDN respectively:

WITH CDN(2 SECONDS)

WITHOUT CDN(5 SECONDS)



1.3.3 Client-Server Network

Q16. Explain about client server network.

Ans :

In client-server network relationships, certain computers act as servers and others act as clients.

A server is simply a computer that provides the network resources and provides service to other computers when they request it. A client is the computer running a program that requests the service from a server. Local area network (LAN) is based on client server network relationship.

A client-server network is one on which all available network resources such as files, directories, applications and shared devices, are centrally managed and hosted and then are accessed by the client.

Client server networks are defined by the presence of servers on a network that provide security and administration of the network.

How Does a Client-Server Network Work?

Before jumping to the main topic of learning how a client-server network works, let's first learn about the hardware used in a client-server network.

Clients' hardware is typically a PC or other mobile device that comes preloaded with network apps. The person on the other side of the computer sends a request to the server via the internet.

As you may have guessed by now, the one that resides on the server-side is a 'server' or data centre that stores myriads of data in files, databases, and applications.

Now we know the hardware used in a client-server network, so let's look at the working of the client-server network:

The client-server network works based on the principle of a two-way street, where the client sends the requests simultaneously and sends an update and appropriate results for the requested queries.

A client-server network comprises multiple clients and servers; therefore, network traffic can be significant. To save bandwidth on the network, the server shuts the connection to the client once the job is completed. As a result, the speed with which results are delivered is determined by the bandwidth efficiency of the client and server.

The client-server architecture can be utilised both on the internet and in a local area network (LAN), such as in a company or organisation.

Advantages

The client-server architectural concept has several advantages:

- **Centralization:** A single server that houses all of the essential data in one location makes data security and user authorization and authentication control much easier. Any issue that arises throughout the whole network may be resolved in a single location.
- **Scalability:** A client-server network may be expanded by adding network segments, servers, and PCs with little downtime. Client-server networks offer scalability. The number of resources, such as clients and servers, can be increased as needed by the user. Consequently, the server's size may be increased without any disruptions. Since the server is centralized, there are no questions regarding access to network resources even as the size grows. As a result, just a small number of staff members are needed for the setups.
- **Easy Management:** Clients and the server do not have to be close to access data effectively. It is really simple to handle files because they are all kept on the same server. The finest management for tracking and finding records of necessary files is offered in client-server networks.
- **Accessibility:** The client-server system's nodes are all self-contained, requesting data only from the server, allowing for simple upgrades, replacements, and relocation.
- **Data Security:** The centralized design of a client-server network ensures that the data is properly safeguarded. Access controls can be used to enforce it and ensure that only authorized users are allowed access. Imposing credentials like a username and password is one such technique. Additionally, if the data were to be destroyed, it would be simple to restore the files from a single backup.

Disadvantages

The client-server network has a few disadvantages:

- **Network Traffic Congestion:** The main disadvantage of a client-server model is the danger of a system overload owing to a lack of resources to service all of the clients. If too many different clients try to connect to the shared network at the same time, the connection may fail or slow down. Additionally, if the internet connection is down, any website or client in the world will be unable to access the information. Large businesses may be at risk if they are unable to get important information.
- **High Cost:** In client-server networks, the cost of setting up and maintaining the server is typically higher than the cost of running the network. The networks might be expensive to buy because of their strength. The users won't all be able to afford them as a result.

- **Robustness:** The whole network will be interrupted, if the primary server experiences failure or interference. Client-server networks lack hence in terms of resilience, since client-server networks are centralized.
- **Maintenance Difficulty:** When the servers are put in place, they will run continuously, which implies they need to receive the necessary care. If there are any mistakes, they must be fixed right away without further delay. As a result, a qualified network manager should be hired to look after the server.
- **Unacquirable Resources:** Not all of the resources on the server are available for acquisition. For instance, you cannot immediately print a document from the web or change any information stored on the client's hard drive.

Types of Clients

Clients are computer hardware or server software that makes requests for resources and services that a server makes available. Clients are often referred to as "service requesters". Thick, Thin, or Hybrid client computing are the three categories.

- **Thick Client:** A client that offers extensive functionality, does the majority of data processing on its own, and depends on the server only a little.
- **Thin Client:** An application server handles the majority of the necessary data processing for a thin-client server, which is a lightweight computer that heavily relies on the resources of the host computer.
- **Hybrid Client:** A hybrid client combines the elements of a thin client and a thick client. It may do local processing but must rely on the server to keep persistent data.

Types of Servers

The different types of servers are given below :

- **File server :** These servers provide the services for storing, retrieving and moving the data. A user can read, write, exchange and manage the files with the help of file servers.
- **Printer server :** The printer server is used for controlling and managing printing on the network. It also offers the fax service to the network users.
- **Application server :** The expensive software and additional computing power can be shared by the computers in a network with the help of application servers.
- **Message server :** It is used to co-ordinate the interaction between users, documents and applications. The data can be used in the form of audio, video, binary, text or graphics.
- **Database server :** It is a type of application server.

1.3.4 Delay-Tolerant Networks

Q17. Explain about delay-tolerant network?

Ans : **(Imp.)**

A delay-tolerant network (DTN) is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

In such environments, the conventional internet does not work; networks are also subject to frequent disruptions, high error rates and latency of hours or even days. A DTN can overcome such challenges and reliably transmit information, ensuring dependable internet working.

Need

Introduced in 2003, delay-tolerant networks have proved most useful in deep space communications. In space, communications between Earth and spacecrafts involve long distances of thousands and even millions of miles, consequently making delays, disruptions, errors and data losses inevitable. Existing terrestrial networking technologies proved unable to handle such issues, which must be addressed at the application level. That's where DTNs come in.

The Consultative Committee for Space Data Systems (CCSDS) has developed other protocols that incorporate some aspects of delay-tolerant networking. However, they cannot provide the same level of flexibility or automated data transfer as DTNs.

Two such protocols are Space Packet Protocol and CCSDS File Delivery Protocol:

- **Space Packet Protocol:** This protocol can forward packets across a managed data path through the network. However, it cannot address the scheduled nature of connectivity, which may be why it has not been implemented in a space system.
- **CCSDS File Delivery Protocol (CFDP):** CFDP provides reliable delivery of files, but it is limited to file transfers only. It does not support messaging, streaming or other applications.

Advantages of delay-tolerant networks

DTN is a suite of protocols developed by the Delay & Disruption Tolerant Networking Research Group administered by the Internet Engineering Task Force (IETF). These protocols are versatile enough to operate either with terrestrial IP protocols or independently

Terrestrial IP networks are based on store-and-forward operation. However, they assume that the storing will persist for only a modest amount of time, depending on the queuing and transmission delay.

DTN architecture expects nodes to store bundles for an extended period. Whenever possible, each received data packet is forwarded immediately. If forwarding is not currently possible but is expected to be possible in the future, the packet is stored for future transmission. Thus, when using a DTN, only the next hop is required to be available. Delay-tolerant networking uses this automatic store-and-forward mechanism to assure data delivery, which conventional terrestrial networks cannot do.

Other important benefits of DTNs include the following :

- enabled interoperability of ground stations and spacecraft;
- more efficient data transmissions and more usable bandwidth;
- improved link reliability;
- support for integrity checks, authentication and encryption for more secure communications; and
- ability for many priority levels to be set for different data types for improved quality of service (QoS).

Delay-tolerant network architecture

The TCP/IP protocol provides a general-purpose network- and transport-layer service for the terrestrial internet. A DTN does the same in a space environment.

The DTN architecture consists of an end-to-end message-oriented overlay known as the bundle layer. Devices implementing the bundle layer are known as DTN nodes. This layer exists above the transport (or other) layers of the network and below applications.

It provides functionality similar to the layer of gateways described in the original internet and ARPANET designs. But unlike ARPANET, the DTN bundle layer is layer-agnostic and focuses on virtual message forwarding rather than on packet switching.

The bundle layer employs persistent storage for store-and-forward. This allows it to combat network interruptions and delays. The DTN architecture uses variable-length or arbitrary-length messages instead of streams or limited-sized packets. These application data units are transformed by the bundle layer into protocol data units called bundles, which are forwarded by DTN nodes.

This communication abstraction enhances the DTN's ability to make good scheduling and path selection decisions.

In the DTN, bundle sources and destinations are identified by endpoint identifiers (EIDs), which may refer to one or more DTN nodes or endpoints. Security mechanisms are also provided in the DTN to protect the infrastructure from unauthorized use.

Traffic in delay-tolerant networks

In a DTN, traffic can be classified in three ways: expedited, normal and bulk. These traffic types move across the DTN in order of decreasing priority:

- **Expedited packets :** These are always transmitted, reassembled and verified before data of any other class from a given source to a given destination.

- **Normal traffic :** This traffic is sent after all expedited packets have been successfully assembled at their intended destination.
- **Bulk traffic :** This is not dealt with until all packets of other classes from the same source and bound for the same destination have been successfully transmitted and reassembled. In this sense, bulk bundles are sent on a "least effort" basis.

Applications of delay-tolerant networks

In addition to space communications and interplanetary networking, DTNs are also useful over terrestrial applications and more modest distances when interference is extreme, high error rates are common or network resources are severely overburdened.

Other key applications of DTNs include the following:

- military and tactical systems;
- disaster recovery networks;
- vehicular communications;
- wildlife tracking/monitoring networks;
- communication in remote or rural areas;
- underwater acoustic networks; and
- other sensor-based networks.

Hardware considerations for delay-tolerant networks

A delay-tolerant network can accommodate different kinds of wireless technologies, including radio frequency (RF), ultra-wide b and (UWB), acoustic (sonar or ultrasonic) and free-space optical technologies. Such networks overcome network problems associated with intermittent connectivity and high error rates using store-and-forward message switching.

For this, they require hardware that can store large amounts of data indefinitely, and such media must be able to survive extended power loss and system restarts. It must also be immediately accessible at any time.

For this purpose, hard drives and high-volume flash memory are ideal. Further, the data stored on these media must be organized and prioritized by software to ensure accurate and reliable store-and-forward functionality.

Short Question and Answers

1. Bandwidth.

Ans :

Bandwidth, or precisely network bandwidth, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time. That simply means that higher is the bandwidth of a network, larger is the amount of data network can be sending to and from across its path. Be careful not to confuse bandwidth with closely related terms such as the data rate and the throughput. Bandwidth is something that deals with the measurement of capacity and not the speed of data transfer.

2. Latency.

Ans :

- Being simple latency means whenever you have given input to the system and the total time period it takes to give output so that particular time period/interval is known as latency.
- Actually, latency is the in-between handling time of computers, as some of you may think that whenever some system connects with another system it happens directly but no it isn't, the signal or data follows the proper traceroute for reaching its final destination.
- Nowadays fiber optic cables are used for transmitting the signals/data from one place to another with the speed of light but obviously before reaching to the final destiny the data/signal has to pass from many checkpoints or posts and follow a proper traceroute so it takes some time to get respond from the receiver and that total round of time is known as latency.
- If you want to know the fastest possible network connection you could have from one place to another then we will suppose light as a medium because light just takes 1/7 milli seconds(approx.) to take a round of earth. So according to the data if you let light as a medium then you can send 20 packets per second across the other sides of the world.

3. ATM.

Ans :

Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication technique that supports data-transfer rates ranging from sub-T1 speeds (less than 1.544 Mbps) up to 10 Gbps. Like other packet-switching services (Frame Relay, SMDS), ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. Instead, it relies on the inherent integrity of digital lines to ensure data integrity.

4. FDDI.

Ans :

FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the token ring protocol.

In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network (WAN).

An FDDI network contains two token rings, one for possible backup in case the essential ring falls flat.

The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps

5. Frame Relay.

Ans :

Frame Relay (frame relay) is a packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection.

It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends. It makes it more efficient than X.25, and a higher process speed achieved (it can transmit over 2,044 Mbps).

If the traffic is hefty, with a large number of small packages, its performance is more excellent than X25.

If large files transferred at high speeds, the price/performance ratio is higher in X25.

6. Net-Centric Computing.

Ans :

Meaning

Net-Centric Computing (NCC) is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network. Net-centric Computing focuses on large-scale distributed computing systems and applications that communicate through open, wide-area networks like the Internet. General examples of large-scale network-centric systems are the World-Wide Web and Computational Grids.

Net-centric computing refers to an emerging technology architecture and an evolutionary stage of client/server computing. It is a common architecture built on open standards that supports in different ways for different people to collaborate and to reach different information sources.

7. Cloud Computing.

Ans :

Cloud computing is the delivery of different computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet without direct active management by the user. Simply stating, cloud computing means storing and accessing data and programs over the internet instead of ones' computer's hard drive. Organizations are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics, and customer-facing web applications. As an example, healthcare services use the cloud to develop more personalized treatments for patients. Financial services are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to players around the world.

8. Distributed Systems.

Ans :

A distributed system is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another from any system in order to appear as a single system to the end-user. The computers that are in a distributed system can be physically together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible components, such as mainframes, personal computers, workstations, minicomputers, and so on. Common use cases of a distributed systems are electronic banking systems, massive multiplayer online games, and sensor networks.

9. Multi access networks.

Ans :

The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD).

As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link.

The Ethernet has its roots in an early packet radio network, called Aloha, developed at the University of Hawaii to support computer communication across the Hawaiian Islands. Like the Aloha network, the fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently (in Aloha, the medium was the atmosphere, while in the Ethernet the medium was originally a coax cable). The core idea in both Aloha and the Ethernet is an algorithm that controls when each node can transmit.

10. Overlay networks.

Ans :

An overlay network is a virtual or logical network that is created on top of an existing physical network. The internet, which connects many nodes via circuit switching, is an example of an overlay network.

An overlay network is any virtual layer on top of physical network infrastructure. This may be as simple as a virtual local area network (VLAN) but typically refers to more complex virtual layers from software-defined networking (SDN) or a software-defined wide area network (SD-WAN).

The overlay creates a new layer where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links. Overlays enable administrators to define and manage traffic flows, irrespective of the underlying physical infrastructure.

11. Delay-tolerant network.

Ans :

A delay-tolerant network (DTN) is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

In such environments, the conventional internet does not work; networks are also subject to frequent disruptions, high error rates and latency of hours or even days. A DTN can overcome such challenges and reliably transmit information, ensuring dependable internet working.

Choose the Correct Answers

1. _____ specifies a complete set of rules for the connections and interactions of its physical and logical components for providing and utilizing communication services. [c]
   (a) Computer Architecture (b) Communication Architecture
   (c) Network Architecture (d) Internet Architecture

2. How many types of networks are there based on architecture? [b]
   (a) one (b) two
   (c) three (d) four

3. The ATM cell header is composed of _____ elements [b]
   (a) 8 (b) 6
   (c) 4 (d) All the above

4. Which one of the following cables is also known as a thin ethernet? [d]
   (a) 10BaseF (b) 10BaseT
   (c) 10Base5 (d) 10Base2

5. Network in which every computer is capable of playing the role of client, server or both at the same time is called [a]
   (a) peer-to-peer network (b) local area network
   (c) dedicated server network (d) wide area network

5. Among the following which detects the error by dividing the data into the segments of equal size and then use 1's complement to find the sum of the segments. [b]
   (a) parity check (b) check sum
   (c) CRC (D) all the above

7. Among the following which client does the majority of data processing on its own, and depends on the server only a little. [a]
   (a) thin client (b) thick client
   (c) hybrid client (d) all the above

8. The expensive software and additional computing power can be shared by the computers in a network with the help of _____ servers. [b]
   (a) File server (b) application server
   (c) database server (d) print server

9. Which one is an error control protocol? [d]
   (a) Stop and Wait (b) Go Back N
   (c) Selective Repeat (d) All of the above

10. In class A IP address the first 8 bits represent _____. [a]
   (a) Network ID (b) Host ID
   (c) Both a and b (d) None of the above

Fill in the Blanks

1. _____ is the organization and arrangement of different network devices (i.e., the clients such as PCs, desktops, laptops, mobiles etc.) at both physical and logical levels in order to fulfil the needs of the end user/customer.
3. The_____ referred to here are the individual devices linked together directly, having equal responsibilities and equal powers without the presence of any central authority.
3. _____ measures of the amount of data that can be sent and received at any instance of time.
4. _____ is a cell-based fast-packet communication technique.
5. _____ is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network
6. The more general name for the technology behind the Ethernet is _____.
7. An _____ is a virtual or logical network that is created on top of an existing physical network.
8. A _____ is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content.
9. _____ server is used to co-ordinate the interaction between users, documents and applications. The data can be used in the form of audio, video, binary, text or graphics.
10. A _____ is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

ANSWERS

1. Network architecture
2. Peers
3. Bandwidth
4. Asynchronous Transfer Mode (ATM)
5. Net-Centric Computing (NCC)
6. CSMA/CD
7. Overlay network
8. CDN
9. Message server
10. Delay-tolerant network (DTN)